Chapter 8

8

Linear Codes with a Prescribed Minimum Distance

8

8 Linear Codes with a Prescribed Minimum Distance

After the *enumeration* of the isometry classes of codes in Chapter 6, we are now approaching the systematic *construction* of representatives of these classes. In this and the following chapter, we will present methods for constructing linear (n, k)-codes with *prescribed minimum distance* d. This means that for a given lower bound d on the minimum distance, we construct all $(n, k, \geq d)$-codes, i.e. codes whose minimum distance is at least as good as the lower bound we have chosen. We present essentially two different methods for solving this problem. Of course, both methods may fail to construct such codes, for instance if the lower bound d on the minimum distance was chosen too large. Nevertheless, in this case both methods provide *proof* that no code with the parameters under consideration exists. Needless to say that this construction problem is a very important and interesting one. In essence, all of coding theory is concerned with finding codes which allow one to transmit more data with fewer errors.

The above-mentioned construction of codes often leads to new and interesting codes either directly or indirectly by means of constructions and modifications in the sense of Section 2.2. In fact, A. Brouwer's helpful tables for the parameters of best known linear codes can sometimes be improved by such a search.

The construction that we have in mind in this chapter applies first of all to projective codes (cf. Exercise 1.3.21 and 6.1.14), i.e. codes whose columns can be taken as representatives of a *set* of points in projective space. The construction problem is then reduced to the problem of finding an equivalent structure in projective space called a *minihyper.* This is essentially a system of points in a suitable projective space with certain intersection properties with respect to hyperplanes. The necessary calculations amount to solving a system of Diophantine equations, similar to the techniques used for the construction of combinatorial designs.

Since for interesting parameter sets the coefficient matrix of the system often is too big to allow a direct solution, a well-known reduction is applied. Namely, we make an assumption about the presence of non-trivial automorphisms. This reduces the size of the coefficient matrix and thereby eases the problem to become more tractable. Of course, such a reduction is risky as it does not allow one to find solutions which do not satisfy the assumption on the presence of automorphisms. In this situation, the algorithm classifies codes with a given minimum distance which are invariant under the chosen group

of automorphisms. In many cases this reduction indeed led to the discovery of new optimal codes (i.e. one could say that the end justifies the means in this case). Lastly, we also search for arbitrary nonredundant codes, i.e. codes which are not necessarily projective. The systematic construction of complete transversals of isometry classes of linear codes with a lower bound on their minimum distance is done in Chapter 9.

8.1

8.1 Minihypers

We begin with a closer examination of the use of generator matrices for encoding. For this purpose we introduce the notation $\gamma_{*,j}^{\top}$ for the j-th column of a generator matrix $\Gamma = (\gamma_{ij})$ and $\gamma_{i,*}$ for its i-th row. Using this notation, we can describe the generator matrix Γ of an (n,k)-code as

$$\Gamma = \left(\gamma_{*,0}^{\top} \mid \ldots \mid \gamma_{*,n-1}^{\top}\right) = \left(\begin{array}{c} \gamma_{0,*} \\ \hline \vdots \\ \hline \gamma_{k-1,*} \end{array}\right).$$

In terms of the standard bilinear form $\langle v, w\rangle = \sum_i v_i w_i$, we express a codeword $c := v \cdot \Gamma$ corresponding to a message $v \in \mathbb{F}_q^k$ as follows:

$$c = v \cdot \Gamma = (\langle v, \gamma_{*,0}\rangle, \ldots, \langle v, \gamma_{*,n-1}\rangle).$$

By definition, $n - \mathrm{wt}(v \cdot \Gamma)$ components of $v \cdot \Gamma$ are zero. In terms of the bilinear form, this means that $n - \mathrm{wt}(v \cdot \Gamma)$ columns of the generator matrix Γ are orthogonal to v, i.e., contained in the *hyperplane*

$$H(v) := P(v)^{\perp} = \left\{ w \in \mathbb{F}_q^k \mid \langle v, w\rangle = 0 \right\} \in \mathcal{U}(k, k-1, q).$$

This fact leads us to the following basic result:

8.1.1 **Theorem** *A $k \times n$-matrix over $\mathbb{F}_q$ generates an (n,k,d,q)-code C if and only if the columns of any generator matrix Γ of C satisfy the following two properties. Every hyperplane $H \in \mathcal{U}(k, k-1, q)$ contains at most $n-d$ columns of Γ and there is at least one hyperplane $H \in \mathcal{U}(k, k-1, q)$ which contains exactly $n-d$ columns of Γ. This property is independent of the choice of the generator matrix Γ of C, in that this property either holds for* all *generator matrices of C or none of the generator matrices of C has this property.*

Proof: 1. By 1.2.8, the minimum distance of a linear code equals the minimum weight of a nonzero codeword $c := v \cdot \Gamma$ for $v \in \mathbb{F}_q^k$, $v \neq 0$. The above argument shows that every hyperplane $H = H(v) \in \mathcal{U}(k, k-1, q)$ contains at most $n - d$ columns of Γ with equality if and only if the codeword $c = v \cdot \Gamma$ is of minimum weight d.

2. Conversely, if $\Gamma = (\gamma_{ij})$ is a $k \times n$-matrix over $\mathbb{F}_q$ satisfying

$$\max\left\{ |\{j \mid \gamma_{*,j} \in H\}| \;\middle|\; H \in \mathcal{U}(k, k-1, q) \right\} = n - d,$$

then it is clear from the first part of the proof that its rows generate an (n, k', d)-code C over $\mathbb{F}_q$ of dimension $k' \leq k$. In order to show that $k' = k$ we have to check that the rows of Γ are linearly independent. Assume that Γ *does not* have full rank k. This means that the rows are linearly dependent, say

$$0 = c = v \cdot \Gamma,$$

for some $v \neq 0$. Since each $c_j = 0$, every column $\gamma_{*,j}$ is contained in the hyperplane $H(v)$, i.e. $\left|\left\{ j \;\middle|\; \gamma_{*,j} \in H(v) \right\}\right| = n$, contradicting the fact that

$$\left|\left\{ j \;\middle|\; \gamma_{*,j} \in H(v) \right\}\right| \leq n - d < n.$$

Thus Γ really generates an (n, k, d, q)-code. □

We now recall from the metric classification of linear codes that permuting columns and/or multiplying columns of a generator matrix Γ with a nonzero element of $\mathbb{F}_q$ yields a generator matrix of a code which is linearly isometric. In fact, it is often simpler to deal not with the generator matrix Γ of a code but instead consider a certain map (or multiset), as described in the next remark. This applied to nonredundant codes only:

Remarks Let Γ denote a generator matrix of a nonredundant linear code C (which means that it does not contain a zero column). Then **8.1.2**

- Γ can be identified with the mapping

$$\Gamma : n \to \mathbb{F}_q^k \backslash \{0\} \;:\; j \mapsto \gamma_{*,j}.$$

- Up to linear isometry, we may consider instead of column vectors the one-dimensional subspaces generated by the column vectors. They are the elements or *points* of the *projective geometry*

$$\mathrm{PG}_{k-1}(q) = \left\{ P(v) \;\middle|\; v \in \mathbb{F}_q^k \backslash \{0\} \right\}.$$

This means in fact that we can replace Γ by the mapping

$$\widetilde{\Gamma} : n \to \mathrm{PG}_{k-1}(q) \;:\; j \mapsto P(\gamma_{*,j}).$$

The reason is that we easily obtain from $\widetilde{\Gamma}$ a matrix Γ' that generates a linear code C' linearly isometric to C, by simply taking from each value $P(\gamma_{*,j})$ of $\widetilde{\Gamma}$ a nonzero element and using it as the j-th column of Γ'.

