Chapter 6

Enumeration of Isometry Classes

6

6

6 Enumeration of Isometry Classes

We have gathered linear codes in classes of codes which are of the same quality with respect to error correction. Since the metric structure of a code determines its error correction properties we have introduced the notion of *isometric* codes and the just mentioned classes of codes are called *isometry classes.* Each of these classes is an orbit of an isometry group of $\mathbb{F}_q^n$. The linear isometry classes are orbits under the linear isometry group $M_n(q)$, the semilinear isometry classes orbits under the semilinear isometry group. This chapter is concerned with the enumeration of isometry classes of codes using methods from Combinatorics, in particular *Pólya's Theory of Enumeration*. This theory deals with the combinatorial properties of finite group actions. In particular, properties of the acting group like numbers of fixed points are used to get results about the number of orbits. The fundamental tool is the *Lemma of Cauchy-Frobenius*, which was introduced in 3.4.2 and refinements thereof. To count the isometry classes of codes we need detailed information about the isometry groups. Depending on whether we count linear isometry classes (in the first sections) or semilinear isometry classes (in Section 6.7) we have to study the projective linear or the projective semilinear groups over the appropriate finite fields.

An interesting and helpful notion introduced in Section 6.2 is the concept of *indecomposable* linear codes. Each code can be written in an essentially unique way as a sum of such codes. We derive the number of indecomposable linear codes, obtaining this way an idea of the complexity of the construction of all the isometry classes of indecomposable linear codes. Furthermore, a special class of indecomposable codes, the *critical indecomposable codes,* are described in detail in Section 6.5.

For the actual computation of the number of linearly nonisometric (n,k)-codes over $\mathbb{F}_q$, we need detailed information about the natural group action of the projective linear group $\mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}^*(q)$. Especially, we describe the conjugacy classes of the linear group $\mathrm{GL}_k(q)$ by using the *Jacobi normal form* of the automorphisms of $\mathbb{F}_q^k$. This approach is based on module theoretic considerations already introduced in Chapter 4. In Section 6.3 we derive a complete description of the cycle index for the natural action of $\mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}^*(q)$.

Numerical results concerning the enumeration of linear isometry classes of codes are displayed in Section 6.4. Extended tables, computed by SYMMETRICA (cf. [190]), can be found online [58] or on the attached CD.

Closely related to the enumeration of nonisometric codes is the *random generation* of linear codes. The algorithm presented in Section 6.6 generates representatives of linear isometry classes which are distributed *uniformly at random*

over all classes of $(n, \leq k)$-codes over $\mathbb{F}_p$ for given n, k and p. We use a quite general method which is due to Dixon and Wilf [46]. This method applies whenever the structure under consideration is defined as an orbit of a finite group acting on a finite set.

At the very end of this chapter in Section 6.8 we prove that every local isometry between two (n,k)-codes over $\mathbb{F}_q$ can be extended to a global isometry of $\mathbb{F}_q^n$. This demonstrates that the seemingly weaker condition of a local isometry is equivalent to our approach from Section 1.4 and Section 1.5. (See also [84, second edition, Section 9.1].)

Normal bases of a finite extension $\mathbb{F}_q$ over $\mathbb{F}_p$ have been introduced in Section 3.3. Finally, in Section 6.9 we prove that it is always possible to construct a normal basis of a finite field extension over a finite field. The proof uses methods from module theory introduced in Chapter 4 and Section 6.3.

6.1

6.1 Enumeration of Linear Isometry Classes

To begin with, we recall that two linear codes C and C' in $\mathbb{F}_q^n$ are said to be *linearly isometric* if there exists a linear isometry

$$\iota : \mathbb{F}_q^n \to \mathbb{F}_q^n$$

which maps C onto C'. The group of *all* linear isometries on $\mathbb{F}_q^n$, the *linear isometry group*, was indicated in Section 1.4 by

$$M_n(q).$$

It is the set of all $n \times n$-matrices over $\mathbb{F}_q$ which contain in each of their rows and columns exactly one nonzero element of $\mathbb{F}_q$. The application of a linear isometry to a generator matrix (via right multiplication) amounts to a permutation of its columns and/or a multiplication of columns by nonzero elements of $\mathbb{F}_q$. We have seen in 1.4.12 that $M_n(q)$ is isomorphic to a wreath product,

$$M_n(q) \simeq \mathbb{F}_q^* \wr_n S_n.$$

The linear isometry group acts on $\mathbb{F}_q^n$, whence also on its power set, and it has already been mentioned that the corresponding set of orbits,

$$\mathbb{F}_q^* \wr_n S_n \backslash\backslash 2^{\mathbb{F}_q^n},$$

is the set of isometry classes of block codes. Some of them are sets of subspaces, the linear isometry classes of linear codes. Using the notation

$$\mathcal{U}(n,q) := \left\{ U \mid U \leq \mathbb{F}_q^n \right\}$$

for the set of all subspaces of $\mathbb{F}_q^n$, we express the set of linear isometry classes of linear codes in $\mathbb{F}_q^n$ as

$$\mathbb{F}_q^* \wr_n S_n \backslash\backslash \mathcal{U}(n,q).$$

This set can still be refined since each linear isometry preserves both the dimension and the minimum distance of a code. For this reason, we introduce the following subsets of $\mathcal{U}(n,q)$

$$\mathcal{U}(n,k,q) := \left\{ U \leq \mathbb{F}_q^n \mid \dim(U) = k \right\}, \qquad 1 \leq k \leq n,$$

and

$$\mathcal{U}(n,k,d,q) := \left\{ U \leq \mathbb{F}_q^n \mid \dim(U) = k,\ \operatorname{dist}(U) = d \right\}.$$

Thus we obtain

The metric classification of linear codes *The set of nontrivial linear isometry classes of linear codes of length n over $\mathbb{F}_q$ is the set of orbits* **6.1.1**

$$\mathbb{F}_q^* \wr_n S_n \backslash\backslash (\mathcal{U}(n,q) \setminus \{0\}) = \bigcup_{k=1}^{n} \bigcup_{d=1}^{d_{\max}(n,k,q)} \mathbb{F}_q^* \wr_n S_n \backslash\backslash \mathcal{U}(n,k,d,q).$$

Each transversal of the orbit set

$$\mathbb{F}_q^* \wr_n S_n \backslash\backslash \mathcal{U}(n,k,d,q)$$

is a complete system of pairwise linearly nonisometric linear (n,k,d,q)-codes. □

Example Considering the set of linear isometry classes of linear (n,k)-codes instead of the set of all (n,k)-codes reduces dramatically the number of objects to be classified. For instance, the numbers $\begin{bmatrix} n \\ k \end{bmatrix}(2)$ of k-dimensional subspaces of $\mathbb{F}_2^n$ (cf. Exercise 6.1.3) are displayed in Table 6.1. **6.1.2**

With the methods described in this section we will be able to determine the numbers U_{nk2} given in Table 6.7. They are the numbers of linear isometry classes of binary (n,k)-codes. From these tables we deduce, for instance, that there are more than 53 million 4-dimensional subspaces of $\mathbb{F}_2^{10}$ but only 516 linear isometry classes of binary $(10,4)$-codes. Later on (cf. Table 6.7) we will see that there are only 276 isometry classes of $(10,4)$-codes without zero columns. Using methods from Chapter 9, we will obtain that there are only 19 isometry classes of $(10,4)$-codes with optimal minimum distance $d = 4$. ◇

If we want to apply the metric classification of linear codes for enumerative or constructive purposes, we run into problems since the sets $\mathcal{U}(n,k,q)$ are abstract sets of vector spaces. But we know from Linear Algebra that each code possesses bases, k-tuples of linearly independent elements. They are the generator matrices of a code. Still there is a problem concerning complexity.

Table 6.1 Values of $\begin{bmatrix} n \\ k \end{bmatrix}(2)$

$n\backslash k$	1	2	3	4	5
1	1	0	0	0	0
2	3	1	0	0	0
3	7	7	1	0	0
4	15	35	15	1	0
5	31	155	155	31	1
6	63	651	1 395	651	63
7	127	2 667	11 811	11 811	2 667
8	255	10 795	97 155	200 787	97 155
9	511	43 435	788 035	3 309 747	3 309 747
10	1 023	174 251	6 347 715	53 743 987	109 221 651
11	2 047	698 027	50 955 971	866 251 507	3 548 836 819
12	4 095	2 794 155	408 345 795	13 910 980 083	114 429 029 715

Table 6.2 Values of U_{nk2}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	2	1	0	0	0	0	0
3	3	3	1	0	0	0	0
4	4	6	4	1	0	0	0
5	5	10	10	5	1	0	0
6	6	16	22	16	6	1	0
7	7	23	43	43	23	7	1
8	8	32	77	106	77	32	8
9	9	43	131	240	240	131	43
10	10	56	213	516	705	516	213
11	11	71	333	1 060	1 988	1 988	1 060
12	12	89	507	2 108	5 468	7 664	5 468
13	13	109	751	4 064	14 724	29 765	29 765
14	14	132	1 088	7 641	39 006	117 169	173 035

Each (n,k)-code has *many bases,* except for very trivial cases. Hence, if we want to describe a subspace by a generator matrix, we are faced with a great variety of possibilities. So, instead of the abstract set of vector spaces we have to manage a big set of matrices. In 1.4.14 and Exercise 1.4.14 we have already introduced for $n \geq k \geq 1$ the set of all generator matrices of (n,k)-codes over $\mathbb{F}_q$ as the set

$$\mathbb{F}_q^{k\times n,k} := \left\{ \Gamma \mid \Gamma \in \mathbb{F}_q^{k\times n},\ \mathrm{rank}(\Gamma) = k \right\}$$

of all $k \times n$-matrices over $\mathbb{F}_q$ of rank k. In the Exercises 1.4.14 and 1.4.16 we have described actions of the general linear group $\mathrm{GL}_k(q)$ and of the full monomial group $M_n(q)$ on $\mathbb{F}_q^{k\times n,k}$, and we have shown that these two actions commute. According to Exercise 1.4.10, two commuting group actions ${}_GX$ and ${}_HX$ induce an action of the direct product $G \times H$ on X.

Since, according to Exercise 1.4.14, exactly the left multiplications by elements $A \in \mathrm{GL}_k(q)$ transform a generator matrix of the space $C \in \mathcal{U}(n,k,q)$ into another generator matrix of C, the orbits of $\mathrm{GL}_k(q)$ on $\mathbb{F}_q^{k\times n,k}$ correspond to the subspaces of dimension k:

$$\mathcal{U}(n,k,q) = \mathrm{GL}_k(q) \backslash\backslash \mathbb{F}_q^{k\times n,k}.$$

The operations of elements of the linear isometry group commute with the operations of the elements of $\mathrm{GL}_k(q)$, and so the set of linear isometry classes of (n,k)-codes is equal to the set of orbits

$$(\mathrm{GL}_k(q) \times \mathbb{F}_q^* \wr_n S_n) \backslash\backslash \mathbb{F}_q^{k\times n,k} \qquad \textbf{6.1.3}$$

with respect to the action

$$(\mathrm{GL}_k(q) \times \mathbb{F}_q^* \wr_n S_n) \times \mathbb{F}_q^{k\times n,k} \to \mathbb{F}_q^{k\times n,k},$$

defined by

$$((A,B),\Gamma) \mapsto A \cdot \Gamma \cdot B^\top.$$

Using Exercise 1.4.9 (which says that the set of orbits of a direct product is the set of orbits of one factor on the set of orbits of the other factor) we rephrase 6.1.3 as

$$\mathrm{GL}_k(q) \backslash\backslash \left(\mathbb{F}_q^* \wr_n S_n \backslash\backslash \mathbb{F}_q^{k\times n,k} \right). \qquad \textbf{6.1.4}$$

Because of the condition on the rank, the set $\mathbb{F}_q^{k\times n,k}$ is not easy to handle. We may thus prefer to work with the even larger set $\mathbb{F}_q^{k\times n}$ of *all* $k \times n$-matrices without any condition on the rank. In 6.1.15 and Exercise 6.1.6 it will be clear that it is possible to determine the number of isometry classes of linear (n,k)-codes from $|\mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^* \wr_n S_n \backslash\backslash \mathbb{F}_q^{k\times n})|$ and $|\mathrm{GL}_{k-1}(q) \backslash\backslash (\mathbb{F}_q^* \wr_n S_n \backslash\backslash \mathbb{F}_q^{(k-1)\times n})|$. The set $\mathbb{F}_q^{k\times n}$ can be reduced a bit, since matrices which contain zero columns are not of interest for coding theoretic purposes. (Such columns are redundant

in coding theory, since the corresponding components are zero in each codeword, and so they give no information. Moreover, two generator matrices of the same code have the same number of columns of zeros, and these columns occur at the same column indices. Generator matrices of isometric codes also have the same number of columns of zeros, but these columns need not occur at the same column indices.) For this reason we introduce the following notion:

6.1.5 **Definition (nonredundant code)** A linear code C is called *nonredundant* if its generator matrix Γ contains no zero column. ◇

In fact, this condition is independent of the choice of the generator matrix Γ.

It is, therefore, reasonable to restrict attention to the set of all $k \times n$-matrices without zero columns. The advantage is that the set of *all $k \times n$-matrices over $\mathbb{F}_q$ which contain no zero column can be written as a set of mappings*

$$(\mathbb{F}_q^k \backslash \{0\})^n = \left\{ f \mid f : n \to \mathbb{F}_q^k \backslash \{0\} \right\}.$$

The generator matrix Γ of a nonredundant (n,k)-code is identified with the mapping $\Gamma : n \to \mathbb{F}_q^k \backslash \{0\}$ where $\Gamma(i)^\top$ is the i-th column of Γ.

Rewriting our problem in these terms shows that instead of the situation in 6.1.4 we are now faced with the set of orbits

6.1.6
$$\mathrm{GL}_k(q) \backslash\backslash \left(\mathbb{F}_q^* \wr_n S_n \backslash\backslash (\mathbb{F}_q^k \backslash \{0\})^n \right).$$

According to Exercise 1.4.9, the general linear group acts in the following way on $\mathbb{F}_q^* \wr_n S_n \backslash\backslash (\mathbb{F}_q^k \backslash \{0\})^n$:

$$\mathrm{GL}_k(q) \times \left(\mathbb{F}_q^* \wr_n S_n \backslash\backslash (\mathbb{F}_q^k \backslash \{0\})^n \right) \to \mathbb{F}_q^* \wr_n S_n \backslash\backslash (\mathbb{F}_q^k \backslash \{0\})^n,$$

6.1.7
$$(A, \mathbb{F}_q^* \wr_n S_n(f)) \mapsto \mathbb{F}_q^* \wr_n S_n(Af).$$

When writing Af, we identify the function $f \in (\mathbb{F}_q^k \backslash \{0\})^n$ with the corresponding $k \times n$-matrix $(f(0)^\top \mid \ldots \mid f(n-1)^\top)$. Then $Af = (A \cdot f(0)^\top \mid \ldots \mid A \cdot f(n-1)^\top)$ and, therefore, $Af(i) = (A \cdot f(i)^\top)^\top = f(i) \cdot A^\top$.

For this reason, we first investigate the action of a wreath product in more detail and explain how to split it into two group actions which are easier to handle (cf. [123], [124]).

6.1.8 **Lehmann's Lemma** *Let ${}_G X$ and ${}_H Y$ be two group actions. For the natural action of the wreath product $H \wr_X G$ on Y^X, defined in 1.4.9, we have:*

1. *If the mapping φ is given by*

$$\varphi : Y^X \to (H \backslash\backslash Y)^X \ : \ f \mapsto \varphi(f) \ \text{ where } \ \varphi(f)(x) = H(f(x)),$$

then the mapping

$$\Phi\colon H \wr_X G \backslash\backslash Y^X \to G \backslash\backslash ((H \backslash\backslash Y)^X) \;:\; H \wr_X G(f) \mapsto G(\varphi(f))$$

is a bijection, where G acts canonically (cf. 1.4.7) on this set of functions.

2. *The orbit of $f \in Y^X$ under the action of $H \wr_X G$ is given by*

$$H \wr_X G(f) = \varphi^{-1}(\Phi(H \wr_X G(f))) = \varphi^{-1}(G(\varphi(f))).$$

Proof: 1. For $f_1, f_2 \in Y^X$ the following facts are equivalent:

$$\begin{aligned}
&\Phi(H \wr_X G(f_1)) = \Phi(H \wr_X G(f_2))\\
&G(\varphi(f_1)) = G(\varphi(f_2))\\
&\varphi(f_2) \in G(\varphi(f_1))\\
&\varphi(f_2) = \varphi(f_1) \circ \overline{g} \text{ for some } g \in G\\
&\varphi(f_2)(x) = \varphi(f_1)(gx) \text{ for some } g \in G \text{ and all } x \in X\\
&H(f_2(x)) = H(f_1(gx)) \text{ for some } g \in G \text{ and all } x \in X\\
&f_2(x) \in H(f_1(gx)) \text{ for some } g \in G \text{ and all } x \in X\\
&f_2 = (\psi; g) f_1 \text{ for some } (\psi; g) \in H \wr_X G\\
&f_2 \in H \wr_X G(f_1)\\
&H \wr_X G(f_2) = H \wr_X G(f_1).
\end{aligned}$$

Reading these implications from the bottom to the top, we deduce that Φ is well-defined. Reading them the other way round it follows that Φ is injective. In order to prove that Φ is surjective, we first realize that φ is surjective, i.e. each $F \in (H \backslash\backslash Y)^X$ is of the form $\varphi(f) = F$ for some $f \in Y^X$. (The function f should be determined in such a way that for each $x \in X$ the value $f(x)$ belongs to $F(x)$, i.e. $F(x) = H(f(x))$.) If $\varphi(f) = F$, then

$$\Phi(H \wr_X G(f)) = G(\varphi(f)) = G(F),$$

whence Φ is also surjective.

2. In order to prove the second assertion, consider a function $F \in (H \backslash\backslash Y)^X$ and assume that $F = \varphi(f)$ for some $f \in Y^X$. Then

$$\begin{aligned}
\varphi^{-1}(\{F\}) \;&=\; \varphi^{-1}(\{\varphi(f)\}) \;=\; H \wr_X \{1\}\,(f)\\
&= \left\{ \tilde{f} \in Y^X \;\middle|\; \tilde{f}(x) = \psi(x) f(x) \text{ for } \psi \in H^X \text{ and } x \in X \right\}.
\end{aligned}$$

Next we prove that

$$\varphi(f \circ \overline{g}) = \varphi(f) \circ \overline{g}, \qquad g \in G.$$

(The reader should realize that on the left hand side we are faced with the natural action of G on Y^X and on the right hand side with the natural action of G on $(H\backslash\backslash Y)^X$.) The action of G commutes with the application of φ, since $\varphi(f\circ\overline{g})(x) = H(f(g(x)))$ and $(\varphi(f)\circ\overline{g})(x) = \varphi(f)(gx) = H(f(gx))$ for all $x\in X$. Finally we obtain

$$\begin{aligned}
H\wr_X G(f) &= \{(\psi;g)f \mid (\psi;g)\in H\wr_X G\}\\
&= \left\{x\mapsto \psi(x)f(g^{-1}x) \;\middle|\; \psi\in H^X,\ g\in G\right\}\\
&= \bigcup_{g\in G}\left\{x\mapsto \psi(x)f(g^{-1}x) \;\middle|\; \psi\in H^X\right\}\\
&= \bigcup_{g\in G} H\wr_X\{1\}\,(f\circ\overline{g}^{-1})\\
&= \bigcup_{g\in G}\varphi^{-1}\left(\left\{\varphi(f\circ\overline{g}^{-1})\right\}\right)\\
&= \bigcup_{g\in G}\varphi^{-1}\left(\left\{\varphi(f)\circ\overline{g}^{-1}\right\}\right)\\
&= \varphi^{-1}\Big(\bigcup_{g\in G}\left\{\varphi(f)\circ\overline{g}^{-1}\right\}\Big)\\
&= \varphi^{-1}\left(\left\{\varphi(f)\circ\overline{g}^{-1} \;\middle|\; g\in G\right\}\right)\\
&= \varphi^{-1}\left(G(\varphi(f))\right)\\
&= \varphi^{-1}\left(\Phi(H\wr_X G(f))\right).
\end{aligned}$$

□

An application of Lehmann's Lemma allows us to rewrite 6.1.6 in the form

6.1.9 $$\mathrm{GL}_k(q)\backslash\backslash\left(S_n\backslash\backslash\left(\mathbb{F}_q^*\backslash\backslash(\mathbb{F}_q^k\backslash\{0\})\right)^n\right).$$

This result shows the close connection between finite geometry and the theory of linear codes: The set of orbits of $\mathbb{F}_q^*$ on $\mathbb{F}_q^k\backslash\{0\}$ is the set of elements (also called points) of the $(k-1)$-dimensional projective space $\mathrm{PG}_{k-1}^*(q)$ (cf. Section 3.7). Hence, we actually investigate

6.1.10 $$\mathrm{GL}_k(q)\backslash\backslash\left(S_n\backslash\backslash \mathrm{PG}_{k-1}^*(q)^n\right).$$

Here the symmetric group S_n acts in a natural way on the domain of the mappings in $\mathrm{PG}_{k-1}^*(q)^n$. How does $\mathrm{GL}_k(q)$ act on the orbits $S_n\backslash\backslash \mathrm{PG}_{k-1}^*(q)^n$? From 6.1.7 we deduce that the application of $A\in\mathrm{GL}_k(q)$ to the $\mathbb{F}_q^*\wr_n S_n$-orbit of $f\in(\mathbb{F}_q^k\backslash\{0\})^n$ yields the orbit $\mathbb{F}_q^*\wr_n S_n(Af)$. If φ is the mapping defined as in Lehmann's Lemma, then the elements of $A(S_n(F))$ for $F\in\mathrm{PG}_{k-1}^*(q)^n$ are

the elements in $\varphi\big(\mathbb{F}_q^* \wr_n S_n(Af)\big)$ for some $f \in \varphi^{-1}(\{F\})$. We want to describe this set again as an orbit under a suitable group action. For this reason, in Section 3.7 we have deduced from Exercise 1.4.13 the natural action of $\mathrm{GL}_k(q)$ on $\mathrm{PG}^*_{k-1}(q)$ as described in 3.7.4. Here it is repeated once again.

$$\mathrm{GL}_k(q) \times \mathrm{PG}^*_{k-1}(q) \to \mathrm{PG}^*_{k-1}(q) \ : \ (A, \mathbb{F}_q^*(v)) \mapsto \mathbb{F}_q^*(v \cdot A^\top).$$

Lemma *Consider $A \in \mathrm{GL}_k(q)$ and let φ be given by* **6.1.11**

$$\varphi\colon (\mathbb{F}_q^k \backslash \{0\})^n \to \mathrm{PG}^*_{k-1}(q)^n \ : \ f \mapsto \varphi(f) \ \text{ where } \ \varphi(f)(i) := \mathbb{F}_q^*(f(i)).$$

Then

$$\varphi\left(\mathbb{F}_q^* \wr_n S_n(Af)\right) = A(S_n(\varphi(f))), \qquad f \in (\mathbb{F}_q^k \backslash \{0\})^n,$$

where on the right hand side the action of $\mathrm{GL}_k(q)$ on $S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n$ appears, which is induced by the natural action of $\mathrm{GL}_k(q)$ on $\mathrm{PG}^*_{k-1}(q)$.

Proof: From the second part of Lehmann's Lemma we obtain

$$\varphi(\mathbb{F}_q^* \wr_n S_n(Af)) = S_n(\varphi(Af)).$$

Using Exercise 1.4.13 we deduce that $\varphi(Af) = A\varphi(f)$, since

$$\varphi(Af)(i) = \mathbb{F}_q^*(f(i) \cdot A^\top) = A\mathbb{F}_q^*(f(i)) = A\varphi(f)(i)$$

for all $i \in n$. Thus, $S_n(\varphi(Af)) = S_n(A\varphi(f))$ and this orbit equals $A(S_n(\varphi(f)))$, since A operates by matrix multiplication from the left, and π permutes the columns of (the matrix) f. □

This way we have just replaced the action of $\mathrm{GL}_k(q) \times \mathbb{F}_q^* \wr_n S_n$ on $(\mathbb{F}_q^k \backslash \{0\})^n$ by the action of $\mathrm{GL}_k(q) \times S_n$ on $\mathrm{PG}^*_{k-1}(q)^n$, where this action is of the form 1.4.11. Therefore, $\mathrm{GL}_k(q)$ acts only on the range $\mathrm{PG}^*_{k-1}(q)$ and S_n acts only on the domain n. Instead of 6.1.10 we are finally dealing with

$$(\mathrm{GL}_k(q) \times S_n) \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n. \qquad \textbf{6.1.12}$$

This proves the following fundamental result:

Theorem *The linear isometry classes of linear, nonredundant (n,k)-codes over $\mathbb{F}_q$ are the orbits of $\mathrm{GL}_k(q) \times S_n$ on $\mathrm{PG}^*_{k-1}(q)^n$, the representatives of which are of rank k. They form a subset of* **6.1.13**

$$\mathrm{GL}_k(q) \backslash\backslash \big(S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n\big).$$

The inner orbit set $S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n$ can be represented by any complete system of mappings $f : n \to \mathrm{PG}^*_{k-1}(q)$ of pairwise different content

$$c(f)\colon \mathrm{PG}^*_{k-1}(q) \to \mathbb{N} \ : \ y \mapsto |f^{-1}(\{y\})|.$$

Hence, the set of all linear isometry classes of linear, nonredundant (n,k)-codes over $\mathbb{F}_q$ can be identified with the set of orbits of $\mathrm{GL}_k(q)$ on the set of mappings $f \in \mathrm{PG}^*_{k-1}(q)^n$ of pairwise different content which form $k \times n$-matrices of rank k. □

Moreover, the class of bijective functions $f : n \to \mathrm{PG}^*_{k-1}(q)$ is the class of the simplex-codes. This fact demonstrates the particular role of simplex-codes and their dual codes, the Hamming-codes.

6.1.14 Definition (projective codes and projective matrices) A nonredundant (n,k)-code C is called *projective* if the columns of any generator matrix Γ of C are pairwise linearly independent. In this case, we call Γ a *projective matrix*. In other words, a $k \times n$ matrix Γ over $\mathbb{F}_q$ is called projective if no two columns are linearly dependent. If $n = 1$ we require that Γ is not the zero matrix. ◇

Thus, projective codes have projective generator matrices and vice-versa. The columns of a projective generator matrix Γ are never zero and are representatives of pairwise distinct one-dimensional (punctured) subspaces of $\mathbb{F}_q^k$. Therefore, they give rise to an injective mapping

$$\overline{\Gamma} : n \to \mathrm{PG}_{k-1}(q) \quad \text{or} \quad \overline{\Gamma} : n \to \mathrm{PG}^*_{k-1}(q).$$

Here we prefer to use $\mathrm{PG}^*_{k-1}(q)$ since its elements are orbits under the action of $\mathbb{F}_q^*$. It is straightforward to verify that being projective is a property of the isometry class of a code. That is, for linearly isometric codes C_1 and C_2 the code C_2 is projective if and only if C_1 has this property.

Generalizing this definition, an arbitrary (n,k)-code C is called *injective* or *reduced* if the mapping

$$\overline{\Gamma} : n \to \mathrm{PG}^*_{k-1}(q) \cup \{0\},$$

corresponding to the columns of an arbitrary generator matrix Γ of C, is injective.

The numbers of linear isometry classes of linear codes will be obtained from a refinement of the metric classification 6.1.1. Besides the total number of linear isometry classes, we also evaluate the number of linear isometry classes of nonredundant codes as well as of projective codes.

The set of all k-dimensional *nonredundant* subspaces of $\mathbb{F}_q^n$ is indicated as

$$\mathcal{V}(n,k,q).$$

By $\overline{\mathcal{V}}(n,k,q)$ we denote the set of all projective $U \in \mathcal{V}(n,k,q)$, and we write $\overline{\mathcal{U}}(n,k,q)$ for the set of all injective $U \in \mathcal{U}(n,k,q)$. For the sets of linear isometry classes in $\mathcal{U}(n,k,q)$ and $\mathcal{V}(n,k,q)$ we use the symbols

$$\mathcal{U}_{n,k,q} := M_n(q) \backslash\backslash \mathcal{U}(n,k,q), \qquad \mathcal{V}_{n,k,q} := M_n(q) \backslash\backslash \mathcal{V}(n,k,q),$$
$$\overline{\mathcal{U}}_{n,k,q} := M_n(q) \backslash\backslash \overline{\mathcal{U}}(n,k,q), \qquad \overline{\mathcal{V}}_{n,k,q} := M_n(q) \backslash\backslash \overline{\mathcal{V}}(n,k,q).$$

In addition, we introduce the following sets:

$$\mathcal{T}_{n,k,q} := \bigcup_{l\le k} \mathcal{V}_{n,l,q} \quad (= \mathcal{V}_{n,\le k,q}),$$
$$\overline{\mathcal{T}}_{n,k,q} := \bigcup_{l\le k} \overline{\mathcal{V}}_{n,l,q} \quad (= \overline{\mathcal{V}}_{n,\le k,q}),$$

comprising the classes of linear (n,l)-codes of dimension $l \le k$. The cardinalities of these sets are denoted by

$$T_{nkq},\ \overline{T}_{nkq},\ V_{nkq},\ \overline{V}_{nkq},\ U_{nkq},\ \overline{U}_{nkq}.$$

Of course, there is a close connection between these numbers. Using Exercise 6.1.6 we obtain the following basic results for the enumeration of linear isometry classes of linear codes (cf. Exercise 6.1.6):

Corollary **6.1.15**

- *T_{nkq} is the number of orbits computed in 6.1.12,*
$$T_{nkq} = |(\mathrm{GL}_k(q)\times S_n)\backslash\backslash \mathrm{PG}^*_{k-1}(q)^n| = |\mathrm{GL}_k(q)\backslash\backslash (S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n)|.$$
If $k > 1$, then $T_{n,k-1,q}$ is also the number of $\mathrm{GL}_k(q)\times S_n$-orbits of mappings $f \in \mathrm{PG}^*_{k-1}(q)^n$ corresponding to matrices of rank not greater than $k-1$.
- *$\overline{T}_{nkq}$ is the number of $\mathrm{GL}_k(q)\times S_n$-orbits on the set of injective functions in $\mathrm{PG}^*_{k-1}(q)^n$,*
$$\overline{T}_{nkq} = |(\mathrm{GL}_k(q)\times S_n)\backslash\backslash \mathrm{PG}^*_{k-1}(q)^n_{\mathrm{inj}}| = |\mathrm{GL}_k(q)\backslash\backslash (S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n_{\mathrm{inj}})|.$$
- *$V_{nkq} = T_{nkq} - T_{n,k-1,q}$, $\overline{V}_{nkq} = \overline{T}_{nkq} - \overline{T}_{n,k-1,q}$ for $1 < k \le n$.*
- *$U_{nkq} = \sum_{i=k}^n V_{ikq}$, $\overline{U}_{kkq} = \overline{V}_{kkq}$, and $\overline{U}_{nkq} = \overline{V}_{n-1,k,q} + \overline{V}_{nkq}$ for $n > k$.*

The initial values for these recursions are $V_{n1q} = 1$ for $n \in \mathbb{N}^*$, $\overline{V}_{11q} = 1$ and $\overline{V}_{n1q} = 0$ for $n > 1$. □

This way we have expressed U_{nkq}, $\overline{U}_{nkq}$, V_{nkq}, and $\overline{V}_{nkq}$ in terms of T_{nkq} and $\overline{T}_{nkq}$. The remaining problem is the evaluation of T_{nkq} and $\overline{T}_{nkq}$. In order to obtain these numbers we could, of course, use the Lemma of Cauchy–Frobenius 3.4.2 and compute the average number of fixed points. But it is our intention to get a more general result which gives a generating function for these numbers. It will turn out that the *weighted form* of the Lemma of Cauchy–Frobenius is more suitable for this purpose. For this reason we introduce *weight functions*. They are mappings defined on the set, on which the group acts, which are constant on each orbit. The range of these weight functions is usually a commutative ring (mostly a polynomial ring) which contains $\mathbb{Q}$ as a subring since we need to allow division by $|G|$. The following generalization of the Lemma of Cauchy–Frobenius allows us to count orbits with additional properties expressed by weights.

6.1.16 **The Lemma of Cauchy–Frobenius, weighted form** *Consider a finite action ${}_GX$ and suppose that $w\colon X \to R$ is a mapping from X into a commutative ring R which contains $\mathbb{Q}$ as a subring. If w is constant on the orbits of G on X, then, for each transversal T of the set of orbits we have*

$$\sum_{t\in T} w(t) = \frac{1}{|G|} \sum_{g\in G} \sum_{x\in X_g} w(x).$$

Proof: The following identities are obvious, possibly up to the final one which uses the fact that w is constant on the orbits:

$$\begin{aligned}\sum_{g\in G} \sum_{x\in X_g} w(x) &= \sum_{x\in X} \sum_{g\in G_x} w(x) = \sum_{x\in X} |G_x| w(x) \\ &= |G| \sum_{x\in X} |G(x)|^{-1} w(x) = |G| \sum_{t\in T} w(t).\end{aligned}$$ □

If the values $w(f)$ of the weight function are monic monomials over $\mathbb{Q}$, then the values in $\{w(f) \mid f \in Y^X\}$ are linearly independent. Hence, the right hand side of the weighted form of the Lemma of Cauchy–Frobenius yields the number of orbits of any given weight.

For group actions on Y^X of the form 1.4.7 we introduce, for any given mapping $W\colon Y \to R$, the *multiplicative weight* $w\colon Y^X \to R$, by

6.1.17
$$w(f) := \prod_{x\in X} W(f(x)).$$

This mapping is clearly constant on the orbits of G on Y^X.

We recall from elementary theory of permutation groups that the permutation $\overline{g}\colon x \mapsto gx$ induced by ${}_GX$ possesses a decomposition into pairwise disjoint cycles. If this decomposition consists of $a_i(\overline{g})$ cycles of length i, for $i = 1, \ldots, |X|$, then the sequence

$$(a_1(\overline{g}), a_2(\overline{g}), \ldots, a_{|X|}(\overline{g}))$$

is called the *cycle type* of $\overline{g}$. In other words, $a_i(\overline{g})$ is the number of orbits of length i of the group $\langle \overline{g} \rangle$ on X, i.e.

$$a_i(\overline{g}) = \left|\{\omega \in \langle \overline{g} \rangle \backslash\backslash X \mid |\omega| = i\}\right| = \left|\{\omega \in \langle g \rangle \backslash\backslash X \mid |\omega| = i\}\right|.$$

The cycle type of $\overline{g}$ satisfies $\sum_{i=1}^{n} i a_i(\overline{g}) = |X|$, since X is the disjoint union of the cycles of $\langle \overline{g} \rangle$.

An application of the weighted form of the Lemma of Cauchy–Frobenius gives:

Pólya's Theorem *Let ${}_GX$ be a finite group action which induces according to 1.4.7 a group action on the finite set of mappings Y^X. Let R be a commutative ring which contains $\mathbb{Q}$ as a subring. If T is a transversal of $G\backslash\backslash Y^X$, then for each $W: Y \to R$ and the corresponding multiplicative weight $w: Y^X \to R$ we have* **6.1.18**

$$\sum_{t\in T} w(t) = \frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{|X|}\left(\sum_{y\in Y} W(y)^i\right)^{a_i(\overline{g})} = \frac{1}{|\overline{G}|}\sum_{\pi\in\overline{G}}\prod_{i=1}^{|X|}\left(\sum_{y\in Y} W(y)^i\right)^{a_i(\pi)},$$

where $a_i(\overline{g})$ or $a_i(\pi)$ is the number of cyclic factors of length i of the permutation $\overline{g} \in S_X$ or $\pi \in S_X$. □

The most general multiplicative weight function is obtained by considering the elements of Y as algebraically independent indeterminates in the polynomial ring $\mathbb{Q}[Y]$. The mapping $W: Y \to \mathbb{Q}[Y]$ which takes $y \in Y$ to itself gives rise to the multiplicative weight

$$w: Y^X \to \mathbb{Q}[Y] \ : \ f \mapsto \prod_{x\in X} f(x) = \prod_{y\in Y} y^{\left|f^{-1}(\{y\})\right|}.$$

The image of f is a monic *monomial* in $\mathbb{Q}[Y]$, which uniquely describes the content (cf. 6.1.13)

$$c(f): Y \to \mathbb{N} \ : \ y \mapsto \left|f^{-1}(\{y\})\right|$$

of f. The sum of weights of the elements in a transversal T of the orbits is

$$\sum_{t\in T} w(t) = \frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{|X|}\left(\sum_{y\in Y} y^i\right)^{a_i(\overline{g})}.$$

This result can be formulated – as it was already done by G. Pólya – in terms of the *cycle index* polynomial corresponding to the action ${}_GX$.

Definition (cycle index polynomial) If G is a finite group acting on a finite set X, then the cycle index $C(G,X)$ of the action ${}_GX$ is the polynomial **6.1.19**

$$C(G,X) := \frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{|X|} z_i^{a_i(\overline{g})} \in \mathbb{Q}[z_1, z_2, \ldots, z_{|X|}],$$

where $(a_1(\overline{g}), \ldots, a_{|X|}(\overline{g}))$ is the cycle type of $\overline{g}$. ◇

Pólya's Theorem shows that the sum of the weights of the elements of a transversal can be obtained from the cycle index by replacing the indeterminate z_i by the sum of the i-th powers of all weights, $\sum_{y\in Y} W(y)^i$, i.e.

$$\sum_{t\in T} w(t) = C(G,X)\big|_{z_i := \sum_y W(y)^i}.$$

Our aim is to evaluate the *generating function* for T_{nkq}. For fixed k and q, this is the formal power series whose coefficient of x^n is T_{nkq}. For this reason we still give a short introduction to

6.1.20 **The ring of formal power series over a ring** Let R be an integral domain, then $R[\![x]\!]$, the ring of formal power series over R in the indeterminate x, is given by

$$R[\![x]\!] = \left\{ \sum_{n\geq 0} a_n x^n \;\middle|\; a_n \in R,\ n \in \mathbb{Z},\ n \geq 0 \right\}.$$

Together with addition and multiplication

$$\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n := \sum_{n\geq 0} (a_n + b_n) x^n$$

$$\left(\sum_{n\geq 0} a_n x^n\right) \cdot \left(\sum_{n\geq 0} b_n x^n\right) := \sum_{n\geq 0} \left(\sum_{r=0}^{n} a_r b_{n-r}\right) x^n,$$

$R[\![x]\!]$ is an integral domain.

If f is a nonzero formal power series of the form $f = \sum_{n\geq N} a_n x^n \in R[\![x]\!]$ with $a_N \neq 0$, then N is called the *order* of f, for short

$$\operatorname{ord}(f) = N.$$

For technical reasons, we associate the zero series with the order $+\infty$.