– Moreover, because of isometry, it is possible to replace

$$\widetilde{\Gamma} = (P(\gamma_{*,0}), \ldots, P(\gamma_{*,n-1}))$$

by its orbit

$$S_n(\widetilde{\Gamma})$$

which consists of all the reorderings of this sequence $\widetilde{\Gamma}$. I.e. instead of the *sequence* of the points we consider the *multiset* of them. (In order to indicate a multiset we use the notation $\{\!\{\ldots\}\!\}$. In such a multiset, elements can occur several times, e.g. in $\{\!\{a, a, b, c, c, c\}\!\}$, a multiset of order 6, the element a occurs twice and c occurs three times.) This means that we replace Γ even by the multiset

$$\widetilde{\widetilde{\Gamma}} := \{\!\{P(\gamma_{*,0}), \ldots, P(\gamma_{*,n-1})\}\!\}$$

of cardinality n. It is clear that we can easily deduce from $\widetilde{\widetilde{\Gamma}}$ a matrix Γ'' that generates a code C'' linearly isometric to C. ◇

For example the matrix

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

generates an $(8, 3)$-code over $\mathbb{F}_3$. The corresponding mapping is

$$\widetilde{\Gamma} = (P(100), P(010), P(001), P(101), P(121), P(121), P(122), P(122))$$

and the resulting multiset is

$$\widetilde{\widetilde{\Gamma}} = \{\!\{P(010), P(001), P(101), P(121), P(121), P(122), P(122), P(100)\}\!\}.$$

8.1.3 Corollary *Both the mapping $\widetilde{\Gamma}$ and the multiset $\widetilde{\widetilde{\Gamma}}$ characterize the isometry class of the code C generated by Γ. Moreover, it is obvious how to obtain from $\widetilde{\Gamma}$ as well as from $\widetilde{\widetilde{\Gamma}}$ a generator matrix that generates a linear code linearly isometric to C.* □

We are now in a position to rephrase 8.1.1 in terms of multisets. For this purpose we introduce the following kind of *restriction* of the multiset $\widetilde{\widetilde{\Gamma}}$ to a hyperplane H:

$$\widetilde{\widetilde{\Gamma}} \downarrow H := \left\{\!\!\left\{ P \in \widetilde{\widetilde{\Gamma}} \mid P \subseteq H \right\}\!\!\right\}.$$

For example the restriction of the multiset $\tilde{\tilde{\Gamma}}$ defined by the above $(8,3)$-code to the hyperplane $H = H(110) = \{x \in \mathbb{F}_3^3 \mid x_0 + x_1 = 0\}$ is

$$\tilde{\tilde{\Gamma}} \downarrow H(110) = \{\!\{P(121), P(121), P(122), P(122)\}\!\}.$$

Its cardinality $|\tilde{\tilde{\Gamma}} \downarrow H(110)|$ is four. Using this notation we formulate the following corollary due to [88]:

Corollary 8.1.4 *There is a nonredundant (n,k,d,q)-code if and only if there is a multiset $\mathcal{X}$ of order n, consisting of points of $\mathrm{PG}_{k-1}(q)$ such that*

$$\max\left\{|\mathcal{X} \downarrow H| \;\middle|\; H \in \mathcal{U}(k,k-1,q)\right\} = n - d. \qquad \square$$

In fact, according to [88], we obtain even the weight distribution in this case:

Theorem 8.1.5 *If $\mathcal{X}$ is a multiset of points in $\mathrm{PG}_{k-1}(q)$ with*

$$\max\left\{|\mathcal{X} \downarrow H| \;\middle|\; H \in \mathcal{U}(k,k-1,q)\right\} = n - d,$$

then each matrix Γ whose columns are generators of the points of $\mathcal{X}$ generates an (n,k,d,q)-code C with weight distribution $W_C(x,y) = \sum_{i=0}^{n} A_i x^i y^{n-i}$, where $A_0 = 1$ and

$$A_i = (q-1) \cdot \left|\left\{H \in \mathcal{U}(k,k-1,q) \;\middle|\; |\mathcal{X} \downarrow H| = n - i\right\}\right|, \quad \text{for } i > 0.$$

Proof: For each codeword $v \cdot \Gamma$ we have $|\mathcal{X} \downarrow H(v)| = n - \mathrm{wt}(v \cdot \Gamma)$. Since the generator matrix Γ has full rank k, a codeword $v \cdot \Gamma$ has weight 0 if and only if $v = 0$, and so $A_0 = 1$. The coefficients A_i, $i > 0$, are

$$\begin{aligned} A_i &= \left|\left\{c \in C \backslash \{0\} \;\middle|\; \mathrm{wt}(c) = i\right\}\right| \\ &= \left|\left\{v \in \mathbb{F}_q^k \backslash \{0\} \;\middle|\; \mathrm{wt}(v \cdot \Gamma) = i\right\}\right| \\ &= \left|\left\{v \in \mathbb{F}_q^k \backslash \{0\} \;\middle|\; |\mathcal{X} \downarrow H(v)| = n - i\right\}\right| \\ &= (q-1) \cdot \left|\left\{H \in \mathcal{U}(k,k-1,q) \;\middle|\; |\mathcal{X} \downarrow H| = n - i\right\}\right|, \end{aligned}$$

as stated. $\square$

Example (simplex-code) 8.1.6 The k-th order q-ary simplex-code defined in 2.1.5 is an example of a nonredundant code. It is generated by any matrix Γ whose columns represent all $\theta_{k-1}(q) := (q^k - 1)/(q-1)$ points of $\mathrm{PG}_{k-1}(q)$ (cf. 3.7.2). Using hyperplane intersections, we can easily deduce its parameters: Recall that every hyperplane contains $\theta_{k-2}(q)$ points, each of which is represented by

exactly one column of the generator matrix Γ. Therefore, the parameter of this code are $n = \theta_{k-1}(q)$ and $n - d = \theta_{k-2}(q)$, i.e.

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

The weight distribution is

$$1 + (q^k - 1)x^{q^{k-1}}.$$

Moreover, since

$$\frac{q^k-1}{q-1} = q^{k-1} + q^{k-2} + \ldots + q + 1 = \sum_{i\in k} \frac{q^{k-1}}{q^i} = \sum_{i\in k} \left\lceil \frac{d}{q^i} \right\rceil,$$

this code meets the Griesmer-bound, it is an optimal linear code. ◇

Codes that are generated by a matrix Γ with pairwise linearly independent columns, so that $\widetilde{\widetilde{\Gamma}}$ is a set in the strict sense, are called *projective* (cf. 6.1.14). For instance simplex-codes are projective. In other words the columns of generator matrices of projective linear (n,k)-codes correspond to pairwise distinct points. In order to emphasize this we shift from the calligraphic $\mathcal{X}$, that we used for multisets, to the notation X. Moreover we note that the restriction of sets to hyperplanes is the intersection. Projective codes are clearly nonredundant. As an immediate consequence we obtain

8.1.7 **Corollary** *There exists a projective linear (n,k,d)-code over $\mathbb{F}_q$ if and only if there exists a subset X of order n in $\mathrm{PG}_{k-1}(q)$ such that*

$$\max\left\{|X\cap H| \;\middle|\; H \in \mathcal{U}(k,k-1,q)\right\} = n - d. \qquad \square$$

The complement of such a *set* X of points is called a minihyper. Minihypers are well-known objects in geometry. Several articles (cf. [25], [26], [54], [75], [79], or [143]) deal with minihypers and also with the connection between minihypers and linear codes. Hamada [78] discovered the relationship between Griesmer optimal linear codes and minihypers which we introduce now. We want to describe them in detail and we also give an algorithm for the construction of these objects.

8.1.8 **Definition (minihyper)** A (b,t)-*minihyper* in $\mathrm{PG}_{k-1}(q)$ is a set B of b points of $\mathrm{PG}_{k-1}(q)$ such that every hyperplane contains at least t points of B and at least one hyperplane contains exactly t points of B. Formally, a set $B \subseteq \mathcal{U}(k,1,q)$ is a (b,t)-minihyper in $\mathrm{PG}_{k-1}(q)$ if and only if

$$|B| = b \quad \text{and} \quad \min\left\{|B\cap H| \;\middle|\; H \in \mathcal{U}(k,k-1,q)\right\} = t. \qquad \diamond$$

Using the concept of minihypers we reformulate the connection between projective codes and projective geometries.

Corollary 8.1.9 *There is a projective (n,k,d)-code over $\mathbb{F}_q$ if and only if there is a (b,t)-minihyper in $\mathrm{PG}_{k-1}(q)$ where*

$$(b,t) = (\theta_{k-1}(q) - n, \theta_{k-2}(q) - n + d).$$

Proof: Let X be a set of n points with

$$\max\left\{|X \cap H| \;\middle|\; H \in \mathcal{U}(k,k-1,q)\right\} = n - d.$$

Since every hyperplane contains $\theta_{k-2}(q)$ points, the set-theoretic complement $B := \mathcal{U}(k,1,q) \setminus X$ satisfies the equation

$$\min\left\{|B \cap H| \;\middle|\; H \in \mathcal{U}(k,k-1,q)\right\} = \theta_{k-2}(q) - (n-d).$$

Being the complement of X in $\mathrm{PG}_{k-1}(q) = \mathcal{U}(k,1,q)$, the set B has $\theta_{k-1}(q) - n$ elements. Thus B is a

$$(\theta_{k-1}(q) - n, \theta_{k-2}(q) - n + d)$$

minihyper in $\mathrm{PG}_{k-1}(q)$. Since all arguments can be reversed, the existence of such a minihyper gives rise to a projective (n,k,d)-code. □