A family $(f_j)_{j\in J}$ is called *summable* if for each $n \geq 0$ the cardinality of the index set

$$J_n := \{j \in J \mid \operatorname{ord}(f_j) \leq n\}$$

is finite. In this case we set

$$\sum_{j\in J} f_j := \sum_{n\geq 0} s_n x^n,$$

where s_n is the coefficient of x^n in the (finite) sum

$$\sum_{j\in J_n} f_j.$$

Finally, if $(a_n)_{n\geq 0}$ is an arbitrary sequence of numbers, then the ordinary generating function for this sequence is given by

$$\sum_{n\geq 0} a_n x^n.$$

Using this, we can now prove the decisive result we need in order to enumerate linear codes:

6.1.21 **Theorem** *Let ${}_H Y$ be a finite group action. The generating function for the number of $(H \times S_n)$-orbits on Y^n is*

$$\sum_{n\in\mathbb{N}} |(H \times S_n) \backslash\backslash Y^n| \cdot x^n = C(H, Y)\big|_{z_i := \sum_{j=0}^{\infty} x^{i\cdot j}}.$$

For the subset Y^n_{inj} of the injective functions in Y^n we obtain

$$\sum_{n\in\mathbb{N}} |(H \times S_n) \backslash\backslash Y^n_{\text{inj}}| \cdot x^n = C(H, Y)\big|_{z_i := 1 + x^i}.$$

Proof: 1. From Exercise 1.4.9 it follows that

$$(H \times S_n)\backslash\backslash Y^n = H\backslash\backslash (S_n\backslash\backslash Y^n)\,.$$

Thus, according to Exercise 6.1.1, the orbit $(H \times S_n)\backslash\backslash Y^n$ corresponds to the set of H-orbits on the set of mappings $f \in Y^n$ of different content. The content $c(f)$ of $f \in Y^n$ maps $y \in Y$ to $c(f)(y) := |f^{-1}(\{y\})|$, the cardinality of the inverse image of y. It is a decomposition of n into $|Y|$ summands. Such a decomposition can be viewed as a mapping $\varphi \in \mathbb{N}^Y$ such that

$$\sum_{y\in Y} \varphi(y) = n.$$

2. If we now define a weight

$$W : \mathbb{N} \to \mathbb{Q}[x] \;:\; W(n) := x^n,$$

then we obtain the first assertion directly from the following generalization of 6.1.18.

Since the action of H on $\mathbb{N}^Y$ is *not a finite group action*, we need a generalization of Pólya's Theorem. For $\varphi \in \mathbb{N}^Y$ we define the weight $w(\varphi)$ by

$$w(\varphi) := \prod_{y\in Y} W(\varphi(y)) = x^{\sum_{y\in Y}\varphi(y)}.$$

Then φ is the content of some $f \in Y^n$ if and only if $w(\varphi) = x^n$. Thus, the set of S_n-orbits on Y^n is in bijection to the set

$$\mathbb{N}_n^Y := \left\{ \varphi \in \mathbb{N}^Y \;\middle|\; w(\varphi) = x^n \right\}.$$

Moreover, the $(H \times S_n)$-orbits on Y^n correspond to the H-orbits on $\mathbb{N}_n^Y$, where H acts on the domain Y as introduced in 1.4.7. The three families $(x^n)_{n\geq 0}$, $(|(H \times S_n)\backslash\backslash Y^n|\, x^n)_{n\geq 0}$, and $\left(|\mathbb{N}_n^Y| x^n\right)_{n\geq 0}$ are summable in $\mathbb{Q}\,[\![x]\!]$, which is the ring of formal power series in the indeterminate x over $\mathbb{Q}$. Hence,

$$\sum_{n\in\mathbb{N}} x^n = \sum_{n\in\mathbb{N}} W(n), \quad \sum_{n\in\mathbb{N}} |(H \times S_n)\backslash\backslash Y^n|\, x^n, \quad \sum_{n\in\mathbb{N}} |\mathbb{N}_n^Y| x^n$$

exist as elements of $\mathbb{Q}\,[\![x]\!]$. Since $\mathbb{N}^Y$ is the disjoint union of $\mathbb{N}_n^Y$ for $n \in \mathbb{N}$, the last sum is equal to $\sum_{\varphi\in\mathbb{N}^Y} w(\varphi)$. Moreover, all elements of an orbit $\omega = H(\varphi)$ have the same weight, which allows us to set $w(\omega) := w(\varphi)$. Consequently, we get

$$\sum_{n\in\mathbb{N}} |(H \times S_n)\backslash\backslash Y^n|\, x^n = \sum_{n\in\mathbb{N}} |H\backslash\backslash \mathbb{N}_n^Y| x^n = \sum_{\omega\in H\backslash\backslash\mathbb{N}^Y} w(\omega).$$

Since $(w(\varphi))_{\varphi\in\mathbb{N}^Y}$ is a summable family, also $(w(\varphi))_{\varphi\in(\mathbb{N}^Y)_h}$ is summable for $h \in H$, where $(\mathbb{N}^Y)_h$ is the set of fixed points of h. Moreover, $\left(|H_\varphi| w(\varphi)\right)_{\varphi\in\mathbb{N}^Y}$

is summable, where H_φ is the stabilizer of φ. Following the ideas of the proof of Pólya's Theorem, we determine the sum of the weights of the fixed points of $h \in H$ in $\mathbb{N}^Y$ as

$$\sum_{\varphi \in (\mathbb{N}^Y)_h} w(\varphi) = \prod_{i=1}^{|Y|} \left(\sum_{n \in \mathbb{N}} W(n)^i \right)^{a_i(\overline{h})},$$

and finally

$$\sum_{\omega \in H \backslash\backslash \mathbb{N}^Y} w(\omega) = C(H,Y)\big|_{z_i = \sum_{n \in \mathbb{N}} W(n)^i} = C(H,Y)\big|_{z_i = \sum_{n \in \mathbb{N}} x^{i \cdot n}}.$$

3. The second assertion follows similarly, since the contents of injective functions are decompositions whose summands are either 0 or 1. Thus, instead of $\mathbb{N}^Y$ we consider $\{0,1\}^Y$, and the weight $W\colon \{0,1\} \to \mathbb{Q}[x]$ is defined by $W(0) := 1$ and $W(1) := x$. This gives the second assertion about the generating function for the number of orbits of injective functions. □

We are now in a position to derive the generating functions for the numbers

$$T_{nkq} = |(\mathrm{GL}_k(q) \times S_n) \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n|$$

and

$$\overline{T}_{nkq} = |(\mathrm{GL}_k(q) \times S_n) \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n_{\mathrm{inj}}|$$

by an application of the last theorem. These numbers are numbers of orbits of the general linear group. As pointed out in Section 3.7, we can restrict our attention to the projective linear group

$$\mathrm{PGL}_k(q) := \mathrm{GL}_k(q) / \mathcal{Z}_k,$$

which is the factor group over the *center* $\mathcal{Z}_k$ of the general linear group. This reduction is possible, since the action of the general linear group is an action on mappings (to be exact, on orbits of mappings), the range of which is the projective space $\mathrm{PG}^*_{k-1}(q)$. It proves

6.1.22 Corollary *Since the general linear group* $\mathrm{GL}_k(q)$ *operates as the projective linear group* $\mathrm{PGL}_k(q)$ *on the projective space* $\mathrm{PG}^*_{k-1}(q)$*, we have*

$$T_{nkq} = \mathrm{GL}_k(q) \backslash\backslash (S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n) = \mathrm{PGL}_k(q) \backslash\backslash \left(S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n\right)$$

and

$$\overline{T}_{nkq} = \mathrm{GL}_k(q) \backslash\backslash (S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n_{\mathrm{inj}}) = \mathrm{PGL}_k(q) \backslash\backslash \left(S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n_{\mathrm{inj}}\right). \quad \square$$

Using these identities we obtain, by an application of 6.1.21, the following result [61]:

Corollary 6.1.23 *The generating functions for the numbers T_{nkq} and $\overline{T}_{nkq}$ can be obtained from the cycle index of the natural action of the projective linear group on the projective space in the following way:*

$$\sum_{n\in\mathbb{N}} T_{nkq}x^n = C(\mathrm{PGL}_k(q), \mathrm{PG}^*_{k-1}(q))\big|_{z_i:=\sum_{j=0}^{\infty} x^{i\cdot j}},$$

and

$$\sum_{n\in\mathbb{N}} \overline{T}_{nkq}x^n = C(\mathrm{PGL}_k(q), \mathrm{PG}^*_{k-1}(q))\big|_{z_i:=1+x^i}. \qquad \square$$

Example 6.1.24 Let us consider isometry classes of binary linear codes. Since the wreath product $\mathbb{F}_2^* \wr_n S_n$ is isomorphic to the symmetric group S_n, we are faced with an action of $S_n \times \mathrm{GL}_k(2)$ on $(\mathbb{F}_2^k \setminus \{0\})^n$. In this situation the projective linear group is simply the linear group, and from 6.1.23 we obtain that

$$\sum_{n=0}^{\infty} T_{nk2}x^n = C(\mathrm{GL}_k(2), \mathbb{F}_2^k \setminus \{0\})\big|_{z_i:=\sum_{j=0}^{\infty} x^{i\cdot j}},$$

and

$$\sum_{n=0}^{\infty} \overline{T}_{nk2}x^n = C(\mathrm{GL}_k(2), \mathbb{F}_2^k \setminus \{0\})\big|_{z_i:=1+x^i}.$$

These cycle indices are known for $q = 2$, see [50], [60], [82], [83], [184], and programs for their evaluation are implemented in SYMMETRICA ([190]), so that tables can be determined easily. Comparing Tables 6.2 and 6.1 shows that the set of isometry classes of (n,k)-codes is much smaller than the set of of all (n,k)-codes for given parameters n and k. $\diamond$

If the cycle indices $C(\mathrm{PGL}_k(q), \mathrm{PG}^*_{k-1}(q))$ are known for general q, it is possible to evaluate the numbers T_{nkq} and $\overline{T}_{nkq}$, from which we can deduce V_{nkq}, $\overline{V}_{nkq}$, U_{nkq}, and $\overline{U}_{nkq}$ for arbitrary fields $\mathbb{F}_q$. A method for computing these cycle indices is described in Section 6.3. Finally, in Section 6.4 we present several tables of these numbers which were calculated using SYMMETRICA (cf. [59]). They extend the results of D. Slepian on binary codes, see [184]. It is also possible to determine the number of linear isometry classes of linear (n,k)-codes over $\mathbb{F}_q$ by using the software of the attached CD for moderate parameters n, k and q.

For later applications to the construction of transversals of isometry classes of projective codes in Chapter 9 we mention the following two facts: From Exercise 6.1.2 it follows that

$$S_n \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n_{\mathrm{inj}} = \binom{\mathrm{PG}^*_{k-1}(q)}{n},$$

the set of all n-subsets of $\mathrm{PG}^*_{k-1}(q)$. This implies

6.1.25
$$\overline{\mathcal{T}}_{n,k,q} = \mathrm{PGL}_k(q) \backslash\backslash \binom{\mathrm{PG}^*_{k-1}(q)}{n}.$$

Exercises

E.6.1.1 **Exercise** Let the symmetric group S_n act on the set of mappings Y^n as described in 1.4.7. Show that two mappings $f_1, f_2 \in Y^n$ belong to the same orbit if and only if they are of the same content, i.e.

$$|f_1^{-1}(\{y\})| = |f_2^{-1}(\{y\})| \text{ for all } y \in Y.$$

E.6.1.2 **Exercise** Let Y^n_{inj} denote the set of mappings $f \in Y^n$ which are injective, i.e. with $|f^{-1}(\{y\})| \leq 1$, for all $y \in Y$. Show that the S_n-orbits on this set can be represented by n-subsets of Y.

E.6.1.3 **Exercise** Let x be an indeterminate over $\mathbb{R}$. Two nonnegative integers n and k define the rational function $\begin{bmatrix} n \\ k \end{bmatrix}$ by

$$\begin{bmatrix} n \\ k \end{bmatrix} := \begin{cases} \dfrac{[n]!}{[k]![n-k]!} & \text{if } k \leq n, \\ 0 & \text{otherwise,} \end{cases}$$

where

$$[0]! := 1, \qquad [n]! := [n][n-1]\cdots[1], \quad n \geq 1,$$

and $[n] = 1 + x + \ldots + x^{n-1}$ for $n \geq 1$. Prove that the number of subspaces of dimension k of $\mathbb{F}_q^n$ is the value of the *Gauss-polynomial* $\begin{bmatrix} n \\ k \end{bmatrix}$ at q:

$$|\mathcal{U}(n,k,q)| = \begin{bmatrix} n \\ k \end{bmatrix}(q) := \frac{(x^n-1)\cdots(x^{n-k+1}-1)}{(x^k-1)\cdots(x-1)}\Big|_{x=q}$$

$$= \frac{(q^n-1)\cdots(q^{n-k+1}-1)}{(q^k-1)\cdots(q-1)}.$$

The numbers $\begin{bmatrix} n \\ k \end{bmatrix}(q)$ are known as the *q-binomial numbers*. In the notation of Section 3.7, we have $\theta_{n-1}(q) = |\mathcal{U}(n,1,q)| = \begin{bmatrix} n \\ 1 \end{bmatrix}(q) = \frac{q^n-1}{q-1}$.

E.6.1.4 **Exercise** Show that the action of $M_n(q)$ on $\mathcal{U}(n,k,q)$ can be restricted to actions on $\mathcal{V}(n,k,q)$, on $\overline{\mathcal{U}}(n,k,q)$, and on $\overline{\mathcal{V}}(n,k,q)$, which means that these subsets of $\mathcal{U}(n,k,q)$ are unions of orbits of the linear isometry group.

Exercise Prove that for finite actions ${}_GX$, ${}_HY$ and the corresponding canonical actions on Y^X the following enumeration formulae hold true: **E.6.1.5**

$$|G\backslash\backslash Y^X| = \frac{1}{|G|}\sum_{g\in G}|Y|^{c(\overline{g})} = C(G,X)\big|_{z_i:=|Y|},$$

where $c(\overline{g}) := \sum_i a_i(\overline{g}) = |\langle g\rangle\backslash\backslash X|$ denotes the number of cycles in the cycle decomposition of the permutation $\overline{g}$, while

$$|(H\times G)\backslash\backslash Y^X| = \frac{1}{|H||G|}\sum_{(h,g)\in H\times G}\prod_{i=1}^{|X|}|Y_{h^i}|^{a_i(\overline{g})} = \frac{1}{|H|}\sum_{h\in H}C(G,X)\big|_{z_i:=|Y_{h^i}|}$$

and

$$|H\wr_X G\backslash\backslash Y^X| = C(G,X)\big|_{z_i:=|H\backslash\backslash Y|}.$$

Exercise Prove the assertions in 6.1.15. Show that the rank of a matrix corresponding to a mapping $\Gamma\in \mathrm{PG}^*_{k-1}(q)^n$ does not depend on the choice of the representatives of the elements $\Gamma(i)$ in $\mathrm{PG}^*_{k-1}(q)$. Check that the matrices in the orbit $(\mathrm{GL}_k(q)\times S_n)(\Gamma)$ are all of the same rank. **E.6.1.6**

For $\ell < k$, show that the mapping

$$\mathrm{GL}_\ell(q)\to\mathrm{GL}_k(q)\ :\ A\mapsto\left(\begin{array}{c|c} A & 0\\ \hline 0 & I_{k-\ell}\end{array}\right),$$

where I_r is the unit matrix of rank r, is an embedding of $\mathrm{GL}_\ell(q)$ into $\mathrm{GL}_k(q)$. Consider the natural embedding of $\mathbb{F}_q^\ell$ in $\mathbb{F}_q^k$ given by $v\mapsto(v\mid \mathbf{0}_{k-\ell})$.

If the function $\Gamma\in\mathrm{PG}^*_{k-1}(q)^n$ describes a matrix of rank $\ell < k$, find a function $\Gamma''\in\mathrm{PG}^*_{\ell-1}(q)^n$ which in a natural way can be identified with a suitable element of the orbit $(\mathrm{GL}_k(q)\times S_n)(\Gamma)$. Show that all elements of the orbit $(\mathrm{GL}_\ell(q)\times S_n)(\Gamma'')$ correspond in the same way to elements of the orbit $(\mathrm{GL}_k(q)\times S_n)(\Gamma)$. (Hint: For finding Γ'', determine by elementary row operations on Γ a matrix Γ' in which the last $k-\ell$ rows consist of zeros only. The mapping Γ'' can be obtained from Γ' by omitting the last $k-\ell$ entries in each column.)

In order to prove that for $k>1$ the number of $\mathrm{GL}_k(q)\times S_n$-orbits of mappings $\Gamma\in\mathrm{PG}^*_{k-1}(q)^n$ corresponding to matrices of rank not greater than $k-1$ is equal to $T_{n,k-1,q}$, show that all matrices in the orbit $(\mathrm{GL}_k(q)\times S_n)(\Gamma)$ in which the last row consists of zeros only, i.e. $\mathrm{GL}_k(q)(\Gamma)\ni\Gamma'=\left(\begin{array}{c}\Gamma''\\ \hline \mathbf{0}_n\end{array}\right)$ with Γ'' corresponding to a mapping in $\mathrm{PG}^*_{k-2}(q)^n$, are of the form

$$\left(\begin{array}{c|c} A & B\\ \hline \mathbf{0}_{k-1} & D\end{array}\right)\cdot\Gamma'\cdot M_\pi = \left(\begin{array}{c} A\cdot\Gamma''\cdot M_\pi\\ \hline \mathbf{0}_n\end{array}\right)$$

for some $A \in \mathrm{GL}_{k-1}(q)$, $B \in \mathbb{F}_q^{(k-1)\times 1}$, $D \in \mathrm{GL}_1(q) = \mathbb{F}_q^*$ and a permutation matrix M_π for $\pi \in S_n$. This is the $(\mathrm{GL}_{k-1}(q) \times S_n)$-orbit of Γ''. Thus the $(\mathrm{GL}_k(q) \times S_n)$-orbits of matrices Γ of rank less than k and without zero columns correspond to the $(\mathrm{GL}_{k-1}(q) \times S_n)$-orbits on $\mathrm{PG}_{k-2}^*(q)^n$.

E.6.1.7 **Exercise** Let R be a ring. Consider the set S of all sequences $(r_n)_{n\geq 0}$ with $r_n \in R$ for $n \geq 0$. Prove that this set together with addition and multiplication

$$(r_n)_{n\geq 0} + (s_n)_{n\geq 0} = (r_n + s_n)_{n\geq 0}, \qquad (r_n)_{n\geq 0}, (s_n)_{n\geq 0} \in S,$$

$$(r_n)_{n\geq 0} \cdot (s_n)_{n\geq 0} = (t_n)_{n\geq 0}, \qquad t_n = \sum_{i=0}^{n} r_i s_{n-i}, \qquad (r_n)_{n\geq 0}, (s_n)_{n\geq 0} \in S,$$

is a ring. In addition, show that

- S is commutative if and only if R is commutative,
- S is a ring with 1 if and only if R is a ring with 1,
- S is an integral domain if and only if R is an integral domain.

Now assume that R is an integral domain. Let $s = (r_n)_{n\geq 0}$ be an element of S different from 0. Then $N = \min\{n \geq 0 \mid r_n \neq 0\}$ is called the order of s, in short $\mathrm{ord}(s)$. The order of 0 is defined to be $+\infty$. Show that the mapping

$$d\colon S \times S \to \mathbb{R} \;:\; d(s^{(1)}, s^{(2)}) := \begin{cases} 2^{-\operatorname{ord}(s^{(1)} - s^{(2)})} & \text{if } s^{(1)} \neq s^{(2)}, \\ 0 & \text{if } s^{(1)} = s^{(2)}, \end{cases}$$

is a metric on S. This metric induces a topology on S, the order topology. Prove that a topological basis of the system of neighborhoods of $s^{(0)} \in S$ is given by

$$U_n(s^{(0)}) = \left\{ s \in S \mid \mathrm{ord}(s - s^{(0)}) > n \right\}, \qquad n \in \mathbb{N}.$$

A family $(s^{(n)})_{n\geq 0}$ with $s^{(n)} \in S$ is called summable if the following limit exists with respect to the order topology:

$$\lim_{N\to\infty} \sum_{n=0}^{N} s^{(n)}.$$

Prove that $(s^{(n)})_{n\geq 0}$ is summable in S if and only if $\lim_{n\to\infty} \mathrm{ord}(s^{(n)}) = +\infty$, which is equivalent to $\lim_{n\to\infty} s^{(n)} = 0$.

If $(s^{(n)})_{n\geq 0}$ is a summable family, then we set

$$\sum_{n\geq 0} s^{(n)} = \lim_{N\to\infty} \left(\sum_{n=0}^{N} s^{(n)} \right).$$

We identify the elements r of R with the series $(r, 0, 0, \ldots)$ in S. Consider the particular element $x = (0, 1, 0 \ldots) \in S$. Show that any sequence $(r_n)_{n\geq 0} \in S$ can be written as

$$\sum_{n\geq 0} r_n x^n,$$

where x^n is the n-fold product of x introduced in Exercise 1.6.6. This representation as a sum makes sense, since the family $(r_n x^n)_{n\geq 0}$ is summable.

Finally, we identify S with the ring $R[\![x]\!]$ of formal power series over r in the indeterminate x.

Exercise Prove the following formulae for the order of formal series over an integral domain R. For $f, g \in R[\![x]\!]$ we have $\mathrm{ord}(f+g) \geq \min\{\mathrm{ord}(f), \mathrm{ord}(g)\}$ and $\mathrm{ord}(fg) = \mathrm{ord}(f) + \mathrm{ord}(g)$. We use the convention $+\infty > n$ for all $n \in \mathbb{N}$, $+\infty \leq +\infty$, and $(+\infty) + n = n + (+\infty) = (+\infty) + (+\infty) = +\infty$ for $n \in \mathbb{N}$. E.6.1.8

6.2 Indecomposable Linear Codes 6.2

The enumerative formulae just derived and the corresponding tables of numbers give us a good idea about the multitude of linear isometry classes of linear codes without zero columns in their generator matrices. But we are mainly interested in the optimal codes, i.e. in the (n, k)-codes with maximal minimum distance d. Hence, we are in fact interested in a small fraction of the total variety of linear isometry classes which we have enumerated. To begin with, we mention that there exists a *Decomposition Theorem* for linear codes. D. Slepian has shown in [184], that every linear code can be decomposed in an essentially unique way into an outer direct sum of *indecomposable* codes, and we recall from Section 2.2, that the minimum distance of an outer direct sum is the least among the minimum distances of its components. This motivates enumeration and the construction of the linear isometry classes of *indecomposable linear codes,* the generator matrices of which do not contain zero columns and whose minimum distance is maximal, for given parameters n, k, q. In this section we restrict our investigations to nonredundant codes.

Definition (indecomposable codes) We call a code *decomposable,* if it is linearly isometric to a code with a generator matrix in the form of a block diagonal matrix 6.2.1

$$\Gamma = \left(\begin{array}{c|c} \Gamma_0 & 0 \\ \hline 0 & \Gamma_1 \end{array}\right) =: \Gamma_0 \dotplus \Gamma_1,$$

consisting of two generator matrices Γ_i of linear (n_i, k_i)-codes with $1 \leq k_i \leq n_i$ for $i \in 2$. Hence, it is linearly isometric to the outer direct sum of at least

two codes. Correspondingly, we speak about a *decomposable generator matrix*. Otherwise, both the code and its generator matrix are said to be *indecomposable*.

◇

At first we prove a Decomposition Theorem for linear codes. For this purpose we recall some concepts and facts from Linear Algebra about independent families. We are dealing with finite families S of elements of $\mathbb{F}_q^k$. These are finite sequences $S = (v_i)_{i\in n}$ of vectors $v_i \in \mathbb{F}_q^k$ of length $n \geq 1$. The families $S_0 = (v_{0i})_{i\in n_0}, \ldots, S_{r-1} = (v_{r-1,i})_{i\in n_{r-1}}$ in $\mathbb{F}_q^k$ are called *independent* if an equation of the form

$$\sum_{i\in r}\sum_{j\in n_i} \alpha_{ij}v_{ij} = 0, \qquad \alpha_{ij} \in \mathbb{F}_q,$$

always implies that

$$\sum_{j\in n_i} \alpha_{ij}v_{ij} = 0 \text{ for } i \in r.$$

In other words, there are no linear relations between vectors of different independent families.

The proof of the next lemma is left to the reader.

6.2.2 Lemma *If $S_0, \ldots, S_{r-1}$ are independent families in $\mathbb{F}_q^k$, and if R_i are nonempty subfamilies of S_i, then also $R_0, \ldots, R_{r-1}$ are independent families in $\mathbb{F}_q^k$.* □

A family $S = (v_i)_{i\in I}$ in $\mathbb{F}_q^k$ is called *indecomposable*, if it cannot be expressed as the union of at least two (nonempty) independent subfamilies $(v_i)_{i\in I'}$ and $(v_i)_{i\in I''}$ where I is the disjoint union $I' \cup I''$. Otherwise, S is called *decomposable*. In the sequel, we want to prove that any decomposable sequence can be decomposed uniquely into the union of indecomposable subfamilies. For doing this, we need some notions about linear combinations.

Let $S = (v_i)_{i\in n}$ be a family in $\mathbb{F}_q^k$. A linear combination

$$\sum_{i\in n} \alpha_i v_i, \qquad \alpha_i \in \mathbb{F}_q,$$

is called *irreducible*, if there does not exist a proper partial sum (consisting of at least one and at most $n-1$ summands) which yields zero. Otherwise, the linear combination is called *reducible*.

6.2.3 Lemma *Let S be a family of vectors in $\mathbb{F}_q^k$. Any reducible linear combination of vectors of S which yields zero can be decomposed into a sum of irreducible linear combinations.*

Proof: If the linear combination

$$\sum_{i \in n} \alpha_i v_i = 0$$

is reducible, then there exist partial sums which also yield zero. Assume that

$$\alpha_{i_0} v_{i_0} + \ldots + \alpha_{i_{r-1}} v_{i_{r-1}} = 0$$

is such a partial sum of minimal length. Then this partial sum is irreducible. Moreover,

$$\sum_{i \in n} \alpha_i v_i - \sum_{j \in r} \alpha_{i_j} v_{i_j} = 0$$

is also a partial sum which yields zero. Either it is also irreducible, or we can repeat the procedure just described, in order to obtain, after a finite number of steps, the desired decomposition into irreducible linear combinations. □

Using the sequence $S = (v_i)_{i \in n}$, we can form $q^n - 1$ different linear combinations such that not all coefficients α_i are equal to zero. Omitting all those linear combinations which do not yield the value zero and also those which are reducible, we end up with a finite list $\mathcal{L}$ of irreducible linear combinations which sum up to zero.

Two vectors v_i and v_j from S are called *directly connected*, if there exists a linear combination in $\mathcal{L}$ with coefficients $\alpha_i \neq 0 \neq \alpha_j$. A vector of S which does not occur in any of the linear combinations in $\mathcal{L}$ is called *directly connected with itself*. Two vectors v_i and v_j from S are called *connected*, if there exists an integer $m \geq 0$ and a sequence $(v_{i_0}, v_{i_1}, \ldots, v_{i_m})$ of vectors in S such that $i = i_0$, $j = i_m$ and v_{i_r} is directly connected with $v_{i_{r+1}}$ for $r \in m$. In order to indicate that v_i and v_j are connected we write $v_i \sim v_j$ and also $i \sim j$. (When v is directly connected with itself we also write $v \sim v$.)

Lemma *Let $S = (v_i)_{i \in n}$ be a family in $\mathbb{F}_q^k$.* **6.2.4**

1. *The relation $\sim$, introduced above, is an equivalence relation on the set of vectors v_i for $i \in n$. The equivalence class of v_i corresponds to the subfamily $(v_j)_{j \sim i}$.*
2. *The family $(v_j)_{j \sim i}$ is indecomposable.*
3. *Let $\{v_i \mid i \in I'\}$ be a complete set of representatives with respect to $\sim$. Then the families $(v_j)_{j \sim i}$ for $i \in I'$ are independent.*
4. *If R is an indecomposable family in S, then there exists exactly one $i \in I'$ such that R is a subfamily of $(v_j)_{j \sim i}$.*

Proof: The proof of the first part is obvious. If we suppose that $(v_j)_{j\sim i}$ is decomposable, then there exist two nonempty, disjoint sets I' and I'' such that $I' \cup I'' = \{j \mid j \sim i\}$ and $(v_j)_{j\in I'}$ and $(v_j)_{j\in I''}$ are independent families. Choose $j_1 \in I'$ and $j_2 \in I''$. Since $v_{j_1} \sim v_{j_2}$, there exists a sequence $v_{j_1} = v_{i_0} \sim \ldots \sim v_{i_m} = v_{j_2}$ such that v_{i_r} is directly connected with $v_{i_{r+1}}$ for $r \in m$. From the special choice of j_1 and j_2 in I' and I'', respectively, we derive the existence of at least one index r such that i_r belongs to I' and i_{r+1} belongs to I''. Then v_{i_r} and $v_{i_{r+1}}$ are directly connected, which is a contradiction to the fact that they belong to two independent families. Consequently, $(v_j)_{j\sim i}$ is indecomposable.

In order to prove the third assertion, assume that

$$\sum_{i\in I'} \sum_{j\sim i} \alpha_{ij} v_j = 0$$

is a linear combination, which contains vectors from at least two different families $(v_j)_{j\sim i}$ with nonzero coefficients. Then this linear combination is not irreducible, since otherwise vectors of different equivalence classes would be directly connected. According to 6.2.3, this reducible linear combination can be written as a sum of irreducible linear combinations, each of which is zero. Since they are irreducible, none of these linear combinations contains vectors from different equivalence classes. Forming the sum of all irreducible linear combinations containing vectors from $(v_j)_{j\sim i}$ we get

$$\sum_{j\sim i} \alpha_{ij} v_j = 0$$

for each $i \in I'$.

Assume that $R = (v_i)_{i\in J}$ for $J \subseteq n$ is an indecomposable subfamily of S. For $i \in I'$ let $R_i = (v_j)_{j\in J,\, j\sim i}$. We have just proved that $(v_j)_{j\sim i}$ for $i \in I'$ are independent families. Then there is exactly one $i_0 \in I'$ such that R_{i_0} is not empty. If we suppose on the contrary that there are at least two nonempty families, then, according to 6.2.2, they are also independent families. Hence, R is the union of at least two independent families, which is a contradiction to the assumption that R is indecomposable. This finishes the proof of the last assertion. □

Based on these results we prove the next

6.2.5 Theorem *A finite family S of vectors in $\mathbb{F}_q^k$ can be written in a unique way as the union of independent, indecomposable sets.*

Proof: According to 6.2.4, we obtain a decomposition of S into independent, indecomposable families by determining the equivalence classes $(v_j)_{j\sim i}$ for $i \in I'$.

Conversely, consider a decomposition of S into independent, indecomposable families R_k for k in an index set K. From the last statement of 6.2.4 we deduce that for each $k \in K$ there exists exactly one $i \in I'$ such that R_k is a subfamily of $(v_j)_{j\sim i}$. Moreover, since the family $(v_j)_{j\sim i}$ is indecomposable, R_ℓ is not a subfamily of $(v_j)_{j\sim i}$ for $\ell \neq k$. Hence, the indecomposable families R_k correspond in a unique way to the independent, indecomposable families $(v_j)_{j\sim i}$ for $i \in I'$. □

Remark Let S denote the family of columns of a generator matrix Γ of an (n,k)-code C. Then C is indecomposable if and only if S is indecomposable. This characterization is, first of all, independent of the choice of a generator matrix Γ of C, since the columns of $A \cdot \Gamma$, for $A \in \mathrm{GL}_k(q)$, satisfy the same dependency relations as the columns of Γ. Secondly, this characterization is independent of the choice of the representative C of its linear isometry class, since a linear isometry permutes the columns of Γ and multiplies them by nonzero elements of $\mathbb{F}_q^*$. (See Exercise 6.2.1.) ◇ **6.2.6**

We are now in a position to prove Slepian's Theorem:

The Decomposition Theorem for Linear Codes *Any (n,k)-code C over $\mathbb{F}_q$ is linearly isometric to an outer direct sum of indecomposable codes C_i:* **6.2.7**

$$C \simeq C_0 \dot{+} \ldots \dot{+} C_{r-1}.$$

This decomposition is unique in the following sense. If we are given another decomposition of C of the form

$$C \simeq C'_0 \dot{+} \ldots \dot{+} C'_{r'-1}$$

with indecomposable codes C'_i, then $r = r'$ and there exists a permutation $\sigma \in S_r$ so that C_i and $C'_{\sigma(i)}$ are linearly isometric.

Proof: We only have to prove the uniqueness of such a decomposition. Assume that C is linearly isometric to two decompositions, say,

$$C_0 \dot{+} \ldots \dot{+} C_{r-1}$$

and

$$C'_0 \dot{+} \ldots \dot{+} C'_{r'-1}$$

with indecomposable (n_i,k_i)-codes C_i and indecomposable (n'_i,k'_i)-codes C'_i with generator matrices Γ_i and Γ'_i, respectively. The parameters n_i, n'_i, k_i, and k'_i satisfy the equations

$$\sum_{i\in r} n_i = n = \sum_{i\in r'} n'_i \text{ and } \sum_{i\in r} k_i = k = \sum_{i\in r'} k'_i. \quad \textbf{6.2.8}$$

By assumption there exist matrices $A \in \mathrm{GL}_k(q)$ and $B \in M_n(q)$ such that

6.2.9 $$A \cdot \Gamma' \cdot B = \Gamma$$

such that

$$\Gamma := \Gamma_0 \dot{+} \ldots \dot{+} \Gamma_{r-1}$$

and

$$\Gamma' := \Gamma'_0 \dot{+} \ldots \dot{+} \Gamma'_{r'-1}.$$

The columns of Γ decompose into indecomposable families $S_0, \ldots, S_{r-1}$, where S_0 consists of the first n_0 columns of Γ, S_1 of the next n_1 columns, and so on. According to 6.2.9, the columns of $A \cdot \Gamma' \cdot B = \Gamma$ and $\Gamma' \cdot B$ satisfy the same dependency relations. Hence, the first n_0 columns of $\Gamma' \cdot B$ form an independent set $\tilde{S}_0$, the following n_1 an independent set $\tilde{S}_1$, and so on.

On the other hand, $\Gamma' \cdot B$ arises from Γ' by reordering the columns and multiplying the columns by elements of $\mathbb{F}_q^*$. Hence after some permutation, the columns of $\Gamma' \cdot B$ satisfy the same dependency relations as the columns of Γ'. But the columns of Γ' decompose into r' independent families which are given by the decomposition of Γ'. The first n'_0 columns form an independent set S'_0, the following n'_1 an independent set S'_1, and so on. From 6.2.5 we deduce that $r = r'$. Moreover, there exists a permutation $\sigma \in S_r$, such that for $i \in r$ the lengths $n'_{\sigma(i)}$ and n_i of the indecomposable families $S'_{\sigma(i)}$ and $\tilde{S}_i$ coincide, and the family $\tilde{S}_i$ consists – up to scalar multiples – of those columns of Γ' which contain the submatrix $\Gamma'_{\sigma(i)}$. Thus, $\Gamma' \cdot B$ can be written in the form $A' \cdot \Gamma''$, where A' is a suitable permutation matrix in $\mathrm{GL}_k(q)$ and Γ'' is given by

$$\Gamma'' = (\Gamma'_{\sigma(0)} \cdot B_0) \dot{+} \ldots \dot{+} (\Gamma'_{\sigma(r-1)} \cdot B_{r-1}),$$

for suitable matrices $B_i \in M_{n_i}(q)$. Finally, if we put $A'' := A \cdot A' \in \mathrm{GL}_k(q)$, then

6.2.10 $$A'' \cdot \Gamma'' = A \cdot \Gamma' \cdot B = \Gamma.$$

Let T_0 be the matrix consisting of the first n_0 columns of Γ, T_1 the matrix, consisting of the next n_1 columns, and so on. Analogously, we define the matrices T''_i as submatrices of Γ''. From this construction it follows immediately that T_i is a matrix of rank k_i and T''_i is of rank $k'_{\sigma(i)}$. Since $T_i = A'' \cdot T''_i$ and A'' is regular, we deduce that $k'_{\sigma(i)} \geq k_i$. This, together with 6.2.8, gives that $k'_{\sigma(i)}$ equals k_i. If we write the matrix A'' as block matrix $(A''_{ij})_{i,j \in r}$, consisting of blocks A''_{ij}, which are $k_i \times k_j$-matrices, from 6.2.10 we obtain

$$A''_{ii} \cdot \Gamma'_{\sigma(i)} \cdot B_i = \Gamma_i, \qquad i \in r.$$

Comparing the degrees we obtain that the diagonal blocks A''_{ii} are all regular. Hence, $\Gamma'_{\sigma(i)}$ and Γ_i are generator matrices of linearly isometric codes C_i and $C'_{\sigma(i)}$. □

Using the notation introduced in Exercise 2.3.17, the last theorem can be restated for linear isometry classes of linear codes as:

Corollary 6.2.11 *The linear isometry class $\hat{C}$ of any linear code C over $\mathbb{F}_q$ can be expressed as an outer direct sum of the linear isometry classes $\hat{C}_i$ of indecomposable codes C_i:*

$$\hat{C} = \hat{C}_0 \dot{+} \ldots \dot{+} \hat{C}_{r-1}.$$

The indecomposable summands $\hat{C}_i$ are uniquely determined by $\hat{C}$ apart from their order. □

Another consequence is the following cancellation law:

Corollary 6.2.12 *Let $\hat{C}_0$, $\hat{C}_1$ and $\hat{C}_2$ be linear isometry classes of linear codes. From $\hat{C}_0 \dot{+} \hat{C}_1 = \hat{C}_0 \dot{+} \hat{C}_2$ we obtain that $\hat{C}_1 = \hat{C}_2$.* □

For systematic linear codes there is an easy and obvious

Test on Indecomposability 6.2.13 *A generator matrix $\Gamma = (I_k \mid A)$ of a linear (n,k)-code with $k < n$ is (together with the generated code) indecomposable if and only if there exists a sequence $a_{ij}, a_{lm}, \ldots$ of nonzero entries in A such that each element (except the first one, of course) lies in the same row or in the same column as its predecessor, and so that each row is represented by at least one element of the sequence.*

Proof: Because of the special form of Γ, the first k columns of Γ define k independent families. Each of these families consists of just that column. The remaining columns of Γ, i.e. the columns of A, can be represented as linear combinations of the first k columns. Moreover, the columns of Γ form an indecomposable family if and only if the first k columns are connected. This implies the statement. □

We can also represent the elements of A as the vertices of a graph $\mathcal{G}_A$. In this graph two vertices are connected by an edge, if they are both different from 0 and occur either in the same row or column of A. Then the code C is indecomposable, if and only if there is a walk in $\mathcal{G}_A$ which visits each of the k rows at least once.

In case $n = k$, this theorem does not apply. It is clear that (n,n)-codes are indecomposable if and only if $n = 1$.

If the codes do not have zero columns (as we assumed in this section), and if there exists a walk in $\mathcal{G}_A$ which visits each of the k rows of A at least once, then there exists a walk in $\mathcal{G}_A$ which visits all columns of A. With this characterization it is easy to prove

6.2.14 **Theorem** *A nonredundant linear code C is indecomposable if and only if its dual code $C^\perp$ is indecomposable.* □

6.2.15 **Examples**

1. The code with generator matrix
$$\Gamma = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$
is indecomposable, since the sequence $\gamma_{05}, \gamma_{15}, \gamma_{25}$ is a sequence of entries of the last $n - k = 3$ columns of Γ which has the required properties.
2. Any nonredundant $(n, 1)$-code is indecomposable.
3. Any (n, k)-MDS-code with $k < n$ is indecomposable. ◇

Indecomposable codes are optimal in the following sense.

6.2.16 **Theorem** *Let C be an (n, k)-code with $k < n$ and with minimum distance d. Then there exists an indecomposable (n, k)-code C' such that* $\operatorname{dist}(C') \geq d$.

Proof: For $r \geq 2$, let $C \simeq C_0 + \ldots + C_{r-1}$ be a decomposable code, where C_i are (n_i, k_i, d_i)-codes. From the properties of the outer direct sum (cf. 2.2.11) it follows that $\operatorname{dist}(C) = \min\{d_i \mid i \in r\}$.

By induction on r we prove the assertion of the theorem: If $r = 2$, we consider the following generator matrix Γ of C:
$$\Gamma = \left(\begin{array}{c|c|c|c} I_{k_0} & A_0 & 0 & 0 \\ \hline 0 & 0 & I_{k_1} & A_1 \end{array}\right)$$
with $(n_i - k_i) \times k_i$-matrices A_i. Without restriction we suppose that $\operatorname{dist}(C) = \operatorname{dist}(C_0) \leq \operatorname{dist}(C_1)$. If $k_1 < n_1$, then 6.2.13 shows that the matrix

6.2.17
$$\Gamma' := \left(\begin{array}{c|c|c|c} I_{k_0} & A_0 & 0 & B \\ \hline 0 & 0 & I_{k_1} & A_1 \end{array}\right) \text{ with } B := \begin{pmatrix} 1 & \ldots & 1 \\ 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$$
generates an indecomposable code C'. Let v denote a nontrivial linear combination of the rows of Γ'. Unless the first k_0 entries of v are all zero, we have $\operatorname{wt}(v) \geq \operatorname{dist}(C_0)$ since the first k_0 entries of v are a codeword in C_0. If the first k_0 entries of v are all zero then the second half of v is a nonzero codeword

in C_1, whence $\mathrm{wt}(v) \geq \mathrm{dist}(C_1)$. Therefore, the minimum distance of C' is at least $\mathrm{dist}(C)$.

If $k_1 = n_1$, we have $n_1 = 1$, since C_1 was supposed to be indecomposable. Hence, $1 = \mathrm{dist}(C_1) \geq \mathrm{dist}(C) \geq 1$. But every indecomposable (n,k)-code has $d \geq 1$, and so the theorem is proved for the case $r = 2$.

Now we assume that $r > 2$. The induction assumption gives the existence of an indecomposable $(n - n_{r-1}, k - k_{r-1})$-code C' with

$$\mathrm{dist}(C') \geq \mathrm{dist}(C_0 \dotplus \ldots \dotplus C_{r-2}) = \min\{\mathrm{dist}(C_0), \ldots, \mathrm{dist}(C_{r-2})\}.$$

Moreover, it implies the existence of an indecomposable (n,k)-code C'' with

$$\begin{aligned}\mathrm{dist}(C'') &\geq \mathrm{dist}(C' \dotplus C_{r-1}) = \min\{\mathrm{dist}(C'), \mathrm{dist}(C_{r-1})\} \\ &\geq \min\{\min\{\mathrm{dist}(C_0), \ldots, \mathrm{dist}(C_{r-2})\}, \mathrm{dist}(C_{r-1})\} = \mathrm{dist}(C). \quad \square\end{aligned}$$

Theorem 6.2.18 *Any indecomposable code of length greater than* 1 *has minimum distance at least* 2. □

Theorem 6.2.19 *Up to linear isometry, for any field $\mathbb{F}_q$ and $n > 2$ there is a unique indecomposable $(n, n-1)$-code C over $\mathbb{F}_q$. It has a generator matrix of the form*

$$\begin{pmatrix} 1 & & & 1 \\ & \ddots & & \vdots \\ & & 1 & 1 \end{pmatrix}.$$

Therefore, C is linearly isometric to the parity check code of $\mathbb{F}_q^{n-1}$. It is also linearly isometric to the dual of a one-dimensional code generated by the all-one vector. If $q = 2$, then C is the set of all vectors of $\mathbb{F}_2^n$ which have even weight.

Proof: Since C is indecomposable and of length greater than 1, by 6.2.18, its minimum distance is at least 2. By the Singleton-bound 2.1.1, it is at most 2, thus $\mathrm{dist}(C) = 2$. There exists a code linearly isometric to C with generator matrix $\Gamma = (I_{n-1} \mid A)$ where A is an $(n-1) \times 1$-matrix. Since the rows of Γ are codewords of weight not smaller than $\mathrm{dist}(C)$, each component of A is different from 0. By a suitable monomial transformation, there exists a code linearly isometric to C which has a generator matrix of the form $(I_{n-1} \mid A')$ where all components of A' are equal to 1. □

We are now going to show how indecomposable codes can be enumerated. For this purpose, we introduce the following sets and symbols for their cardinalities:

- Let $\mathcal{R}_{nkq}$ denote the set of linear isometry classes of nonredundant, indecomposable (n,k)-codes over $\mathbb{F}_q$,

$$\mathcal{R}_{nkq} := \left\{ M_n(q)(C) \in \mathcal{V}_{nkq} \mid C \text{ is indecomposable} \right\}.$$

- $R_{nkq} := |\mathcal{R}_{nkq}|$ indicates the number of linear isometry classes of nonredundant, indecomposable (n,k)-codes over $\mathbb{F}_q$.
- The symbol $\overline{\mathcal{R}}_{nkq}$ denotes the set of linear isometry classes of (nonredundant), indecomposable, projective (n,k)-codes over $\mathbb{F}_q$, i.e.

$$\overline{\mathcal{R}}_{nkq} := \left\{ M_n(q)(C) \in \overline{\mathcal{V}}_{nkq} \mid C \text{ is indecomposable} \right\}.$$

- $\overline{R}_{nkq} := |\overline{\mathcal{R}}_{nkq}|$ indicates the number of linear isometry classes of (nonredundant), indecomposable, projective (n,k)-codes over $\mathbb{F}_q$.

From 6.2.19 it follows immediately that $R_{21q} = 1$, $\overline{R}_{21q} = 0$, and $R_{n,n-1,q} = 1 = \overline{R}_{n,n-1,q}$ for $n > 2$. Moreover, we already know $R_{11q} = 1 = \overline{R}_{11q}$, $R_{nnq} = 0 = \overline{R}_{nnq}$ for $n > 1$, $R_{n1q} = 1$ for $n \geq 1$, and $\overline{R}_{n1q} = 0$ for $n \geq 2$. The following theorem (cf. [61]) gives a recursive procedure for the evaluation of the numbers R_{nkq} and $\overline{R}_{nkq}$ from V_{nkq} and $\overline{V}_{nkq}$, respectively.

6.2.20 Theorem *For $n \geq 2$ we have*

$$R_{nkq} = V_{nkq} - \sum_a \sum_b \prod_{\substack{j=1 \\ a_j \neq 0}}^{n-1} \left(\sum_c U(c) \right),$$

where

6.2.21
$$U(c) = \prod_{i=1}^{j} C(S_{\nu(i,c)}, \nu(i,c))\big|_{z_\ell = R_{jiq}}$$

is a product computed from substitutions into the cycle indices of symmetric groups of degree $\nu(i,c)$ for

$$\nu(i,c) = |\{\ell \in a_j \mid c_\ell = i\}|, \qquad 1 \leq i \leq j.$$

The first sum runs through the cycle types $a = (a_1, \ldots, a_{n-1})$ of n with at least two summands, i.e. $a_i \in \mathbb{N}$ and $\sum i a_i = n$, and with the additional property $\sum a_i \leq k$, whereas the second sum is taken over the $(n-1)$-tuples $b = (b_1, \ldots, b_{n-1}) \in \mathbb{N}^{n-1}$, for which $a_i \leq b_i \leq i a_i$, and $\sum b_i = k$. The third sum runs over all a_j-tuples $c = (c_0, \ldots, c_{a_j - 1}) \in \mathbb{N}^{a_j}$ satisfying $j \geq c_0 \geq \ldots \geq c_{a_j - 1} \geq 1$ and $\sum c_i = b_j$.

Analogously, $\overline{R}_{nkq}$ can be evaluated recursively from $\overline{V}_{nkq}$ and $\overline{R}_{jiq}$ with $j < n$.

We would like to remark that the numbers $U(c)$ in 6.2.21 are expressed solely in terms of cycle indices of symmetric groups in their natural action (see Exercise 6.3.3).

Proof: In order to obtain R_{nkq}, we have to subtract from V_{nkq} the number of all classes of nonredundant, decomposable (n,k)-codes over $\mathbb{F}_q$. In other words, we have to evaluate the number of isometry classes of (n,k)-codes which can be written as a direct sum of indecomposable (n_i,k_i)-codes where

$$\sum_{i\in r} n_i = n, \quad \sum_{i\in r} k_i = k, \qquad 1 \le k_i \le n_i, \quad 2 \le r \le k. \tag{6.2.22}$$

According to 6.2.7, the (n_i,k_i)-codes in a decomposition can be arranged so that $n_0 \ge n_1 \ge \ldots \ge n_{r-1}$ holds true, and, if successive n_i are equal, for example $n_i = n_{i+1}$, then we can assume, in addition, that the inequality $k_i \ge k_{i+1}$ is satisfied. In order to describe all decompositions, first we list all partitions of n into at least two but not more than k parts. Hence, we suppose that $n = n_0 + n_1 + \ldots + n_{r-1}$ is a partition with $n_0 \ge \ldots \ge n_{r-1} \ge 1$ and $2 \le r \le k$. Its type is of the form $(a_1, a_2, \ldots, a_{n-1})$ with $a_j := |\{i \mid i \in r,\ n_i = j\}|$. Decomposable codes corresponding to different types $(a_1, a_2, \ldots, a_{n-1})$ are not linearly isometric.

In a second step we calculate for each such partition of n all sequences $(k_0, \ldots, k_{r-1})$ satisfying 6.2.22. If we are given such a sequence $(k_0, \ldots, k_{r-1})$, we put

$$b_j := \sum_{i:n_i=j} k_i, \qquad 1 \le j \le n-1.$$

Then

$$\sum_{j=1}^{n-1} b_j = \sum_{i\in r} k_i = k \ \text{ and } \ a_j \le b_j \le j \cdot a_j. \tag{6.2.23}$$

Decomposable codes corresponding to the same type $(a_1, a_2, \ldots, a_{n-1})$ which give rise to different vectors b are not linearly isometric. Conversely, we can start with any sequence $(b_1, \ldots, b_{n-1})$ satisfying 6.2.23 and evaluate all sequences $(k_0, \ldots, k_{r-1})$ with $b_j = \sum_{i:n_i=j} k_i$ which give linearly nonisometric codes with parameters (n_i, k_i) for $i \in r$. According to 6.2.7, for each j with $b_j \ne 0$ (which implies $a_j \ne 0$) we have to determine all partitions of b_j into exactly a_j parts of the following form:

$$b_j = \sum_{i\in a_j} c_i, \qquad j \ge c_0 \ge \ldots \ge c_{a_j-1} \ge 1. \tag{6.2.24}$$

These sequences c describe all possible ways of writing a $(j \cdot a_j, b_j)$-code as the outer direct sum of a_j codes of length j and dimension c_i for $i \in a_j$. Codes with different sequences are clearly not isometric.

In a final step we have to evaluate the number of linearly nonisometric decomposable $(j \cdot a_j, b_j)$-codes which are outer direct sums of a_j codes of length j. For each partition c of b_j with the properties 6.2.24 let $U(c)$ be the number of linearly nonisometric $(j \cdot a_j, b_j)$-codes which are the outer direct sum of indecomposable (j, c_i)-codes for $i \in a_j$.

We may assume that during the recursive procedure for the evaluation of the R_{nkq}, the numbers $R_{j,c_i,q}$ for $j < n$ have already been computed. If all components c_i of c are pairwise different, then the number $U(c)$ is equal to the product

6.2.25

$$\prod_{i \in a_j} R_{j,c_i,q},$$

which is a special case of 6.2.21. (See Exercise 6.2.8.)

Otherwise, there exist s, t with $s < t$ and $c_s = c_t$. Since $c_s = c_{s+1} = \ldots = c_t$, and according to 6.2.7, any permutation of the summands with the same parameters in a given direct decomposition into indecomposable codes leads to linearly isometric codes. Hence, for $1 \leq i \leq j$ let $\nu(i) := \nu(i,c)$ denote the cardinality of the set $\{\ell \in a_j \mid c_\ell = i\}$. Obviously, there is a bijection between the classes of codes which are outer direct sums of $\nu(i)$ indecomposable (j,i)-codes and the orbits of the symmetric group $S_{\nu(i)}$ acting on the set of all mappings from $\nu(i)$ into a set of R_{jiq} elements. In this case, the symmetric group acts canonically on the set of these mappings:

$$S_{\nu(i)} \times {R_{jiq}}^{\nu(i)} \to {R_{jiq}}^{\nu(i)} \; : \; (\pi, f) \mapsto f \circ \pi^{-1}.$$

A combination of Pólya's Theorem and the result of Exercise 6.1.5 completes the proof that $U(c)$ is given by 6.2.21.

Since $U(c)$ is the number of decomposable $(j \cdot a_j, b_j)$-codes which are an outer direct sum of indecomposable (j, c_i)-codes for $i \in a_j$, we can determine the number of all decomposable $(j \cdot a_j, b_j)$-codes which are the outer direct sum of a_j indecomposable codes of length j, by summing over all sequences c satisfying 6.2.24.

By summing these numbers over all cycle types $(a_1, \ldots, a_{n-1})$ of n with $\sum a_i = k$, and over all sequences b with the properties 6.2.23, we compute the number of all linearly nonisometric, nonredundant, decomposable (n,k)-codes over $\mathbb{F}_q$. It must be subtracted from V_{nkq} in order to obtain the number of all linearly nonisometric, nonredundant, indecomposable (n,k)-codes over $\mathbb{F}_q$. □

In Section 6.4 we present tables of R_{nkq} and $\overline{R}_{nkq}$ which were computed by using SYMMETRICA. They can also be determined with the software included on the attached CD. In the case $q = 2$, these tables confirm (and in some parts also correct) the numbers given by D. Slepian in [184]. Moreover, these numbers lead to the conjecture that the sequences $(R_{nkq})_{1 \leq k < n}$ are unimodal and symmetric for fixed n and q. The symmetry follows directly from the fact that the dual of an indecomposable code is again indecomposable (cf. Exercise 6.2.9). However, the unimodality has not yet been proved (see [61]).

For fixed n and q, the sequences R_{nkq} are symmetric, i.e.

$$R_{nkq} = R_{n,n-k,q}, \qquad 1 \leq k \leq \lfloor n/2 \rfloor.$$

Therefore, it is possible to use the formula from 6.2.20 in order to compute further values of V_{nkq}. Let n_0 be a positive integer and q the cardinality of a field. At first we compute the numbers V_{nkq} for $1 \leq n \leq n_0$ and $1 \leq k \leq \lfloor n_0/2 \rfloor$ as described in the previous section. This allows us to determine the numbers R_{nkq} for $1 \leq n \leq n_0$ and $1 \leq k \leq \lfloor n_0/2 \rfloor$. For $1 \leq n \leq n_0$ and $\lfloor n_0/2 \rfloor < k \leq n_0$ we determine the missing numbers R_{nkq} either by symmetry (for $k < n$) or by setting $R_{nkq} = 0$ for $k \geq n$. From 6.2.20 we immediately obtain the following formula

$$V_{nkq} = R_{nkq} + \sum_a \sum_b \prod_{\substack{j=1 \\ a_j \neq 0}}^{n-1} \left(\sum_c U(c) \right),$$

which allows us to compute the missing values V_{nkq} for $1 \leq n \leq n_0$ and $\lfloor n_0/2 \rfloor < k \leq n_0$.

Example Let $n_0 = 12$ and $q = 2$. From Table 6.21 on page 508 we obtain the numbers R_{nk2} for $1 \leq n \leq 12$ and $1 \leq k \leq 6$. Now we determine the values R_{nk2} for $7 \leq k \leq 12$ as shown in Table 6.3 on the left hand side. This allows the computation of the values V_{nk2} for $1 \leq n \leq 12$ and $7 \leq k \leq 12$, shown in the right hand side of Table 6.3, without determining the cycle indices of $\mathrm{PGL}_k(2)$ for $7 \leq k \leq 12$. ◇ **6.2.26**

Table 6.3 Extending tables by using the symmetry of R_{nk2}

	R_{nk2}							V_{nk2}					
$n\backslash k$	7	8	9	10	11	12	$n\backslash k$	7	8	9	10	11	12
1	0	0	0	0	0	0	1	0	0	0	0	0	0
2	0	0	0	0	0	0	2	0	0	0	0	0	0
3	0	0	0	0	0	0	3	0	0	0	0	0	0
4	0	0	0	0	0	0	4	0	0	0	0	0	0
5	0	0	0	0	0	0	5	0	0	0	0	0	0
6	0	0	0	0	0	0	6	0	0	0	0	0	0
7	0	0	0	0	0	0	7	1	0	0	0	0	0
8	1	0	0	0	0	0	8	7	1	0	0	0	0
9	7	1	0	0	0	0	9	35	8	1	0	0	0
10	51	8	1	0	0	0	10	170	47	9	1	0	0
11	361	79	10	1	0	0	11	847	277	61	10	1	0
12	2484	754	121	12	1	0	12	4408	1775	436	78	11	1

Exercises

E.6.2.1 **Exercise** Let Γ be a generator matrix of an (n,k)-code over $\mathbb{F}_q$ and let M be a monomial matrix in $M_n(q)$. Discuss the relations between the linear dependencies occurring between the columns of Γ and between the columns of $\Gamma \cdot M$.

E.6.2.2 **Exercise** Prove 6.2.11.

E.6.2.3 **Exercise** Find a proof of 6.2.12.

E.6.2.4 **Exercise** Use Exercise 1.3.9 in order to prove that 6.2.14 is true.

E.6.2.5 **Exercise** Prove that any (n,k)-MDS-code with $k < n$ is indecomposable.

E.6.2.6 **Exercise** Show that the code which is generated by the matrix in 6.2.17 is indecomposable.

E.6.2.7 **Exercise** Prove 6.2.18.

E.6.2.8 **Exercise** Prove that 6.2.25 is a special case of 6.2.21.

E.6.2.9 **Exercise** Prove that $R_{nkq} = R_{n,n-k,q}$ is true for $1 \leq k \leq \lfloor n/2 \rfloor$.

6.3 Cycle Indices of Projective Linear Groups

We have seen how the linear isometry classes of (n,k)-codes over $\mathbb{F}_q$ can be enumerated using cycle indices of projective linear groups $\mathrm{PGL}_k(q)$. It remains to discuss the evaluation of these multivariate polynomials. The formal definition

$$C(G,X) := \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} z_i^{a_i(\overline{g})} \in \mathbb{Q}[z_1, z_2, \ldots, z_{|X|}]$$

of cycle indices, given in 6.1.19, shows that we must determine the cycle types

$$a(\overline{g}) = (a_1(\overline{g}), \ldots, a_{|X|}(\overline{g}))$$

of the homomorphic images $\overline{g}$ of the elements and the order of the acting group $\mathrm{GL}_k(q)$ or of its epimorphic image $\mathrm{PGL}_k(q)$. According to Exercise 6.3.1, the

orders of these groups are

$$|\mathrm{GL}_k(q)| = [q]_k := (q^k - 1)(q^k - q)\cdots(q^k - q^{k-1}) \tag{6.3.1}$$

and

$$|\mathrm{PGL}_k(q)| = [q]_k/(q-1). \tag{6.3.2}$$

These groups are quite big, and so it is not efficient to establish a complete catalog of all their elements, except for very small values of q and k. A much more economic way is to use the fact that the cycle types of conjugate elements (as well as of images of conjugate elements under homomorphisms) are the same (see Exercise 6.3.2). It reduces the problem to a characterization of the conjugacy classes and the evaluation of the cycle types of representatives of each of these classes. Using this fact we rewrite the cycle index of a group G which acts on a set X in the following form:

$$C(G,X) = \frac{1}{|G|}\sum_{\mathcal{C}} |\mathcal{C}| \prod_{i=1}^{|X|} z_i^{a_i(\overline{g}_{\mathcal{C}})}, \tag{6.3.3}$$

where $g_{\mathcal{C}}$ is a representative of the conjugacy class $\mathcal{C}$, the summation is over all the conjugacy classes $\mathcal{C}$ of elements in G, and

$$a(\overline{g}_{\mathcal{C}}) = (a_1(\overline{g}_{\mathcal{C}}), \ldots, a_{|X|}(\overline{g}_{\mathcal{C}}))$$

denotes the cycle type of $\overline{g}_{\mathcal{C}}$, the permutation induced by $g_{\mathcal{C}}$ on X. As we already know, the cycle type of $\overline{g}$ satisfies

$$\sum_{i=1}^{|X|} i a_i(\overline{g}) = |X|\,.$$

In general, we call a sequence $a = (a_1, \ldots, a_n)$ of nonnegative integers a *cycle type of* n, if $\sum_{i=1}^{n} i \cdot a_i = n$ is satisfied. For short, we write $a \vdash n$, and we note in passing that each cycle type $a \vdash n$ occurs as type of a permutation of n.

Let us now concentrate on the evaluation of the cycle index of the natural action of $G := \mathrm{PGL}_k(q)$ on $X := \mathrm{PG}^*_{k-1}(q)$. The action 3.7.4 of $\mathrm{GL}_k(q)$ on $\mathrm{PG}^*_{k-1}(q)$ induces this action of the projective linear group. According to 3.7.6, it can be written as

$$(\mathbb{F}^*_q(A), \mathbb{F}^*_q(v)) \mapsto \mathbb{F}^*_q(v \cdot A^\top), \qquad A \in \mathrm{GL}_k(q),\ v \in \mathbb{F}^k_q. \tag{6.3.4}$$

Here in this section it is more convenient to represent vectors as column vectors, so 6.3.4 is written as

$$(\mathbb{F}^*_q(A), \mathbb{F}^*_q(v)) \mapsto \mathbb{F}^*_q(A \cdot v), \qquad A \in \mathrm{GL}_k(q),\ v \in \mathbb{F}^k_q.$$

The notation $A \cdot v$ is similar to the notation of applying an endomorphism A of $\mathbb{F}_q^k$ to the vector v which we indicate just by Av.

In order to evaluate the cycle index of the projective linear group we proceed as follows. In a first step each conjugacy class of $\mathrm{GL}_k(q)$ will be described by a *normal form* which is a particular representative of the conjugacy class. Then we evaluate the cardinalities of the conjugacy classes and the cycle types of their representatives.

The announced normal forms of the elements in $\mathrm{GL}_k(q)$ are obtained by using a general approach known from linear algebra, and described in most of the standard lectures on this subject, e.g. in [155].

First we determine a normal form of an arbitrary endomorphism A of $\mathbb{F}^k$. Let x be an indeterminate over $\mathbb{F}$. Then the vector space $\mathbb{F}^k$ together with the outer composition

6.3.5
$$\mathbb{F}[x] \times \mathbb{F}^k \to \mathbb{F}^k \ : \ (f, v) \mapsto fv := \sum_{i=0}^{d} \kappa_i A^i v,$$

becomes an $\mathbb{F}[x]$-module, where f denotes the polynomial $f = \sum_{i=0}^{d} \kappa_i x^i$.

Let $\{e^{(0)}, \ldots, e^{(k-1)}\}$ be the canonical basis of $\mathbb{F}^k$ consisting of the unit vectors. Then

$$\mathbb{F}^k = \sum_{i \in k} \mathbb{F}\, e^{(i)} = \sum_{i \in k} \mathbb{F}[x] e^{(i)}.$$

Since $\mathbb{F}[x]e^{(i)}$ is a subset of $\mathbb{F}^k$, the cyclic $\mathbb{F}[x]$-module $\mathbb{F}[x]e^{(i)}$ is of finite dimension, and the canonical epimorphism from $\mathbb{F}[x]$ to $\mathbb{F}[x]e^{(i)}$ has a kernel different from 0. This kernel is an ideal in the principal ideal domain $\mathbb{F}[x]$, whence it is generated by a monic polynomial $g_i \in \mathbb{F}[x]$ of degree at least 1.

The polynomial $f \in \mathbb{F}[x]$ annihilates $v \in \mathbb{F}^k$ if $fv = 0$. The polynomial $f \in \mathbb{F}[x]$ annihilates $W \subseteq V$ if f annihilates each vector of W. The monic polynomial $f \in \mathbb{F}[x] \setminus \{0\}$ of smallest degree which annihilates v is called the *minimal polynomial* of v. The monic polynomial $f \in \mathbb{F}[x] \setminus \{0\}$ of smallest degree which annihilates $\mathbb{F}^k$ is called the *minimal polynomial* of A. It is usually indicated by M_A. The most important property of minimal polynomials is described in the next

6.3.6 **Lemma** *Let A be an endomorphism of $\mathbb{F}^k$. The polynomial $g \in \mathbb{F}[x]$ annihilates $v \in \mathbb{F}^k$ or $\mathbb{F}^k$ if and only if g is a multiple of the minimal polynomial of v or A, respectively.* □

The proof is left to the reader.

From the Homomorphism Theorem (Exercise 3.2.3) we deduce that $\mathbb{F}[x]e^{(i)}$ is isomorphic to $\mathbb{F}[x]/\mathrm{I}(g_i)$, and the polynomial g_i annihilates the module $\mathbb{F}[x]e^{(i)}$ completely, since $g_i e^{(i)} = 0$. If g denotes the least common multiple of

$g_0, \ldots, g_{k-1}$, then g annihilates the whole vector space $\mathbb{F}^k$. Consequently, g is the minimal polynomial of A, and $\mathbb{F}^k$ can also be seen as an $\overline{\mathbb{F}[x]} := \mathbb{F}[x]/\mathrm{I}(g)$-module. Now we decompose g into its pairwise distinct monic, irreducible factors $f_i \in \mathbb{F}[x]$,

$$g = \prod_{i \in t} f_i^{c_i},$$

where t denotes the number of different factors, and $c_i \geq 1$ is the multiplicity of the i-th factor. For $i \in t$ the polynomials $h_i := \prod_{j \neq i} f_j^{c_j}$ are relatively prime by construction, i.e. $\gcd(h_0, \ldots, h_{t-1}) = 1$, and according to Bézout's Identity (cf. Exercise 3.1.6) there exist polynomials $H_i \in \mathbb{F}[x]$ such that 1 can be expressed as

$$1 = H_0 h_0 + \ldots + H_{t-1} h_{t-1}.$$

Putting $E_i := H_i h_i$, we obtain a decomposition of $\overline{1} \in \overline{\mathbb{F}[x]}$ into a sum of pairwise orthogonal and idempotent elements

$$\overline{1} = \overline{E}_0 + \ldots + \overline{E}_{t-1}. \tag{6.3.7}$$

This decomposition of $\overline{1}$ yields, according to Exercise 4.5.2, a decomposition – the *primary decomposition* – of $\mathbb{F}^k$ as a direct sum of *primary components* of the form

$$\mathbb{F}^k = \overline{E}_0 \mathbb{F}^k \oplus \ldots \oplus \overline{E}_{t-1} \mathbb{F}^k.$$

The $\overline{\mathbb{F}[x]}$-module $\overline{E}_i \mathbb{F}^k$ and the $\mathbb{F}[x]$-module $E_i \mathbb{F}^k$ describe the same set, therefore the primary components are A-invariant, since

$$A(\overline{E}_i \mathbb{F}^k) = x E_i \mathbb{F}^k = E_i x \mathbb{F}^k \subseteq E_i \mathbb{F}^k = \overline{E}_i \mathbb{F}^k, \qquad i \in t.$$

Now we consider each of these components $E_i \mathbb{F}^k$ as an $\mathbb{F}[x]/\mathrm{I}(f_i^{c_i})$-module. According to 4.7.11, the ring $\mathbb{F}[x]/\mathrm{I}(f_i^{c_i})$ has exactly one composition series. Thus it follows from 4.7.12 that $E_i \mathbb{F}^k$ is a direct sum of submodules

$$E_i \mathbb{F}^k = U_{i0} \oplus \ldots \oplus U_{i,n_i-1}, \;\; U_{ij} = \mathbb{F}[x] u_{ij} \simeq \mathbb{F}[x]/\mathrm{I}(f_i^{t_{ij}}), \;\; 1 \leq t_{ij} \leq c_i, \tag{6.3.8}$$

where U_{ij} is cyclic over the ring $\mathbb{F}[x]/\mathrm{I}(f_i^{c_i})$. These submodules can be ordered in such a way that $1 \leq t_{i0} \leq t_{i1} \leq \ldots \leq t_{i,n_i-1} = c_i$ holds true. Also the submodules U_{ij} are A-invariant. Summarizing, the vector space $\mathbb{F}^k$ is the direct sum of cyclic subspaces

$$\mathbb{F}^k = \bigoplus_{i \in t} \bigoplus_{j \in n_i} U_{ij}, \;\; U_{ij} = \mathbb{F}[x] u_{ij} \simeq \mathbb{F}[x]/\mathrm{I}(f_i^{t_{ij}}), \;\; 1 \leq t_{ij} \leq c_i. \tag{6.3.9}$$

Let $f := \sum_{i=0}^{d} \kappa_i x^i$, $\kappa_d = 1$, be a monic, irreducible polynomial of degree d. Assume that f is the minimal polynomial of $v \in \mathbb{F}^k$, whence $U = \mathbb{F}[x]v \simeq \mathbb{F}[x]/\mathrm{I}(f)$ is a d-dimensional cyclic subspace of $\mathbb{F}^k$. Using the basis

$(v, Av, \ldots, A^{d-1}v)$ of U, the restriction of the endomorphism A to U is represented by the *companion matrix* $C(f)$ of f given by

$$C(f) := \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -\kappa_0 \\ 1 & 0 & \ldots & 0 & 0 & -\kappa_1 \\ 0 & 1 & \ldots & 0 & 0 & -\kappa_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -\kappa_{d-2} \\ 0 & 0 & \ldots & 0 & 1 & -\kappa_{d-1} \end{pmatrix}.$$

Assume that f^n is the minimal polynomial of $v \in \mathbb{F}^k$, whence $U = \mathbb{F}[x]v \simeq \mathbb{F}[x]/\mathrm{I}(f^n)$ is an nd-dimensional cyclic subspace of $\mathbb{F}^k$. We choose a basis of U of the form $(v, Av, \ldots, A^{d-1}v, fv, Afv, \ldots, A^{d-1}fv, \ldots, f^{n-1}v, Af^{n-1}v, \ldots, A^{d-1}f^{n-1}v)$, so that the normal form of the restriction of A to U is the following square block-matrix

$$H(f^n) := \left(\begin{array}{c|c|c|c|c|c} C(f) & 0 & 0 & \ldots & 0 & 0 \\ \hline I'_d & C(f) & 0 & \ldots & 0 & 0 \\ \hline 0 & I'_d & C(f) & \ldots & 0 & 0 \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \hline 0 & 0 & 0 & \ldots & C(f) & 0 \\ \hline 0 & 0 & 0 & \ldots & I'_d & C(f) \end{array}\right) \Bigg\} n \text{ blocks},$$

where I'_d is the elementary matrix $B^{(2)}_{0,d-1,1}$ of dimension d (cf. Exercise 1.7.3), which is the identity matrix I_d with an additional 1 in the right upper corner. The matrix $H(f^n)$ is an $nd \times nd$-matrix and is called the *hyper companion matrix* of f^n. In the case $n = 1$ the matrices $H(f^1)$ and $C(f)$ coincide.

Now we introduce the following notion. Assume that $f_0, \ldots, f_{t-1}$ are pairwise distinct monic, irreducible polynomials over $\mathbb{F}$. If there exists a decomposition 6.3.9 of $\mathbb{F}^k$ with exactly $a_j^{(i)}$ cyclic subspaces isomorphic to $\mathbb{F}[x]/\mathrm{I}(f_i^j)$ for $1 \le j \le c_i$ and for $i \in t$, then the *Jacobi normal form* of A is a block-diagonal matrix of the form

6.3.10
$$\operatorname{diag}\left(D(f_0, a^{(0)}), \ldots, D(f_{t-1}, a^{(t-1)})\right)$$

where $a^{(i)}$ is a cycle type of $\sum_{j=1}^{c_i} j a_j^{(i)}$, for $i \in t$. The block-diagonal matrix $D(f, a)$, determined by a monic irreducible polynomial f and a cycle type a, is built from companion and hyper companion matrices of f in the following way:

$$D(f, a) = \operatorname{diag}\Big(\underbrace{C(f), \ldots, C(f)}_{a_1 \text{ times}}, \underbrace{H(f^2), \ldots, H(f^2)}_{a_2 \text{ times}}, \ldots\Big).$$

A different approach to normal forms can be found in [60].

The *characteristic polynomial* of an $(n \times n)$-matrix A over $\mathbb{F}$ is defined as $\chi_A(x) := \det(xI_n - A)$. Developing this determinant for $A = C(f)$ with respect to the top row, we get $\chi_{C(f)} = f$. Consequently, $\chi_{H(f^n)} = f^n$, and if $A = \operatorname{diag}\left(D(f_0, a^{(0)}), \ldots, D(f_{t-1}, a^{(t-1)})\right)$, then

$$\chi_A = \prod_{i \in t} f_i^{\gamma_i},$$

where $\gamma_i = \sum_j j a_j^{(i)}$. In other words, the sequence $a^{(i)}$ is a cycle type of γ_i.

By construction, the minimal polynomial of the companion matrix $C(f)$ is equal to f, and $M_{H(f^n)} = f^n$. Consequently, the minimal polynomial of $A = \operatorname{diag}\left(D(f_0, a^{(0)}), \ldots, D(f_{t-1}, a^{(t-1)})\right)$ is given by

$$M_A = \prod_{i \in t} f_i^{c_i},$$

where c_i is the maximal j such that $a_j^{(i)} \neq 0$. From this description it is obvious that M_A is a divisor of χ_A. This proves the

Cayley–Hamilton Theorem *If A is an endomorphism of $\mathbb{F}^k$, then $\chi_A(A) = 0$.* □ **6.3.11**

Now we come back to our main situation $\mathbb{F} = \mathbb{F}_q$. As we have seen in the proof of 3.2.25, there exist exactly

$$m_q(d) = \frac{1}{d} \sum_{t \mid d} \mu(t) q^{\frac{d}{t}}$$

monic, irreducible polynomials of degree d over $\mathbb{F}_q$, where μ is the number theoretic Möbius function (cf. Exercise 3.2.15). Each of these polynomials of degree not greater than k, with exception of the polynomial $f(x) = x$, can occur as a divisor of the characteristic polynomial of a regular matrix $A \in \mathrm{GL}_k(q)$. We indicate these polynomials by $f_0, f_1, \ldots, f_{t_k - 1}$, where

$$t_k := \left(\sum_{i=1}^{k} m_q(i) \right) - 1.$$

If, moreover, d_i indicates the degree of the polynomial f_i for $i \in t_k$, then we obtain the following description of the conjugacy classes in $\mathrm{GL}_k(q)$:

Theorem *For each conjugacy class in $\mathrm{GL}_k(q)$ there exists exactly one pair (γ, a), where $\gamma = (\gamma_0, \ldots, \gamma_{t_k - 1}) \in \mathbb{N}^{t_k}$ is a solution of* **6.3.12**

$$\sum_{i \in t_k} \gamma_i d_i = k, \qquad \textbf{6.3.13}$$

and $a = (a^{(0)}, \ldots, a^{(t_k-1)})$ *is a sequence of cycle types* $a^{(i)} \vdash \gamma_i$*, so that*

6.3.14 $$\operatorname{diag}\left(D(f_0, a^{(0)}), \ldots, D(f_{t_k-1}, a^{(t_k-1)})\right)$$

is the normal form of this class. Conversely, to each such pair (γ, a) *there exists exactly one conjugacy class the normal form of which is the block-diagonal matrix 6.3.14.* □

Our next task is the evaluation of the size of the conjugacy classes. Conjugation on $\mathrm{GL}_k(q)$ is a particular group action of $\mathrm{GL}_k(q)$ on itself (cf. Exercise 3.4.2). The centralizer of $A \in \mathrm{GL}_k(q)$ is the stabilizer of A with respect to this action.

6.3.15 **Theorem (J.P.S. Kung [117])** *Let* $f \in \mathbb{F}_q[x]$ *be a monic, irreducible polynomial of degree* d*, and let* $a \vdash \gamma$ *be a cycle type of the positive integer* γ*. For* $i \in \{0, 1, \ldots, \gamma\}$ *determine* m_i *by*

$$m_i := \sum_{k=1}^{i} k a_k + \sum_{k=i+1}^{\gamma} i a_k.$$

Then the order of the centralizer of $D(f, a)$ *in* $\mathrm{GL}_{\gamma d}(q)$ *is*

6.3.16 $$b(d, a) := \prod_{i=1}^{\gamma} \prod_{j \in a_i} \left(q^{d m_i} - q^{d(m_i - j - 1)}\right).$$

Proof: Let $n = \gamma d$ be the dimension of a vector space V equipped with the basis $B = (e_0, \ldots, e_{n-1})$ so that the linear mapping $A \colon V \to V$ has a representation with respect to this basis in the form $D(f, a)$, where f is a monic, irreducible polynomial in $\mathbb{F}_q[x]$ of degree d and $a \vdash \gamma$. (The vectors e_i should not be mixed up with the unit vectors $e^{(i)}$.) We also consider V as an $\mathbb{F}_q[x]$-module. Determine c by

$$c := \max\{i \mid 1 \le i \le \gamma,\ a_i \neq 0\},$$

then $\ker f^c = V$, $m_c = \gamma$, and

$$\dim(\ker f^i) = d\left(\sum_{k=1}^{i} k a_k + \sum_{k=i+1}^{\gamma} i a_k\right) = d m_i \ \text{ for } \ 1 \le i \le c.$$

Consequently, the sets

$$U_i := \left\{v \in V \mid f^i v = 0 \ \text{ and } \ f^{i-1} v \neq 0\right\} = \ker f^i \setminus \ker f^{i-1}$$

contain $q^{d m_i} - q^{d m_{i-1}}$ elements for $1 \le i \le c$. Now we want to choose a particular series of elements of the given basis of V – called *canonical generators* of A – by taking exactly one element of B from each cyclic subspace in the

decomposition 6.3.8 of V. For example, a list of canonical generators is given by

$$e_0,\ e_d,\ e_{2d},\ \ldots,\ e_{(a_1-1)d},$$
$$e_{a_1 d},\ e_{(a_1+2)d},\ e_{(a_1+2\cdot 2)d},\ \ldots,\ e_{(a_1+2(a_2-1))d},$$
$$\ldots$$
$$e_{(a_1+\ldots+(c-1)a_{c-1})d},\ e_{(a_1+\ldots+(c-1)a_{c-1}+c)d},\ \ldots,\ e_{(a_1+\ldots+(c-1)a_{c-1}+c(a_c-1))d}.$$

Now we label these canonical generators consecutively as $\hat{e}_0, \hat{e}_1, \ldots$. To be more precise, for $j \in a_i$, $i \geq 1$ we have

$$\hat{e}_{a_1+\ldots+a_{i-1}+j} = e_{(a_1+2a_2+\ldots+(i-1)a_{i-1}+ij)d}.$$

In order to complete the proof, we still need to characterize the vector space automorphisms which commute with A.