Lemma 8.1.10 *If $d \leq q^{k-1}$ and C is an (n,k,d,q)-code which attains the Griesmer-bound $n = \sum_{i\in k}\lceil d/q^i\rceil$, then C is a projective code.* □

This lemma, the proof of which is left as Exercise 8.1.3, together with 8.1.9 implies the following corollary which is due to Hamada:

Corollary 8.1.11 *Let $d \leq q^{k-1}$ and assume that $n = \sum_{i\in k}\lceil d/q^i\rceil$ which is taken from the Griesmer-bound. Then there exists a nonredundant linear (n,k,d)-code over $\mathbb{F}_q$ if and only if there exists a $(\theta_{k-1}(q) - n, \theta_{k-2}(q) - n + d)$-minihyper in $\mathrm{PG}_{k-1}(q)$.* □

Example (Fano-plane) 8.1.12 A well-known example is provided by the projective geometry $\mathrm{PG}_2(2)$, which is also known as the *Fano-plane*. It consists of the seven points and seven hyperplanes shown in the following table:

$$\begin{array}{ll}
P_0 = P(100) = \{000,100\} & H_0 = \{000,100,010,110\} = P_0 \cup P_1 \cup P_3 \\
P_1 = P(010) = \{000,010\} & H_1 = \{000,010,001,011\} = P_1 \cup P_2 \cup P_4 \\
P_2 = P(001) = \{000,001\} & H_2 = \{000,100,001,101\} = P_0 \cup P_2 \cup P_5 \\
P_3 = P(110) = \{000,110\} & H_3 = \{000,100,011,111\} = P_0 \cup P_4 \cup P_6 \\
P_4 = P(011) = \{000,011\} & H_4 = \{000,010,101,111\} = P_1 \cup P_5 \cup P_6 \\
P_5 = P(101) = \{000,101\} & H_5 = \{000,001,110,111\} = P_2 \cup P_3 \cup P_6 \\
P_6 = P(111) = \{000,111\} & H_6 = \{000,110,011,101\} = P_3 \cup P_4 \cup P_5
\end{array}$$

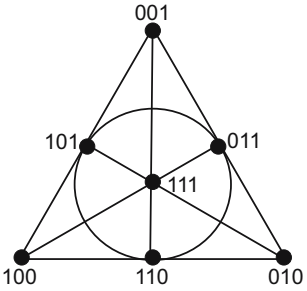


Fig. 8.1 The Fano-plane

The incidence relation between these points and hyperplanes is represented by the famous graph shown in Fig. 8.1. Each of the hyperplanes, which are the lines, together with the cycle, yields a $(3,1)$-minihyper in $\mathrm{PG}_2(2)$. This property can easily be verified by looking at the figure. For example, take the line

$$B = \{P_3 = P(110), P_4 = P(011), P_5 = P(101)\}.$$

If we write the representatives of the four elements of the complement

$$X = \{P(100), P(010), P(001), P(111)\}$$

in a matrix column by column, we obtain the generator matrix

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

of a binary $(4,3,2)$-code. ◇

Now we are interested in a general approach to the construction of such a minihyper and, correspondingly, of codes with a prescribed minimum distance. For this purpose we introduce the following notion:

8.1.13 **Definition (blocking set)** A *t-blocking set* in $\mathrm{PG}_{k-1}(q)$ is a set B of points of $\mathrm{PG}_{k-1}(q)$ such that every hyperplane contains at least t points of B:

$$\min\left\{|B \cap H| \;\middle|\; H \in \mathcal{U}(k, k-1, q)\right\} \geq t. \qquad \diamond$$

Hence, minihypers are t-blocking sets with additional properties. The largest possible size of an intersection of B and a hyperplane H is $\theta_{k-2}(q)$. Therefore B is a t-blocking set in $\mathrm{PG}_{k-1}(q)$ if

$$t \leq |B \cap H| \leq \theta_{k-2}(q)$$

for all hyperplanes $H \in \mathcal{U}(k, k-1, q)$. As t-blocking sets are suitable selections of points, they can be described by the *incidence matrix* $M_{k,q} = (m_{ij})$, the rows of which correspond to the hyperplanes $H_i \in \mathcal{U}(k, k-1, q)$, $i \in \theta_{k-1}(q)$, and the columns of which correspond to the points $P_j \in \mathcal{U}(k, 1, q)$, $j \in \theta_{k-1}(q)$. The entry m_{ij} of the i-th row and j-th column is defined as follows:

$$m_{ij} := \begin{cases} 1 & \text{if } P_j \subseteq H_i, \\ 0 & \text{otherwise.} \end{cases}$$

Hence a t-blocking set B is nothing but a selection of columns of the matrix $M_{k,q}$, or a 0-1-vector $x = (x_0, \ldots, x_{\theta_{k-1}(q)-1})^\top$ which satisfies the condition

$$M_{k,q} \cdot x \in \{t, \ldots, \theta_{k-2}(q)\}^{\theta_{k-1}(q)}.$$

This means that there is a vector $y = (y_0, \ldots, y_{\theta_{k-1}(q)-1})^\top$ with components $y_i \in \{t, \ldots, \theta_{k-2}(q)\}$ fulfilling the equation $M_{k,q} \cdot x = y$, which is equivalent to the equation

$$\left(M_{k,q} \mid -I\right) \cdot \begin{pmatrix} x \\ y \end{pmatrix} = 0,$$

where I is the identity matrix. Summarizing, we obtain the desired construction of blocking sets:

Corollary 8.1.14 *There is a bijection between the set of all t-blocking sets in $\mathrm{PG}_{k-1}(q)$ and the set of vectors $\binom{x}{y}$ with $x_i \in \{0,1\}$ and $y_i \in \{t, \ldots, \theta_{k-2}(q)\}$ that solve the linear system of equations:*

$$\left(M_{k,q} \mid -I\right) \cdot \begin{pmatrix} x \\ y \end{pmatrix} = 0.$$

If $\binom{x}{y}$ denotes such a solution then the corresponding t-blocking set B in $\mathrm{PG}_{k-1}(q)$ is

$$B = \left\{P_j \mid x_j = 1\right\}. \qquad \square$$

Example (Fano-plane, cont.) 8.1.15 We again consider the Fano-plane and construct all 1-blocking sets in $\mathrm{PG}_2(2)$. There are seven hyperplanes and points as mentioned in Example 8.1.12. The corresponding incidence matrix is

$$M_{3,2} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Solving the corresponding linear system of equations from 8.1.14 we obtain 64 solutions $\binom{x}{y}$ with the required properties $x \in \{0,1\}^7$ and $y \in \{1,2,3\}^7$. Seven solutions correspond to the lines which are $(3,1)$-minihypers in $\mathrm{PG}_2(2)$. The minihyper $B = \{P_3, P_4, P_5\}$ corresponds to the solution

$$\binom{x}{y} = (0,0,0,1,1,1,0;1,1,1,1,1,1,3)^\top. \qquad \diamond$$

So far, we have constructed minihypers in the Fano-plane. In order to obtain new linear codes, we need to search for t-blocking sets or minihypers. The method proposed in 8.1.14 may not work because the incidence matrix $M_{k,q}$ can become too big for solving the system of Diophantine equations for interesting parameters. In these cases, the intention is to *reduce* the incidence matrix $M_{k,q}$ to a much smaller matrix so that it is possible to solve the corresponding system of Diophantine equations applying the lattice point enumeration algorithm described in the previous chapter. To achieve this goal we make an assumption about the presence of non-trivial automorphisms, similar to the methods that are used to construct combinatorial t-designs [18], [14], [15], [17]. In fact, such an assumption about the presence of non-trivial automorphisms leads to a very interesting area of Algebraic Combinatorics, the theory of groups acting on lattices. This is the topic of the following section.

Exercises

E.8.1.1 **Exercise** Show that the set of points in $\mathrm{PG}_2(q)$ defined by the *conic*

$$\left\{ \langle (x,y,z) \rangle \mid x^2 = yz \right\}$$

corresponds to a q-ary $(q+1, 3, q-1)$-code.

E.8.1.2 **Exercise** Verify that the set of points in $\mathrm{PG}_3(q)$ defined by the *hyperbolic quadric*

$$\left\{ \langle (x,y,z,w) \rangle \mid zw = xy \right\}$$

corresponds to a q-ary $((q+1)^2, 4, q^2)$-code.

E.8.1.3 **Exercise** Prove 8.1.10. Hint: Check that the generator matrix Γ of C does not contain zero columns. Assume that Γ has a repeated column. In this case, the matrix

$$\left(\begin{array}{cc|c} 1 & 1 & \dots \\ \hline 0 & 0 & \\ \vdots & \vdots & \Gamma' \\ 0 & 0 & \end{array}\right)$$

generates a code which is linearly isometric to C. Here, Γ' is a generator matrix of an $(n-2, k-1, d')$-code C' with $d' \geq d$. The inequality from the Griesmer-bound for C' then leads to a contradiction.