Lemma *Let ψ be a vector space endomorphism which commutes with $A := D(f,a)$. Then:* **6.3.17**

1. *ψ is uniquely determined on V by the values $\psi(\hat{e}_i)$ on the canonical generators.*
2. *If $v \in U_i$ is a canonical generator, then $\psi(v)$ belongs to* $\ker f^i$ *for $1 \leq i \leq c$.*
3. *ψ is a vector space automorphism if and only if there are no linear relations with coefficients in $\mathbb{F}_q[x]$ among the values $\psi(\hat{e}_i)$. In particular, any canonical generator $v \in U_i$ is mapped onto $\psi(v) \in U_i$.*

Proof: The proof of the first two assertions is left to the reader (cf. Exercise 6.3.8). As was shown in 6.3.8, assume that the vector space V has a decomposition into a direct sum of cyclic subspaces

$$V = \bigoplus_{\ell=0}^{a_1+\ldots+a_c-1} V_\ell \ \text{ with } \ V_\ell \simeq \mathbb{F}_q[x]/\mathrm{I}(f^{j_\ell}) \ \text{ for } \ 1 \leq j_\ell \leq c.$$

Moreover, let $\hat{e}_\ell$ be the unique canonical generator of A which belongs to V_ℓ. Then

$$(\hat{e}_\ell, A \cdot \hat{e}_\ell, \ldots, A^{dj_\ell - 1} \cdot \hat{e}_\ell)$$

is a basis of V_ℓ. Finally we assume that the monic polynomial f is of the form $f = \sum_{i=0}^{d} \alpha_i x^i$ with $\alpha_d = 1$.

If ψ is an automorphism of V, then

$$\big(\psi(\hat{e}_\ell), A \cdot \psi(\hat{e}_\ell), \ldots, A^{dj_\ell - 1} \cdot \psi(\hat{e}_\ell)\big)$$

is a basis of $\psi(V_\ell)$. In other words, $\psi(V_\ell)$ is also a dj_ℓ-dimensional cyclic subspace of V. And $\mathbb{F}_q[x]\psi(\hat{e}_\ell) = \psi(V_\ell)$, since $A^{dj_\ell} \cdot \psi(\hat{e}_\ell) = \psi(A^{dj_\ell} \cdot \hat{e}_\ell)$ and

$$\psi(A^{dj_\ell} \cdot \hat{e}_\ell) = \psi\Big(\sum_{i \in d}(-\alpha_i) A^{ij_\ell} \cdot \hat{e}_\ell\Big) = \sum_{i \in d}(-\alpha_i) A^{ij_\ell} \cdot \psi(\hat{e}_\ell) \in \psi(V_\ell).$$

Conversely, if ψ is an endomorphism which is not an automorphism of V, then the vectors $\psi(e_0), \dots, \psi(e_{n-1})$ are linearly dependent. Thus, there exist $\alpha_i \in \mathbb{F}_q$, $i \in n$, not all equal to 0, such that

$$\sum_{i \in n} \alpha_i \psi(e_i) = 0.$$

This is a nontrivial linear combination of $\psi(e_i)$. Equipping each subspace V_ℓ with the basis $(\hat{e}_\ell, A \cdot \hat{e}_\ell, \dots, A^{dj_\ell - 1} \cdot \hat{e}_\ell)$ described above, we derive

$$0 = \sum_{\ell=0}^{a_1+\dots+a_c-1} \underbrace{\sum_{r \in dj_\ell} \alpha_{\ell r} A^r}_{=:\phi_\ell(A)} \cdot \psi(\hat{e}_\ell) = \sum_{\ell=0}^{a_1+\dots+a_c-1} \phi_\ell(x) \psi(\hat{e}_\ell)$$

for suitable $\alpha_{\ell r} \in \mathbb{F}_q$. By construction, not all polynomials ϕ_ℓ are equal to zero, whence we have found a nontrivial linear relation between the vectors $\psi(\hat{e}_\ell)$ with coefficients in $\mathbb{F}_q[x]$. This contradicts our assumption. □

6.3.17 shows that the image of a canonical generator $v \in U_i$ under an automorphism ψ is again an element of U_i. In the notation of 6.3.8, this means that ψ only permutes the subspaces U_{ij} of a submodule $E_i \mathbb{F}_q^k$ which are isomorphic to the *same* factor module $\mathbb{F}_q[x]/\mathrm{I}(f^j)$.

In order to complete the proof of 6.3.15, we determine the number of all possible automorphisms ψ of V by an application of 6.3.17. Starting with the last canonical generator of A, the value $\psi(\hat{e}_{a_1+\dots+a_c-1})$ must be chosen in U_c. There are $q^{dm_c} - q^{dm_{c-1}}$ possibilities to do so. If $\hat{e}_{a_1+\dots+a_c-2}$ also belongs to U_c, then there remain $q^{dm_c} - q^{dm_{c-1}} q^d = q^{dm_c} - q^{d(m_{c-1}+1)}$ possibilities to determine $\psi(\hat{e}_{a_1+\dots+a_c-2})$ in U_c so that ψ is an automorphism. (This is just the overall number of vectors in V which do not belong to the $\mathbb{F}_q[x]$-submodule generated by $\ker f^{c-1}$ and $\psi(\hat{e}_{a_1+\dots+a_c-1})$.) In a similar fashion, the values of the other canonical generators of A which also belong to U_c are determined. Altogether there are

$$\prod_{j \in a_c} \left(q^{dm_c} - q^{d(m_{c-1}+j)} \right) = \prod_{j \in a_c} \left(q^{dm_c} - q^{d(m_c - j - 1)} \right)$$

possibilities to determine an automorphism ψ on U_c.

Now assume that W_k, $0 \le k \le a_1 + \dots + a_c - 1$, denotes the $\mathbb{F}_q[x]$-module generated by $\psi(\hat{e}_j)$ for $j \ge k$. Assume that the canonical generator $\hat{e}_k$ belongs to U_i and that the values $\psi(\hat{e}_j)$ are already determined for $j > k$. In order to determine an automorphism, the vector $\psi(\hat{e}_k)$ must be chosen from $\ker f^i$, but it may not belong to the $\mathbb{F}_q[x]$-module generated by $\ker f^{i-1}$ and $\ker f^i \cap W_{k+1}$. This shows that if ψ is an automorphism already determined on $U_{i+1}, \dots, U_c$, then there are

$$\prod_{j \in a_i} \left(q^{dm_i} - q^{d(m_{i-1}+a_{i+1}+\dots+a_c+j)} \right) = \prod_{j \in a_i} \left(q^{dm_i} - q^{d(m_i - j - 1)} \right)$$

possibilities to determine the values of ψ for the canonical generators belonging to U_i (these are the generators $\hat{e}_{a_1+\ldots+a_{i-1}}, \ldots, \hat{e}_{a_1+\ldots+a_i-1}$) such that ψ is also an automorphism of $\ker f^i$. Eventually, the product of these expressions for $i = 1, \ldots, c$ (or $i = 1, \ldots, \gamma$) yields $b(d, a)$. □

As we have seen in the previous proof, the order $b(d, a)$ of the centralizer of $D(f, a)$ in $\mathrm{GL}_{\gamma d}(q)$, where f is an irreducible polynomial of degree d and $a \vdash \gamma$, depends only on the degree of f and on the cycle type a. It does not depend on the particular polynomial f itself. According to 3.4.1, the size of the conjugacy class of a normal form 6.3.14 is

$$\frac{[q]_k}{\prod_{i \in t_k} b(d_i, a^{(i)})}.$$

Before we compute the cycle type of the permutation representation of the natural action 6.3.4 of $\mathbb{F}_q^*(A) \in \mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}^*(q)$, we investigate once more the action of $\mathrm{GL}_k(q)$ on $\mathbb{F}_q^k$. From Exercise 1.4.13 it follows that this action can be reduced to an action on $\mathbb{F}_q^k \setminus \{0\}$. In the next step, we determine the subcycle index of the following action:

$$\mathrm{GL}_k(q) \times \mathbb{F}_q^k \setminus \{0\} \to \mathbb{F}_q^k \setminus \{0\} \ : \ (A, v) \mapsto A \cdot v,$$

from which we will later on determine the cycle index $C(\mathrm{PGL}_k(q), \mathrm{PG}_{k-1}^*(q))$. Recall that in the present section we write vectors as columns and not as rows.

We introduce subcycles and integral elements of vectors $v \in \mathbb{F}_q^k \setminus \{0\}$ in the following way: The vector v belongs to a *subcycle* of A *of length* s if and only if

$$s = \min \left\{ n \in \mathbb{N}^* \mid A^n \cdot v \in \mathbb{F}_q^*(v) \right\}.$$

The *integral element* of v is the element $\alpha_0 \in \mathbb{F}_q^*$ for which $A^s \cdot v = \alpha_0 v$. The set

$$\langle A \rangle(\mathbb{F}_q^*(v)) = \left\{ A^i \cdot \alpha v \mid i \in \mathbb{N},\ \alpha \in \mathbb{F}_q^* \right\}$$

is the disjoint union of s subsets, each containing $q - 1$ elements, since

$$\begin{aligned} \langle A \rangle(\mathbb{F}_q^*(v)) &= \dot{\bigcup_{i \in s}} A^i \mathbb{F}_q^*(v) = \dot{\bigcup_{i \in s}} \left\{ A^i \cdot \alpha v \mid \alpha \in \mathbb{F}_q^* \right\} \\ &= \dot{\bigcup_{i \in s}} \left\{ \alpha A^i \cdot v \mid \alpha \in \mathbb{F}_q^* \right\} = \dot{\bigcup_{i \in s}} \mathbb{F}_q^*(A^i \cdot v). \end{aligned}$$

These $s(q-1)$ vectors in $\mathbb{F}_q^k \setminus \{0\}$ describe exactly s elements of the projective space $\mathrm{PG}_{k-1}^*(q)$, which are the elements of exactly one cycle of length s of $A \in \mathrm{GL}_k(q)$ or $\mathbb{F}_q^*(A) \in \mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}^*(q)$, namely

$$\left(\mathbb{F}_q^*(v), \ldots, \mathbb{F}_q^*(A^{s-1} \cdot v)\right).$$

Moreover, each vector $v' \in \langle A \rangle(\mathbb{F}_q^*(v))$ belongs to a subcycle of A of length s with integral element α_0. Using indeterminates z attached with two indices

– the first one giving the length s of a subcycle and the second one indicating the integral element α_0 corresponding to the subcycle – the operation of A on $\langle A \rangle(\mathbb{F}_q^*(v))$ is described by the subcycle expression $sc(A,v) := z_{s,\alpha_0}^{q-1}$. Since the set $\mathbb{F}_q^k \setminus \{0\}$ is the disjoint union of $\langle A \rangle(\mathbb{F}_q^*(v_i))$, $i \in I$, we define the *subcycle type* of A to be the product of the subcycle expressions $\prod_{i\in I} sc(A,v_i)$. A term of the form z_{s,α_0}^r in the subcycle type of A indicates that there exist $r \cdot s$ vectors $v \in \mathbb{F}_q^k \setminus \{0\}$ such that $s = \min\{n \in \mathbb{N}^* \mid A^n \cdot v \in \mathbb{F}_q^*(v)\}$ and $A^s \cdot v = \alpha_0 v$. Moreover, the exponent r is always a multiple of $q-1$.

6.3.18 **Definition (subcycle index)** The *subcycle index* for the action of the general linear group $\mathrm{GL}_k(q)$ on $\mathbb{F}_q^k \setminus \{0\}$ is the sum of the subcycle types of $A \in \mathrm{GL}_k(q)$ divided by the order of $\mathrm{GL}_k(q)$, i.e.

$$SC(\mathrm{GL}_k(q), \mathbb{F}_q^k \setminus \{0\}) = \frac{1}{|\mathrm{GL}_k(q)|} \sum_{A\in \mathrm{GL}_k(q)} \prod_{\langle A \rangle(\mathbb{F}_q^*(v))} sc(A,v).$$

The last product must be computed over all $\langle A \rangle(\mathbb{F}_q^*(v))$ in the set

$$\left\{ \langle A \rangle(\mathbb{F}_q^*(v)) \mid v \in \mathbb{F}_q^k \setminus \{0\} \right\}. \qquad \diamond$$

6.3.19 **Remark (cycle index of $\mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}^*(q)$)** From the subcycle index of $\mathrm{GL}_k(q)$ on $\mathbb{F}_q^k \setminus \{0\}$ it is quite easy to obtain the cycle index of the action of $\mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}^*(q)$ by omitting the second index of each indeterminate and by dividing each exponent by $q-1$. $\diamond$

Hence, as the next step we compute the subcycle index of $\mathrm{GL}_k(q)$ acting on $\mathbb{F}_q^k \setminus \{0\}$. Since the subcycle types of conjugate matrices in $\mathrm{GL}_k(q)$ are the same, it is enough to determine the subcycle types of the normal forms 6.3.14. First we determine them for hyper companion matrices, later we will deduce a method which allows us to compute the subcycle type of block-diagonal matrices.

The companion and hyper companion matrices depend on polynomials $f \in \mathbb{F}_q[x]$. The subcycle types of these matrices can be obtained from the subexponents of the corresponding polynomials. Therefore, next we introduce exponent and subexponent of a polynomial.

6.3.20 **Definition (exponent, order, period)** The *exponent, order,* or *period* of a polynomial $f \in \mathbb{F}_q[x]$ with $f(0) \neq 0$, is the smallest positive integer e, for which f is a divisor of $x^e - 1$ (cf. [131]). We indicate it as

$$\mathrm{Exp}(f) := \min\{e \in \mathbb{N}^* \mid f \text{ is a divisor of } x^e - 1\}. \qquad \diamond$$

Some properties of the exponent of a polynomial are collected in the next

Lemma *Let $f \in \mathbb{F}_q[x]$ be a monic, irreducible polynomial of degree d with $f(0) \neq 0$.* **6.3.21**

1. *The exponent of f is equal to the order of an arbitrary root β of f in the multiplicative group $\mathbb{F}_{q^d}^*$. In other words, for any root β of f we have*
$$\mathrm{Exp}(f) = \min\{n \in \mathbb{N}^* \mid \beta^n = 1\} = \mathrm{ord}(\beta).$$
2. *$\mathrm{Exp}(f)$ is a divisor of $q^d - 1$, but it does not divide $q^r - 1$ for $1 \leq r < d$.*
3. *The set $E(d,q)$ of all positive integers, which occur as exponents of monic, irreducible polynomials of degree d over $\mathbb{F}_q$, is*
$$E(d,q) = \left\{ e \in \mathbb{N}^* \;\middle|\; e \mid (q^d - 1) \text{ and } e \nmid (q^r - 1) \text{ for } 1 \leq r < d \right\}.$$
4. *The number of all monic, irreducible polynomials f of degree d over $\mathbb{F}_q$ with $f(0) \neq 0$ and with exponent $e \in E(d,q)$ is $\nu(d,e) := \phi(e)/d$, where ϕ is the* Euler function *(cf. 3.4.15).*
5. *For $n \in \mathbb{N}^*$, the polynomial f is a divisor of $x^n - 1$ if and only if $\mathrm{Exp}(f)$ is a divisor of n. (This assertion holds true for arbitrary $f \in \mathbb{F}_q[x]$ with $f(0) \neq 0$.)*
6. *For $n \in \mathbb{N}^*$, the exponent $\mathrm{Exp}(f^n)$ is equal to $\mathrm{Exp}(f)p^t$, where p is the characteristic of $\mathbb{F}_q$, and t is given by $t := \min\{r \in \mathbb{N} \mid p^r \geq n\}$.*

Proof: 1. Let $\beta \in \mathbb{F}_{q^d}$ be a root of f. From 3.2.19 we know that f is the minimal polynomial of β. Moreover, $\beta, \beta^q, \ldots, \beta^{q^{d-1}}$ are all the roots of f, they all are simple and have the same order in $\mathbb{F}_{q^d}^*$. Consequently, β satisfies the equation $\beta^n = 1$ if and only if f is a divisor of $x^n - 1$. From the definitions of $\mathrm{ord}(\beta)$ and $\mathrm{Exp}(f)$ it is clear that $\mathrm{ord}(\beta) = \mathrm{Exp}(f)$.

2. Since β is an element of $\mathbb{F}_{q^d}^*$, its order is a divisor of $q^d - 1$, and moreover $d = \min\left\{ n \in \mathbb{N}^* \mid \beta^{q^n} = \beta \right\}$, since β is a root of an irreducible polynomial over $\mathbb{F}_q$ of degree d. Hence, $d = \min\left\{ n \in \mathbb{N}^* \mid \beta^{q^n - 1} = 1 \right\}$, and, therefore, $\mathrm{ord}(\beta)$ is not a divisor of $q^r - 1$ for $1 \leq r < d$.

3. Thus, $E(d,q)$ is a subset of
$$\left\{ e \in \mathbb{N}^* \;\middle|\; e \mid q^d - 1 \text{ and } e \nmid q^r - 1 \text{ for } 1 \leq r < d \right\}.$$
We still prove that for each positive integer e with $e \mid q^d - 1$ and $e \nmid q^r - 1$ for $1 \leq r < d$ there exists an irreducible polynomial f of degree d such that $\mathrm{Exp}(f) = e$. Assume that e is a divisor of $q^d - 1$ and $e \nmid q^r - 1$ for $1 \leq r < d$. Since $\mathbb{F}_{q^d}^*$ is cyclic, there exist $\phi(e)$ elements $\beta \in \mathbb{F}_{q^d}^*$, which are of order e. According to the particular choice of e, these β do not belong to a proper subfield

$\mathbb{F}_{q^r}$ of $\mathbb{F}_{q^d}$ for $r < d$. Thus, their minimal polynomials are of degree d and exponent e.

4. Each of these minimal polynomials has exactly d distinct roots in $\mathbb{F}_{q^d}$, which are all of the same order. Hence, there are $\phi(e)/d$ different monic, irreducible polynomials over $\mathbb{F}_q$ of degree d with exponent e.

5. Assume that $e = \mathrm{Exp}(f)$ is a divisor of n. Then

$$f \mid x^e - 1 \mid x^n - 1.$$

Conversely, let f be a divisor of $x^n - 1$. According to the division algorithm, there exist $m \in \mathbb{N}$ and $0 \leq r < e$ such that $n = me + r$ and, therefore,

$$x^n - 1 = (x^{me} - 1)x^r + (x^r - 1).$$

Consequently, f is a divisor of $x^r - 1$. This is only possible for $r = 0$, which proves that e is a divisor of n.

6. Assume that $e = \mathrm{Exp}(f)$ and e_n denotes the exponent of f^n. From $f \mid f^n \mid x^{e_n} - 1$ and from the fifth assertion we deduce that $e \mid e_n$. As a consequence of $f \mid x^e - 1$, we derive

$$f^n \mid (x^e - 1)^n \mid (x^e - 1)^{p^t} = x^{ep^t} - 1,$$

whence $e_n \mid ep^t$. Hence, e_n is of the form $e_n = ep^r$ where, $0 \leq r \leq t$. Since e is a divisor of $q^d - 1$, the integers e and p are relatively prime, thus $x^e - 1$ has only simple roots. All roots of the polynomial $x^{ep^r} - 1 = (x^e - 1)^{p^r}$ occur with the multiplicity p^r, all roots of f^n, however, with the multiplicity n. Finally, f^n is a divisor of $x^{ep^r} - 1$, whence comparing the multiplicities of their roots we obtain that $n \leq p^r$ and, consequently, $r = t$. □

6.3.22 Definition (subexponent) The *subexponent* of a polynomial $f \in \mathbb{F}_q[x]$ with $f(0) \neq 0$ is defined as

$$\mathrm{Subexp}(f) := \min\left\{ n \in \mathbb{N}^* \mid \exists\, \alpha_0 \in \mathbb{F}_q^* \text{ such that } f \mid x^n - \alpha_0 \right\}.$$

If $f \mid x^n - \alpha_0$ with $\alpha_0 \in \mathbb{F}_q^*$ and $n = \mathrm{Subexp}(f)$, then α_0 is called the *integral element* of f (cf. [89]). ◇

Using the notation from 6.3.21, some properties of the subexponent of a polynomial are collected in the next lemma, the proof of which is left as an exercise for the reader.

Lemma *Let $f \in \mathbb{F}_q[x]$ be a monic, irreducible polynomial of degree d with $f(0) \neq 0$.* **6.3.23**

1. *Any root $\beta \in \mathbb{F}_{q^d}$ of f satisfies*
$$\mathrm{Subexp}(f) = \min\left\{n \in \mathbb{N}^* \mid \beta^n \in \mathbb{F}_q^*\right\}.$$
In other words, $\mathrm{Subexp}(f)$ *is equal to the order of $\beta\mathbb{F}_q^*$ in the cyclic factor group $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$.*
2. $\mathrm{Subexp}(f)$ *is a divisor of $(q^d-1)/(q-1)$.*
3. *For $n \in \mathbb{N}^*$, the subexponent* $\mathrm{Subexp}(f^n)$ *is equal to* $\mathrm{Subexp}(f)p^t$*, where p is the characteristic of $\mathbb{F}_q$ and t is given by $t := \min\{r \in \mathbb{N} \mid p^r \geq n\}$. If α denotes the integral element of f, then α^{p^t} is the integral element of f^n.*
4. $\mathrm{Subexp}(f)$ *is a divisor of* $\mathrm{Exp}(f)$ *and the quotient*
$$h := \frac{\mathrm{Exp}(f)}{\mathrm{Subexp}(f)}$$
is a divisor of $q-1$. Moreover, h is the multiplicative order of the integral element of f and $h = \gcd(q-1, \mathrm{Exp}(f))$.
5. *The subexponent of f can be computed from its exponent by*
$$\mathrm{Subexp}(f) = \frac{\mathrm{Exp}(f)}{\gcd(q-1, \mathrm{Exp}(f))}.$$
6. *Consider $e \in E(d,q)$ and let $h := \gcd(q-1, e)$. For each $\alpha \in \mathbb{F}_q^*$ of multiplicative order h there exist exactly $\phi(e)/(d \cdot \phi(h))$ monic, irreducible polynomials $f \in \mathbb{F}_q[x]$ of degree d, exponent e, subexponent e/h, and with integral element α.*
7. *The number of all monic, irreducible polynomials over $\mathbb{F}_q$ of degree d and of subexponent s is*
$$\sum_e \frac{\phi(e)}{d},$$
where the sum is taken over all $e \in E(d,q)$ with $e/\gcd(e, q-1) = s$.
8. *In the case $q = 2$ the subexponent and the exponent of f coincide.*
9. *Let $S(d,q)$ be the set of all pairs (s,α) such that there exists a monic, irreducible polynomial over $\mathbb{F}_q$ of degree d with subexponent s and integral element α. Then*
$$S(d,q) = \bigcup_{e \in E(d,q)} \left\{(s,\alpha) \;\middle|\; s = \frac{e}{\gcd(e, q-1)},\ \mathrm{ord}(\alpha) = \gcd(e, q-1)\right\}.$$
For each $(s,\alpha) \in S(d,q)$ there are exactly
$$m(d,s,\alpha) := \frac{\nu(d, s\,\mathrm{ord}(\alpha))}{\phi(\mathrm{ord}(\alpha))}$$

monic, irreducible polynomials over $\mathbb{F}_q$ of degree d with subexponent s and integral element α. □

The connection between the subcycle type of a hyper companion matrix $H(f^r)$ and the subexponent and the integral element of f is described in

6.3.24 Lemma *Let $f \in \mathbb{F}_q[x]$ be a monic, irreducible polynomial of degree d with $f(0) \neq 0$, subexponent s, and integral element α. Then the subcycle type of $H(f^r)$ on $\mathbb{F}_q^{rd} \setminus \{0\}$ is equal to*

$$\prod_{i=1}^{r} z_{s_i,\alpha_i}^{(q^{id}-q^{(i-1)d})/s_i},$$

where $s_i = \mathrm{Subexp}(f^i)$ and $\alpha_i = \alpha^{s_i/s}$ is the integral element of f^i for $1 \leq i \leq r$.

Proof: For $1 \leq i \leq r$ let $U_i := \ker f^i \setminus \ker f^{i-1}$ be the set of those $v \in \mathbb{F}_q^{rd}$, which are annihilated by f^i, but not by f^{i-1}. Consider $v \in U_i$, $A = H(f^r)$, a positive integer n, and $\beta \in \mathbb{F}_q^*$. Since f^i is the minimal polynomial of v,

$$A^n \cdot v = \beta v \Longleftrightarrow A^n \cdot v - \beta v = 0 \Longleftrightarrow (x^n - \beta)v = 0 \Longleftrightarrow f^i \mid x^n - \beta.$$

Consequently, v belongs to a subcycle of $H(f^r)$ of length $s_i = \mathrm{Exp}(f^i)$ with integral element $\alpha_i = \alpha^{s_i/s}$, where α is the integral element of f. Since the set U_i contains $q^{id} - q^{(i-1)d}$ vectors, it contributes the term

$$z_{s_i,\alpha_i}^{(q^{id}-q^{(i-1)d})/s_i}$$

to the subcycle type of $H(f^r)$. □

Next we describe the announced method for computing the subcycle type of a 2×2-block diagonal matrix from the known subcycle types of the two diagonal blocks. By induction, this allows us to compute the subcycle type of any matrix in normal form 6.3.14.

Assume that $A_1 \in \mathrm{GL}_{k_1}(q)$ and $A_2 \in \mathrm{GL}_{k_2}(q)$ are regular matrices. Then $\mathrm{diag}(A_1, A_2) \in \mathrm{GL}_{k_1+k_2}(q)$. The set $\mathbb{F}_q^{k_1+k_2} \setminus \{0\}$ can be decomposed in the following way

$$\left(\mathbb{F}_q^{k_1} \setminus \{0\} \times \{0\}^{k_2}\right) \dot\cup \left(\{0\}^{k_1} \times \mathbb{F}_q^{k_2} \setminus \{0\}\right) \dot\cup \left(\mathbb{F}_q^{k_1} \setminus \{0\} \times \mathbb{F}_q^{k_2} \setminus \{0\}\right).$$

In the sequel, let β denote a primitive element of $\mathbb{F}_q^*$.

6.3.25 Lemma *Assume that we have indeterminates $z_{n,\alpha}$ attached with two indices, where $n \in \mathbb{N}^*$ and $\alpha \in \mathbb{F}_q^*$. We define a multiplication $\circledast$ by*

$$z_{s_1,\beta^{r_1}}^{j_1} \circledast z_{s_2,\beta^{r_2}}^{j_2} := z_{s_3,\beta^{r_3}}^{j_3},$$

where

$$s_3 = \operatorname{lcm}(s_1, s_2) \frac{q-1}{\gcd\left(q-1, \operatorname{lcm}(s_1, s_2) r_1 / s_1 - \operatorname{lcm}(s_1, s_2) r_2 / s_2\right)},$$

$$r_3 \equiv \frac{r_1 s_3}{s_1} \equiv \frac{r_2 s_3}{s_2} \bmod q-1,$$

and

$$j_3 = \frac{s_1 j_1 s_2 j_2}{s_3}.$$

Using this multiplication, we define a multiplication $\star$ of subcycle types by

$$\left(\prod_{i=1}^{\nu_1} z_{u_i,\alpha_i}^{t_i}\right) \star \left(\prod_{j=1}^{\nu_2} z_{v_j,\kappa_j}^{w_j}\right) := \left(\prod_{i=1}^{\nu_1} z_{u_i,\alpha_i}^{t_i}\right) \left(\prod_{j=1}^{\nu_2} z_{v_j,\kappa_j}^{w_j}\right) \prod_{i=1}^{\nu_1} \prod_{j=1}^{\nu_2} \left(z_{u_i,\alpha_i}^{t_i} \circledast z_{v_j,\kappa_j}^{w_j}\right).$$

The subcycle type of the matrix $\operatorname{diag}(A_1, A_2)$ *is the $\star$-product of the subcycle types of A_1 and A_2. (The n-th power with respect to the multiplication $\star$ will be denoted by $(\ldots)^{\star n}$.) The operator $\star$ can be extended linearly to $\mathbb{Q}[\{z_{n,\alpha} \mid n \in \mathbb{N}^*,\ \alpha \in \mathbb{F}_q^*\}]$.*

Proof: Assume that $v_1 \in \mathbb{F}_q^{k_1} \setminus \{0\}$ belongs to a subcycle of A_1 of length s_1 with integral element β^{r_1}. Then also $(v_1^\top \mid \mathbf{0}_{k_2}^\top)^\top$ belongs to a subcycle of $\operatorname{diag}(A_1, A_2)$ of length s_1 with integral element β^{r_1}. (In the present section we write vectors as columns, thus $(v_1^\top \mid \mathbf{0}_{k_2}^\top)^\top$ is a column of length $k_1 + k_2$.) Similarly, the subcycles of A_2 containing a vector $v_2 \in \mathbb{F}_q^{k_2} \setminus \{0\}$ correspond to the subcycles of $\operatorname{diag}(A_1, A_2)$ containing $(\mathbf{0}_{k_1}^\top \mid v_2^\top)^\top$. Thus, we only have to investigate pairs $(v_1^\top \mid v_2^\top)^\top \in \mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2}$ with $v_1 \neq 0$ and $v_2 \neq 0$. Moreover, we suppose that v_1 belongs to a subcycle of A_1 of length s_1 with integral element β^{r_1} and v_2 to a subcycle of A_2 of length s_2 with integral element β^{r_2}. Then $\operatorname{lcm}(s_1, s_2)$ is equal to

$$\min\left\{n \in \mathbb{N}^* \mid \exists\, \alpha_1, \alpha_2 \in \mathbb{F}_q^* :\ \operatorname{diag}(A_1^n, A_2^n) \cdot (v_1^\top \mid v_2^\top)^\top = (\alpha_1 v_1^\top \mid \alpha_2 v_2^\top)^\top\right\}.$$

In particular, for $i = 1, 2$ we have

$$\alpha_i = (\beta^{r_i})^{\operatorname{lcm}(s_1,s_2)/s_i} = \beta^{r_i \operatorname{lcm}(s_1,s_2)/s_i}.$$

Now we determine the length s_3 and the integral element α of the subcycle containing $(v_1^\top \mid v_2^\top)^\top$. They satisfy the identity

$$s_3 = \min\left\{n \in \mathbb{N}^* \mid \exists\, \alpha \in \mathbb{F}_q^* :\ \operatorname{diag}(A_1^n, A_2^n)(v_1^\top \mid v_2^\top)^\top = \alpha (v_1^\top \mid v_2^\top)^\top\right\}.$$

Thus, we have to determine the smallest positive integer n such that $\alpha_1^n = \alpha_2^n$. This number is the multiplicative order of $\alpha_1 \alpha_2^{-1}$ in $\mathbb{F}_q^*$, which can be computed by

$$\operatorname{ord}(\alpha_1 \alpha_2^{-1}) = \frac{\operatorname{ord}(\beta)}{\gcd(\operatorname{ord}(\beta), r_1 \operatorname{lcm}(s_1, s_2)/s_1 - r_2 \operatorname{lcm}(s_1, s_2)/s_2)}.$$

Hence, $s_3 = \operatorname{lcm}(s_1, s_2)\operatorname{ord}(\alpha_1\alpha_2^{-1})$ and the corresponding integral element is of the form

$$\beta^{r_3} = \alpha_i^{\operatorname{ord}(\alpha_1\alpha_2^{-1})} = \beta^{r_i \operatorname{lcm}(s_1,s_2)\operatorname{ord}(\alpha_1\alpha_2^{-1})/s_i} = \beta^{r_i s_3/s_i}.$$

If the subcycle type of A_i contains a term $z^{j_i}_{s_i,\beta^{r_i}}$, then, by construction, there are exactly $s_i j_i$ elements in $\mathbb{F}_q^{k_i} \setminus \{0\}$ in the subcycles of A_i of length s_i with integral element β^{r_i}, for $i = 1, 2$. Consequently, all pairs of these elements, these are $s_1 j_1 s_2 j_2$ vectors in $\mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2}$, belong to subcycles of $\operatorname{diag}(A_1, A_2)$ of length s_3 with integral element β^{r_3}. Since all these subcycles are of length s_3, by this construction we get exactly $s_1 j_1 s_2 j_2 / s_3$ subcycles of length s_3 with integral element β^{r_3}. This yields the factor $z^{s_1 j_1 s_2 j_2/s_3}_{s_3,\beta^{r_3}} = z^{j_1}_{s_1,\beta^{r_1}} \circledast z^{j_2}_{s_2,\beta^{r_2}}$ in the subcycle type of $\operatorname{diag}(A_1, A_2)$. Therefore, the subcycle type of $\operatorname{diag}(A_1, A_2)$ is the product of expressions of the form

$$z^{j_1}_{s_1,\beta^{r_1}}, \quad z^{j_2}_{s_2,\beta^{r_2}}, \quad \left(z^{j_1}_{s_1,\beta^{r_1}} \circledast z^{j_2}_{s_2,\beta^{r_2}}\right)$$

which are due to the vectors of the form $(v_1^\top \mid \mathbf{0}_{k_2}^\top)^\top$, $(\mathbf{0}_{k_1}^\top \mid v_2^\top)^\top$, and $(v_1^\top \mid v_2^\top)^\top$, where $v_i \in \mathbb{F}_q^{k_i} \setminus \{0\}$ is contained in a subcycle of A_i of length s_i with integral element β^{r_i}, for $i = 1, 2$. Finally considering all possible combinations $(v_1^\top \mid v_2^\top)^\top$ yields the desired subcycle type of $\operatorname{diag}(A_1, A_2)$. □

The multiplication $\star$ is associative and commutative (cf. Exercise 6.3.11). Moreover the empty product is defined to be 1.

Collecting all the results of the present section, we have proved the following formula for the computation of the cycle index $C(\mathrm{PGL}_k(q), \mathrm{PG}^*_{k-1}(q))$.

6.3.26 Theorem *Assume that f_i for $i \in t_k$ are the monic, irreducible polynomials of degree $d_i \le k$ over $\mathbb{F}_q$ which can occur as divisors of a characteristic polynomial of a regular matrix of rank k (thus $f_i \neq x$). For $n > 1$ we use 6.3.23.3 in order to compute both the subexponents $s_{i,n}$ of f_i^n and the corresponding integral elements $\alpha_{i,n}$ from $s_{i,1}$, the subexponent of f_i, and from $\alpha_{i,1}$, the integral element of f_i.*

The subcycle index $SC(\mathrm{GL}_k(q), \mathbb{F}_q^k \setminus \{0\})$ of the action of $\mathrm{GL}_k(q)$ on $\mathbb{F}_q^k \setminus \{0\}$ is

$$\frac{1}{[q]_k} \sum_\gamma \sum_a \frac{[q]_k}{\prod_{i\in t_k} b(d_i, a^{(i)})} \bigstar_{i\in t_k} \bigstar_{j=1}^{\gamma_i} \left(\prod_{\ell=1}^{j} z^{u_{i,\ell}}_{s_{i,\ell},\alpha_{i,\ell}}\right)^{\star a_j^{(i)}},$$

where $u_{i,\ell}$ is given by

$$u_{i,\ell} = \frac{q^{\ell d_i} - q^{(\ell-1)d_i}}{s_{i,\ell}}.$$

Moreover, $[q]_k$ denotes the order of $\mathrm{GL}_k(q)$, and $b(d_i, a^{(i)})$ is the order of the centralizer of $D(f_i, a^{(i)})$ as computed in 6.3.16. The first sum is taken over all solutions

$\gamma = (\gamma_0, \ldots, \gamma_{t_k-1}) \in \mathbb{N}^{t_k}$ *of 6.3.13. For each solution* γ *and for each* $i \in t_k$ *we have to determine the set of all cycle types of* γ_i

$$CT(\gamma_i) := \{a \mid a \vdash \gamma_i\}.$$

The second sum is taken over all t_k*-tuples*

$$a = (a^{(0)}, \ldots, a^{(t_k-1)}) \in \underset{i \in t_k}{\times} CT(\gamma_i).$$

As already mentioned before, by omitting the second index of each indeterminate and by dividing the exponent of each indeterminate (in the subcycle index of $\mathrm{GL}_k(q)$*) by* $q-1$*, we obtain the cycle index of the action of* $\mathrm{PGL}_k(q)$ *on* $\mathrm{PG}^*_{k-1}(q)$. □

Example In order to present a nontrivial example we determine the cycle index of $\mathrm{PGL}_3(3)$ acting on $\mathrm{PG}^*_2(3)$. At first we need a list of all monic, irreducible polynomials different from $f = x$ of degree at most 3 over $\mathbb{F}_3$ together with their exponents, subexponents and integral elements (cf. Table 6.4). **6.3.27**

Table 6.4 The irreducible polynomials of degree at most 3 over $\mathbb{F}_3$ different from $f = x$

i	f_i	d_i	e_i	s_i	α_i
0	$x+1$	1	2	1	2
1	$x+2$	1	1	1	1
2	x^2+1	2	4	2	2
3	x^2+x+2	2	8	4	2
4	x^2+2x+2	2	8	4	2
5	x^3+2x+1	3	26	13	2
6	x^3+2x+2	3	13	13	1
7	x^3+x^2+2	3	13	13	1
8	x^3+x^2+x+2	3	13	13	1
9	x^3+x^2+2x+1	3	26	13	2
10	x^3+2x^2+1	3	26	13	2
11	x^3+2x^2+x+1	3	26	13	2
12	x^3+2x^2+2x+2	3	13	13	1

With these polynomials we determine the following normal forms. In addition to each normal form we also indicate its subcycle type.

- The polynomials of degree 3 occur only in the form

$$D(f_i, (1, 0, \ldots)) \text{ for } i \geq 5.$$

They have subcycle types

$$z_{s_i,\alpha_i}^{26/s_i} = z_{13,\alpha_i}^2.$$

– In the normal forms of $\mathrm{GL}_3(3)$ companion matrices of polynomials of degree 2 occur only in combination with polynomials of degree 1. These normal forms are described by

$$\mathrm{diag}(D(f_i,(1,0,\ldots)),D(f_j,(1,0,\ldots))) \text{ for } 0\le i\le 1,\ 2\le j\le 4.$$

They have subcycle types

$$z_{s_i,\alpha_i}^{2/s_i}\star z_{s_j,\alpha_j}^{8/s_j}=z_{1,\alpha_i}^{2}\star z_{s_j,2}^{8/s_j}.$$

– In all other normal forms just polynomials of degree 1 occur. For $0\le i,j\le 1$ and $i\ne j$ they can be described as:

normal form	subcycle type
$D(f_i,(3,0,\ldots))$	$\left(z_{1,\alpha_i}^2\right)^{\star 3}$
$D(f_i,(1,1,0,\ldots))$	$z_{1,\alpha_i}^2\star\left(z_{1,\alpha_i}^2z_{3,\alpha_i}^2\right)$
$D(f_i,(0,0,1,0,\ldots))$	$z_{1,\alpha_i}^2z_{3,\alpha_i}^8$
$\mathrm{diag}(D(f_i,(2,0,\ldots)),D(f_j,(1,0,\ldots)))$	$\left(z_{1,\alpha_i}^2\right)^{\star 2}\star z_{1,\alpha_j}^2$
$\mathrm{diag}(D(f_i,(0,1,0,\ldots)),D(f_j,(1,0,\ldots)))$	$\left(z_{1,\alpha_i}^2z_{3,\alpha_i}^2\right)\star z_{1,\alpha_j}^2$

In order to derive the subcycle index of $\mathrm{GL}_3(3)$ acting on $\mathbb{F}_3^3\setminus\{0\}$, the subcycle type of every normal form must be multiplied by the cardinality of its conjugacy class and, finally, the sum of these subcycle types must be divided by the order of $\mathrm{GL}_3(3)$.

$$\begin{aligned}SC(\mathrm{GL}_3(3),\mathbb{F}_3^3\setminus\{0\}) &= 1/11232\Big(1728z_{13,1}^2+1728z_{13,2}^2+702z_{1,1}^2z_{2,2}^4z_{4,1}^4\\ &+702z_{1,2}^2z_{2,2}^4z_{4,1}^4+1404z_{1,1}^2z_{4,2}^2z_{8,1}^2+1404z_{1,2}^2z_{4,2}^2z_{8,1}^2+z_{1,1}^{26}+z_{1,2}^{26}\\ &+104z_{1,1}^8z_{3,1}^6+104z_{1,2}^8z_{3,2}^6+624z_{1,1}^2z_{3,1}^8+624z_{1,2}^2z_{3,2}^8+117z_{1,1}^8z_{1,2}^2z_{2,1}^8\\ &+117z_{1,2}^8z_{1,1}^2z_{2,1}^8+936z_{1,1}^2z_{1,2}^2z_{2,1}^2z_{3,1}^2z_{6,1}^2+936z_{1,1}^2z_{1,2}^2z_{2,1}^2z_{3,2}^2z_{6,1}^2\Big).\end{aligned}$$

This yields the cycle index

$$\begin{aligned}C(\mathrm{PGL}_3(3),\mathrm{PG}_2^*(3)) &= 1/5616\Big(1728z_{13}+1404z_1z_4z_8\\ &+624z_1z_3^4+702z_1z_2^2z_4^2+936z_1^2z_2z_3z_6+104z_1^4z_3^3+117z_1^5z_2^4+z_1^{13}\Big).\end{aligned}$$ ◇

The computation of the subcycle index can still be simplified. Actually, it is not necessary to know all the different monic, irreducible polynomials over $\mathbb{F}_q$ of degree at most k. As we have seen in part 9 of 6.3.23, for each $(s,\alpha)\in S(d,q)$ it is possible to determine the exact number of monic, irreducible polynomials over $\mathbb{F}_q$ of degree d with subexponent s and integral element α. Since the subcycle type of $H(f^n)$ depends only on the three parameters (d,s,α) and on

n, of course, we need not determine the conjugacy classes of $\mathrm{GL}_k(q)$ themselves. It suffices to know how many different monic, irreducible polynomials with parameters (d, s, α, n) occur in the normal forms. This approach motivates the following formula for the computation of the subcycle index of $\mathrm{GL}_k(q)$ on $\mathbb{F}_q^k \setminus \{0\}$:

$$\sum_{c \vdash k} \overset{k}{\underset{d=1}{\star}} \sum_{r} \overset{}{\underset{(s,\alpha)\in S(d,q)}{\star}} \sum_{t} \xi(m(d,s,\alpha),t) \overset{r(s,\alpha)}{\underset{j=1}{\star}} \left(\sum_{a \vdash j} \frac{1}{b(d,a)} z(d,s,\alpha,a) \right)^{\star t_j}$$

Here $z(d, s, \alpha, a)$ stands for the subcycle type of a matrix $D(f, a)$, where f is an arbitrary monic irreducible polynomial in $\mathbb{F}_q[x]$ of degree d with subexponent s and integral element α, and where $a \vdash j$ is a cycle type of j. This subcycle type can be computed by

$$z(d,s,\alpha,a) = \overset{j}{\underset{\ell=1}{\star}} \left(\prod_{n=1}^{\ell} z_{s_n,\alpha_n}^{u_n} \right)^{\star a_\ell},$$

where s_n stands for sp^t and α_n for α^{p^t}, where p is the characteristic of $\mathbb{F}_q$, and t is the smallest nonnegative integer such that $p^t \geq n$. The exponents u_n are computed via

$$u_n = \frac{q^{nd} - q^{(n-1)d}}{s_n}.$$

The first sum in the subcycle index of $\mathrm{GL}_k(q)$ is taken over all cycle types $c \vdash k$. Here c is of the form $c = (c_1, \ldots, c_k)$ and the number c_d represents the number of monic, irreducible polynomials of degree d (counted with their multiplicities), which occur as factors of the characteristic polynomial of a normal form in $\mathrm{GL}_k(q)$.

The second sum is taken over all functions r from $S(d, q)$ to $\mathbb{N}$ which satisfy

$$\sum_{(s,\alpha)\in S(d,q)} r(s,\alpha) = c_d.$$

If the characteristic polynomial has exactly c_d irreducible factors of degree d, then the value $r(s, \alpha)$ stands for the number of irreducible factors with parameters (d, s, α).

The third sum is taken over all cycle types $t \vdash r(s, \alpha)$ with the additional property that

$$\sum_j t_j \leq m(d,s,\alpha).$$

Such a cycle type t describes the type of a set-partition of a set of cardinality $r(s, \alpha)$ into at most $m(d, s, \alpha)$ subsets. For any $t \vdash r(s, \alpha)$ there are

$$\xi(m(d,s,\alpha),t) := \binom{m(d,s,\alpha)}{t_1, t_2 \ldots, m(d,s,\alpha) - \sum_j t_j}$$

possibilities to choose – among the $m(d,s,\alpha)$ different monic, irreducible polynomials with parameters (d,s,α) – for each j exactly t_j polynomials, which occur with the multiplicity j in the considered characteristic polynomial.

Finally the last sum is taken over all cycle types $a \vdash j$. These cycle types describe all possible normal forms whose characteristic polynomials are the j-th power of one monic irreducible polynomial. The reader should recall that the characteristic polynomial of $D(f,a)$ equals f^j in this situation.

6.3.28 **Example** We continue 6.3.27 by determining the sets $E(d,q)$, $S(d,q)$ for $q = 3$, $1 \le d \le 3$, and the numbers $\nu(d,e)$ and $m(d,s,\alpha)$ for $e \in E(d,q)$ and $(s,\alpha) \in S(d,q)$. This provides all the necessary information for computing the subcycle index of $\mathrm{GL}_3(3)$. In fact, the information contained in Table 6.4 is not needed for this purpose.

$E(1,3) = \{1,2\}$	$\nu(1,1) = 1$	$\nu(1,2) = 1$
$E(2,3) = \{4,8\}$	$\nu(2,4) = 1$	$\nu(2,8) = 2$
$E(3,3) = \{13,26\}$	$\nu(3,13) = 4$	$\nu(3,26) = 4$
$S(1,3) = \{(1,1),(1,2)\}$	$m(1,1,1) = 1$	$m(1,1,2) = 1$
$S(2,3) = \{(2,2),(4,2)\}$	$m(2,2,2) = 1$	$m(2,4,2) = 2$
$S(3,3) = \{(13,1),(13,2)\}$	$m(3,13,1) = 4$	$m(3,13,2) = 4$

◇

In [142], explicit formulae for the numbers T_{nkq}, $\overline{T}_{nkq}$, V_{nkq}, $\overline{V}_{nkq}$, R_{nkq}, and $\overline{R}_{nkq}$ are given for $k \le 3$. This is done by a careful analysis of the conjugacy classes of elements of $\mathrm{PGL}_k(q)$. The formulae result from counting fixed points and applying the Lemma of Cauchy–Frobenius. Since in the general formula too many different cases must be considered, we present some of the resulting formulae for $n = 7$.

For example, for any field of characteristic $p = 2$ we obtain

$$\overline{T}_{73q} = \frac{q^6+7q^5+9q^4+183q^3+632q^2-364q+1344}{5040} + \\ + \left[\frac{q^2+18q+20}{36}\right]_{3|q-1} + \left[\frac{16}{5}\right]_{5|q-1} + \left[\frac{6}{7}\right]_{7|q-1},$$

where

$$[x]_{a|b} := \begin{cases} x & \text{if } a \mid b, \\ 0 & \text{else.} \end{cases}$$

For characteristic $p > 2$ we get

$$\overline{T}_{73q} = \frac{q^6+7q^5+9q^4+183q^3+1157q^2+56q-201}{5040} + \\ + \left[\frac{q^2+10q-15}{72}\right]_{3|q} + \left[\frac{q^2+18q+77}{36}\right]_{3|q-1} + \left[\frac{4q+13}{12}\right]_{4|q-1} +$$

$$+\left[\frac{1}{3}\right]_{12|q-1}+\left[\frac{1}{6}\right]_{12|q-9}+\left[\frac{16}{5}\right]_{5|q-1}+\left[\frac{2}{5}\right]_{5|q}+\left[\frac{8}{7}\right]_{7|q-1}+$$

$$+\left[\frac{6}{7}\right]_{7|q+1}+\left[\frac{2}{7}\right]_{7|q}+\left[\frac{2}{7}\right]_{7|q^2+q+1}.$$

Similar formulae can be found for $\overline{V}_{nkq}$ and $\overline{R}_{nkq}$. For $p = 2$ and $n = 7$ we obtain

$$\overline{V}_{73q} = \frac{q^6+7q^5+8q^4+197q^3+456q^2+420q+384}{5040}+$$

$$+\left[\frac{q^2+14q+36}{36}\right]_{3|q-1}+\left[\frac{14}{5}\right]_{5|q-1}+\left[\frac{3}{7}\right]_{7|q-1},$$

and

$$\overline{R}_{73q} = \frac{q^6+7q^5+8q^4+190q^3+414q^2+588q+272}{5040}+$$

$$+\left[\frac{q^2+14q+40}{36}\right]_{3|q-1}+[2]_{5|q-1}+\left[\frac{3}{7}\right]_{7|q-1}.$$

For $p > 2$ and $n = 7$ we have

$$\overline{V}_{73q} = \frac{q^6+7q^5+8q^4+197q^3+981q^2+1050q-1896}{5040}+$$

$$+\left[\frac{q^2+6q-3}{72}\right]_{3|q}+\left[\frac{q^2+14q+81}{36}\right]_{3|q-1}+\left[\frac{4q+13}{12}\right]_{4|q-1}+$$

$$+\left[\frac{1}{3}\right]_{12|q-1}+\left[\frac{1}{6}\right]_{12|q-9}+\left[\frac{14}{5}\right]_{5|q-1}+\left[\frac{2}{5}\right]_{5|q}+\left[\frac{5}{7}\right]_{7|q-1}+$$

$$+\left[\frac{3}{7}\right]_{7|q+1}+\left[\frac{1}{7}\right]_{7|q}+\left[\frac{2}{7}\right]_{7|q^2+q+1}$$

and

$$\overline{R}_{73q} = \frac{q^6+7q^5+8q^4+190q^3+939q^2+903q-2008}{5040}+$$

$$+\left[\frac{q^2+6q+13}{72}\right]_{3|q}+\left[\frac{q^2+14q+85}{36}\right]_{3|q-1}+\left[\frac{2q+5}{6}\right]_{4|q-1}+$$

$$+\left[\frac{1}{3}\right]_{12|q-1}+\left[\frac{1}{6}\right]_{12|q-9}+[2]_{5|q-1}+\left[\frac{1}{5}\right]_{5|q}+\left[\frac{5}{7}\right]_{7|q-1}+$$

$$+\left[\frac{3}{7}\right]_{7|q+1}+\left[\frac{1}{7}\right]_{7|q}+\left[\frac{2}{7}\right]_{7|q^2+q+1}.$$

The expressions for T_{nkq}, V_{nkq}, and R_{nkq} are even more complicated.

Exercises

E.6.3.1 **Exercise** Prove that the orders of the groups $\mathrm{GL}_k(q)$ and $\mathrm{PGL}_k(q)$ are given by

$$|\mathrm{GL}_k(q)| = (q^k-1)(q^k-q)\dots(q^k-q^{k-1}) =: [q]_k, \qquad |\mathrm{PGL}_k(q)| = \frac{[q]_k}{q-1}.$$

E.6.3.2 **Exercise** Let ${}_GX$ be a group action. Prove that conjugate elements $g_1, g_2 \in G$ induce permutations $\overline{g_1}, \overline{g_2}$ of X of the same cycle type. In other words, if $g_2 = gg_1g^{-1}$ for some $g \in G$, then $a_i(\overline{g_1}) = a_i(\overline{g_2})$ for all i. Hint: Which relation holds between the cycles of π and $\rho\pi\rho^{-1}$ for $\pi, \rho \in S_X$?

E.6.3.3 **Exercise** Prove that the cycle index of the natural action of the symmetric group S_n on the set $n = \{0, 1, \dots, n-1\}$ is given by

$$C(S_n, n) = \sum_{a \vdash n} \prod_{k=1}^{n} \frac{1}{a_k! k^{a_k}} z_k^{a_k}.$$

Hint: Prove first the following propositions:

1. The cycle type $a(\pi)$ of a permutation $\pi \in S_n$ characterizes the conjugacy class of π in S_n. Hence, elements in different conjugacy classes of S_n have different cycle types.
2. For each cycle type $a \vdash n$ there exist permutations $\pi \in S_n$ with $a(\pi) = a$.
3. The number of elements of S_n of cycle type $a \vdash n$ is

$$\frac{n!}{\prod_{k=1}^{n} a_k! k^{a_k}}.$$

E.6.3.4 **Exercise** Let A be an endomorphism of $\mathbb{F}^k$. Show that $\mathbb{F}^k$ together with the outer composition 6.3.5 is an $\mathbb{F}[x]$-module, that is, for all $f, f_1, f_2 \in \mathbb{F}[x]$ and all $v, v_1, v_2 \in \mathbb{F}^k$ we have $f_1(f_2 v) = (f_1 f_2)v$, $(f_1 + f_2)v = f_1 v + f_2 v$, $f(v_1 + v_2) = fv_1 + fv_2$ and $1_{\mathbb{F}} v = v$.

E.6.3.5 **Exercise** Prove 6.3.6.

E.6.3.6 **Exercise** Prove that 6.3.7 is a decomposition of 1 into pairwise orthogonal idempotents.

Exercise Let A be an endomorphism of $\mathbb{F}^k$. Prove that $\mathbb{F}^k$ is a cyclic $\mathbb{F}[x]$-module if and only if the characteristic polynomial χ_A and the minimal polynomial M_A of A coincide. **E.6.3.7**

Exercise Prove 6.3.17. **E.6.3.8**

Exercise Prove that conjugate matrices in $\mathrm{GL}_k(q)$ have the same subcycle type. **E.6.3.9**

Exercise Prove 6.3.23. **E.6.3.10**

Exercise Prove that the multiplication $\star$ of 6.3.25 is commutative and associative. **E.6.3.11**

6.4 Numerical Data for Linear Isometry Classes 6.4

In Tables 6.7–6.12 we present the numbers of linear isometry classes of nonredundant linear codes and of projective linear codes for $q = 2, 3, 4$. For computing these numbers we had to determine the auxiliary data T_{nkq} and $\overline{T}_{nkq}$ given in Tables 6.13–6.18. The numbers of all linear isometry classes of linear codes are displayed in Tables 6.19–6.20. Some values for U_{nk2} were already presented in Table 6.2. Finally the numbers of indecomposable linear codes are presented in Tables 6.21–6.26. These numbers were computed with the computer algebra system SYMMETRICA ([190]). Due to restrictions of the page size in some tables the entries for $n = 13$ or $n = 14$ are omitted. It is also possible to determine tables of $\begin{bmatrix} n \\ k \end{bmatrix}(q)$, T_{nkq}, $\overline{T}_{nkq}$, V_{nkq}, $\overline{V}_{nkq}$, U_{nkq}, R_{nkq} and $\overline{R}_{nkq}$ with the software from the attached CD.

Table 6.5 Values of $\begin{bmatrix} n \\ k \end{bmatrix}(3)$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	4	1	0	0
3	13	13	1	0
4	40	130	40	1
5	121	1 210	1 210	121
6	364	11 011	33 880	11 011
7	1 093	99 463	925 771	925 771
8	3 280	896 260	25 095 280	75 913 222
9	9 841	8 069 620	678 468 820	6 174 066 262
10	29 524	72 636 421	18 326 727 760	500 777 836 042
11	88 573	653 757 313	494 894 285 941	40 581 331 447 162
12	265 720	5 883 904 390	13 362 799 477 720	3 287 582 741 506 063
13	797 161	52 955 405 230	360 801 469 802 830	266 307 564 861 468 823

Table 6.6 Values of $\begin{bmatrix} n \\ k \end{bmatrix}(4)$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	5	1	0	0
3	21	21	1	0
4	85	357	85	1
5	341	5 797	5 797	341
6	1 365	93 093	376 805	93 093
7	5 461	1 490 853	24 208 613	24 208 613
8	21 845	23 859 109	1 550 842 085	6 221 613 541
9	87 381	381 767 589	99 277 752 549	1 594 283 908 581
10	349 525	6 108 368 805	6 354 157 930 725	408 235 958 349 285
11	1 398 101	97 734 250 405	406 672 215 935 205	104 514 759 495 347 685

Table 6.7 Values of V_{nk2}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	1	0	0	0	0	0
3	1	2	1	0	0	0	0
4	1	3	3	1	0	0	0
5	1	4	6	4	1	0	0
6	1	6	12	11	5	1	0
7	1	7	21	27	17	6	1
8	1	9	34	63	54	25	7
9	1	11	54	134	163	99	35
10	1	13	82	276	465	385	170
11	1	15	120	544	1 283	1 472	847
12	1	18	174	1 048	3 480	5 676	4 408
13	1	20	244	1 956	9 256	22 101	24 297
14	1	23	337	3 577	24 282	87 404	143 270

Table 6.8 Values of V_{nk3}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	1	0	0	0	0	0
3	1	2	1	0	0	0	0
4	1	4	3	1	0	0	0
5	1	5	8	4	1	0	0
6	1	8	19	15	5	1	0
7	1	10	39	50	24	6	1
8	1	14	78	168	118	37	7
9	1	17	151	538	628	255	53
10	1	22	280	1 789	3 759	2 266	518
11	1	26	506	5 981	26 131	28 101	7 967
12	1	33	904	20 502	208 045	500 237	230 165
13	1	38	1 571	70 440	1 788 149	11 165 000	11 457 192
14	1	46	2 687	241 252	15 675 051	269 959 051	734 810 177

Table 6.9 Values of V_{nk4}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	1	0	0	0	0	0
3	1	2	1	0	0	0	0
4	1	4	3	1	0	0	0
5	1	6	9	4	1	0	0
6	1	9	24	17	5	1	0
7	1	12	55	70	28	6	1
8	1	17	131	323	189	44	7
9	1	22	318	1 784	1 976	490	65
10	1	30	772	12 094	36 477	13 752	1 240
11	1	37	1 881	89 437	923 978	948 361	102 417
12	1	48	4 568	668 922	25 124 571	91 149 571	25 983 495
13	1	59	10 857	4 843 901	665 246 650	9 163 203 790	9 229 228 790

Table 6.10 Values of $\overline{V}_{nk2}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	0	1	0	0	0	0	0
3	0	1	1	0	0	0	0
4	0	0	2	1	0	0	0
5	0	0	1	3	1	0	0
6	0	0	1	4	4	1	0
7	0	0	1	5	8	5	1
8	0	0	0	6	15	14	6
9	0	0	0	5	29	38	22
10	0	0	0	4	46	105	80
11	0	0	0	3	64	273	312
12	0	0	0	2	89	700	1 285
13	0	0	0	1	112	1 794	5 632
14	0	0	0	1	128	4 579	26 792

Table 6.11 Values of $\overline{V}_{nk3}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	0	1	0	0	0	0	0
3	0	1	1	0	0	0	0
4	0	1	2	1	0	0	0
5	0	0	3	3	1	0	0
6	0	0	4	8	4	1	0
7	0	0	4	19	15	5	1
8	0	0	3	44	61	26	6
9	0	0	3	91	277	162	40
10	0	0	2	199	1 439	1 381	375
11	0	0	1	401	8 858	17 200	5 923
12	0	0	1	806	62 311	311 580	182 059
13	0	0	1	1 504	459 828	6 876 068	9 427 034
14	0	0	0	2 659	3 346 151	159 373 844	608 045 192

Table 6.12 Values of $\overline{V}_{nk4}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	0	1	0	0	0	0	0
3	0	1	1	0	0	0	0
4	0	1	2	1	0	0	0
5	0	1	4	3	1	0	0
6	0	0	8	10	4	1	0
7	0	0	10	35	19	5	1
8	0	0	13	136	122	33	6
9	0	0	17	657	1 320	376	52
10	0	0	19	3 849	25 619	11 632	1 057
11	0	0	19	23 456	645 751	845 949	95 960
12	0	0	17	138 200	16 822 798	81 806 606	25 058 580
13	0	0	13	761 039	418 686 704	8 140 667 601	8 935 079 862

Table 6.13 Values of T_{nk2}

$n\backslash k$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	1	2	2	2	2	2	2
3	1	3	4	4	4	4	4
4	1	4	7	8	8	8	8
5	1	5	11	15	16	16	16
6	1	7	19	30	35	36	36
7	1	8	29	56	73	79	80
8	1	10	44	107	161	186	193
9	1	12	66	200	363	462	497
10	1	14	96	372	837	1 222	1 392
11	1	16	136	680	1 963	3 435	4 282
12	1	19	193	1 241	4 721	10 397	14 805
13	1	21	265	2 221	11 477	33 578	57 875
14	1	24	361	3 938	28 220	115 624	258 894

Table 6.14 Values of T_{nk3}

$n\backslash k$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	1	2	2	2	2	2	2
3	1	3	4	4	4	4	4
4	1	5	8	9	9	9	9
5	1	6	14	18	19	19	19
6	1	9	28	43	48	49	49
7	1	11	50	100	124	130	131
8	1	15	93	261	379	416	423
9	1	18	169	707	1 335	1 590	1 643
10	1	23	303	2 092	5 851	8 117	8 635
11	1	27	533	6 514	32 645	60 746	68 713
12	1	34	938	21 440	229 485	729 722	959 887
13	1	39	1 610	72 050	1 860 199	13 025 199	24 482 391
14	1	47	2 734	243 986	15 919 037	285 878 088	1 020 688 265

Table 6.15 Values of T_{nk4}

$n\backslash k$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	1	2	2	2	2	2	2
3	1	3	4	4	4	4	4
4	1	5	8	9	9	9	9
5	1	7	16	20	21	21	21
6	1	10	34	51	56	57	57
7	1	13	68	138	166	172	173
8	1	18	149	472	661	705	712
9	1	23	341	2 125	4 101	4 591	4 656
10	1	31	803	12 897	49 374	63 126	64 366
11	1	38	1 919	91 356	1 015 334	1 963 695	2 066 112
12	1	49	4 617	673 539	25 798 110	116 947 681	142 931 176
13	1	60	10 917	4 854 818	670 101 468	9 833 305 258	19 062 534 048

Table 6.16 Values of $\overline{T}_{nk2}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	0	1	1	1	1	1	1
3	0	1	2	2	2	2	2
4	0	0	2	3	3	3	3
5	0	0	1	4	5	5	5
6	0	0	1	5	9	10	10
7	0	0	1	6	14	19	20
8	0	0	0	6	21	35	41
9	0	0	0	5	34	72	94
10	0	0	0	4	50	155	235
11	0	0	0	3	67	340	652
12	0	0	0	2	91	791	2 076
13	0	0	0	1	113	1 907	7 539
14	0	0	0	1	129	4 708	31 500

Table 6.17 Values of $\overline{T}_{nk3}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	0	1	1	1	1	1	1
3	0	1	2	2	2	2	2
4	0	1	3	4	4	4	4
5	0	0	3	6	7	7	7
6	0	0	4	12	16	17	17
7	0	0	4	23	38	43	44
8	0	0	3	47	108	134	140
9	0	0	3	94	371	533	573
10	0	0	2	201	1 640	3 021	3 396
11	0	0	1	402	9 260	26 460	32 383
12	0	0	1	807	63 118	374 698	556 757
13	0	0	1	1 505	461 333	7 337 401	16 764 435
14	0	0	0	2 659	3 348 810	162 722 654	770 767 846

Table 6.18 Values of $\overline{T}_{nk4}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	0	1	1	1	1	1	1
3	0	1	2	2	2	2	2
4	0	1	3	4	4	4	4
5	0	1	5	8	9	9	9
6	0	0	8	18	22	23	23
7	0	0	10	45	64	69	70
8	0	0	13	149	271	304	310
9	0	0	17	674	1 994	2 370	2 422
10	0	0	19	3 868	29 487	41 119	42 176
11	0	0	19	23 475	669 226	1 515 175	1 611 135
12	0	0	17	138 217	16 961 015	98 767 621	123 826 201
13	0	0	13	761 052	419 447 756	8 560 115 357	17 495 195 219

Table 6.19 Values of U_{nk3}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	2	1	0	0	0	0	0
3	3	3	1	0	0	0	0
4	4	7	4	1	0	0	0
5	5	12	12	5	1	0	0
6	6	20	31	20	6	1	0
7	7	30	70	70	30	7	1
8	8	44	148	238	148	44	8
9	9	61	299	776	776	299	61
10	10	83	579	2 565	4 535	2 565	579
11	11	109	1 085	8 546	30 666	30 666	8 546
12	12	142	1 989	29 048	238 711	530 903	238 711
13	13	180	3 560	99 488	2 026 860	11 695 903	11 695 903
14	14	226	6 247	340 740	17 701 911	281 654 954	746 506 080

Table 6.20 Values of U_{nk4}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	2	1	0	0	0	0	0
3	3	3	1	0	0	0	0
4	4	7	4	1	0	0	0
5	5	13	13	5	1	0	0
6	6	22	37	22	6	1	0
7	7	34	92	92	34	7	1
8	8	51	223	415	223	51	8
9	9	73	541	2 199	2 199	541	73
10	10	103	1 313	14 293	38 676	14 293	1 313
11	11	140	3 194	103 730	962 654	962 654	103 730
12	12	188	7 762	772 652	26 087 225	92 112 225	26 087 225

Table 6.21 Values of R_{nk2}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	0	0	0	0	0	0
3	1	1	0	0	0	0	0
4	1	1	1	0	0	0	0
5	1	2	2	1	0	0	0
6	1	3	5	3	1	0	0
7	1	4	10	10	4	1	0
8	1	5	18	28	18	5	1
9	1	7	31	71	71	31	7
10	1	8	51	165	250	165	51
11	1	10	79	361	809	809	361
12	1	12	121	754	2 484	3 759	2 484
13	1	14	177	1 503	7 240	16 749	16 749
14	1	16	254	2 893	20 341	72 828	113 662

Table 6.22 Values of R_{nk3}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	0	0	0	0	0	0
3	1	1	0	0	0	0	0
4	1	2	1	0	0	0	0
5	1	3	3	1	0	0	0
6	1	5	10	5	1	0	0
7	1	7	24	24	7	1	0
8	1	10	55	105	55	10	1
9	1	13	116	403	403	116	13
10	1	17	231	1 506	3 000	1 506	231
11	1	21	438	5 425	23 579	23 579	5 425
12	1	27	813	19 440	199 473	469 473	199 473
13	1	32	1 451	68 478	1 758 953	10 925 684	10 925 684
14	1	39	2 533	237 709	15 575 102	267 929 503	723 109 414

Table 6.23 Values of R_{nk4}

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	0	0	0	0	0	0
3	1	1	0	0	0	0	0
4	1	2	1	0	0	0	0
5	1	4	4	1	0	0	0
6	1	6	14	6	1	0	0
7	1	9	38	38	9	1	0
8	1	13	104	238	104	13	1
9	1	18	276	1 573	1 573	276	18
10	1	25	711	11 566	34 288	11 566	711
11	1	32	1 793	88 140	909 664	909 664	88 140
12	1	42	4 446	665 736	25 020 688	90 186 547	25 020 688
13	1	53	10 691	4 836 136	664 473 418	9 137 113 963	9 137 113 963

Table 6.24 Values of $\overline{R}_{nk2}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	1	0	0	0	0	0
4	0	0	1	0	0	0	0
5	0	0	1	1	0	0	0
6	0	0	1	2	1	0	0
7	0	0	1	4	3	1	0
8	0	0	0	5	9	4	1
9	0	0	0	5	22	19	6
10	0	0	0	4	40	70	35
11	0	0	0	3	60	220	190
12	0	0	0	2	86	629	977
13	0	0	0	1	110	1 700	4 875
14	0	0	0	1	127	4 463	24 920

Table 6.25 Values of $\overline{R}_{nk3}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	1	0	0	0	0	0
4	0	1	1	0	0	0	0
5	0	0	2	1	0	0	0
6	0	0	4	4	1	0	0
7	0	0	4	14	6	1	0
8	0	0	3	39	39	9	1
9	0	0	3	88	227	93	12
10	0	0	2	196	1 340	1 078	199
11	0	0	1	399	8 652	15 695	4 468
12	0	0	1	805	61 904	302 573	164 499
13	0	0	1	1 503	459 017	6 813 448	9 113 636
14	0	0	0	2 658	3 344 644	158 913 391	601 158 522

Table 6.26 Values of $\overline{R}_{nk4}$

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	1	0	0	0	0	0
4	0	1	1	0	0	0	0
5	0	1	3	1	0	0	0
6	0	0	7	5	1	0	0
7	0	0	10	26	8	1	0
8	0	0	13	124	83	12	1
9	0	0	17	643	1 173	244	17
10	0	0	19	3 831	24 942	10 266	663
11	0	0	19	23 437	641 872	820 142	84 184
12	0	0	17	138 181	16 799 302	81 159 989	24 211 108
13	0	0	13	761 022	418 548 455	8 123 840 077	8 853 245 774

6.5 Critical Codes

6.5

According to 6.2.13, appending a nonzero column to an indecomposable code yields a code which is again indecomposable. This shows that there exists an infinite family of k-dimensional indecomposable linear codes over any field $\mathbb{F}_q$ and for any dimension k. On the other hand, the $(n-1,k)$-code obtained by deleting an arbitrary column of a generator matrix of an indecomposable (n,k)-code can be either decomposable or indecomposable. For this reason, we investigate a restricted class of indecomposable codes, the *critical, indecomposable* codes, for short *critical* codes, introduced in [6]. An indecomposable code is called critical if the removal of any column of a generator matrix results in a decomposable code. In this section we prove that for a given dimension there are only finitely many critical, indecomposable codes and that any indecomposable code is obtained from a critical code by appending columns to a generator matrix of the critical code. Similarly as in Section 6.2, we may always assume that the codes are nonredundant. The present section is mainly a summary of [6]. All theorems and examples are quoted or excerpted from [6]. However, the order of the material presented is changed slightly.

Given an arbitrary code C, we may consider the subcode which is generated by the codewords of weight 1. If such words exist, the subcode generated by them splits off as an outer direct summand. Therefore, C is not indecomposable. If $\operatorname{dist}(C) > 1$, we investigate the subcode E of C which is generated by the vectors of weight 2. If such vectors exist, then E may or may not be an outer direct summand. The code E itself turns out to be an outer direct sum of codes, each summand being equivalent to a code which is the dual of a one-dimensional code generated by the all-one vector.

The support of a vector was defined in Section 1.6. The *support* of a vector space is the union of the supports of its elements. If the support of E is sufficiently large compared to the support of the code C and C is indecomposable, then we will prove that C is a critical code.

A particular class of vector space homomorphisms plays an important role for the following considerations.

Definition (code homomorphism) Let C and D be two linear codes over $\mathbb{F}_q$. A *code homomorphism* is a vector space homomorphism $\varphi\colon C \to D$ such that 6.5.1

$$\operatorname{wt}(\varphi(c)) \leq \operatorname{wt}(c), \qquad c \in C. \qquad \diamond$$

In other words, code homomorphisms are linear mappings which are contractions with respect to the Hamming metric.

6.5.2 Examples

1. Let Y be a subset of $n = \{0, \dots, n-1\}$ and $n \geq 1$. For $f \in \mathbb{F}_q^n$ let $f \downarrow Y$ be the restriction of f to Y. If C is a subspace of $\mathbb{F}_q^n$ and $D = \{f \downarrow Y \mid f \in C\}$, then the mapping $\varphi\colon C \to D$ defined by $\varphi(f) := f \downarrow Y$ is a code homomorphism. It is called a *projection* of C onto D. If $\dim(D) = \dim(C)$, then in coding theory we usually say that D is obtained from C by puncturing (cf. 2.2.8). We call D the projection of C onto Y.
2. If C' is a subspace of $C \subseteq \mathbb{F}_q^n$, then the natural injection of C' into C is a code homomorphism.
3. If C is a critical, indecomposable code of length $n > 1$, then the projections of C onto $n \setminus \{i\}$ are decomposable for $i \in n$.
4. A projection D of a decomposable code C is decomposable or indecomposable. If it is indecomposable, then $\dim(D) < \dim(C)$. ◇

Based on code homomorphisms it is possible to introduce the category of linear codes. We will not do it here. For further details consult [6].

If $\varphi\colon C \to D$ is a vector space isomorphism so that both φ and its inverse $\varphi^{-1}\colon D \to C$ are code homomorphisms, then φ is called a *code isomorphism*. It follows, therefore, that a code isomorphism preserves weights. If $\varphi\colon C \to D$ is a code isomorphism and C and D are of the same length, then φ is a linear isometry in the sense of Section 1.4. Hence, if we do not restrict our attention to nonredundant codes, then the notion "up to isomorphism" is a generalization of the notion "up to linear isometry". Two codes which are the same up to isomorphism can have different block-lengths. Restricting ourselves to nonredundant codes the two notions mean the same. The projection $C \to D$ of a nonredundant code C is a code isomorphism if and only if $C = D$.

Even if the code homomorphism is a vector space isomorphism its inverse need not be a code homomorphism.

6.5.3 Example For $n > 1$ let C be the $(n, n-1)$-parity check code and D the puncturing of C in the first component. Then the projection $\varphi\colon C \to D$ is a vector space isomorphism. For each $c \in C$ whose first component is different from 0 we have $\mathrm{wt}(\varphi(c)) < \mathrm{wt}(c)$ and, consequently, $\mathrm{wt}(\varphi^{-1}(\varphi(c)) > \mathrm{wt}(\varphi(c))$. Thus, φ^{-1} is not a code homomorphism. ◇

6.5.4 Definition (critical code) An indecomposable code C is called *critical, indecomposable* or just *critical* if, whenever $\varphi\colon C \to D$ is a projection which is not a code isomorphism, either $\dim(D) < \dim(C)$, or D is decomposable. ◇

Examples 6.5.5

1. Up to isomorphism, there is exactly one critical code of dimension 1 over $\mathbb{F}_q$, namely $\mathbb{F}_q$.
2. In dimension 2 there is up to isomorphism one critical code, namely the $(3,2)$-code with generator matrix
$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$
3. For $n \geq 3$, the unique indecomposable $(n, n-1)$-code (cf. 6.2.19) is a critical code. It has a generator matrix of the form
$$\begin{pmatrix} 1 & & & 1 \\ & \ddots & & \vdots \\ & & 1 & 1 \end{pmatrix} \qquad 6.5.6$$
where all entries, which are not specified, are equal to 0.
4. There is no critical code of length 2.
5. Consider an indecomposable code C with a repeated column, the last column say. Projecting this code onto all but the last column yields a surjective code homomorphism, which is not an isomorphism. The image is indecomposable and has the same dimension as C, whence C is not critical. In particular, a critical, indecomposable code has no repeated columns. For example, according to Table 6.21 there exist two indecomposable binary $(5,2)$-codes. They are given by the generator matrices
$$\Gamma_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ and } \Gamma_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$
They both project onto the unique critical binary code of dimension 2.
6. According to Table 6.22, there exist exactly two indecomposable binary $(5,3)$-codes. They are given by the generator matrices
$$\Gamma_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \text{ and } \Gamma_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$
Their weight distributions are
$$w_{C_1}(x) = 1 + 2x^2 + 4x^3 + x^4 \text{ and } w_{C_2}(x) = 1 + 3x^2 + 3x^3 + x^5.$$
Deleting the second column of Γ_1 and the last column of Γ_2 shows that both codes project onto the same critical binary $(4,3)$-code with generator matrix
$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

◇

It is possible to generalize the last example.

6.5.7 **Theorem** *Over any field there is a unique critical code of dimension* 3. *Up to isomorphism, it is the* $(4,3)$*-code with generator matrix.*

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Proof: Assume that C is a three-dimensional, critical code over $\mathbb{F}_q$. Then we can find a linearly isometric code with generator matrix $(I_3 \mid A)$.

If A has a column of weight three, then the columns of I_3 together with this additional column are the generator matrix of a projection of C. Moreover, this projection is a critical, three-dimensional, indecomposable code. Hence, it must be the generator matrix for the code linearly isometric to C. By changing the basis suitably, one can achieve that the column of weight 3 consists of three ones. A monomial transformation then gives the desired generator matrix.