8.2 Group Actions on Lattices

8.2

In this section we investigate actions of subgroups of the general linear group $\mathrm{GL}_k(q)$ on the set $\mathcal{U}(k,q) = \mathrm{PG}(\mathbb{F}_q^k)$ of all subspaces of $\mathbb{F}_q^k$. This action is interesting because $\mathcal{U}(k,q)$ forms a lattice, the *linear lattice*, and since the action preserves the partial order, i.e. we have the implication

$$S \leq T \implies AS \leq AT$$

for all subspaces $S, T \in \mathcal{U}(k,q)$ and all $A \in \mathrm{GL}_k(q)$. Hence let us introduce first the general concept of group actions on posets respectively lattices.

Definition (poset action) Let $(X, \leq)$ denote a poset on which a group G acts from the left. Then we call the action ${}_GX$ a *poset action* if the implication 8.2.1

$$x \leq x' \implies gx \leq gx'$$

holds for all $x, x' \in X$ and $g \in G$. This will be abbreviated by

$${}_G(X, \leq). \qquad \diamond$$

We note that we can in fact replace the implication by an equivalence since $gx \leq gx'$ also implies $x \leq x'$ if we apply g^{-1} from the left.

Analogously, we define a lattice action if the group elements commute with the infimum and supremum operator.

Definition (lattice action) Let $(X, \wedge, \vee)$ denote a lattice and let G be a group acting on X. Then ${}_GX$ is called a *lattice action* if and only if 8.2.2

$$g(x \wedge x') = gx \wedge gx' \quad \text{and} \quad g(x \vee x') = gx \vee gx'$$

for all $x, x' \in X$ and $g \in G$. We indicate this situation as follows:

$${}_G(X, \wedge, \vee). \qquad \diamond$$

Recall that a lattice $(X, \wedge, \vee)$ is always a poset, the corresponding order relation $\leq$ can be obtained by

$$x \leq x' :\iff x \wedge x' = x \iff x \vee x' = x'.$$

Using this equivalence we prove the following lemma.

8.2.3 **Lemma** *Let $(X, \wedge, \vee)$ be a lattice, $(X, \leq)$ the corresponding partial order and let G be a group acting on X. Then ${}_GX$ is a poset action if and only if ${}_GX$ is a lattice action.*

Proof: 1. Assume that ${}_GX$ is a poset action. We have $x \wedge x' \leq x$ and $x \wedge x' \leq x'$ for all $x, x' \in X$. Since G preserves the order relation we obtain $g(x \wedge x') \leq gx$ and $g(x \wedge x') \leq gx'$ for all $g \in G$ and hence $g(x \wedge x') \leq gx \wedge gx'$. If we assume that $g(x \wedge x') < gx \wedge gx'$ we obtain, after applying g^{-1} from the left, that

$$x \wedge x' = g^{-1}(g(x \wedge x')) < g^{-1}(gx \wedge gx') \leq g^{-1}(gx) \wedge g^{-1}(gx') = x \wedge x',$$

which yields the contradiction $x \wedge x' < x \wedge x'$. Thus we have $g(x \wedge x') = gx \wedge gx'$. The statement $g(x \vee x') = gx \vee gx'$ follows analogously.

2. Now we assume that ${}_GX$ is a lattice action. We have the following chain of equivalences:

$$x \leq x' \Leftrightarrow x = x \wedge x' \Leftrightarrow gx = g(x \wedge x') = gx \wedge gx' \Leftrightarrow gx \leq gx',$$

for all $x, x' \in X$ and $g \in G$. This completes the proof. □

8.2.4 **Definition (poset automorphism)** Let $(X, \leq)$ denote a poset. Then a bijection $f : X \to X$ is called a *poset automorphism* if and only if

$$x \leq x' \implies f(x) \leq f(x')$$

for all elements $x, x' \in X$. ◇

The set of all poset automorphisms of a poset $(X, \leq)$ forms a subgroup of the symmetric group S_X, the *automorphism group* of $(X, \leq)$, which will be abbreviated by $\mathrm{Aut}(X, \leq)$. A subgroup of this full automorphism group is called *a* group of automorphisms of $(X, \leq)$. Now recall the image $\overline{G} = \delta(G)$ of the permutation representation

$$\delta : G \to S_X \ : \ g \mapsto \overline{g} \text{ with } \overline{g} : x \mapsto gx$$

that obviously can be used to characterize a poset action: ${}_GX$ is a poset action if and only if

8.2.5
$$\overline{G} \leq \mathrm{Aut}(X, \leq).$$

For this reason we also say that G acts on a poset $(X, \leq)$ as a group of automorphisms in order to express that ${}_GX$ is a poset action. The most important properties of poset actions are the following ones:

Lemma 8.2.6 *If ${}_G(X,\leq)$ denotes a poset action with finite G, then it has the following properties:*

1. *Any two elements in the same orbit are incomparable, i.e. the orbits are* antichains.
2. *If ω and ω' are orbits such that there exist $x \in \omega$ and $x' \in \omega'$ where $x < x'$, then we have, for any comparable pair of elements $y \in \omega$ and $y' \in \omega'$, that $y < y'$.*
3. *The partial order on X induces the following partial order on $G\backslash\backslash X$:*

$$\omega \leq \omega' :\Longleftrightarrow \exists\, x \in \omega, x' \in \omega' : x \leq x'.$$

4. *Consider an orbit $\omega \in G\backslash\backslash X$ and an arbitrary representative $x \in \omega$. For any orbit ω' the numbers*

$$\left|\{x' \in \omega' \mid x \leq x'\}\right| \quad \text{and} \quad \left|\{x' \in \omega' \mid x \geq x'\}\right|$$

depend only on the orbit ω and not on the chosen representative $x \in \omega$.

5. *For any $x, x' \in X$, we have*

$$|G(x)| \cdot \left|\{z \in G(x') \mid x \leq z\}\right| = \left|G(x')\right| \cdot \left|\{y \in G(x) \mid x' \geq y\}\right|.$$

Proof: 1. If $x \in X$ were comparable with $gx \neq x$, say (without restriction) $x < gx$, then we had $x < gx < g^2x < \ldots < g^{-1}x < x$, which is a contradiction.

2. Suppose $x, y \in \omega$, $x', y' \in \omega'$, where $x < x'$ and y and y' are comparable. Then $y > y'$ would yield, for suitable $g, g' \in G$: $gx = y > y' = g'x'$, and hence also $x > g^{-1}g'x'$, which contradicts the first part that posets are antichains.

3. The reflexivity of $\leq$ on $G\backslash\backslash X$ is obvious as well as the antisymmetry, and so it remains to prove the transitivity. Hence we assume that $\omega < \omega'$ and $\omega' < \omega''$, and consider elements $x \in \omega$, $x', y' \in \omega'$, $y'' \in \omega''$ which satisfy $x < x', y' < y''$. There exists $g \in G$ with $gx' = y'$, and hence

$$\omega \ni gx < gx' = y' < y'' \in \omega'',$$

so that $\omega < \omega''$, as stated.

4. This follows from $x \leq x' \iff gx \leq gx'$.

5. Using 4., this follows from a trivial "double count" of the set

$$\left\{(y,z) \mid y \in G(x),\, z \in G(x'),\, y \leq z\right\}. \qquad \square$$

As mentioned in Section 3.2 we represent a poset $(X, \leq)$ by its *zeta function* $\zeta : X \times X \to \{0, 1\}$ which is defined by

$$\zeta(x, x') := \begin{cases} 1 & \text{if } x \leq x', \\ 0 & \text{otherwise.} \end{cases}$$

If X is finite we can assume $X = \{x_0, \ldots, x_{m-1}\}$ to be topologically sorted, in the following sense:

8.2.7 **Definition (topological sorting)** A poset $(X, \leq)$ is *topologically sorted* if the elements of X are numbered in such a way that $x_i < x_j$ implies $i < j$ for all elements $x_i, x_j \in X$. ◇

It is not difficult to check (Exercise 8.2.1) that every finite poset $(X, \leq)$ can be sorted topologically. Therefore, in the following we always assume that the elements of the finite poset X in question have been numbered topologically as $\{x_0, \ldots, x_{m-1}\}$. In this case, the *zeta matrix*

$$Z(X, \leq) := (\zeta_{ij}), \text{ where } \zeta_{ij} := \zeta(x_i, x_j),$$

is upper triangular with ones along the main diagonal, and hence invertible over $\mathbb{Z}$. Its inverse

$$Z(X, \leq)^{-1} =: M(X, \leq) = (\mu_{ij}),$$

the Möbius matrix of the poset, defines the *Möbius function* of the finite poset: $\mu(x_i, x_j) := \mu_{ij} \in \mathbb{Z}$. In addition we remark that an action on a poset is a poset action if and only if

$$\zeta(x, x') = \zeta(gx, gx')$$

for all $g \in G$ and $x, x' \in X$. Here is our main example of a poset action:

8.2.8 **Example (the linear lattice)** As we have already mentioned at the beginning of this section, the set $\mathcal{U}(k, q)$ of subspaces of $\mathbb{F}_q^k$ forms a lattice with infimum $S \wedge T := S \cap T$ and supremum $S \vee T := \langle S \cup T \rangle$ (the subspace generated by the union of S and T). The general linear group $\mathrm{GL}_k(q)$ acts on this linear lattice in the following canonical way: For $M \in \mathrm{GL}_k(q)$ and $S \in \mathcal{U}(k, q)$ we have

$$MS := \left\{ v \cdot M^\top \mid v \in S \right\}.$$

This action is clearly a poset action, $\mathcal{U}(k, q)$ is partially ordered by inclusion, and it is obvious that the action respects inclusion:

$$S \leq T \Longrightarrow MS \leq MT.$$

Hence, by 8.2.3, this action is also a lattice action,

$$_{\mathrm{GL}_k(q)} \left(\mathcal{U}(k, q), \wedge, \vee \right),$$

and so the general linear group acts as a group of automorphisms on $\mathcal{U}(k,q)$. The zeta function of this linear lattice is

$$\zeta(S,T) = \begin{cases} 1 & \text{if } S \leq T, \\ 0 & \text{otherwise.} \end{cases}$$

Since this lattice is of great importance for the following, let us evaluate its Möbius function. To begin with, we claim that the sum of the values of the Möbius function over a full nontrivial interval is zero for each poset $(X, \leq)$, where all intervals are finite. Such posets are called *locally finite* (cf. 3.2.24 and Exercise 3.2.16).

$$\sum_{y:x\leq y\leq z} \mu(x,y) = \sum_{y:x\leq y\leq z} \mu(y,z) = \delta_{x,z} = \begin{cases} 0 & \text{if } x \neq z, \\ 1 & \text{if } x = z. \end{cases} \qquad \textbf{8.2.9}$$

In order to verify the first equation we use that the Möbius matrix is the inverse of the zeta matrix: $(\mu(x,y)) \cdot (\zeta(x,y)) = I$ gives

$$\sum_{y:x\leq y\leq z} \mu(x,y) = \sum_{y:x\leq y\leq z} \mu(x,y)\zeta(y,z) = (\mu * \zeta)(x,z) = \delta(x,z) = \delta_{x,z},$$

the second statement follows similarly. The next result is on the Möbius function of a finite lattice L with its elements

$$0 := \bigwedge_{\lambda\in L} \lambda \text{ and } 1 := \bigvee_{\lambda\in L} \lambda.$$

We state that

$$0 < \lambda \in L \Longrightarrow \sum_{\kappa:\kappa\vee\lambda=1} \mu(0,\kappa) = 0. \qquad \textbf{8.2.10}$$

In order to prove this we consider the expression

$$\sigma(\lambda) := \sum_{\kappa,\nu} \mu(0,\kappa)\zeta(\kappa,\nu)\zeta(\lambda,\nu)\mu(\nu,1) = \sum_{\kappa} \mu(0,\kappa) \sum_{\nu\geq\kappa\vee\lambda} \mu(\nu,1).$$

Since, by 8.2.9, the inner sum $\sum_{\nu\geq\kappa\vee\lambda} \mu(\nu,1)$ is zero, except for the case when $\kappa \vee \lambda = 1$, we find that

$$\sigma(\lambda) = \sum_{\kappa:\kappa\vee\lambda=1} \mu(0,\kappa).$$

Hence it remains to prove that $\sigma(\lambda) = 0$. In order to do this we rewrite $\sigma(\lambda)$ in the following form:

$$\sigma(\lambda) = \sum_{\nu\geq\lambda} \mu(\nu,1) \sum_{\kappa\leq\nu} \mu(0,\kappa).$$

The inner sum is zero, and hence $\sigma(\lambda) = 0$, which completes the proof.

We are now in a position to evaluate the Möbius function of the linear lattice. We claim that

$$\mu(S,T) = \begin{cases} (-1)^m q^{\binom{m}{2}} & \text{if } S \leq T, \\ 0 & \text{otherwise,} \end{cases} \qquad \textbf{8.2.11}$$

where $m := \dim(T) - \dim(S)$ and $\binom{0}{2} = \binom{1}{2} = 0$.

For its proof (by induction on m) we note first that if $S = T$, then $\mu(S,T) = 1$ and $m = 0$. If $S < T$, then $\mu(S,T) = \mu(0,\mathbb{F}_q^m)$, $m > 0$, since the lattice of subspaces between S and T is order isomorphic to the lattice of subspaces of $\mathbb{F}_q^m$. This is known from Linear Algebra (the Homomorphism Theorem). Hence it suffices to prove that

8.2.12
$$\mu(0,\mathbb{F}_q^m) = (-1)^m q^{\binom{m}{2}}, \qquad m > 0.$$

In order to check this we pick a one-dimensional subspace U and deduce from 8.2.10 that

$$\mu(0,\mathbb{F}_q^m) = -\sum_{S \vee U = \mathbb{F}_q^m,\ S \neq \mathbb{F}_q^m} \mu(0,S),$$

where the sum is taken over all proper subspaces S such that $S \vee U = \mathbb{F}_q^m$, i.e. over all the $(m-1)$-dimensional subspaces S of $\mathbb{F}_q^m$ that do not contain U. For all these S we have, by induction assumption, that

$$\mu(0,S) = (-1)^{m-1} q^{\binom{m-1}{2}}.$$

Moreover, the number of such subspaces is (Exercise 8.2.2)

8.2.13
$$\begin{bmatrix} m \\ m-1 \end{bmatrix}(q) - \begin{bmatrix} m-1 \\ m-2 \end{bmatrix}(q) = \begin{bmatrix} m \\ m-1 \end{bmatrix}(q) - \begin{bmatrix} m-1 \\ 1 \end{bmatrix}(q) = q^{m-1}.$$

Thus, we finally obtain that

$$\mu(0,\mathbb{F}_q^m) = (-1)^m q^{\binom{m}{2}},$$

which completes the proof of 8.2.12 on the values of the Möbius function of the linear lattice. ◇

Our next step is a helpful *reduction process* that can be applied both to the zeta matrix and to the Möbius matrix of a poset or lattice, provided that we are given a poset or a lattice action. In this case, 8.2.6 implies the following

---

8.2.14 **Corollary** *Let ${}_GX$ be a poset action and let $\omega_0, \ldots, \omega_{l-1}$ be the orbits of G on the poset X. Then the values*

$$\sum_{x \in \omega_j} \zeta(x_i, x) \quad \text{and} \quad \sum_{x \in \omega_j} \zeta(x, x_i), \qquad i,j \in l,$$

are independent of the chosen representative $x_i \in \omega_i$. □

This result enables us to introduce the *Plesken matrices* [162]

$$A^\wedge := A^\wedge(G) = (a_{ij}^\wedge), \text{ and } A^\vee := A^\vee(G) = (a_{ij}^\vee),$$

defined by

$$a_{ij}^{\wedge} := \sum_{x \in \omega_j} \zeta(x_i, x) = \left|\left\{x \in \omega_j \mid x_i = x_i \wedge x\right\}\right| = \left|\left\{x \in \omega_j \mid x_i \leq x\right\}\right|$$

and

$$a_{ij}^{\vee} := \sum_{x \in \omega_j} \zeta(x, x_i) = \left|\left\{x \in \omega_j \mid x_i = x_i \vee x\right\}\right| = \left|\left\{x \in \omega_j \mid x \leq x_i\right\}\right|.$$

We note that these numbers are well-defined because of the 4th item of 8.2.6. In this language, the 5th item of 8.2.6 can be restated as

$$|\omega_i| \cdot a_{ij}^{\wedge} = |\omega_j| \cdot a_{ji}^{\vee}. \tag{8.2.15}$$

Using topological sorting of the orbits we obtain

Corollary 8.2.16 *For the Plesken matrices $A^{\wedge}(G)$ and $A^{\vee}(G)$ corresponding to a poset action of a finite group G on a poset X the following is true:*