If there is no column of weight 3 in A, then all columns of A have weight 2. There are no columns of weight 1, since they would be repeated columns, contradicting the fact that C is critical. Moreover, since C is indecomposable, there must be at least two columns in A whose zeros are in different rows. We want to prove that there is no critical $(5,3)$-code. Again, by a suitable monomial transformation we can assume that the generator matrix is of the form

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Projecting C onto the last four coordinates gives a three-dimensional critical, indecomposable code which is easily seen to be linearly isometric to the $(4,3)$-code. This shows that no critical, three-dimensional, indecomposable code with block length greater than four exists. □

The situation in dimension 4 is more interesting.

6.5.8 **Example** The binary $(5,4)$-parity check code is a critical code.

The projection of the binary $(7,4)$-Hamming-code onto any 6 coordinates is a critical $(6,4)$-code. A suitable generator matrix of this code is given by

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

This critical code belongs to an infinite class of critical binary $(2m, m+1)$-codes, $m \geq 2$, with generator matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 \\ & & & & \ddots & & \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 1 & 0 & 1 & \dots & 0 & 1 \end{pmatrix}.$$

For $m = 2$ we have the $(4,3)$-parity check code, for $m = 3$ the code above. $\diamond$

If C is an indecomposable code which is not critical, then there exists a projection of C onto an indecomposable code of the same dimension but smaller length. This proves the next

Corollary 6.5.9 *For any indecomposable code C, there exists a critical code D of the same dimension as C and a projection of C onto D.* $\square$

All indecomposable codes are given by adjoining columns to the generator matrix of a critical code. For example, all 2-dimensional binary indecomposable codes have generator matrices of the form

$$\begin{pmatrix} 1 & \dots & 1 & 0 & \dots & 0 & 1 & \dots & 1 \\ 0 & \dots & 0 & 1 & \dots & 1 & 1 & \dots & 1 \end{pmatrix}$$

and project onto the unique critical $(3,2)$-code over $\mathbb{F}_2$ by eliminating repeated columns.

By eliminating repeated columns we obtain the reduced code of C. By further deleting zero columns we obtain a projective code. The reduced code is indecomposable if and only if the original code had this property.

Definition (critical column) 6.5.10 Let C be an indecomposable code of length $n > 1$. The i-th column, $i \in n$, of C is *critical* if the projection of C onto $n \setminus \{i\}$ is a decomposable code. In other words, the i-th column is critical if the code which is obtained from C by puncturing the i-th coordinate is decomposable. $\diamond$

Corollary 6.5.11 *An indecomposable code C of length $n > 1$ is critical if and only if all its columns are critical.* $\square$

Now we determine all critical $(n, n-2)$-codes for $n > 2$.

Theorem 6.5.12 *If C is a critical (nonredundant) $(n, n-2)$-code over $\mathbb{F}_q$, then $n > 3$. It has minimum distance 2 and the subcode E of C generated by all codewords of*

weight 2 *has support* n. *Moreover,* C *is linearly isometric to a code with a generator matrix of the form*

$$\Gamma = (I_{n-2} \mid A) \text{ with } A = \begin{pmatrix} 1 & a_0 \\ \vdots & \vdots \\ 1 & a_{r-1} \\ 0 & 1 \\ \vdots & \vdots \\ 0 & 1 \end{pmatrix},$$

where the weight of the second column of A *is greater than* $n-2-r$ *but less than* $n-2$. *Moreover, if* $a_i \neq 0$, *then there exists some* $j \in r \setminus \{i\}$ *with* $a_j = a_i$.

Conversely, any matrix A *as above yields a critical* $(n, n-2)$*-code over* $\mathbb{F}_q$.

Proof: For $n = 3$ there is no critical, nonredundant $(3,1)$-code. Hence, we assume that $n > 3$. The code C is linearly isometric to a code with generator matrix of the form $(I_{n-2} \mid A)$ where neither of the two columns of A can have weight $n-2$, since otherwise C would not be critical. By a monomial transformation we can assure that the first column of A is a sequence of r ones, $r < n-2$, followed by a sequence of zeros. If $a = (a_0, \ldots, a_{r-1}, a_r, \ldots, a_{n-3})^\top$ is the second column of A, then necessarily $a_i \neq 0$ for $i \geq r$, since C cannot have minimum weight 1. By a further monomial transformation, we can assume that these entries are equal to 1. Moreover, since C is indecomposable there must be some $i \in r$ so that $a_i \neq 0$. Thus, the weight of the second column of A is greater than $n-2-r$ but less than $n-2$.

We next prove that for each $i \in r$ with $a_i \neq 0$ there exists some $j \in r$, $j \neq i$, such that $a_j = a_i$. If for i with $a_i \neq 0$ there were no j with $a_i = a_j$, then we can proceed as follows: Multiply the last column by a_i^{-1} so that there is a single 1 in the last column. (Then the elements in the last column are of the form $a_j a_i^{-1}$.) By elementary row operations it is possible to replace all nonzero entries different from 1 in the last column by 0. (For each j different from i we have to multiply the i-th row by $a_j a_i^{-1}$ and subtract the result from the j-th row.) After these row operations all entries of the last but one column are different from 0. Hence this matrix contains the $n-2$ unit vectors, a column of weight $n-2$ and a further column. Thus it is a generator matrix of a code which is not critical. This is a contradiction, since this code is linearly isometric to a critical code.

Lastly, we prove the assertion concerning the subcode E. The last $n-2-r$ rows of Γ belong to E, whence $\{i \in n \mid r \leq i \leq n-3\} \cup \{n-1\}$ is a subset of the support of E. Moreover, there exists $i \in r$ such that $a_i = 0$. Consequently, $\{n-2\} \cup \{i \in r \mid a_i = 0\}$ is also contained in the support of E. Finally, consider some $i \in r$ with $a_i \neq 0$, then there is some $j \in r$ with $a_j = a_i$, and the sum

of the i-th and j-th row is contained in E. Its support is $\{i, j\}$. Therefore, i and j also belong to the support of E. This proves that E has full support. □

Now we want to describe the structure of critical codes. This way we find a "quasicanonical form" of critical and indecomposable codes.

First we need the following lemma describing the subspace generated by all codewords of weight 2.

Lemma 6.5.13 *Let E be a code over $\mathbb{F}_q$ with minimum distance 2 which is generated by its vectors of weight 2. Then*

$$E = E_0 \dot{+} \ldots \dot{+} E_{r-1}$$

where each E_i is linearly isometric to an indecomposable $(n_i, n_i - 1)$-parity check code with $n_i \geq 2$.

Proof: We consider E as a code of length n with support $n = \{0, \ldots, n-1\}$. We introduce an equivalence relation on n by saying that i is in relation to j whenever there exists a codeword $c \in E$ of weight 2 so that $c_i \neq 0 \neq c_j$. Let $X_0, \ldots, X_{r-1}$ be the equivalence classes of this relation.

For $i \in r$ let E_i be the subspace of E which is generated by all vectors of weight 2 with support in X_i. Then $E_i \cap E_j = \{0\}$ for $i \neq j$ and $E_0 \dot{+} \ldots \dot{+} E_{r-1} = E$. By construction $|X_i| = n_i \geq 2$. Projecting E_i to its support X_i yields an indecomposable $(n_i, n_i - 1)$-code. □

Corollary 6.5.14 *Any code with minimum distance 2 which is generated by its vectors of weight 2 is linearly isometric to a code with generator matrix*

$$\left(\begin{array}{c|c|c|c} \Gamma_0 & 0 & \ldots & 0 \\ \hline 0 & \Gamma_1 & & 0 \\ \hline \vdots & & \ddots & \vdots \\ \hline 0 & 0 & \ldots & \Gamma_{r-1} \end{array}\right),$$

where Γ_i, $i \in r$, is an $(n_i - 1) \times n_i$-matrix, $n_i \geq 2$, of the form 6.5.6. □

Note that this code is indecomposable if and only if $r = 1$.

From the test on indecomposability, 6.2.13, we obtain the following

Corollary 6.5.15 *If C is a critical code with generator matrix of the form $(I_k \mid A)$, then any walk visiting all the k rows of the graph $\mathcal{G}_A$ defined on page 469 also visits every column of $\mathcal{G}_A$.*

Proof: If there were a walk visiting all rows but not all columns, then some columns of A could be eliminated and the resulting code would still be indecomposable. This is a contradiction to the assumption that C is critical. □

This, however, is only a necessary, not a sufficient property for a code to be critical. We proceed with the following combinatorial lemma, which will later be applied to the supports of the columns of A.

6.5.16 Lemma *Let R be a finite set and $\mathcal{C}$ a collection of subsets of R satisfying the two conditions:*

1. *There is a sequence $R_0, R_1, \ldots, R_{m-1}$ of elements of $\mathcal{C}$ such that $R_i \cap R_{i+1} \neq \emptyset$ for $i \in m-1$ and $\bigcup_{i \in m} R_i = R$.*
2. *$\mathcal{C}$ is minimal with respect to the above property, i.e. no proper subset of $\mathcal{C}$ posses a sequence of elements satisfying this property.*

Then there exists some $r \in R$ and $i \in m$ such that $r \in R_i$ and $r \notin R_j$ for $j \neq i$. Moreover, if $|\mathcal{C}| > 1$, then there exist at least two elements $r, r' \in R$, $r \neq r'$, and $i, i' \in m$, $i \neq i'$, with $r \in R_i$, $r \notin R_j$ for $j \neq i$ and $r' \in R_{i'}$, $r' \notin R_j$ for $j \neq i'$.

Proof: Any sequence from $\mathcal{C}$ having the required property must contain each element of $\mathcal{C}$ at least once by the minimality assumption. Choose a sequence $R_0, \ldots, R_{m-1}$ from $\mathcal{C}$ with the required property and with m minimal. If $m = 1$, then $\mathcal{C} = \{R_0\}$ and the assertion is trivial. Otherwise, consider the shorter sequences $R_1, \ldots, R_{m-1}$ and $R_0, \ldots, R_{m-2}$. Since they both enjoy the intersection property, necessarily

$$\bigcup_{i=1}^{m-1} R_i \neq R \neq \bigcup_{i=0}^{m-2} R_i.$$

Due to the fact that m was minimal neither R_0 occurs among $R_2, \ldots, R_{m-1}$ nor R_{m-1} occurs among $R_0, \ldots, R_{m-2}$. Choose $r_0 \in R_0$, $r_0 \notin \bigcup_{i=1}^{m-1} R_i$ and $r_{m-1} \in R_{m-1}$, $r_{m-1} \notin \bigcup_{i=0}^{m-2} R_i$. Then $r_0 \neq r_{m-1}$ and we get the desired result. □

6.5.17 Theorem *Every critical (n,k)-code with $n > 2$ has minimum distance 2. If $n \geq 4$, then the code contains at least two vectors of weight 2 with disjoint support.*

Let E be the subcode of C generated by all codewords of weight 2. Then either $C = E$ or there exists a subspace F of C of minimum distance greater than 2 so that $C = E + F$ and $E \cap F = \{0\}$. The subcode E can be expressed as $E = E_0 \dotplus \ldots \dotplus E_{r-1}$, $r \geq 1$, where each E_i is linearly isometric to an indecomposable $(n_i, n_i - 1)$-parity check code.

When $C = E + F$ with $F \neq \{0\}$, then F is an indecomposable code. Assume without loss of generality, that the support of E is equal to $s = \{0, \ldots, s-1\}$. If $s < n$, then the columns of F with column index in $\{s, \ldots, n-1\}$ are critical columns of F. The code F is also known as the auxiliary *indecomposable code attached to C.*

A generator matrix of a code linearly isometric to C is of the form

$$\Gamma = \left(\begin{array}{c|c|c|c|c} \Gamma_0 & 0 & \dots & 0 & 0 \\ \hline 0 & \Gamma_1 & \dots & 0 & 0 \\ \hline \vdots & & \ddots & & \vdots \\ \hline 0 & 0 & \dots & \Gamma_{r-1} & 0 \\ \hline \Lambda_0 & \Lambda_1 & \dots & \Lambda_{r-1} & \Lambda_r \end{array}\right),$$

where Γ_i, $i \in r$, is an $(n_i - 1) \times n_i$-matrix, $n_i \geq 2$, of the form 6.5.6. Each Λ_i, $i \in r$, is of the form

$$\Lambda_i = \begin{pmatrix} 0 & \dots & 0 & \ell_{0i} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & \ell_{\delta-1,i} \end{pmatrix}$$

where $\delta = \dim(F) = k - \sum_i (n_i - 1)$, and $(\ell_{0i}, \dots, \ell_{\delta-1,i}) \in \mathbb{F}_q^\delta \setminus \{0\}$. Finally, all columns of the $\delta \times (n-s)$-matrix Λ_r are nonzero and critical. The matrix Γ is called a quasicanonical *form of C. The submatrix $(\Lambda_0 \mid \dots \mid \Lambda_r)$ is a generator matrix of F. The nonzero columns of this submatrix yield a generator matrix*

$$\left(\begin{array}{ccc|c} \ell_{00} & \dots & \ell_{0,r-1} & \\ \vdots & \ddots & \vdots & \Lambda_r \\ \ell_{\delta-1,0} & \dots & \ell_{\delta-1,r-1} & \end{array}\right)$$

of F projected onto its support which is a nonredundant, indecomposable code.

Proof: Assume that C is a nonredundant, critical (n,k)-code with $n > 2$ and systematic generator matrix $\Gamma = (I_k \mid A)$, where necessarily $k < n$. Let R be k, the set of all row-indices of Γ, and let $\mathcal{C}$ be the set of the supports of the columns of A. According to 6.5.15, $\mathcal{C}$ satisfies the assumptions of 6.5.16. Consequently, there exists some $i \in k$ such that i belongs to exactly one column of A, thus the i-th row of Γ is a codeword of weight 2. By 6.2.18, any indecomposable code of length greater than 1 has minimum distance at least 2. Hence, $\operatorname{dist}(C) = 2$.

Assume that $n \geq 4$. If $n - k \geq 2$, then $|\mathcal{C}| > 1$, whence there exist $i, j \in k$, $i \neq j$, so that there is exactly one column of A the support of which contains i and there is exactly one column of A the support of which contains j. Consequently, the i-th and the j-th row of Γ are two codewords of weight 2 with disjoint support. If $n - k = 1$, then C is the $(n, n-1)$-parity check code which contains at least two codewords of weight 2 with disjoint support.

Let E be the subcode of C generated by the vectors of weight 2. By 6.5.13

$$E = E_0 \dotplus \dots \dotplus E_{r-1},$$

where each E_i is linearly isometric to a unique indecomposable $(n_i, n_i - 1)$-code, $n_i \geq 2$. If $n_i = 2$, then E_i is the repetition code, otherwise E_i is a critical

code. It is possible that the support of E is a proper subset of n. In this case assume, without loss of generality, that the support of E is s. Moreover, we assume that the support X_0 of E_0 consists of the first n_0 columns, and the support X_i of E_i consists of the n_i columns following the support of E_{i-1}, for $1 \leq i < r$. Thus $X_0 = \{0, \ldots, n_0 - 1\} = n_0$, $X_1 = \{n_0, \ldots, n_0 + n_1 - 1\} = (n_0 + n_1) \setminus n_0$, and so on.

If $r = 1$ and $C = E$, we are done. Otherwise E is properly contained in C and $C = E + F$ where $F \cap E = \{0\}$. Since E contains all codewords of C of weight 2, the code F has minimum distance at least 3. By suitable row operations it is possible to find generators of F the support of which is contained in

$$S = \left\{ \sum_{j=0}^{i} n_j - 1 \;\middle|\; i \in r \right\} \cup \{s, s+1, \ldots, n-1\}.$$

Recall that $\sum_{j=0}^{i} n_j - 1$ belongs to the support of E_i, $i \in r$. Moreover, since C is indecomposable, S is the support of F.

The fact that C is indecomposable implies that also F is indecomposable. The fact that C is critical implies that all columns with index in $\{s, \ldots, n-1\}$ are critical. □

If $r > 1$ and $s = n$, then necessarily $r \geq 3$, since otherwise the weight of the generators of F would be less than 3, what is impossible since all codewords of weight 2 belong to E and there are no codewords of weight 1 in C.

This way we obtain only a quasicanonical form of critical codes since we have specified neither the order of the Γ_i nor the order of the nonzero columns of the matrices Λ_i. This description of the quasicanonical form yields a method for constructing critical codes and arbitrary indecomposable codes. Any indecomposable code is linearly isometric to a code with generator matrix

$$\Gamma = \left(\begin{array}{c|c|c|c|c|c} \Gamma_0 & 0 & \ldots & 0 & 0 & N_0 \\ \hline 0 & \Gamma_1 & \ldots & 0 & 0 & N_1 \\ \hline \vdots & & \ddots & & \vdots & \vdots \\ \hline 0 & 0 & \ldots & \Gamma_{r-1} & 0 & N_{r-1} \\ \hline \Lambda_0 & \Lambda_1 & \ldots & \Lambda_{r-1} & \Lambda_r & N_r \end{array}\right),$$

with suitable matrices N_i, $0 \leq i \leq r$.

6.5.18 **Example** Consider the binary $(5, 2, 3)$-code F with generator matrix

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

which is indecomposable and has one critical column, the last. Now we want to construct a nonredundant, critical $(9, 6)$-code with auxiliary code F. Since

$n_i \geq 2$, we have $r = 4$, $n_0 = n_1 = n_2 = n_3 = 2$ and $s = 8$. Therefore, a quasicanonical form of the critical $(9,6)$-code is

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

◇

Using these quasicanonical forms, we are able to classify the critical $(n, n-2)$-codes in more details.

Corollary *The quasicanonical generator matrix of a critical, indecomposable $(n, n-2)$-code over $\mathbb{F}_q$ with $n > 3$ is of the form* **6.5.19**

$$\Gamma = \left(\begin{array}{c|c|c|c} \Gamma_0 & 0 & \dots & 0 \\ \hline 0 & \Gamma_1 & \dots & 0 \\ \hline \vdots & & \ddots & \\ \hline 0 & 0 & \dots & \Gamma_{r-1} \\ \hline \Lambda_0 & \Lambda_1 & \dots & \Lambda_{r-1} \end{array}\right),$$

where $r \geq 3$, Γ_i is an $(n_i - 1) \times n_i$-matrix, $n_i \geq 2$, given by 6.5.6, $i \in r$. Moreover, $\Lambda_i = (0 \mid \dots \mid 0 \mid e^{(i)})$ is an $(r-2) \times n_i$-matrix for $i \in r-2$,

$$\Lambda_{r-2} = \begin{pmatrix} 0 & \dots & 0 & 1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 \end{pmatrix} \text{ and } \Lambda_{r-1} = \begin{pmatrix} 0 & \dots & 0 & \ell_0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & \ell_{r-3} \end{pmatrix}$$

with pairwise different, nonzero elements $\ell_0, \dots, \ell_{r-3}$. Thus, we obtain the following estimates: $q - 1 \geq r - 2$ and $n \geq 6$.

Proof: The quasicanonical form of critical codes was described in 6.5.17. According to 6.5.12, the code E generated by all codewords of weight 2 has full support. Whence, $n - s = 0$ and the matrix Λ_r does not occur in this quasicanonical form. By construction $r = 1$ and $r = 2$ are impossible. If $r \geq 3$, then the auxiliary code F projected onto its nonzero columns is an $(r, r-2)$-code $\tilde{F}$ with minimum distance $d \geq 3$. Therefore, it is an MDS-code. According to 2.5.6, there exists a systematic generator matrix of a code linearly isometric to $\tilde{F}$ with generator matrix of the form

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 1 & \ell_0 \\ 0 & 1 & \dots & 0 & 1 & \ell_1 \\ \vdots & & \ddots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1 & \ell_{r-3} \end{pmatrix}.$$

□

For the binary case we obtain even a canonical form of critical $(n, n-2)$-codes.

6.5.20 Corollary *The binary critical $(n, n-2)$-codes, $n \geq 6$, have the canonical form*

$$\Gamma = \left(\begin{array}{c|c|c} \Gamma_0 & 0 & 0 \\ \hline 0 & \Gamma_1 & 0 \\ \hline 0 & 0 & \Gamma_2 \\ \hline \Lambda_0 & \Lambda_1 & \Lambda_2 \end{array}\right),$$

where Γ_i is an $(n_i - 1) \times n_i$-matrix given by 6.5.6, $i \in 3$, with $n_0 \geq n_1 \geq n_2 \geq 2$, and Λ_i is an $1 \times n_i$-matrix of the form

$$\Lambda_i = (0 \quad \ldots \quad 0 \quad 1), \qquad i \in 3.$$

Proof: Since $\mathbb{F}_2$ contains exactly two elements, we obtain from $1 \geq r - 2$ that $r \leq 3$, thus $r = 3$. Another proof of this fact is based on 2.5.7, where we have shown that there exist only trivial binary MDS-codes. Hence, only for $r = 3$ there exist binary $(r, r-2, 3)$-codes. □

6.5.21 Corollary *The number of linearly nonisometric critical binary $(n, n-2)$-codes with $n \geq 6$ is the same as the number of partitions of $n - 3$ into three parts.*

Proof: The matrices Λ_i in the last row of a canonical form of a critical binary $(n, n-2)$-code have exactly one row. Therefore,

$$\sum_{i=0}^{2} (n_i - 1) = n - 3$$

is the sum of the ranks of the matrices Γ_i for $i \in 3$. Since $n_0 \geq n_1 \geq n_2$ and $n_2 - 1 \geq 1$, the sequence $(n_0 - 1, n_1 - 1, n_2 - 1)$ is a partition of $n - 3$. □

6.5.22 Example For $n = 6$ there is exactly one partition of 3 with three parts, namely $3 = 1 + 1 + 1$. We have met the corresponding critical $(6, 4)$-code in 6.5.8. For $n = 7$ there is the unique partition $4 = 2 + 1 + 1$ which yields the canonical form

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

◇

Theorem 6.5.23 *A nonredundant, binary, critical $(n, n-2)$-code C contains the all-one vector if and only if it comes from a partition of $n-3$ into three parts all of the same parity (this means, that all three parts are either odd or even).*

Proof: Assume that $n-3$ has a partition $k_0+k_1+k_2$ with $k_0 \geq k_1 \geq k_2 \geq 1$. Using the canonical form 6.5.20 of C we have: If all three k_i are odd, then

$$(\underbrace{1,\ldots,1}_{k_0},\underbrace{1,\ldots,1}_{k_1},\underbrace{1,\ldots,1}_{k_2},0)\cdot\Gamma=(1,\ldots,1).$$

If all three k_i are even, then

$$(\underbrace{1,\ldots,1}_{k_0},\underbrace{1,\ldots,1}_{k_1},\underbrace{1,\ldots,1}_{k_2},1)\cdot\Gamma=(1,\ldots,1).$$

Conversely, assume that $c=(1,\ldots,1)$ is contained in C. Then there exists some $v \in \mathbb{F}_2^{n-2}$ so that $v\cdot\Gamma = c$. Moreover, assume that Γ corresponds to a partition $k_0+k_1+k_2 = n-3$ with $k_i = n_i - 1$, $i \in 3$. If k_0 is odd, then the first k_0 entries of v must be equal to 1. These entries guarantee that $c_0 = c_1 = \ldots = c_{k_0-1} = 1$. The first k_0 components of c are not influenced by the remaining v_i, $k_0 \leq i < k$. Since $c_{k_0} = 1$, necessarily v_{n-3}, the last component of v, must be 0. Therefore, k_1 and k_2 are also odd, since otherwise $c_{n_0+n_1-1} = 0$ or $c_{n_0+n_1+n_2-1} = 0$. If k_0 is even, then similar considerations show, that necessarily $v_{n-3} = 1$, in order to have $c_{k_0} = 1$ and consequently, both k_1 and k_2 must be even. □

Now we investigate the dual of a critical code.

Examples 6.5.24

1. If C is the critical $(n, n-1)$-code, $n > 2$, over $\mathbb{F}_q$, then, according to Exercise 1.3.9 its dual code $C^\perp$ is generated by $(-1,\ldots,-1,1)$. Thus, it is linearly isometric to the code generated by the all-one vector and its reduced code is the $(1,1)$-code $\mathbb{F}_q$.
2. If C is a critical (n,k)-code over $\mathbb{F}_q$ different from the critical $(n, n-1)$-code, then C has an auxiliary code F. Let $\tilde{F}$ be the projection of F onto its support, then $\tilde{F}$ is a nonredundant, indecomposable code. We want to prove that the reduced code of $C^\perp$ is linearly isometric to the reduced code of $\tilde{F}^\perp$. By 6.2.14 the dual of $\tilde{F}$, whence also the reduced code of $\tilde{F}$, is indecomposable.

Using the quasicanonical form described in 6.5.17, the code C is linearly isometric to a code C' with generator matrix

$$\left(\begin{array}{c|c|c|c|c|c} I_{k_0} & 0 & \dots & 0 & 0 & A_0 \\ \hline 0 & I_{k_1} & \dots & 0 & 0 & A_1 \\ \hline \vdots & & \ddots & & \vdots & \vdots \\ \hline 0 & 0 & \dots & I_{k_{r-1}} & 0 & A_{r-1} \\ \hline 0 & 0 & \dots & 0 & I_\delta & A \end{array}\right)$$

where $k_i = n_i - 1$, I_{k_i} is the unit matrix, $i \in r$, and $(I_\delta \mid A)$ is a systematic generator matrix of a code linearly isometric to $\tilde{F}$, where $\delta = n - \sum_i k_i$ and A is a $\delta \times (n-k)$-matrix. Moreover, the rows of the matrix A_i, $i \in r$, are copies of a nonzero multiple of a single row of A or they are unit vectors. The dual of C' has a generator matrix of the form

$$(-A_0^\top \mid \dots \mid -A_{r-1}^\top \mid -A^\top \mid I_{n-k}).$$

All columns of $-A_i^\top$, $i \in r$, are nonzero multiples of columns of $-A^\top$ or they are unit vectors, therefore, the reduced code of $C^\perp$ is linearly isometric to the reduced code of $\tilde{F}^\perp$. ◇

It seems natural to ask from which critical, indecomposable codes a given indecomposable code might arise by augmentation of their quasicanonical generator matrices. Or, equivalently, given an indecomposable (n,k)-code C, what are the the critical, indecomposable (m,k)-codes which arise as projections from C?

6.5.25 Definition (spectrum of a code) The *spectrum* $\mathrm{spec}(C)$ of an indecomposable code C is the set of all linear isometry classes of critical, indecomposable codes D which satisfy

- $\dim(D) = \dim(C)$
- there exists a projection of C onto D. ◇

6.5.26 Theorem *The spectrum of an (n,k)-MDS-code with $1 < k < n$ contains only the linear isometry class of the unique critical $(k+1,k)$-parity check code.*

Proof: In each systematic generator matrix $(I_k \mid A)$ of any code linearly isometric to C all columns of A have weight k. Thus, the only critical k-dimensional code obtained as a projection of C is linearly isometric to the unique critical, $(k+1,k)$-parity check code. □

Corollary 6.5.27 *The spectrum of the m-th order q-ary Hamming-code C contains only one element.*

If $m > 2$, projecting C onto all but one coordinate yields a critical code in which the code generated by all vectors of weight 2 is the sum of the unique indecomposable q-ary $(q, q-1)$-code repeated $(q^{m-1}-1)/(q-1)$ times and the auxiliary code is the $(m-1)$-th order q-ary Hamming-code.

Proof: The first assertion follows from 6.5.26. The proof of the second assertion is based on design theory. The reader should consult [7]. □

Example 6.5.28 The second order ternary Hamming-code has a generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}.$$

Therefore, the quasicanonical form of the critical code in the spectrum of the third order ternary Hamming-code is

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}.$$

No matter which nonzero column we append as the last column, we obtain an indecomposable $(13, 10)$-code. In order to obtain the Hamming-code, we must append a column so that the minimum distance of the new code is equal to 3. For this reason the nonzero entries in the first two rows must have opposite signs. Similar arguments hold for all but the last two rows. Using for instance $(1, -1, 1, -1, 1, -1, 1, -1, 0, 0)^\top$ as the last column we obtain a generator matrix of the Hamming-code. ◇

It is also possible that the spectrum contains more than one linear isometry class.

Example 6.5.29 Consider the binary $(7, 4)$-code with the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Projecting onto the first five columns gives the unique critical $(5,4)$-code while projecting onto all but the fifth column gives the critical $(6,4)$-code of 6.5.8. $\diamond$

The proof of the following theorem is left to the reader.

6.5.30 Theorem *Let C be a nonredundant, binary, indecomposable (n,k)-code.*

1. *If C contains the all-one vector, then each code in its spectrum contains the all-one vector.*
2. *Let $k > 1$. If C contains the all-one vector, and $\operatorname{spec}(C)$ contains the critical $(k+1,k)$-parity check code, then k is odd.*
3. *Assume that k is even and C contains the all-one vector. Then the critical $(k+1,k)$-parity check code is not in $\operatorname{spec}(C)$. If a critical $(k+2,k)$-code is contained in $\operatorname{spec}(C)$, then it must come from a partition of $k-1$ into three odd parts.* $\square$

Now we come back to binary Reed–Muller-codes.

6.5.31 Theorem

1. *The $(m-1)$-th order Reed–Muller-code $\mathrm{RM}^2_{m,m-1}$ of degree $m > 1$ is the unique critical $(2^m, 2^m-1)$-code.*
2. *The spectrum of $\mathrm{RM}^2_{m,m-2}$, for $m \geq 2$, contains exactly one code. This is the critical code underlying the m-th order binary Hamming-code (cf. 6.5.27).*
3. *Assume that $m > 3$. The spectrum of $\mathrm{RM}^2_{m,1}$ consists of all critical codes of dimension $m+1$ containing the all-one vector. Thus, there is a difference between the spectra depending on the parity of m. If m is odd, then the critical $(m+2,m+1)$-code is not in the spectrum, whereas it is contained in the spectrum when m is even. The critical $(m+3,m+1)$-codes in the spectrum of $\mathrm{RM}^2_{m,1}$ are described in 6.5.23.*

Proof: 1. According to Exercise 2.4.3, the code $\mathrm{RM}^2_{m,m-1}$ contains all vectors of length 2^m of even weight, therefore, it is the unique critical $(2^m, 2^m-1)$-code.

2. From 2.4.11 we obtain that $\mathrm{RM}^2_{m,m-2}$ is the parity extension of the m-th order binary Hamming-code. Projecting on all but 2 coordinates gives the underlying critical code. Any two coordinates yield the same critical code.

3. Every binary Reed–Muller-code contains the all-one vector. By the first part of 6.5.30, all codes in the spectrum of $\mathrm{RM}^2_{m,1}$ contain the all-one vector. Since $\dim(\mathrm{RM}^2_{m,1}) = m+1$, (cf. 2.4.7) we obtain the assertion on the $(m+2,m+1)$-code from the second part of 6.5.30. $\square$

The spectra of the ternary and binary Golay-codes are described in [6].

Exercises

Exercise Prove 6.5.30. **E.6.5.1**

6.6 Random Generation of Linear Codes **6.6**

In Sections 6.1–6.3 we have shown how to enumerate the linear isometry classes of linear codes, in Chapter 9 we will describe how to determine a (complete) set of representatives for given parameters n, k and q. From the tables of numbers of linear isometry classes we immediately realize that only for relatively small values of these parameters it will be possible to determine the sets of representatives completely. The order of the acting group increases, and the number of representatives quickly gets out of hand. In such situations, probabilistic methods may still allow the construction of linear codes which are distributed uniformly at random over all isometry classes.

The *Dixon–Wilf-algorithm* allows the generation of linear codes which are distributed uniformly at random over all linear isometry classes. Actually this algorithm was first developed for the random generation of unlabeled graphs (cf. [46]). It can always be applied for the random generation of objects, which are orbits of a finite group acting on a finite set.

Therefore, we present the algorithm for an arbitrary finite action of a group G on a set X. The algorithm describes a method how to choose elements x_0 of X at random such that the probability that x_0 belongs to a given orbit $\omega \in G\backslash\backslash X$ is $1/|G\backslash\backslash X|$ for each orbit ω. This allows us to sample elements of X which are uniformly distributed over the G-orbits on X.

Dixon–Wilf-algorithm *Let G be a finite group acting on a finite, nonempty set X. Choose a conjugacy class $\mathcal{C}$ of elements of G with the probability* **6.6.1**

$$p(\mathcal{C}) := \frac{|\mathcal{C}| \cdot |X_g|}{|G| \cdot |G\backslash\backslash X|} \text{ for an arbitrary } g \in \mathcal{C}.$$

Pick any $g \in \mathcal{C}$ and determine at random a fixed point x of g. Then the probability that x lies in a given orbit $\omega \in G\backslash\backslash X$ is equal to $1/|G\backslash\backslash X|$.

Proof: Let $\mathcal{C}_0, \ldots, \mathcal{C}_{N-1}$ be the conjugacy classes of elements of G with representatives $g_i \in \mathcal{C}_i$. As a consequence of the Lemma of Cauchy–Frobenius 3.4.2, it follows

$$\sum_{i \in N} p(\mathcal{C}_i) = \frac{\sum_{i \in N} |\mathcal{C}_i| \, |X_{g_i}|}{\sum_{g \in G} |X_g|} = 1,$$

whence $p(.)$ is a probability distribution. Then for each $\omega \in G\backslash\backslash X$ we determine the probability that x belongs to ω as

$$\begin{aligned} p(x \in \omega) &= \sum_{i \in N} p(\mathcal{C}_i) p(x \in X_{g_i} \cap \omega) \\ &= \sum_{i \in N} p(\mathcal{C}_i) \frac{\left|X_{g_i} \cap \omega\right|}{\left|X_{g_i}\right|} = \sum_{i \in N} \frac{|\mathcal{C}_i|\left|X_{g_i}\right|}{|G|\,|G\backslash\backslash X|} \frac{\left|X_{g_i} \cap \omega\right|}{\left|X_{g_i}\right|} \\ &= \frac{1}{|G|\,|G\backslash\backslash X|} \sum_{i \in N} |\mathcal{C}_i|\left|X_{g_i} \cap \omega\right| = \frac{1}{|G|\,|G\backslash\backslash X|} \sum_{g \in G} \left|X_g \cap \omega\right|. \end{aligned}$$

The last sum is equal to $|G|$, since for $\omega = G(x)$ we have

$$\sum_{g \in G} \left|X_g \cap \omega\right| = \sum_{g \in G} \sum_{x \in X_g \cap \omega} 1 = \sum_{x \in \omega} \sum_{g \in G_x} 1 = \sum_{x \in \omega} |G_x| = |G_x|\,|\omega| = |G|. \quad \square$$

As we have seen in 6.1.15, the linear isometry classes of linear (n,l)-codes for $1 \leq l \leq k$ with $k \leq n$ correspond to the $\mathrm{GL}_k(q) \times S_n$-orbits on the set of mappings from n to $\mathrm{PG}^*_{k-1}(q)$.

For this reason we formulate the Dixon–Wilf-algorithm for the canonical action of a direct product $H \times G$ on Y^X introduced in 1.4.11.

6.6.2 **Corollary** *Let ${}_GX$ and ${}_HY$ be two finite group actions. Choose a conjugacy class $\mathcal{C}$ of elements of $H \times G$ with the probability*

$$p(\mathcal{C}) := \frac{|\mathcal{C}|\,|Y^X_{(h,g)}|}{|G|\,|H|\,|(H \times G)\backslash\backslash Y^X|} \text{ for arbitrary } (h,g) \in \mathcal{C}.$$

Pick any $(h,g) \in \mathcal{C}$ and determine at random a function $f \in Y^X$ which is fixed under the action of (h,g), i.e. $f(gx) = hf(x)$ for all $x \in X$. Then the probability that f lies in a given orbit $\omega \in (H \times G)\backslash\backslash Y^X$ is equal to $1/|(H \times G)\backslash\backslash Y^X|$. $\square$

According to Exercise 6.3.3, the conjugacy classes of $G := S_n$ are characterized by the cycle types $a \vdash n$. The conjugacy classes of $H := \mathrm{GL}_k(q)$ were described completely in 6.3.12. Hence, the conjugacy classes of $\mathrm{GL}_k(q) \times S_n$ are exactly the elements of the cartesian product $\mathcal{C}_1 \times \mathcal{C}_2$, where $\mathcal{C}_1$ is a conjugacy class of $\mathrm{GL}_k(q)$ and $\mathcal{C}_2$ is a conjugacy class of S_n. This shows how to obtain representatives of the conjugacy classes of $\mathrm{GL}_k(q) \times S_n$. In 6.3.14 the representatives of the conjugacy classes of $\mathrm{GL}_k(q)$ are described as block diagonal matrices of companion and hyper companion matrices of monic irreducible polynomials over $\mathbb{F}_q$. In order to list them all, it is necessary to know all these polynomials of degree up to k. As we have seen in Section 6.3, it was not necessary to know these polynomials explicitly as far as enumeration of linear isometry classes is concerned.

For certain values of k and q, tables of these polynomials exist. Recall from the beginning of Section 3.5 that all irreducible polynomials of a given degree n over $\mathbb{F}_q$ can be computed once a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is known.

This motivates the following strategy. For $2 \leq r \leq k$ we generate monic polynomials of degree r over $\mathbb{F}_q$ at random. Using 3.5.20 we test these polynomials whether they are irreducible. We repeat this till for each r we have found an irreducible polynomial of degree r. With these polynomials we are able to determine a normal basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ for each r. For more details see Section 6.9. Then we compute all Lyndon words of length r over an alphabet of q elements as described in 3.5.5. We consider these Lyndon words as the coefficient vectors of elements of $\mathbb{F}_{q^r}$ with respect to the normal basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ just constructed. Using 3.5.2, we compute the minimal polynomials of these elements. These minimal polynomials provide a complete list of irreducible polynomials of degree r over $\mathbb{F}_q$.

The number of $\mathrm{GL}_k(q) \times S_n$-orbits on $\mathrm{PG}^*_{k-1}(q)^n$ was already computed as T_{nkq} in 6.1.23. The number of fixed points of $(A, \pi) \in \mathrm{GL}_k(q) \times S_n$ in $\mathrm{PG}^*_{k-1}(q)^n$ can be deduced from the next

Lemma **6.6.3** *Assume that ${}_GX$ and ${}_HY$ are two finite group actions which induce natural actions of G, H and $H \times G$ on Y^X (as described in 1.4.7, 1.4.10, and 1.4.11).*

- *The number of fixed points of $g \in G$ on Y^X is given by*

$$|Y|^{c(\overline{g})} \quad \text{for} \quad c(\overline{g}) := \sum_{i=1}^{|X|} a_i(\overline{g}),$$

  where $(a_1(\overline{g}), \ldots, a_{|X|}(\overline{g}))$ is the cycle type of the induced permutation $\overline{g}$ on X.

- *The number of fixed points of $h \in H$ on Y^X is given by*

$$|Y_h|^{|X|},$$

  where Y_h is the set of fixed points of h on Y.

- *The number of fixed points of $(h, g) \in H \times G$ on Y^X is given by*

$$\prod_{i=1}^{|X|} |Y_{h^i}|^{a_i(\overline{g})},$$

  where $(a_1(\overline{g}), \ldots, a_{|X|}(\overline{g}))$ is the cycle type of the induced permutation $\overline{g}$ on X, and Y_h is the set of fixed points of h on Y. □

A method for constructing the set of fixed points of (A, π) on $\mathrm{PG}^*_{k-1}(q)^n$ is described in

6.6.4 Lemma *Consider the natural action of $H \times G$ on Y^X induced by two finite group actions ${}_GX$ and ${}_HY$ as described in 1.4.11. The fixed points $f \in Y^X$ of $(h,g) \in H \times G$ have the following form. For each cycle Z of $\overline{g}$ on X, pick a representative $x_Z \in Z$. Then $f(x_Z) = y_0 \in Y$ with $|\langle h \rangle (y_0)|$ dividing $|Z|$ (that is, $y_0 \in Y_{h^{|Z|}}$, the set of fixed points of $h^{|Z|}$ on Y). The remaining values of f on Z are determined by*

$$f(g^i x_Z) := h^i y_0 \text{ for } 1 \leq i < |Z|. \qquad \square$$

The proofs of the previous two lemmata are left to the reader as Exercise 6.6.1 and Exercise 6.6.2.

As mentioned above, applying the Dixon–Wilf-algorithm for the random generation of linear codes produces generator matrices of linear (n,l)-codes for $l \leq k$. Therefore, after the generation the rank of each matrix must still be determined.

Some numerical results are presented in Table 6.27. For different parameters q, n and k, the table shows the distribution of ranks when 10 000 matrices were generated at random in each case.

For further illustration here are the numbers of conjugacy classes of $\mathrm{GL}_k(2)$.

k	3	4	5	6	7	8	9	10
# of conjugacy classes	6	14	27	60	117	246	490	1002

The choice of a conjugacy class of S_n amounts to the choice of a cycle type (or partition) of n. The number of partitions of $n \in \mathbb{N}$ increases rapidly with n. Here are some of these numbers:

n	number of cycle types of n
10	42
15	176
20	627
25	1 958
40	37 338
60	$\approx 10^6$
100	$\approx 2 \cdot 10^8$

For this reason we should try to avoid computing and storing the probabilities of all conjugacy classes of $\mathrm{GL}_k(q) \times S_n$ before the generation process starts. For practical purposes we label the conjugacy classes by $\mathcal{C}_0, \ldots, \mathcal{C}_{N-1}$. Usually $\mathcal{C}_0$ is the conjugacy class of the identity element. The random choice of a conjugacy class $\mathcal{C}_{i_0}$ is done by first computing a random number $r \in [0,1)$ and then determining the index $i_0 \in N$ so that

$$\sum_{j \in i_0} p(\mathcal{C}_j) \leq r \text{ and } \sum_{j \in i_0+1} p(\mathcal{C}_j) > r.$$

Table 6.27 Distribution of ranks of 10 000 $k \times n$-matrices over $\mathbb{F}_q$ generated at random

q	n	k	rank distribution
2	15	3	(17, 534, 9449)
2	15	4	(1, 53, 677, 9269)
2	15	5	(0, 5, 68, 908, 9019)
2	15	6	(0, 0, 16, 142, 1488, 8354)
2	15	7	(0, 1, 5, 51, 492, 2672, 6779)
2	15	8	(0, 0, 1, 27, 272, 1523, 3970, 4207)
2	15	9	(0, 0, 1, 27, 246, 1374, 3289, 3507, 1556)
2	15	10	(0, 0, 2, 22, 228, 1179, 3279, 3434, 1531, 325)
2	20	3	(8, 218, 9774)
2	20	4	(0, 7, 185, 9808)
2	20	5	(0, 0, 3, 140, 9857)
2	20	6	(0, 0, 0, 2, 175, 9823)
2	20	7	(0, 0, 0, 0, 3, 225, 9772)
2	20	8	(0, 0, 0, 0, 0, 18, 529, 9453)
2	25	3	(3, 121, 9876)
2	25	4	(0, 2, 70, 9928)
2	25	5	(0, 0, 0, 30, 9970)
2	25	6	(0, 0, 0, 0, 10, 9990)
2	25	7	(0, 0, 0, 0, 0, 6, 9994)
2	25	8	(0, 0, 0, 0, 0, 0, 29, 9971)
3	15	3	(1, 122, 9877)
3	15	4	(0, 0, 50, 9950)
3	15	5	(0, 0, 0, 68, 9932)
3	25	5	(0, 0, 0, 0, 10000)

One can start the generation process immediately and evaluate probabilities of the conjugacy classes only if required. This means that we need to evaluate $p(\mathcal{C}_i)$ only if the chosen random number exceeds $\sum_{j \in i} p(\mathcal{C}_j)$. The efficiency of this revised method depends heavily on the numbering of the conjugacy classes. Clearly, the numbering should be chosen in such a way that $p(\mathcal{C}_i) \geq p(\mathcal{C}_{i+1})$.

We have applied the random generation of linear codes in order to describe the distribution of the minimum distance of linear codes with given parameters n, k and q. Two examples are presented in Table 6.28 and Table 6.29.

Table 6.28 Distribution of the minimum distances of 10 000 binary codes of length 20 and maximal dimension 8

$k\backslash d$	1	2	3	4	5	6
5	0	0	0	1	0	0
6	0	0	2	5	3	1
7	3	45	102	226	150	16
8	81	1 158	2 502	4 346	1 344	15

Table 6.29 Distribution of the minimum distances of 30 000 000 codes of length 12 and maximal dimension 5 over $\mathbb{F}_5$

$k\backslash d$	1	2	3	4	5	6	7	8
3	1	5	4	40	99	196	136	9
4	120	1060	5644	37440	137047	139665	5651	0
5	24017	243558	1486385	10048367	17047580	822975	0	0

Exercises

E.6.6.1 **Exercise** Prove 6.6.3.

E.6.6.2 **Exercise** Prove 6.6.4.

E.6.6.3 **Exercise** Use the enclosed software to obtain lower bounds for the minimum distance of linear (n,k)-codes over $\mathbb{F}_p$ for small parameters n, k and p. Compare these results with the list of best known linear codes [32].

6.7 Enumeration of Semilinear Isometry Classes

So far we were concerned only with the enumeration of linear isometry classes of codes. In this section we show how to generalize these methods in order to derive the number of semilinearly nonisometric codes.

In 1.5.10 we have described a semilinear isometry ι as $\iota = (\psi, (\alpha; \pi))$ where $\alpha \in \mathrm{Aut}(\mathbb{F}_q) = \mathrm{Gal}\,[\,\mathbb{F}_q : \mathbb{F}_p\,]$ and $(\psi; \pi)$ is a linear isometry. Thus $(\psi; \pi)$ belongs to the wreath product

$$\mathbb{F}_q^* \wr_n S_n = \left\{ (\psi; \pi) \;\middle|\; \psi : n \to \mathbb{F}_q^*,\ \pi \in S_n \right\}.$$

Since $\mathrm{Gal}\,[\,\mathbb{F}_p : \mathbb{F}_p\,]$ contains just one element, we assume in this section that $q = p^r$ with $r > 1$. In the sequel we indicate the Galois group $\mathrm{Gal}\,[\,\mathbb{F}_q : \mathbb{F}_p\,]$,

generated by the Frobenius automorphism $\tau(\kappa) = \kappa^q$, $\kappa \in \mathbb{F}_q$, by Gal. As we already know, it is a cyclic group of order r.

According to 1.5.11 two codes are called semilinearly isometric if there exists a semilinear isometry ι which maps one code onto the other code.

Our first aim is to show that the group of semilinear isometries is a generalized wreath product. Therefore, we apply the two semilinear isometries $\iota_2 = (\phi;(\beta,\rho))$ and $\iota_1 = (\psi;(\alpha,\pi))$ to the vector $v = (v_0,\dots,v_{n-1}) \in \mathbb{F}_q^n$ and indicate $\iota_1(v)$ by $v' = (v'_0,\dots,v'_{n-1})$. Then we obtain

$$\begin{aligned}\iota_2(\iota_1(v)) &= \iota_2(v') = \big(\phi(0)\beta(v'_{\rho^{-1}(0)}),\dots,\phi(n-1)\beta(v'_{\rho^{-1}(n-1)})\big)\\ &= \Big(\dots,\phi(i)\beta\big(\psi(\rho^{-1}(i))\alpha(v_{\pi^{-1}(\rho^{-1}(i))})\big),\dots\Big)\\ &= \Big(\dots,\phi(i)\beta(\psi(\rho^{-1}(i)))(\beta\circ\alpha)(v_{(\rho\circ\pi)^{-1}(i)}),\dots,\Big).\end{aligned}$$

This formula motivates the following

Lemma *The group of all semilinear isometries of $\mathbb{F}_q^n$ is the semidirect product* **6.7.1**

$$(\mathbb{F}_q^*)^n \rtimes (\mathrm{Gal}\times S_n),$$

with the normal subgroup on the left, where the multiplication is given by

$$(\phi;(\beta,\rho))\cdot(\psi;(\alpha,\pi)) := (\phi\psi_{(\beta,\rho)};(\beta\alpha,\rho\circ\pi)),$$

with

$$\psi_{(\beta,\rho)}(i) := \beta(\psi(\rho^{-1}(i))), \qquad i \in n,$$

and

$$\phi\psi(i) := \phi(i)\psi(i), \qquad i \in n. \qquad \square$$

Therefore, the identity element is $(1;(\tau^0,\mathrm{id}))$, where 1 is the mapping $i \mapsto 1$, $i \in n$. The inverse of $(\psi;(\alpha,\pi))$ is $(\psi^{-1}_{(\alpha^{-1},\pi^{-1})};(\alpha^{-1},\pi^{-1}))$ where $\psi^{-1}(i) := (\psi(i))^{-1}$, $i \in n$, and $\psi^{-1}_{(\alpha,\pi)} := (\psi_{(\alpha,\pi)})^{-1} = (\psi^{-1})_{(\alpha,\pi)}$.

Representing the product of two semilinear isometries in this way, it is easy to realize certain similarities with the ordinary wreath product $H \wr_X G$. In 1.4.8 we had considered a group G acting on a set X and an arbitrary group H. For defining the multiplication in $H \wr_X G$ we used the canonically induced action of G on H^X given by 1.4.7.

Here in the situation of the group of semilinear isometries, we have $X = n$ and $H = \mathbb{F}_q^*$. The group $\mathrm{Gal}\times S_n$ does not act on n, but it operates already on $(\mathbb{F}_q^*)^n$ and we do not have to consider an induced action on $(\mathbb{F}_q^*)^n$. Therefore, we say that the group of semilinear isometries is the *generalized wreath product* of $\mathbb{F}_q^*$ and $\mathrm{Gal}\times S_n$ which we indicate by

$$\mathbb{F}_q^* \wr\!\wr_n (\mathrm{Gal}\times S_n).$$

Its order is equal to $(q-1)^n \cdot r \cdot n!$, and the generalization of the natural action of a wreath product (cf. 1.4.9) to this generalized wreath product is

$$(\psi;(\alpha,\pi))(v) = \big(\psi(0)\alpha(v_{\pi^{-1}(0)}),\dots,\psi(n-1)\alpha(v_{\pi^{-1}(n-1)})\big)$$

which is the action of the semilinear isometry $(\psi;(\alpha,\pi))$ on $\mathbb{F}_q^n$.

Similarly as in Section 6.1 we describe codes by their generator matrices, and obtain that the set of semilinear isometry classes of (n,k)-codes is equal to the set of orbits

$$\mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash \mathbb{F}_q^{k\times n,k}\right),$$

where the operation of $(\psi;(\alpha,\pi)) \in \mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n)$ on the orbit $\mathrm{GL}_k(q)(\Gamma)$ is given by

$$\big((\psi;(\alpha,\pi)),\mathrm{GL}_k(q)(\Gamma)\big) \mapsto \mathrm{GL}_k(q)(\hat{\Gamma}) \text{ where } \hat{\Gamma}(i) = \psi(i)\alpha(\Gamma(\pi^{-1}(i))).$$

Here again we identify the matrix Γ with the function $\Gamma\colon n \to \mathbb{F}_q^k$ where $\Gamma(i)^\top$ is the i-th column of Γ. When writing Af, we identify the function $f \in (\mathbb{F}_q^k)^n$ with the corresponding $k \times n$-matrix $(f(0)^\top \mid \dots \mid f(n-1)^\top)$. Then $Af = (A \cdot f(0)^\top \mid \dots \mid A \cdot f(n-1)^\top)$ and $Af(i) = (A \cdot f(i)^\top)^\top = f(i) \cdot A^\top$ for $A \in \mathrm{GL}_k(q)$.

We want to prove that this operation is well-defined. For $A \in \mathrm{GL}_k(q)$ and $\tilde{\Gamma}$ given by $\tilde{\Gamma}(i) := \psi(i)\alpha((A \cdot \Gamma)(\pi^{-1}(i)))$ we have $\mathrm{GL}_k(q)(\tilde{\Gamma}) = \mathrm{GL}_k(q)(\hat{\Gamma})$, since $\tilde{\Gamma}(i) = \psi(i)\alpha(A)\alpha(\Gamma(\pi^{-1}(i)))$ and $\alpha(A) \in \mathrm{GL}_k(q)$. (In Exercise 3.7.5 we have mentioned that α induces a group automorphism of $\mathrm{GL}_k(q)$ by applying α to all components of the matrices in $\mathrm{GL}_k(q)$.)

In the situation of linear isometries the actions of the isometry group and of the linear group were commuting and we obtained an action of the direct product of these two groups on $\mathbb{F}_q^{k\times n,k}$ (cf. 6.1.3).

In general, the action of the semilinear isometry group does not commute with the action of $\mathrm{GL}_k(q)$. For $A \in \mathrm{GL}_k(q)$, $(\psi;(\alpha,\pi)) \in \mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n)$ and $\Gamma \in \mathbb{F}_q^{k\times n,k}$ we have

$$A \cdot (\psi;(\alpha,\pi))\Gamma =$$
$$\big(\psi(0)A\alpha(\Gamma(\pi^{-1}(0))),\dots,\psi(n-1)A\alpha(\Gamma(\pi^{-1}(n-1)))\big)$$

and

$$(\psi;(\alpha,\pi))A \cdot \Gamma =$$
$$\big(\psi(0)\alpha(A)\alpha(\Gamma(\pi^{-1}(0))),\dots,\psi(n-1)\alpha(A)\alpha(\Gamma(\pi^{-1}(n-1)))\big).$$

Therefore, we do not get an action of the direct product as in 6.1.3.

Again, similarly as in Section 6.1 we eliminate the rank condition on the $k \times n$-matrices and consider the set of *all* $k \times n$-matrices over $\mathbb{F}_q$ which do not contain zero columns. Thus, our task is to determine the cardinality of

$$\mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^k \setminus \{0\})^n\right).$$

For this reason we describe a generalization of Lehmann's Lemma 6.1.8. We generalize it in two ways, since on the one hand we are dealing with an action of the generalized wreath product, and on the other hand this wreath product operates on $\mathrm{GL}_k(q)$-orbits of functions and not just on a set of functions. However we do not formulate it for arbitrary group actions but for the situation of the present problem.

Generalization of Lehmann's Lemma *If the mapping* **6.7.2**

$$\varphi\colon \mathrm{GL}_k(q)\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})^n \to \mathrm{GL}_k(q)\backslash\backslash\left(\mathbb{F}_q^*\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})\right)^n$$

is given by

$$\mathrm{GL}_k(q)(\Gamma)\mapsto \mathrm{GL}_k(q)(\overline{\Gamma}) \text{ where } \overline{\Gamma}(i)=\mathbb{F}_q^*(\Gamma(i)),$$

then the mapping

$$\Phi\colon \left(\mathbb{F}_q^*\wr_n(\mathrm{Gal}\times S_n)\right)\backslash\backslash\left(\mathrm{GL}_k(q)\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})^n\right)\to (\mathrm{Gal}\times S_n)\backslash\backslash\left(\mathrm{GL}_k(q)\backslash\backslash\left(\mathbb{F}_q^*\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})\right)^n\right)$$

defined by

$$\left(\mathbb{F}_q^*\wr_n(\mathrm{Gal}\times S_n)\right)(\mathrm{GL}_k(q)(\Gamma))\mapsto(\mathrm{Gal}\times S_n)(\varphi(\mathrm{GL}_k(q)(\Gamma)))$$

is a bijection. On the right hand side we have an operation of $(\mathrm{Gal}\times S_n)$ *on the set of orbits* $\mathrm{GL}_k(q)\backslash\backslash\left(\mathbb{F}_q^*\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})\right)^n$ *of the form*

$$(\alpha,\pi)\,\mathrm{GL}_k(q)(\overline{\Gamma})=\mathrm{GL}_k(q)(\hat{\Gamma})$$

where $\hat{\Gamma}(i)=\alpha(\overline{\Gamma}(\pi^{-1}(i)))=\alpha(\mathbb{F}_q^*(\Gamma(\pi^{-1}(i))))=\mathbb{F}_q^*(\alpha(\Gamma(\pi^{-1}(i)))), i\in n.$

Proof: As in the proof of 6.1.8 we see that for $f_1,f_2\in Y^X$ the following facts are equivalent:

$$\Phi(\mathbb{F}_q^*\wr_n(\mathrm{Gal}\times S_n)(f_1))=\Phi(\mathbb{F}_q^*\wr_n(\mathrm{Gal}\times S_n)(f_2))$$
$$(\mathrm{Gal}\times S_n)(\varphi(f_1))=(\mathrm{Gal}\times S_n)(\varphi(f_2))$$
$$\varphi(f_2)\in(\mathrm{Gal}\times S_n)(\varphi(f_1))$$
$$\varphi(f_2)=\alpha\circ\varphi(f_1)\circ\pi \text{ for some } \alpha\in\mathrm{Gal} \text{ and some } \pi\in S_n$$
$$\varphi(f_2)(x)=\alpha(\varphi(f_1)(\pi(x))) \text{ for some } \alpha\in\mathrm{Gal},\ \pi\in S_n, \text{ and all } x\in X$$
$$\varphi(f_2)(x)=\varphi(\alpha\circ f_1)(\pi(x)) \text{ for some } \alpha\in\mathrm{Gal},\ \pi\in S_n, \text{ and all } x\in X$$
$$\mathbb{F}_q^*(f_2(x))=\mathbb{F}_q^*((\alpha\circ f_1)(\pi(x))) \text{ for some } \alpha\in\mathrm{Gal},\ \pi\in S_n, \text{ and all } x\in X$$
$$f_2(x)\in\mathbb{F}_q^*((\alpha\circ f_1)(\pi(x))) \text{ for some } \alpha\in\mathrm{Gal},\ \pi\in S_n, \text{ and all } x\in X$$

$$f_2 = (\psi;(\alpha,\pi))f_1 \text{ for some } (\psi;(\alpha,\pi)) \in \mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n)$$
$$f_2 \in \mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n)(f_1)$$
$$\mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n)(f_2) = \mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n)(f_1).$$

Reading these implications from bottom to top we deduce that Φ is well-defined. From top to bottom it follows that Φ is injective. In order to prove that Φ is surjective, we notice that φ is surjective. □

As an immediate consequence we obtain that

$$\left|\left(\mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n)\right) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^k \setminus \{0\})^n\right)\right| =$$
$$\left|(\mathrm{Gal} \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash \mathrm{PG}_{k-1}^*(q)^n\right)\right|.$$

It is still possible to find a simpler expression for

$$(\mathrm{Gal} \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash \mathrm{PG}_{k-1}^*(q)^n\right).$$

According to Exercise 1.4.9 we can split the action of the direct product obtaining

$$\mathrm{Gal} \backslash\backslash \left(S_n \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash \mathrm{PG}_{k-1}^*(q)^n\right)\right)$$

what is the same as

$$\mathrm{Gal} \backslash\backslash \left((\mathrm{GL}_k(q) \times S_n) \backslash\backslash \mathrm{PG}_{k-1}^*(q)^n\right)$$

since the actions of $\mathrm{GL}_k(q)$ and S_n commute. An application of the automorphism α to the orbit $(\mathrm{GL}_k(q) \times S_n)(\overline{\Gamma})$ yields the orbit $(\mathrm{GL}_k(q) \times S_n)(\hat{\Gamma})$ where $\hat{\Gamma}(i) = \alpha(\overline{\Gamma}(i)) = \mathbb{F}_q^*(\alpha(\Gamma(i)))$. These orbits can be represented as the elements of

6.7.3
$$(\mathrm{P\Gamma L}_k(q) \times S_n) \backslash\backslash \mathrm{PG}_{k-1}^*(q)^n,$$

since $\mathrm{P\Gamma L}_k(q) = (\mathrm{GL}_k(q) \rtimes \mathrm{Gal})/\mathcal{Z}_k$.

The reader should carefully check the following

6.7.4 **Lemma** *Let C be a code and ι a semilinear isometry.*

- *C is nonredundant if and only if $\iota(C)$ is nonredundant.*
- *C is projective if and only if $\iota(C)$ is projective.*
- *C is injective if and only if $\iota(C)$ is injective.*
- *C is indecomposable if and only if $\iota(C)$ is indecomposable.* □

Analogously to Section 6.1 and Section 6.2 we introduce the notions

$$t_{nkq} := \left|(\mathrm{P\Gamma L}_k(q) \times S_n) \backslash\backslash \mathrm{PG}_{k-1}^*(q)^n\right|,$$

$$\overline{t}_{nkq} := \left|(\mathrm{P\Gamma L}_k(q) \times S_n) \backslash\backslash \mathrm{PG}^*_{k-1}(q)^n_{\mathrm{inj}}\right|.$$

Moreover, let v_{nkq} denote the number of semilinear isometry classes of nonredundant (n,k)-codes over $\mathbb{F}_q$ and $\overline{v}_{nkq}$ the number of semilinear isometry classes of projective (n,k)-codes over $\mathbb{F}_q$. The symbols u_{nkq} and $\overline{u}_{nkq}$ indicate the number of semilinear isometry classes of all, respectively injective, (n,k)-codes which may contain columns of zeros. The number of semilinear isometry classes of nonredundant indecomposable (n,k)-codes over $\mathbb{F}_q$ is denoted by r_{nkq} and of projective indecomposable (n,k)-codes over $\mathbb{F}_q$ by $\overline{r}_{nkq}$. These symbols are the lowercase versions of the corresponding numbers of linear isometry classes. The relations corresponding to 6.1.15 and 6.2.20 are collected in

Corollary **6.7.5**

- *t_{nkq} is the number of semilinear isometry classes of linear codes of length n and dimension at most k. If $k > 1$, then $t_{n,k-1,q}$ is also the number of $\mathrm{P\Gamma L}_k(q) \times S_n$-orbits of mappings $f \in \mathrm{PG}^*_{k-1}(q)^n$ corresponding to matrices of rank not greater than $k-1$.*
- *$\overline{t}_{nkq}$ is the number of semilinear isometry classes of injective linear codes of length n and dimension at most k.*
- *$v_{nkq} = t_{nkq} - t_{n,k-1,q}$, $\overline{v}_{nkq} = \overline{t}_{nkq} - \overline{t}_{n,k-1,q}$ for $1 < k \leq n$. The initial values for these recursions are $v_{n1q} = 1$ for $n \in \mathbb{N}^*$, $\overline{v}_{11q} = 1$ and $\overline{v}_{n1q} = 0$ for $n > 1$.*
- *$u_{nkq} = \sum_{i=k}^{n} v_{ikq}$, $\overline{u}_{kkq} = \overline{v}_{kkq}$, and $\overline{u}_{nkq} = \overline{v}_{n-1,k,q} + \overline{v}_{nkq}$ for $n > k$.*
- *For $n \geq 2$ we have*

$$r_{nkq} = v_{nkq} - \sum_a \sum_b \prod_{\substack{j=1 \\ a_j \neq 0}}^{n-1} \left(\sum_c U(c)\right),$$

where

$$U(c) = \prod_{i=1}^{j} C(S_{\nu(i,c)}, \nu(i,c))\big|_{z_\ell = r_{jiq}}$$

is a product computed from substitutions into the cycle indices of symmetric groups of degree $\nu(i,c)$ given by

$$\nu(i,c) = |\{\ell \in a_j \mid c_\ell = i\}|, \qquad 1 \leq i \leq j.$$

The first sum runs through the cycle types $a = (a_1, \ldots, a_{n-1})$ of n with at least two summands, i.e. $a_i \in \mathbb{N}$, $\sum i a_i = n$ and $\sum a_i \leq k$, while the second sum is taken over the $(n-1)$-tuples $b = (b_1, \ldots, b_{n-1}) \in \mathbb{N}^{n-1}$, for which $a_i \leq b_i \leq i a_i$, and $\sum b_i = k$. The third sum runs over all a_j-tuples $c = (c_0, \ldots, c_{a_j - 1}) \in \mathbb{N}^{a_j}$ with

the properties $j \geq c_0 \geq \ldots \geq c_{a_j-1} \geq 1$ *and* $\sum c_i = b_j$. *Analogously,* $\overline{r}_{nkq}$ *can be recursively evaluated from* $\overline{v}_{nkq}$ *and* $\overline{r}_{jiq}$ *with* $j < n$. *The initial values for these recursions are* $r_{11q} = 1 = \overline{r}_{11q}$. □

This way we have expressed all these numbers in terms of t_{nkq} and $\overline{t}_{nkq}$. The remaining problem is the evaluation of t_{nkq} and $\overline{t}_{nkq}$. In 6.7.3 we have the canonical action of a direct product on a set of functions. Since the group acting on the domain is the symmetric group it is possible to apply 6.1.21 in order to compute the generating function for the cardinalities of these orbit sets and we obtain the following

6.7.6 **Corollary** *The generating functions for the numbers* t_{nkq} *and* $\overline{t}_{nkq}$ *can be obtained from the cycle index of the natural action of the projective semilinear group on the projective space in the following way:*

$$\sum_{n\in\mathbb{N}} t_{nkq}x^n = C(\mathrm{P\Gamma L}_k(q), \mathrm{PG}^*_{k-1}(q))\big|_{z_i:=\sum_{j=0}^{\infty} x^{i\cdot j}},$$

and

$$\sum_{n\in\mathbb{N}} \overline{t}_{nkq}x^n = C(\mathrm{P\Gamma L}_k(q), \mathrm{PG}^*_{k-1}(q))\big|_{z_i:=1+x^i}.$$ □

Finally, it remains to determine the cycle index of the natural action of the projective semilinear group on the projective space. In order to obtain some numerical results we used the computer algebra system GAP [63] together with a particular extension for projective spaces [74]. Based on 6.3.3 we determined a complete system of representatives of the conjugacy classes of elements of $\mathrm{P\Gamma L}_k(q)$. We computed the cardinality of each class, and for each representative we determined the cycle type of the natural action on $\mathrm{PG}^*_{k-1}(q)$.

For $q = 4$ we obtain the Tables 6.30 to 6.35, which should be compared with the Tables 6.15 , 6.9, 6.23, 6.20, 6.12 and 6.26. (Differences between corresponding tables are marked by boldface numbers.) The next field where differences occur between linear and semilinear isometries is $\mathbb{F}_8$. On the pages 542–548 we present some tables comparing the numbers T_{nk8} and t_{nk8}, V_{nk8} and v_{nk8}, R_{nk8} and r_{nk8}, U_{nk8} and u_{nk8}, $\overline{T}_{nk8}$ and $\overline{t}_{nk8}$, $\overline{V}_{nk8}$ and $\overline{v}_{nk8}$, and $\overline{R}_{nk8}$ and $\overline{r}_{nk8}$. Extended tables can be found on the attached CD-ROM.

Exercises

E.6.7.1 **Exercise** Prove 6.7.1.

E.6.7.2 **Exercise** Prove 6.7.4.

Table 6.30 Values of t_{nk4}

$n\backslash k$	1	2	3	4	5	6
1	1	1	1	1	1	1
2	1	2	2	2	2	2
3	1	3	4	4	4	4
4	1	5	8	9	9	9
5	1	7	16	20	21	21
6	1	10	34	51	56	57
7	1	13	68	138	166	172
8	1	18	**144**	**445**	**629**	**673**
9	1	23	**309**	**1 728**	**3 322**	**3 775**
10	1	**30**	**670**	**8 640**	**31 045**	**40 323**
11	1	**37**	**1 468**	**52 924**	**543 062**	**1 047 635**
12	1	**47**	**3 251**	**360 473**	**13 107 137**	**59 070 798**
13	1	**57**	**7 156**	**2 503 187**	**336 291 123**	**4 922 753 104**
14	1	**70**	**15 665**	**16 976 798**	**8 362 677 597**	**452 322 657 324**

Table 6.31 Values of v_{nk4}

$n\backslash k$	1	2	3	4	5	6
1	1	0	0	0	0	0
2	1	1	0	0	0	0
3	1	2	1	0	0	0
4	1	4	3	1	0	0
5	1	6	9	4	1	0
6	1	9	24	17	5	1
7	1	12	55	70	28	6
8	1	17	**126**	**301**	**184**	44
9	1	22	**286**	**1 419**	**1 594**	**453**
10	1	**29**	**640**	**7 970**	**22 405**	**9 278**
11	1	**36**	**1 431**	**51 456**	**490 138**	**504 573**
12	1	**46**	**3 204**	**357 222**	**12 746 664**	**45 963 661**
13	1	**56**	**7 099**	**2 496 031**	**333 787 936**	**4 586 461 981**
14	1	**69**	**15 595**	**16 961 133**	**8 345 700 799**	**443 959 979 727**

Table 6.32 Values of r_{nk4}

$n\backslash k$	1	2	3	4	5	6
1	1	0	0	0	0	0
2	1	0	0	0	0	0
3	1	1	0	0	0	0
4	1	2	1	0	0	0
5	1	4	4	1	0	0
6	1	6	14	6	1	0
7	1	9	38	38	9	1
8	1	13	**99**	**216**	**99**	13
9	1	18	**244**	**1 213**	**1 213**	**244**
10	1	**24**	**579**	**7 479**	**20 603**	**7 479**
11	1	**31**	**1 344**	**50 328**	**480 335**	**480 335**
12	1	**40**	**3 084**	**354 655**	**12 685 278**	**45 448 958**
13	1	**50**	**6 937**	**2 490 249**	**333 368 938**	**4 573 198 774**
14	1	**62**	**15 381**	**16 948 216**	**8 342 784 710**	**443 612 918 007**

Table 6.33 Values of u_{nk4}

$n\backslash k$	1	2	3	4	5	6
1	1	0	0	0	0	0
2	2	1	0	0	0	0
3	3	3	1	0	0	0
4	4	7	4	1	0	0
5	5	13	13	5	1	0
6	6	22	37	22	6	1
7	7	34	92	92	34	7
8	8	51	**218**	**393**	**218**	51
9	9	73	**504**	**1 812**	**1 812**	**504**
10	10	**102**	**1 144**	**9 782**	**24 217**	**9 782**
11	11	**138**	**2 575**	**61 238**	**514 355**	**514 355**
12	12	**184**	**5 779**	**418 460**	**13 261 019**	**46 478 016**
13	13	**240**	**12 878**	**2 914 491**	**347 048 955**	**4 632 939 997**
14	14	**309**	**28 473**	**19 875 624**	**8 692 749 754**	**448 592 919 724**

Table 6.34 Values of $\overline{v}_{nk4}$

$n\backslash k$	1	2	3	4	5	6
1	1	0	0	0	0	0
2	0	1	0	0	0	0
3	0	1	1	0	0	0
4	0	1	2	1	0	0
5	0	1	4	3	1	0
6	0	0	8	10	4	1
7	0	0	10	35	19	5
8	0	0	13	**124**	**118**	33
9	0	0	17	**499**	**1 018**	**342**
10	0	0	**18**	**2 421**	**15 076**	**7 571**
11	0	0	**18**	**13 113**	**336 911**	**444 690**
12	0	0	17	**72 823**	**8 495 389**	**41 172 182**
13	0	0	13	**390 069**	**209 826 910**	**4 073 567 723**
14	0	0	10	**1 963 645**	**4 881 485 820**	**387 971 461 593**

Table 6.35 Values of $\overline{r}_{nk4}$

$n\backslash k$	1	2	3	4	5	6
1	1	0	0	0	0	0
2	0	0	0	0	0	0
3	0	1	0	0	0	0
4	0	1	1	0	0	0
5	0	1	3	1	0	0
6	0	0	7	5	1	0
7	0	0	10	26	8	1
8	0	0	13	**112**	**79**	12
9	0	0	17	**485**	**883**	**214**
10	0	0	**18**	**2 403**	**14 557**	**6 507**
11	0	0	**18**	**13 095**	**334 460**	**429 438**
12	0	0	17	**72 805**	**8 482 236**	**40 834 575**
13	0	0	13	**390 052**	**209 754 039**	**4 065 069 206**
14	0	0	10	**1 963 632**	**4 881 095 698**	**387 761 618 484**

Table 6.36 Values of T_{nk8}

$n\backslash k$	1	2	3	4
1	1	1	1	1
2	1	2	2	2
3	1	3	4	4
4	1	5	8	9
5	1	7	16	20
6	1	14	57	78
7	1	21	273	555
8	1	39	2 034	13 931
9	1	64	16 668	714 573
10	1	109	132 237	40 746 243
11	1	173	986 453	2 188 928 772
12	1	286	6 876 180	108 587 171 103
13	1	439	44 880 936	4 985 542 976 595
14	1	686	275 497 786	212 944 610 369 565

Table 6.37 Values of t_{nk8}

$n\backslash k$	1	2	3	4
1	1	1	1	1
2	1	2	2	2
3	1	3	4	4
4	1	5	8	9
5	1	7	16	20
6	1	12	43	62
7	1	17	143	289
8	1	27	792	4 979
9	1	40	5 806	239 355
10	1	61	44 619	13 586 393
11	1	89	329 959	729 659 322
12	1	136	2 294 446	36 195 786 755
13	1	197	14 965 218	1 661 847 901 869
14	1	292	91 842 474	70 981 537 714 473

Table 6.38 Values of V_{nk8}

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	1	1	0	0
3	1	2	1	0
4	1	4	3	1
5	1	6	9	4
6	1	13	43	21
7	1	20	252	282
8	1	38	1 995	11 897
9	1	63	16 604	697 905
10	1	108	132 128	40 614 006
11	1	172	986 280	2 187 942 319
12	1	285	6 875 894	108 580 294 923
13	1	438	44 880 497	4 985 498 095 659
14	1	685	275 497 100	212 944 334 871 779

Table 6.39 Values of v_{nk8}

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	1	1	0	0
3	1	2	1	0
4	1	4	3	1
5	1	6	9	4
6	1	11	31	19
7	1	16	126	146
8	1	26	765	4 187
9	1	39	5 766	233 549
10	1	60	44 558	13 541 774
11	1	88	329 870	729 329 363
12	1	135	2 294 310	36 193 492 309
13	1	196	14 965 021	1 661 832 936 651
14	1	291	91 842 182	70 981 445 871 999

Table 6.40 Values of R_{nk8}

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	1	0	0	0
3	1	1	0	0
4	1	2	1	0
5	1	4	4	1
6	1	10	33	10
7	1	17	231	231
8	1	34	1 956	11 596
9	1	59	16 529	695 614
10	1	103	131 993	40 595 108
11	1	167	986 040	2 187 791 284
12	1	279	6 875 485	108 579 157 553
13	1	432	44 879 807	4 985 490 082 276
14	1	678	275 495 976	212 944 281 977 581

Table 6.41 Values of r_{nk8}

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	1	0	0	0
3	1	1	0	0
4	1	2	1	0
5	1	4	4	1
6	1	8	21	8
7	1	13	107	107
8	1	22	732	4 024
9	1	35	5 709	232 626
10	1	55	44 465	13 535 084
11	1	83	329 720	729 278 112
12	1	129	2 294 075	36 193 111 160
13	1	190	14 964 655	1 661 830 261 138
14	1	284	91 841 624	70 981 428 231 327

Table 6.42 Values of U_{nk8}

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	2	1	0	0
3	3	3	1	0
4	4	7	4	1
5	5	13	13	5
6	6	26	56	26
7	7	46	308	308
8	8	84	2 303	12 205
9	9	147	18 907	710 110
10	10	255	151 035	41 324 116
11	11	427	1 137 315	2 229 266 435
12	12	712	8 013 209	110 809 561 358
13	13	1 150	52 893 706	5 096 307 657 017
14	14	1 835	328 390 806	218 040 642 528 796

Table 6.43 Values of u_{nk8}

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	2	1	0	0
3	3	3	1	0
4	4	7	4	1
5	5	13	13	5
6	6	24	44	24
7	7	40	170	170
8	8	66	935	4 357
9	9	105	6 701	237 906
10	10	165	51 259	13 779 680
11	11	253	381 129	743 109 043
12	12	388	2 675 439	36 936 601 352
13	13	584	17 640 460	1 698 769 538 003
14	14	875	109 482 642	72 680 215 410 002

Table 6.44 Values of $\overline{T}_{nk8}$

$n\backslash k$	1	2	3	4
1	1	1	1	1
2	0	1	1	1
3	0	1	2	2
4	0	1	3	4
5	0	1	5	8
6	0	1	25	39
7	0	1	132	364
8	0	1	901	11 408
9	0	1	6 155	619 402
10	0	0	38 344	34 810 827
11	0	0	217 432	1 812 498 279
12	0	0	1 119 290	86 640 720 291
13	0	0	5 242 484	3 818 392 707 185
14	0	0	22 449 375	156 004 978 540 987

Table 6.45 Values of $\overline{t}_{nk8}$

$n\backslash k$	1	2	3	4
1	1	1	1	1
2	0	1	1	1
3	0	1	2	2
4	0	1	3	4
5	0	1	5	8
6	0	1	15	27
7	0	1	58	164
8	0	1	327	3 940
9	0	1	2 101	206 934
10	0	0	12 870	11 605 307
11	0	0	72 638	604 172 431
12	0	0	373 366	28 880 263 069
13	0	0	1 747 940	1 272 797 652 589
14	0	0	7 483 895	52 001 659 817 699

Table 6.46 Values of $\overline{V}_{nk8}$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	0	1	0	0
3	0	1	1	0
4	0	1	2	1
5	0	1	4	3
6	0	1	24	14
7	0	1	131	232
8	0	1	900	10 507
9	0	1	6 154	613 247
10	0	0	38 344	34 772 483
11	0	0	217 432	1 812 280 847
12	0	0	1 119 290	86 639 601 001
13	0	0	5 242 484	3 818 387 464 701
14	0	0	22 449 375	156 004 956 091 612

Table 6.47 Values of $\overline{v}_{nk8}$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	0	1	0	0
3	0	1	1	0
4	0	1	2	1
5	0	1	4	3
6	0	1	14	12
7	0	1	57	106
8	0	1	326	3 613
9	0	1	2 100	204 833
10	0	0	12 870	11 592 437
11	0	0	72 638	604 099 793
12	0	0	373 366	28 879 889 703
13	0	0	1 747 940	1 272 795 904 649
14	0	0	7 483 895	52 001 652 333 804

Table 6.48 Values of $\overline{R}_{nk8}$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	0	0	0	0
3	0	1	0	0
4	0	1	1	0
5	0	1	3	1
6	0	1	23	9
7	0	1	130	207
8	0	1	899	10 374
9	0	1	6 153	612 345
10	0	0	38 343	34 766 326
11	0	0	217 432	1 812 242 500
12	0	0	1 119 290	86 639 383 565
13	0	0	5 242 484	3 818 386 345 408
14	0	0	22 449 375	156 004 950 849 125

Table 6.49 Values of $\overline{r}_{nk8}$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	0	0	0	0
3	0	1	0	0
4	0	1	1	0
5	0	1	3	1
6	0	1	13	7
7	0	1	56	91
8	0	1	325	3 554
9	0	1	2 099	204 505
10	0	0	12 869	11 590 334
11	0	0	72 638	604 086 920
12	0	0	373 366	28 879 817 061
13	0	0	1 747 940	1 272 795 531 280
14	0	0	7 483 895	52 001 650 585 861

6.8 Local Isometries

6.8

Let C and C' be two (n,k)-codes over $\mathbb{F}_q$. A *local linear isometry* between these two codes is a vector space isomorphism $\iota\colon C \to C'$ which preserves the distances between all pairs of codewords, i.e. $d(c_1,c_2) = d(\iota(c_1),\iota(c_2))$ for all $c_1,c_2 \in C$. So far we have shown in Section 1.4 that the linear isometries of $\mathbb{F}_q^n$, the *global linear isometries*, are the elements of $M_n(q)$. From 1.4.12 we know that $M_n(q)$ is isomorphic to the wreath product $\mathbb{F}_q^* \wr_n S_n$.