1. *If $D(G) := \operatorname{diag}(|\omega_0|, \ldots, |\omega_{l-1}|)$ denotes the diagonal matrix containing the lengths of the orbits of G on X on its diagonal, then*
$$A^{\vee}(G) = (D(G) \cdot A^{\wedge}(G) \cdot D(G)^{-1})^{\top}.$$
2. *The diagonal entries of the matrices $A^{\wedge}(G)$ and $A^{\vee}(G)$ are all one.*
3. *The orbits ω_i can be numbered such that $A^{\wedge}(G)$ is an upper triangular and $A^{\vee}(G)$ a lower triangular matrix.* □

Example (the linear lattice cont.) 8.2.17 The orbits ω_i of the general linear group on the lattice $\mathcal{U}(k, q)$ are the sets of subspaces of the same dimension i, $0 \leq i \leq k$. Hence

$$A^{\vee}(\mathrm{GL}_k(q)) = \left(\begin{bmatrix} i \\ j \end{bmatrix}(q)\right)_{i,j \in k+1}.$$

Using 8.2.15 we obtain

$$A^{\wedge}(\mathrm{GL}_k(q)) = \left(\begin{bmatrix} k-i \\ j-i \end{bmatrix}(q)\right)_{i,j \in k+1}.$$

Of course, things become more complicated if we consider subgroups G of the general linear group $\mathrm{GL}_k(q)$. The reason is that the orbits of the general linear group, which are the sets of subspaces of same dimension, may split into several orbits. Nevertheless we consider this more general situation, since we find that certain submatrices of $A^{\wedge}(G)$ respectively $A^{\vee}(G)$ are crucial for the construction of minihypers respectively linear codes with prescribed minimum distance.

The dimension of a subspace is invariant under multiplication by an invertible matrix $M \in \mathrm{GL}_k(q)$. Thus

$$G\backslash\backslash\mathcal{U}(k,q) = \bigcup_{s=0}^{k} G\backslash\backslash\mathcal{U}(k,s,q).$$

This simple fact causes a block structure of the matrices $A^\wedge := A^\wedge(G)$ and $A^\vee := A^\vee(G)$. Namely, if

$$G\backslash\backslash\mathcal{U}(k,s,q) = \left\{\omega_0^{(s)}, \ldots, \omega_{l_s-1}^{(s)}\right\}$$

is the set of orbits of G on the s-subspaces, we obtain, for $S_i \in \omega_i^{(s)}$, the matrix

$$A_{s,t}^\wedge(G) = \left(a_{ij}^{(\wedge,s,t)}\right)_{i\in l_s,\, j\in l_t}$$

with entries

$$a_{ij}^{(\wedge,s,t)} := \left|\left\{T \in \omega_j^{(t)} \mid S_i = S_i \wedge T\right\}\right| = \left|\left\{T \in \omega_j^{(t)} \mid S_i \leq T\right\}\right|.$$

In the same vein, we get

$$A_{s,t}^\vee(G) = \left(a_{ij}^{(\vee,s,t)}\right)_{i\in l_s,\, j\in l_t},$$

where

$$a_{ij}^{(\vee,s,t)} := \left|\left\{T \in \omega_j^{(t)} \mid S_i = S_i \vee T\right\}\right| = \left|\left\{T \in \omega_j^{(t)} \mid T \leq S_i\right\}\right|.$$

Recall once again that the entries of these matrices only depend on the respective orbit $\omega_i^{(s)}$, not on the chosen representative S_i.

These two matrices are exactly the submatrices of $A^\wedge$ respectively $A^\vee$ the rows of which belong to the orbits of G on the s-subspaces and whose columns belong to the orbits of G on the t-subspaces. If

$$\omega_0^{(0)}, \omega_0^{(1)}, \ldots, \omega_{l_1-1}^{(1)}, \ldots, \omega_0^{(k-1)}, \ldots, \omega_{l_{k-1}-1}^{(k-1)}, \omega_0^{(k)}$$

denotes the ordering of all orbits of G on $\mathcal{U}(k,q)$ we obtain the following block decomposition:

$$A^\wedge(G) = \left(A_{s,t}^\wedge(G)\right)_{s,t\in k+1} \quad \text{and} \quad A^\vee(G) = \left(A_{s,t}^\vee(G)\right)_{s,t\in k+1},$$

where $A_{s,t}^\wedge(G)$ and $A_{s,t}^\vee(G)$ are $l_s \times l_t$-matrices. ◇

From 8.2.16 we deduce the relation between the different block matrices:

Corollary *If* $D_s(G) = \operatorname{diag}\big(|\omega_0^{(s)}|, \ldots, |\omega_{l_s-1}^{(s)}|\big)$, $s \in k+1$, *then the following is true:* **8.2.18**

$$A_{s,t}^{\vee}(G) = \Big(D_t(G) \cdot A_{t,s}^{\wedge}(G) \cdot D_s^{-1}(G)\Big)^{\top}. \qquad \square$$

Here are several special cases of these matrices: For $t \in k+1$ we have

$$A_{t,t}^{\wedge}(G) = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}, \quad A_{t,k}^{\wedge}(G) = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

For all $s, t \in k+1$ with $s > t$:

$$A_{s,t}^{\wedge}(G) = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}.$$

For all $t \in k+1$:

$$A_{0,t}^{\wedge}(G) = \Big(|\omega_0^{(t)}|, \ldots, |\omega_{l_t-1}^{(t)}|\Big).$$

The proofs are very easy. We continue with two numerical examples:

Example For the parameters $k := 8$, $q := 2$ and the general linear group $G := \mathrm{GL}_k(q)$ we obtain the following Plesken matrices: **8.2.19**

$$A^{\wedge} = \left(\begin{array}{c|c|c|c|c|c|c|c|c} 1 & 255 & 10795 & 97155 & 200787 & 97155 & 10795 & 255 & 1 \\ \hline & 1 & 127 & 2667 & 11811 & 11811 & 2667 & 127 & 1 \\ \hline & & 1 & 63 & 651 & 1395 & 651 & 63 & 1 \\ \hline & & & 1 & 31 & 155 & 155 & 31 & 1 \\ \hline & & & & 1 & 15 & 35 & 15 & 1 \\ \hline & & & & & 1 & 7 & 7 & 1 \\ \hline & & & & & & 1 & 3 & 1 \\ \hline & & & & & & & 1 & 1 \\ \hline & & & & & & & & 1 \end{array}\right)$$

and

$$A^{\vee} = \left(\begin{array}{c|c|c|c|c|c|c|c|c} 1 & & & & & & & & \\ \hline 1 & 1 & & & & & & & \\ \hline 1 & 3 & 1 & & & & & & \\ \hline 1 & 7 & 7 & 1 & & & & & \\ \hline 1 & 15 & 35 & 15 & 1 & & & & \\ \hline 1 & 31 & 155 & 155 & 31 & 1 & & & \\ \hline 1 & 63 & 651 & 1395 & 651 & 63 & 1 & & \\ \hline 1 & 127 & 2667 & 11811 & 11811 & 2667 & 127 & 1 & \\ \hline 1 & 255 & 10795 & 97155 & 200787 & 97155 & 10795 & 255 & 1 \end{array}\right).$$

$\diamond$

8.2.20 **Example** Let $k := 3$ and $q := 2$. We consider the action of the complete monomial group $M_3(2)$ which is in fact isomorphic to the symmetric group S_3, acting by permuting the 3 coordinates:

$$M_3(2) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

Figrue 8.2 shows the Hasse diagram of this lattice. The vector space $\mathbb{F}_2^3$ corresponds to the vertex on top level. Subspaces in the same orbit are connected by a horizontal edge. The orbits, shown in the table next to the diagram, are arranged from the left to the right in each level. ◇

Let us now restrict attention to the matrix $A^{\vee}_{k-1,1}(G)$, which can be used to construct minihypers with a prescribed group $G \leq \mathrm{GL}_k(q)$ of automorphisms, as we will see in the following section. Before that, let us mention an efficient way of computing this matrix.