A *local semilinear isometry* between the two codes C and C' is a semilinear bijection $\sigma\colon C \to C'$ which preserves the distances between all pairs of codewords, i.e. $d(c_1,c_2) = d(\sigma(c_1),\sigma(c_2))$ for all $c_1,c_2 \in C$. So far we have shown in Section 6.7 that the semilinear isometries of $\mathbb{F}_q^n$, the *global semilinear isometries*, are the elements of the generalized wreath product $\mathbb{F}_q^* \wr\wr_n (\mathrm{Gal} \times S_n)$.

In general a *local isometry* is a local linear or semilinear isometry. We want to prove that every local isometry between two (n,k)-codes can be extended to a global isometry of $\mathbb{F}_q^n$. This means that the set of local linear isometries between two linear (n,k)-codes is the wreath product $\mathbb{F}_q^* \wr_n S_n$ (cf. also [84, second edition, Section 9.1]) and the set of local semilinear isometries between two linear (n,k)-codes is the generalized wreath product $\mathbb{F}_q^* \wr\wr_n (\mathrm{Gal} \times S_n)$.

As a generalization of Exercise 1.2.6 we obtain

Theorem *If C is a linear code of length n over $\mathbb{F}_q$, then for any $i \in n$ either the i-th component of all codewords is equal to 0, or each element $\alpha \in \mathbb{F}_q$ occurs as the i-th component of exactly $|C|/q$ codewords.* □ **6.8.1**

First we associate an (n,k)-code C over $\mathbb{F}_q$ with the $q^k \times n$-matrix

$$M(C) = \begin{pmatrix} c^{(0)} \\ \vdots \\ c^{(q^k-1)} \end{pmatrix},$$

where the rows of the matrix are the codewords of C in a fixed but arbitrary order. If ι is a local isometry between C and C', then we assume that

$$M(C') = M(\iota(C)) = \begin{pmatrix} \iota(c^{(0)}) \\ \vdots \\ \iota(c^{(q^k-1)}) \end{pmatrix},$$

where the ordering of the rows of $M(C')$ is determined by the ordering of the rows of C.

Moreover, let $d_i^\top$, $d_i \in \mathbb{F}_q^{q^k}$, $i \in n$, be the i-th column of the matrix

$$M(C) = \left(d_0^\top \mid \ldots \mid d_{n-1}^\top\right).$$

We introduce an equivalence relation on the columns of $M(C)$. Two columns $d_i^\top$ and $d_j^\top$ are considered to be equivalent if there exists some $\kappa \in \mathbb{F}_q^*$ such that $d_i = \kappa d_j$. We call them proportional. (In general, two vectors v, w over $\mathbb{F}_q$ are *proportional* if there exists some $\kappa \in \mathbb{F}_q^*$ such that $v = \kappa w$.) A column $d_i^\top$ is called a zero column if all the components of d_i are equal to 0. The equivalence class of a zero column consists of all zero columns of $M(C)$. If $d_i^\top$ is not a zero column, then the equivalence class of $d_i^\top$ consists of all columns of $M(C)$ which are proportional to $d_i^\top$.

6.8.2 Lemma *Two locally isometric linear (n,k)-codes C and C' have the same number of zero columns.*

Proof: Assume that $d_i^\top$ is not a zero column of $M(C)$. According to 6.8.1, each element $\kappa \in \mathbb{F}_q$ occurs exactly q^{k-1} times in d_i. If we assume that C and C' have r, respectively, r' zero columns, then we obtain

$$(n-r)q^{k-1}(q-1) = \sum_{c \in C} \mathrm{wt}(c) = \sum_{c \in C'} \mathrm{wt}(c) = (n-r')q^{k-1}(q-1).$$

Consequently, $r = r'$. □

In the next step we want to describe the equivalence class of a nonzero column. The *cross section* of a code C is similarly defined as the shortening of C (cf. 2.2.17). Let i be the index of a column of $M(C)$ which is not a zero column, then the cross section of C at position i is the code

$$C_i := \{c = (c_0, \ldots, c_{n-1}) \in C \mid c_i = 0\}.$$

Consequently, C_i is an $(n, k-1, \geq d, q)$-code. The shortening of C in position i is obtained from the cross section of C in position i by deleting the i-th column of C_i.

6.8.3 Lemma *Let C be a linear (n,k)-code over $\mathbb{F}_q$. Two columns $d_i^\top \neq 0 \neq d_j^\top$ of $M(C)$ are proportional if and only if the cross sections C_i and C_j coincide.*

Proof: Assume that $d_i^\top$ and $d_j^\top$ are proportional. Then for each $c \in C$ we have $c_i = 0$ if and only if $c_j = 0$. Hence, the cross sections C_i and C_j describe the same code.

Conversely, we assume that $C_i = C_j$. We choose any two codewords $c, \tilde{c}$ of C which do not belong to C_i, whence $c_i \neq 0$, $\tilde{c}_i \neq 0$, $c_j \neq 0$, and $\tilde{c}_j \neq 0$. Then $f := c_i^{-1}c - \tilde{c}_i^{-1}\tilde{c}$ belongs to C and $f_i = 0$. Thus $f \in C_i$ and, consequently, $f_j = 0$. Since $f_j = c_i^{-1}c_j - \tilde{c}_i^{-1}\tilde{c}_j$, we obtain $c_i^{-1}c_j = \tilde{c}_i^{-1}\tilde{c}_j = \alpha \in \mathbb{F}_q^*$, and thus $c_j = \alpha c_i$ and $\tilde{c}_j = \alpha \tilde{c}_i$. This fact holds true for fixed $c \in C \setminus C_i$ and for any $\tilde{c} \in C \setminus C_i$, whence the columns $d_i^\top$ and $d_j^\top$ are proportional. □

Now we prove that if $\iota\colon C \to C'$ is a local linear isometry, then there exists a permutation $\pi \in S_n$ such that the i-th column of $M(C)$ is proportional to the $\pi(i)$-th column of $M(C')$ for $i \in n$. This fact shows then that ι can be described as an element $(\psi;\pi)$ of $\mathbb{F}_q^* \wr_n S_n$. Thus it is a linear isometry of $\mathbb{F}_q^n$.

Theorem 6.8.4 *Assume that $\iota\colon C \to C'$ is a local linear isometry between two linear (n,k)-codes over $\mathbb{F}_q$. Then there exists a permutation $\pi \in S_n$ such that the i-th column of $M(C)$ is proportional to the $\pi(i)$-th column of $M(C')$ for $i \in n$.*

Proof: To begin with, we determine the equivalence classes of the columns of $M(C)$. From 6.8.2 we know that $M(C)$ and $M(C')$ have the same number of zero columns, which we indicate by s.

Let $d_i^\top$ be a nonzero column of $M(C)$, and let $i = i_0, \dots, i_{r-1}$ indicate the indices of the columns of $M(C)$ proportional to $d_i^\top$. Then all the cross sections $C_i = C_{i_0}, C_{i_1}, \dots, C_{i_{r-1}}$ determine the same $(n,k-1)$-code. The matrix $M(C_i)$ has $r+s$ zero columns, namely $d_{i_0}^\top, \dots, d_{i_{r-1}}^\top$, which come from the construction as a cross section in these columns, and $d_{i_r}^\top, \dots, d_{i_{r+s-1}}^\top$, which are the zero columns appearing already in $M(C)$.

Since ι is a local linear isometry between C and C', also the restriction $\iota|_{C_i}$ is a linear isometry between C_i and $\iota(C_i)$, whence by 6.8.2, $M(C_i)$ and $M(\iota(C_i))$ have the same number of zero columns. Let us assume that the indices of the zero columns of $M(\iota(C_i))$ are given by $j_0, \dots, j_{r+s-1}$, and that $j_r, \dots, j_{r+s-1}$ are the indices of the s zero columns of $M(C')$. From 6.8.1 we know that in any of the columns $d_{j_0}'^\top, \dots, d_{j_{r-1}}'^\top$ of $M(C')$ each element of $\mathbb{F}_q$ occurs exactly q^{k-1} times. Hence, $\iota(C_i)$ is the cross section of C' in any of the components $j_0, \dots, j_{r-1}$, for instance, $M(\iota(C_i)) = M(C'_{j_0})$. According to 6.8.3, the columns of $M(C')$ with indices $j_0, \dots, j_{r-1}$ are proportional and form an equivalence class of columns of $M(C')$.

Next we claim that the columns $d_{i_0}^\top$ and $d_{j_0}'^\top$ are proportional, i.e. there exists an element $\lambda \in \mathbb{F}_q^*$ such that $d_{j_0}'^\top = \lambda d_{i_0}^\top$. Assume that $b = (b_0, \dots, b_{n-1})$ with $b_{i_0} = 1$ belongs to $C \setminus C_{i_0}$. Then $\iota(b) \in \iota(C \setminus C_{i_0}) = \iota(C) \setminus \iota(C_{i_0}) = C' \setminus C'_{j_0}$, whence the j_0-th component of $\iota(b)$, which we indicate as $\iota(b)_{j_0}$, is different from zero. Now take an arbitrary $c \in C \setminus C_{i_0}$. Since C_{i_0} is a $(k-1)$-dimensional subspace of C, there exist uniquely determined $\tilde{c} \in C_{i_0}$ and $\kappa \in \mathbb{F}_q$ such that $c = \tilde{c} + \kappa b$. Consequently, $\kappa = c_{i_0} \neq 0$. Since $\iota(\tilde{c}) \in C'_{j_0}$, the j_0-th component of $\iota(c) = \iota(\tilde{c}) + \kappa\iota(b)$ is equal to $c_{i_0}\iota(b)_{j_0}$. This holds true for any $c \in C \setminus C_{i_0}$, whence the i_0-th column of $M(C)$ is proportional to the j_0-th column of $M(C')$ with the nonzero factor $\lambda = \iota(b)_{j_0}$.

Finally, this method allows us to determine a permutation $\pi \in S_n$ in the following way. From the previous discussion we already know that C and C'

have the same number of zero columns, and if $d_i^\top \neq 0$ belongs to an equivalence class of r columns of $M(C)$, then we can find an equivalence class containing exactly r columns of $M(C')$ which are all proportional to $d_i^\top$. Hence, it is possible to determine π so that π maps zero columns of $M(C)$ to zero columns of $M(C')$ and each nonzero column $d_i^\top$ of $M(C)$ to a proportional column of $M(C')$. □

Thus for each $c \in C$ we have

$$\iota(c) = \big(\psi(0)c_{\pi^{-1}(0)}, \ldots, \psi(n-1)c_{\pi^{-1}(n-1)}\big),$$

for some $\psi(\mathbb{F}_q^*)^n$.

Now let $\sigma\colon C \to C'$ be a local semilinear isometry with $\sigma(\kappa c) = \alpha(\kappa)\sigma(c)$ for $c \in C$, $\kappa \in \mathbb{F}_q$, where $\alpha \in \mathrm{Gal} := \mathrm{Gal}\,[\,\mathbb{F}_q : \mathbb{F}_p\,]$. We want to show that there exists a permutation $\pi \in S_n$ such that the image of the i-th column of $M(C)$ under α is proportional to the $\pi(i)$-th column of $M(C')$ for $i \in n$. This fact shows then that σ can be described as an element $(\psi; (\alpha, \pi))$ of $\mathbb{F}_q^* \wr_n (\mathrm{Gal} \times S_n)$. Thus it is a semilinear isometry of $\mathbb{F}_q^n$. The proof is based on the fact that the image of a subspace under a semilinear mapping is again a subspace.

6.8.5 Theorem *Assume that $\sigma\colon C \to C'$ is a local semilinear isometry between two linear (n,k)-codes over $\mathbb{F}_q$ with $\sigma(\kappa c) = \alpha(\kappa)\sigma(c)$ for $c \in C$, $\kappa \in \mathbb{F}_q$, where $\alpha \in \mathrm{Gal}$. Let $d_i^\top$ and $d_j'^\top$ be the columns of $M(C)$, respectively $M(C')$. Then there exists a permutation $\pi \in S_n$ such that $\alpha(d_i^\top)$ is proportional to $d_{\pi(i)}'^\top$ for $i \in n$.*

Proof: Only a few arguments must be changed in order to adapt the previous proof to local semilinear isometries. From 6.8.2 we know that $M(C)$ and $M(C')$ have the same number of zero columns, which we indicate by s.

Let $d_i^\top$ be a nonzero column of $M(C)$, and let $i = i_0, \ldots, i_{r-1}$ indicate the indices of the columns of $M(C)$ proportional to $d_i^\top$. Then all the cross sections $C_i = C_{i_0}, C_{i_1}, \ldots, C_{i_{r-1}}$ determine the same $(n, k-1)$-code. The matrix $M(C_i)$ has $r+s$ zero columns, namely $d_{i_0}^\top, \ldots, d_{i_{r-1}}^\top$, which come from the construction as a cross section in these columns, and $d_{i_r}^\top, \ldots, d_{i_{r+s-1}}^\top$, which are the zero columns appearing already in $M(C)$.

Since σ is a local semilinear isometry between C and C', also the restriction $\sigma|_{C_i}$ is a semilinear isometry between C_i and $\sigma(C_i)$, whence by 6.8.2, $M(C_i)$ and $M(\sigma(C_i))$ have the same number of zero columns. Let us assume that the indices of the zero columns of $M(\sigma(C_i))$ are given by $j_0, \ldots, j_{r+s-1}$, and that $j_r, \ldots, j_{r+s-1}$ are the indices of the s zero columns of $M(C')$. As above, $\sigma(C_i)$ is the cross section of C' in any of the components $j_0, \ldots, j_{r-1}$, for instance, $M(\iota(C_i)) = M(C'_{j_0})$. According to 6.8.3, the columns of $M(C')$ with indices $j_0, \ldots, j_{r-1}$ are proportional and form an equivalence class of columns of $M(C')$.

Next we claim that the columns $\alpha(d_{i_0}^\top)$ and $d_{j_0}'^\top$ are proportional, i.e. there exists some $\lambda \in \mathbb{F}_q^*$ such that $d_{j_0}'^\top = \lambda\alpha(d_{i_0}^\top)$. Assume that $b = (b_0, \ldots, b_{n-1})$ with $b_{i_0} = 1$ belongs to $C \setminus C_{i_0}$. Then $\sigma(b) \in C' \setminus C'_{j_0}$, whence the j_0-th component of $\sigma(b)$, which we indicate as $\sigma(b)_{j_0}$, is different from zero. Now take an arbitrary $c \in C \setminus C_{i_0}$. Since C_{i_0} is a $(k-1)$-dimensional subspace of C, there exist uniquely determined $\tilde{c} \in C_{i_0}$ and $\kappa \in \mathbb{F}_q$ such that $c = \tilde{c} + \kappa b$. Consequently, $\kappa = c_{i_0} \neq 0$. Since $\sigma(\tilde{c}) \in C'_{j_0}$, the j_0-th component of $\sigma(c) = \sigma(\tilde{c}) + \alpha(\kappa)\sigma(b)$ is equal to $\alpha(c_{i_0})\sigma(b)_{j_0}$. This holds true for any $c \in C \setminus C_{i_0}$, whence $\alpha(d_{i_0}^\top)$, the image of the i_0-th column of $M(C)$ under α, is proportional to the j_0-th column of $M(C')$ with the nonzero factor $\lambda = \sigma(b)_{j_0}$.

Using the same ideas as in the previous proof, we determine a permutation $\pi \in S_n$ so that $\alpha(d_i^\top)$ and $d_{\pi(i)}'^\top$, $i \in n$, are proportional. □

Thus for each $c \in C$ we have

$$\sigma(c) = \big(\psi(0)\alpha(c_{\pi^{-1}(0)}), \ldots, \psi(n-1)\alpha(c_{\pi^{-1}(n-1)})\big),$$

for some $\psi \in (\mathbb{F}_q^*)^n$.

Exercises

Exercise Prove 6.8.1. **E.6.8.1**

6.9 Existence and Construction of Normal Bases 6.9

In Section 3.3 normal bases of a field extension were introduced. So far we have not shown that it is always possible to find a normal basis. Our proof is based on some notions from module theory, which were presented in the meantime. An interesting and detailed discussions of normal bases can be found in [62].

In Section 6.3 we have shown that for any endomorphism A of $\mathbb{F}_q^n$ the vector space $\mathbb{F}_q^n$ becomes an $\mathbb{F}_q[x]$-module by 6.3.5. Here we repeat the outer multiplication once again

$$\mathbb{F}_q[x] \times \mathbb{F}_q^n \to \mathbb{F}_q^n \ : \ (f, v) \mapsto fv := f(A)v := \sum_{i=0}^{d} \kappa_i A^i v,$$

where f is the polynomial $\sum_{i=0}^{d} \kappa_i x^i$. If A is represented by a matrix then $A^i v$ is the matrix multiplication $v \cdot (A^i)^\top$. The minimal polynomial M_A of A is the monic polynomial $f \in \mathbb{F}_q[x]$ of least degree so that $f(A) = 0$. If we have a matrix representation of the endomorphism A with respect to the basis B of $\mathbb{F}_q^n$ over $\mathbb{F}_q$, then the characteristic polynomial χ_A of A is defined as the determinant $\chi_A(x) := \det(xI_n - A) \in \mathbb{F}_q[x]$, where I_n is the $n \times n$-unit matrix. The

characteristic polynomial is always a polynomial of degree n. It does not depend on the particular choice of the basis B. By the Cayley–Hamilton Theorem 6.3.11 it satisfies $\chi_A(A) = 0$, whence the minimal polynomial M_A is a divisor of the characteristic polynomial χ_A.

Considered as a linear $\mathbb{F}_q$-space, $\mathbb{F}_{q^n}$ is isomorphic to $\mathbb{F}_q^n$, thus it is also an $\mathbb{F}_q[x]$-module: For any endomorphism α of $\mathbb{F}_{q^n}$ we obtain a module structure

$$\mathbb{F}_q[x] \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \;:\; (f, \kappa) \mapsto f\kappa := f(\alpha)(\kappa) := \sum_{i=0}^{d} \kappa_i \alpha^i(\kappa),$$

where f is the polynomial $\sum_{i=0}^{d} \kappa_i x^i$. In the present section we always consider $\alpha = \tau$, the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In order to show that a normal basis exists for each extension field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we apply Dedekind's Independence Theorem 3.3.6 to the n distinct powers of the Frobenius automorphism τ.

6.9.1 **Lemma** *For $n \geq 1$ let $\tau : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be the Frobenius automorphism $\tau(\beta) = \beta^q$. Then the vector space $\mathbb{F}_{q^n}$ is a cyclic $\mathbb{F}_q[x]$-module.*

Proof: Since τ^n is the identity on $\mathbb{F}_{q^n}$, the minimal polynomial of τ is a divisor of $x^n - 1$. The automorphisms $\tau^0, \tau^1, \ldots, \tau^{n-1}$ are pairwise distinct, whence by Dedekind's Independence Theorem they are linearly independent over $\mathbb{F}_q$. For this reason, the degree of the minimal polynomial of τ is at least n. Consequently, $x^n - 1$ is the minimal polynomial of τ.

Moreover, n is the dimension of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$. Therefore, $x^n - 1$ is also the characteristic polynomial of τ. Thus, the minimal polynomial and the characteristic polynomial of τ coincide, and according to Exercise 6.3.7, the $\mathbb{F}_q[x]$-module $\mathbb{F}_{q^n}$ is cyclic. □

This allows us to prove the existence of a normal basis.

6.9.2 **The Existence of normal bases** *Let n be a positive integer. For any finite field $\mathbb{F}_q$ and its extension $\mathbb{F}_{q^n}$ there exists $\kappa \in \mathbb{F}_{q^n}$ so that*

$$\left\{\kappa, \tau(\kappa), \ldots, \tau^{n-1}(\kappa)\right\}$$

is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Proof: Since $\mathbb{F}_{q^n}$ is a cyclic $\mathbb{F}_q[x]$-module, according to 6.9.1, there exists some $\kappa \in \mathbb{F}_{q^n}$ so that

$$\mathbb{F}_{q^n} = \mathbb{F}_q[x]\kappa = \left\{f\kappa \mid f \in \mathbb{F}_q[x]\right\}.$$

Since the minimal polynomial of τ is of degree n, we can restrict ourselves to polynomials f of degree less than n, obtaining

$$\mathbb{F}_{q^n} = \left\{f\kappa \mid f \in \mathbb{F}_q[x],\ \deg f < n\right\}.$$

Consequently, there exist n polynomials $f_0, \ldots, f_{n-1}$ with $\deg f_i < n$ for $i \in n$, so that $\{f_0\kappa, \ldots, f_{n-1}\kappa\}$ is a basis of $\mathbb{F}_{q^n}$. Since each f_i is a linear combination of x^j for $j \in n$, we finally deduce that $\{\kappa, \tau(\kappa), \ldots, \tau^{n-1}(\kappa)\}$ is also a basis of $\mathbb{F}_{q^n}$. (Here we use the polynomials $f_i(x) = x^i$.) This is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. □

It is even possible to show that for any finite field $\mathbb{F}_q$ and its extension $\mathbb{F}_{q^n}$, where n is a positive integer, there exists a primitive element $\kappa \in \mathbb{F}_{q^n}$ so that

$$\left\{\kappa, \tau(\kappa), \ldots, \tau^{n-1}(\kappa)\right\}$$

is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ (cf. [127]).

Now we describe how to construct a normal basis. There exist both probabilistic and deterministic algorithms for finding a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We will present both approaches.

Definition (trace function) The *trace function* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is defined by **6.9.3**

$$\mathrm{Tr}\colon \mathbb{F}_{q^n} \to \mathbb{F}_q \;:\; \alpha \mapsto \mathrm{Tr}(\alpha) := \sum_{i\in n} \alpha^{q^i}. \qquad \diamond$$

It is easy to prove that the trace function is a homomorphism.

An element $\kappa \in \mathbb{F}_{q^n}$ is called *normal* over $\mathbb{F}_q$ if $\{\kappa, \tau(\kappa), \ldots, \tau^{n-1}(\kappa)\}$ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

In order to characterize whether a given set of n elements forms a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ we introduce the *discriminant* $\Delta\colon \mathbb{F}_{q^n}^n \to \mathbb{F}_q$ defined by

$$\Delta(\alpha_0, \ldots, \alpha_{n-1}) := \det \begin{pmatrix} \mathrm{Tr}(\alpha_0\alpha_0) & \ldots & \mathrm{Tr}(\alpha_0\alpha_{n-1}) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}(\alpha_{n-1}\alpha_0) & \ldots & \mathrm{Tr}(\alpha_{n-1}\alpha_{n-1}) \end{pmatrix}.$$

Theorem *The set $\{\alpha_0, \ldots, \alpha_{n-1}\} \subseteq \mathbb{F}_{q^n}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\Delta(\alpha_0, \ldots, \alpha_{n-1}) \neq 0$.* **6.9.4**

Proof: Assume that $\{\alpha_0, \ldots, \alpha_{n-1}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We show that the row vectors of the matrix used to define Δ are linearly independent over $\mathbb{F}_q$. Assume that for $c_0, \ldots, c_{n-1} \in \mathbb{F}_q$ we have

$$\sum_{i\in n} c_i \big(\mathrm{Tr}(\alpha_i\alpha_0), \ldots, \mathrm{Tr}(\alpha_i\alpha_{n-1})\big) = 0,$$

then

$$\sum_{i\in n} c_i \,\mathrm{Tr}(\alpha_i\alpha_j) = 0, \qquad j \in n.$$

For $\beta := \sum_{i\in n} c_i\alpha_i$ we have

$$\begin{aligned}\operatorname{Tr}(\beta\alpha_j) &= \sum_{k\in n}(\beta\alpha_j)^{q^k} = \sum_{k\in n}\Big(\sum_{i\in n} c_i\alpha_i\alpha_j\Big)^{q^k}\\ &= \sum_{k\in n}\sum_{i\in n} c_i\,(\alpha_i\alpha_j)^{q^k} = \sum_{i\in n} c_i\operatorname{Tr}(\alpha_i\alpha_j) = 0, \qquad j\in n.\end{aligned}$$

Since the trace is a vector space homomorphism and $\{\alpha_0,\dots,\alpha_{n-1}\}$ is a basis of $\mathbb{F}_{q^n}$, we have $\operatorname{Tr}(\beta\alpha) = 0$ for all $\alpha \in \mathbb{F}_{q^n}$. This is only possible for $\beta = 0$, whence $\sum_{i\in n} c_i\alpha_i = 0$ and consequently $c_0 = \ldots = c_{n-1} = 0$.

Conversely, assume that $\Delta(\alpha_0,\dots,\alpha_{n-1}) \neq 0$ and $\sum_{i\in n} c_i\alpha_i = 0$ for some $c_0,\dots,c_{n-1} \in \mathbb{F}_q$. Then $\sum_{i\in n} c_i\alpha_i\alpha_j = 0$ for $j \in n$ and by applying the trace function

$$0 = \operatorname{Tr}(0) = \operatorname{Tr}\Big(\sum_{i\in n} c_i\alpha_i\alpha_j\Big) = \sum_{i\in n} c_i\operatorname{Tr}(\alpha_i\alpha_j), \qquad j\in n.$$

By assumption the rows of the matrix in the definition of $\Delta(\alpha_0,\dots,\alpha_{n-1})$ are linearly independent, whence $c_0 = \ldots = c_{n-1} = 0$ and, therefore, $\alpha_0,\dots,\alpha_{n-1}$ are linearly independent over $\mathbb{F}_q$. □

6.9.5 **Corollary** *The set $\{\alpha_0,\dots,\alpha_{n-1}\} \subseteq \mathbb{F}_{q^n}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if the matrix*

$$A := \begin{pmatrix} \alpha_0 & \dots & \alpha_{n-1}\\ \alpha_0^q & \dots & \alpha_{n-1}^q\\ \vdots & \ddots & \vdots\\ \alpha_0^{q^{n-1}} & \dots & \alpha_{n-1}^{q^{n-1}}\end{pmatrix}$$

is regular.

Proof: $\{\alpha_0,\dots,\alpha_{n-1}\}$ is a basis if and only if $\Delta(\alpha_0,\dots,\alpha_{n-1}) \neq 0$. As a matter of fact, $\Delta(\alpha_0,\dots,\alpha_{n-1}) = \det(A^\top\cdot A) = (\det A)^2$. □

The probabilistic algorithm for finding a normal basis is based upon

6.9.6 **Theorem (Artin [3])** *Consider an irreducible polynomial f of degree n over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ a root of f. Let*

$$g(x) := \frac{f(x)}{(x-\alpha)f'(\alpha)} \in \mathbb{F}_{q^n}[x].$$

Then there exist at least $q - n(n-1)$ elements $\kappa \in \mathbb{F}_q$ so that $g(\kappa)$ is normal over $\mathbb{F}_q$.

Proof: For $i \in n$ let $\alpha_i := \tau^i(\alpha)$ and $g_i(x) := \tau^i(g(x))$, where τ is the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then

$$g_i(x) = \frac{f(x)}{(x-\alpha_i)f'(\alpha_i)}$$

is a polynomial in $\mathbb{F}_{q^n}[x]$ of degree $n-1$ with roots α_k for $k \neq i$ and $g_i(\alpha_i) = 1$. Hence,

$$g_i(x)g_k(x) \equiv 0 \bmod \mathrm{I}(f), \qquad i \neq k. \tag{6.9.7}$$

Moreover,

$$\sum_{i\in n} g_i(x) - 1 = 0, \tag{6.9.8}$$

since the left-hand side is a polynomial of degree at most $n-1$ with n roots $\alpha_0, \ldots, \alpha_{n-1}$. Multiplying 6.9.8 by $g_i(x)$ and using 6.9.7 yields

$$g_i(x) \equiv \big(g_i(x)\big)^2 \bmod \mathrm{I}(f). \tag{6.9.9}$$

Let D be the matrix

$$D := \begin{pmatrix} g_0(x) & g_1(x) & \ldots & g_{n-1}(x) \\ g_1(x) & g_2(x) & \ldots & g_0(x) \\ \ldots & \ldots & \ldots & \\ g_{n-1}(x) & g_0(x) & \ldots & g_{n-2}(x) \end{pmatrix},$$

then $D^\top = D$. Because of 6.9.9 and 6.9.8, the diagonal elements of $D^\top \cdot D$ are of the form

$$\sum_{i\in n} g_i(x)^2 \equiv \sum_{i\in n} g_i(x) = 1 \bmod \mathrm{I}(f).$$

All the other entries of $D^\top \cdot D$ are 0 because of 6.9.7. Let $D(x) := \det D$. We obtain $D(x)^2 \equiv 1 \bmod \mathrm{I}(f)$. This means that $D(x)$ is a nonzero polynomial. By construction its degree is at most $n(n-1)$. Therefore, $D(x)$ has at most $n(n-1)$ roots.

Consider some $u \in \mathbb{F}_q$ with $D(u) \neq 0$. Then the matrix

$$\begin{pmatrix} g_0(u) & g_1(u) & \ldots & g_{n-1}(u) \\ g_1(u) & g_2(u) & \ldots & g_0(u) \\ \ldots & \ldots & \ldots & \\ g_{n-1}(u) & g_0(u) & \ldots & g_{n-2}(u) \end{pmatrix} =$$

$$\begin{pmatrix} g(u) & \tau(g(u)) & \ldots & \tau^{n-1}(g(u)) \\ \tau(g(u)) & \tau^2(g(u)) & \ldots & g(u) \\ \ldots & \ldots & \ldots & \\ \tau^{n-1}(g(u)) & g(u) & \ldots & \tau^{n-2}(g(u)) \end{pmatrix}$$

is regular, whence by 6.9.5, $\{g(u), \tau(g(u)), \ldots, \tau^{n-1}(g(u))\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In fact, it is a normal basis. □

6.9.10 Algorithm (Generate a normal element)

Input: q, n, an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree n, and α a root of f.

Output: A normal element or an error message. If $q > n(n-1)$ the output β is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

(1) If $q \leq n(n-1)$ terminate the algorithm and output an error message.

(2) Determine g as in 6.9.6.

(3) Choose $u \in \mathbb{F}_q$ at random.

(4) Let $\kappa = g(u)$.

(5) If κ is normal over $\mathbb{F}_q$ output κ. Otherwise goto (3).

If $q > 2n(n-1)$, then, by 6.9.6, κ is normal with probability at least $1/2$. □

Finally, we present a deterministic algorithm, due to Lenstra (cf. [126]), for constructing a normal basis.

6.9.11 Definition (τ-order) Let τ be the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For $\kappa \in \mathbb{F}_{q^n} \setminus \{0\}$ determine the least positive integer k and $c_0, \ldots, c_{k-1} \in \mathbb{F}_q$ so that

$$\tau^k(\kappa) = \sum_{i \in k} c_i \tau^i(\kappa).$$

Then the polynomial

$$\mathrm{Ord}_\kappa(x) := x^k - \sum_{i \in k} c_i x^i \in \mathbb{F}_q[x]$$

is called the *τ-order* of κ. ◇

The τ-order of $\kappa \neq 0$ is uniquely determined. Since $\tau^n(\kappa) = \kappa$, it is clear that $\mathrm{Ord}_\kappa(x)$ is a divisor of $x^n - 1$. Moreover, the element κ is normal over $\mathbb{F}_q$ if and only if $\mathrm{Ord}_\kappa(x) = x^n - 1$.

6.9.12 Lemma *Consider $\alpha \in \mathbb{F}_{q^n} \setminus \{0\}$ with $\mathrm{Ord}_\alpha(x) \neq x^n - 1$, and let*

$$g(x) := \frac{x^n - 1}{\mathrm{Ord}_\alpha(x)}.$$

Then there exists $\beta \in \mathbb{F}_{q^n}$ so that $g(x)\beta = \alpha$.

Proof: Let γ be a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then there exists some $f \in \mathbb{F}_q[x]$ so that $f(x)\gamma = \alpha$. Since $\mathrm{Ord}_\alpha(x)\alpha = 0$, we have $\big(\mathrm{Ord}_\alpha(x) f(x)\big)\gamma = 0$. So $\mathrm{Ord}_\gamma(x) = x^n - 1$ is a divisor of $\mathrm{Ord}_\alpha(x) f(x)$. Thus, $g(x)$ is a divisor of $f(x)$. Let $f(x) = g(x)h(x)$, then $\alpha = f(x)\gamma = g(x)\big(h(x)\gamma\big)$. This proves that $\beta := h(x)\gamma$ satisfies the assertion. □

Lemma *Consider* $\alpha, \beta \in \mathbb{F}_{q^n} \setminus \{0\}$ *with* $\mathrm{Ord}_\alpha(x) \neq x^n - 1$, **6.9.13**

$$g(x) := \frac{x^n - 1}{\mathrm{Ord}_\alpha(x)},$$

and $\alpha = g(x)\beta$ *as in the previous lemma. If* $\deg \mathrm{Ord}_\beta(x) \leq \deg \mathrm{Ord}_\alpha(x)$, *then there exists a nonzero* $\eta \in \mathbb{F}_{q^n}$ *so that*

$$g(x)\eta = 0, \tag{6.9.14}$$

and

$$\deg \mathrm{Ord}_{\alpha+\eta}(x) > \deg \mathrm{Ord}_\alpha(x). \tag{6.9.15}$$

Proof: Let γ be a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then $\eta := \mathrm{Ord}_\alpha(x)\gamma$ is different from 0 and satisfies

$$g(x)\eta = \frac{x^n - 1}{\mathrm{Ord}_\alpha(x)} \mathrm{Ord}_\alpha(x)\gamma = (x^n - 1)\gamma = 0.$$

Now we prove that each nonzero solution η of 6.9.14 satisfies 6.9.15. From $\mathrm{Ord}_\beta(x)\alpha = \mathrm{Ord}_\beta(x)g(x)\beta = 0$ we obtain that $\mathrm{Ord}_\alpha(x)$ divides $\mathrm{Ord}_\beta(x)$. From the assumption on the degrees of these two polynomials we deduce that $\mathrm{Ord}_\alpha(x) = \mathrm{Ord}_\beta(x)$. Thus, by Exercise 6.9.2 we have $\gcd\big(g(x), \mathrm{Ord}_\alpha(x)\big) = 1$. Since $\mathrm{Ord}_\eta(x)$ is a divisor of $g(x)$, also $\gcd\big(\mathrm{Ord}_\eta(x), \mathrm{Ord}_\alpha(x)\big) = 1$. An application of Exercise 6.9.3 yields that $\mathrm{Ord}_{\alpha+\eta}(x) = \mathrm{Ord}_\alpha(x)\,\mathrm{Ord}_\eta(x)$, whence $\deg \mathrm{Ord}_{\alpha+\eta}(x) > \deg \mathrm{Ord}_\alpha(x)$. □

Algorithm (Construct a normal element) **6.9.16**

Input: q and n.

Output: A normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

(1) Choose $\alpha \in \mathbb{F}_q$ at random and determine $\mathrm{Ord}_\alpha(x)$.

(2) If $\mathrm{Ord}_\alpha(x) = x^n - 1$ then output α and terminate the algorithm.

(3) Calculate $g(x) := (x^n - 1) / \mathrm{Ord}_\alpha(x)$.

(4) Find $\beta \in \mathbb{F}_{q^n}$ so that $g(x)\beta = \alpha$ and determine $\mathrm{Ord}_\beta(x)$.

(5) If $\deg \mathrm{Ord}_\beta(x) > \deg \mathrm{Ord}_\alpha(x)$, replace α by β and goto (2).

(6) If $\deg \mathrm{Ord}_\beta(x) \leq \deg \mathrm{Ord}_\alpha(x)$, then find a nonzero element $\eta \in \mathbb{F}_{q^n}$ so that $g(x)\eta = 0$. Replace α by $\alpha + \eta$, determine $\mathrm{Ord}_\alpha(x)$ and goto (2).

This algorithm terminates after finitely many steps, because in (6) the degree of $\mathrm{Ord}_\alpha(x)$ increases at least by 1. □

Exercises

Exercise Why is the τ-order of $\kappa \neq 0$ is uniquely determined? **E.6.9.1**

E.6.9.2 **Exercise** For $\alpha \in \mathbb{F}_{q^n}$ and $g \in \mathbb{F}_q[x]$ show that if $g(x)\alpha \neq 0$, then the τ-order of $g(x)\alpha$ is equal to $\mathrm{Ord}_\alpha(x)/\gcd(\mathrm{Ord}_\alpha(x), g(x))$.

E.6.9.3 **Exercise** Consider $\alpha, \eta \in \mathbb{F}_{q^n} \setminus \{0\}$ such that $\mathrm{Ord}_\alpha(x)$ and $\mathrm{Ord}_\eta(x)$ are relatively prime. Show that

$$\mathrm{Ord}_{\alpha+\eta}(x) = \mathrm{Ord}_\alpha(x)\,\mathrm{Ord}_\eta(x).$$

E.6.9.4 **Exercise** Let $\alpha \in \mathbb{F}_{3^4}$ be a root of the irreducible polynomial $f(x) = x^4 + x^3 + 2 \in \mathbb{F}_3[x]$. Using α, compute a normal basis of $\mathbb{F}_{3^4}$ over $\mathbb{F}_3$ and determine by an application of 3.5.5 the list of all irreducible polynomials of degree 4 over $\mathbb{F}_3$.