8.2.21 **Lemma** *For a matrix $M \in \mathrm{GL}_k(q)$ and a subspace S of $\mathbb{F}_q^k$ the following equation holds:*

$$(MS)^{\perp} = (M^{\top})^{-1} S^{\perp}.$$

Proof: Since $(M^{\top})^{-1} = (M^{-1})^{\top}$, we have

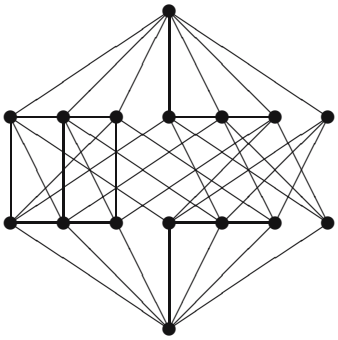
$$\begin{aligned} (MS)^{\perp} &= \left\{ v \in \mathbb{F}_q^k \mid \forall\, w \in MS : \langle v, w \rangle = 0 \right\} \\ &= \left\{ v \in \mathbb{F}_q^k \mid \forall\, w \in S : \langle v, w \cdot M^{\top} \rangle = 0 \right\} \\ &= \left\{ v \in \mathbb{F}_q^k \mid \forall\, w \in S : \langle v \cdot M, w \rangle = 0 \right\} \\ &= \left\{ v \cdot M^{-1} \in \mathbb{F}_q^k \mid v \in \mathbb{F}_q^k : \forall\, w \in S : \langle v, w \rangle = 0 \right\} \\ &= \left\{ v \cdot M^{-1} \in \mathbb{F}_q^k \mid v \in S^{\perp} \right\} \\ &= (M^{\top})^{-1} S^{\perp}. \end{aligned}$$

□

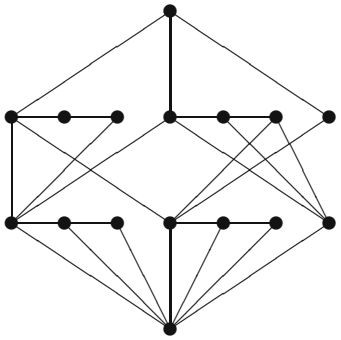
8.2.22 **Definition (dual group)** Let G be a subgroup of $\mathrm{GL}_k(q)$, then we define G^* to be the set of all transposed matrices of G

$$G^* := \{ M^{\top} \mid M \in G \}$$

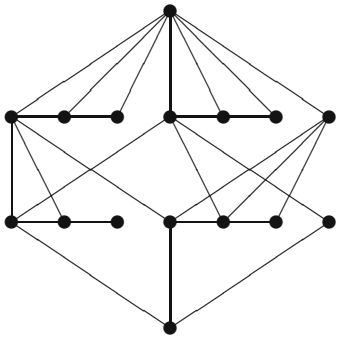
which is called the *dual group* of G. ◇



orbit	representative	orbit-length
ω_0	$\{(000)\}$	1
ω_1	$\langle(001)\rangle$	3
ω_2	$\langle(011)\rangle$	3
ω_3	$\langle(111)\rangle$	1
ω_4	$\langle(001),(010)\rangle$	3
ω_5	$\langle(111),(001)\rangle$	3
ω_6	$\langle(101),(011)\rangle$	1
ω_7	$\mathbb{F}_2^3$	1



$$A^{\wedge} = \left(\begin{array}{c|ccc|ccc|c} 1 & 3 & 3 & 1 & 3 & 3 & 1 & 1 \\ \hline & 1 & 0 & 0 & 2 & 1 & 0 & 1 \\ & & 1 & 0 & 1 & 1 & 1 & 1 \\ & & & 1 & 0 & 3 & 0 & 1 \\ \hline & & & & 1 & 0 & 0 & 1 \\ & & & & & 1 & 0 & 1 \\ & & & & & & 1 & 1 \\ \hline & & & & & & & 1 \end{array}\right)$$



$$A^{\vee} = \left(\begin{array}{c|ccc|ccc|c} 1 & & & & & & & \\ \hline 1 & 1 & & & & & & \\ 1 & 0 & 1 & & & & & \\ 1 & 0 & 0 & 1 & & & & \\ \hline 1 & 2 & 1 & 0 & 1 & & & \\ 1 & 1 & 1 & 1 & 0 & 1 & & \\ 1 & 0 & 3 & 0 & 0 & 0 & 1 & \\ \hline 1 & 3 & 3 & 1 & 3 & 3 & 1 & 1 \end{array}\right)$$

Fig. 8.2 Lattice action of $M_3(2)$ on $\mathbb{F}_2^3$

The dual group G^* is isomorphic to G via the mapping

$$\iota\colon G \to G^* \ : \ M \mapsto (M^\top)^{-1}$$

since the equation

$$((M \cdot N)^\top)^{-1} = (M^\top)^{-1} \cdot (N^\top)^{-1}$$

holds for invertible matrices M and N.

8.2.23 **Corollary** *If $P(v)$ runs through a transversal of the orbits of G^* on the set of points $\mathcal{U}(k,1,q)$, then $H(v)$ runs through a transversal of the orbits of G on the set of hyperplanes $\mathcal{U}(k,k-1,q)$. Furthermore, for the orbit of G on $H(v)$ we have*

$$G(H(v)) = \left\{ H(w) \;\middle|\; P(w) \in G^*(P(v)) \right\}. \qquad \square$$

This corollary enables us to compute the orbits of a group $G \leq \mathrm{GL}_k(q)$ on the set of hyperplanes $\mathcal{U}(k,k-1,q)$. Instead of computing these orbits we construct orbit representatives of $G^* \backslash\backslash \mathcal{U}(k,1,q)$ which is much easier since the representation of points needs one basis vector while hyperplanes are represented by $k-1$ basis vectors.

Exercises

E.8.2.1 **Exercise** Prove that every finite poset can be sorted topologically.

E.8.2.2 **Exercise** Prove 8.2.13.

E.8.2.3 **Exercise** Prove that

$$\begin{bmatrix} r-s \\ r-t \end{bmatrix}(q) \cdot A^{\wedge}_{s,r} = A^{\wedge}_{s,t} \cdot A^{\wedge}_{t,r}.$$

for $s,t,r \in k+1$ with $s \leq t \leq r$.

E.8.2.4 **Exercise** Show that we have, for the action of the monomial group,

$$A^{\wedge}_{t,k}(M_k(q)) = A^{\vee}_{n-t,n-k}(M_k(q)), \text{ resp. } A^{\vee}_{t,k}(M_k(q)) = A^{\wedge}_{n-t,n-k}(M_k(q)).$$

8.3 Prescribing a Group of Automorphisms 8.3

As announced we are now going to use the prescription of a group of automorphisms for a construction of certain blocking sets respectively minihypers in projective geometries. Of course, such a prescription is risky since there may no exist a blocking set with this automorphism group. On the other hand, if there are such linear codes, then it will pay off since the number of columns of the incidence matrix $M_{k,q}$, which correspond to the points, will reduce to the number of orbits of the group on the set of 1-subspaces, and the same will happen to the rows which correspond to the hyperplanes. Quite often, this *data reduction* will bring the construction of linear codes within the reach of current computers.

Definition (automorphism of a blocking set) An element $M \in \mathrm{GL}_k(q)$ is called an *automorphism* of a t-blocking set $B \subseteq \mathrm{PG}_{k-1}(q)$ if M permutes the points of B, i.e. 8.3.1

$$MB := \{MP \mid P \in B\} = B.$$

Recall from 8.2.8 that the action is $MP = MP(v) = P(v \cdot M^\top)$.

A group consisting only of automorphisms of B is called *a* group of automorphisms of B, the maximal group with this property is called the *full* group of automorphisms and it is abbreviated by $\mathrm{Aut}(B)$. ◇

The crucial facts for the construction of t-blocking sets with a prescribed group of automorphisms are the following ones.

Remarks Let G be a subgroup of $\mathrm{GL}_k(q)$. 8.3.2

- The group G is a group of automorphism of a t-blocking set B in $\mathrm{PG}_{k-1}(q)$ if and only if B is a union of G-orbits on $\mathcal{U}(k,1,q)$.
- The incidence between points P and hyperplanes H is invariant under the action of G, i.e. if $P \subseteq H$ then $MP \subseteq MH$ for all $M \in G$.
- The number m of G-orbits on the set of points $\mathcal{U}(k,1,q)$ is equal to the number of G-orbits on the set of hyperplanes $\mathcal{U}(k,k-1,q)$.
- If $\{\omega_0,\ldots,\omega_{r-1}\}$ respectively $\{\Omega_0,\ldots,\Omega_{r-1}\}$ are the sets of G-orbits on $\mathcal{U}(k,1,q)$ respectively $\mathcal{U}(k,k-1,q)$ with representatives $P_i \in \omega_i$ respectively $H_i \in \Omega_i$, then the cardinality $|\omega_j \cap H_i| = |\{P \in \omega_j \mid P \subseteq H_i\}|$ is independent of the chosen representative H_i of the orbit Ω_i. ◇

These facts embed the construction problem of blocking sets into the theory of group actions on lattices. They motivate the reduction of the incidence matrix $M_{k,q}$ between 1-subspaces and $(k-1)$-subspaces to the incidence matrix

$M_{k,q}^G = (m_{ij}^G)$ between the *G-orbits* of 1-subspaces and the *G-orbits* of $(k-1)$-subspaces:

$$m_{ij}^G := |\omega_j \cap H_i|,$$

i.e. this matrix is a Plesken matrix:

8.3.3
$$M_{k,q}^G = A_{k-1,1}^{\vee}(G).$$

The following theorem describes the fundamental construction:

8.3.4 **Theorem** *There is a bijection between the set of all t-blocking sets in* $\mathrm{PG}_{k-1}(q)$ *with* $G \leq \mathrm{GL}_k(q)$ *as a group of automorphisms and the set of solutions* $\binom{x}{y}$*, with* $x_i \in \{0,1\}$ *and* $y_i \in \{t,\ldots,\theta_{k-2}(q)\}$*, of the following system of linear equations:*

$$\left(M_{k,q}^G \mid -I\right) \cdot \begin{pmatrix} x \\ y \end{pmatrix} = 0,$$

where $x = (x_0,\ldots,x_{r-1})^\top$*,* $y = (y_0,\ldots,y_{r-1})^\top$ *for* $r = |G\backslash\backslash\mathcal{U}(k,1,q)|$*. If* $\binom{x}{y}$ *denotes a solution, then the corresponding t-blocking set B is*

$$B = \bigcup_{j:x_j=1} \omega_j.$$

Proof: Let **B** be the set of all t-blocking sets in $\mathrm{PG}_{k-1}(q)$ having $G \leq \mathrm{GL}_k(q)$ as a group of automorphisms and let **S** be the set of all solutions $\binom{x}{y}$ of the linear system of equations $(M_{k,q}^G \mid -I) \cdot \binom{x}{y} = 0$ with $x_j \in \{0,1\}$ and $y_j \in \{t,\ldots,\theta_{k-2}(q)\}$. It is easy to see that the mappings

$$\varphi\colon \mathbf{S} \to \mathbf{B} \;:\; \begin{pmatrix} x \\ y \end{pmatrix} \mapsto B \text{ with } B := \bigcup_{j:x_j=1} \omega_j$$

and

$$\psi\colon \mathbf{B} \to \mathbf{S} \;:\; B \mapsto \begin{pmatrix} x \\ y \end{pmatrix} \text{ with } x_j := \begin{cases} 1 & \text{if } \omega_j \subseteq B, \\ 0 & \text{otherwise,} \end{cases} \text{ and } y_i := |B \cap H_i|,$$

are mutually inverse bijections. □

If $\binom{x}{y}$ denotes an admissible solution of this linear system of equations and $B = \bigcup_{j:x_j=1} \omega_j$ the corresponding t-blocking set in $\mathrm{PG}_{k-1}(q)$, then the cardinality of B is

$$b = \sum_{j:x_j=1} |\omega_j|.$$

If we add this equation as as further row to the linear system of equations we obtain the corresponding construction of (b,t)-minihypers in $\mathrm{PG}_{k-1}(q)$ with a prescribed group of automorphisms and hence projective codes.

Corollary 8.3.5 *The set of all t-blocking sets in* $\mathrm{PG}_{k-1}(q)$ *with cardinality b, having a subgroup* $G \leq \mathrm{GL}_k(q)$ *as a group of automorphisms can be obtained from the set of vectors* $\binom{x}{y}$ *with* $x_i \in \{0,1\}$ *and* $y_i \in \{t,\ldots,\theta_{k-2}(q)\}$, $i \in r := |G\backslash\backslash\mathcal{U}(k,1,q)|$, *solving the linear system of equations:*

$$\left(\begin{array}{ccc|ccc} m^G_{0,0} & \ldots & m^G_{0,r-1} & -1 & & \\ \vdots & & \vdots & & \ddots & \\ m^G_{r-1,0} & \ldots & m^G_{r-1,r-1} & & & -1 \\ \hline |\omega_0| & \ldots & |\omega_{r-1}| & 0 & \ldots & 0 \end{array}\right) \cdot \left(\begin{array}{c} x_0 \\ \vdots \\ x_{r-1} \\ \hline y_0 \\ \vdots \\ y_{r-1} \end{array}\right) = \left(\begin{array}{c} 0 \\ \vdots \\ 0 \\ \hline b \end{array}\right)$$

If $\binom{x}{y}$ *denotes such a solution, then the corresponding t-blocking set B with* $|B| = b$ *is*

$$B = \bigcup_{j:x_j=1} \omega_j.$$

This blocking set B is a (b,t)*-minihyper in* $\mathrm{PG}_{k-1}(q)$ *if and only if the vector y contains a component which is exactly t, i.e. if and only if there is an index j with* $y_j = t$. □

Example 8.3.6 We want to construct $(6,1)$-blocking sets in $\mathrm{PG}_2(3)$, i.e. the parameters are $q = 3$, $k = 3$, $t = 1$, $b = 6$, $\theta_2(3) = (3^3-1)/(3-1) = 13$ and $\theta_1(3) = (3^2-1)/(3-1) = 4$. The projective geometry $\mathrm{PG}_2(3)$ consists of the following 13 points

$$\begin{array}{lll} P_0 = P(001), & P_5 = P(101), & \\ P_1 = P(010), & P_6 = P(102), & P_{10} = P(120), \\ P_2 = P(011), & P_7 = P(110), & P_{11} = P(121), \\ P_3 = P(012), & P_8 = P(111), & P_{12} = P(122). \\ P_4 = P(100), & P_9 = P(112), & \end{array}$$

Hence the incidence matrix $M_{3,3}$ is of size 13×13. Now we prescribe the complete monomial group $G := M_3(3)$ which yields three orbits on the set of points $\mathcal{U}(3,1,3)$:

$$\begin{aligned} \omega_0 &= \{P_0, P_1, P_4\}, \\ \omega_1 &= \{P_2, P_3, P_5, P_6, P_7, P_{10}\}, \\ \omega_2 &= \{P_8, P_9, P_{11}, P_{12}\}. \end{aligned}$$

In addition we obtain the orbits on the set of hyperplanes $\mathcal{U}(3,2,3)$:

$$\begin{aligned} \Omega_0 &= \{P_0^\perp, P_1^\perp, P_4^\perp\}, \\ \Omega_1 &= \{P_2^\perp, P_3^\perp, P_5^\perp, P_6^\perp, P_7^\perp, P_{10}^\perp\}, \\ \Omega_2 &= \{P_8^\perp, P_9^\perp, P_{11}^\perp, P_{12}^\perp\} \end{aligned}$$

and the reduced matrix turns out to be of size 3×3:

$$M_{3,3}^{G} = A_{2,1}^{\vee}(M_3(3)) = \begin{pmatrix} 2 & 2 & 0 \\ 1 & 1 & 2 \\ 0 & 3 & 1 \end{pmatrix}.$$

This shows that we have obtained a data reduction by the *factor* $169/9$ which is nearly 20. The corresponding system of Diophantine equations is

$$\left(\begin{array}{ccc|ccc} 2 & 2 & 0 & -1 & 0 & 0 \\ 1 & 1 & 2 & 0 & -1 & 0 \\ 0 & 3 & 1 & 0 & 0 & -1 \\ \hline 3 & 6 & 4 & 0 & 0 & 0 \end{array}\right) \cdot \left(\begin{array}{c} x_0 \\ x_1 \\ x_2 \\ \hline y_0 \\ y_1 \\ y_2 \end{array}\right) = \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ \hline 6 \end{array}\right)$$

where $x_i \in \{0,1\}$ and $y_i \in \{1,2,3,4\}$. It is easy to see that $(0,1,0;2,1,3)^{\top}$ is the only solution of this system which corresponds to a $(6,1)$-blocking set

$$B = \omega_1 = \{P_2, P_3, P_5, P_6, P_7, P_{10}\}. \qquad \diamond$$

8.4 Linear Codes of Prescribed Type

We have seen that codes with minimum distance $d \leq q^{k-1}$ meeting the Griesmer-bound are always projective. If such a code is regarded as an n-set in $\mathrm{PG}_{k-1}(q)$, then the complement of that n-set defines a minihyper and vice versa. The minihyper approach only works for projective codes. It does not work work general codes, since it is not clear how to define complements of multisets. In order to avoid such investigations we construct the n-multiset defining the linear code directly, using the same construction that we used for minihypers: We solve a linear system of Diophantine equations.

In Section 8.1, we have shown how to construct blocking sets with the aid of the incidence matrix $M_{k,q} = (m_{ij})$ by solving a system of Diophantine equations. The 0-1-vector x corresponds to a selection of points defining the blocking set B. The complement of the blocking set B then was a projective code. After changing some entries in the system of equations, this method allows us to construct the projective codes directly.

If $\mathcal{U}(k,1,q) = \{P_0, \ldots, P_{r-1}\}$ respectively $\mathcal{U}(k,k-1,q) = \{H_0, \ldots, H_{r-1}\}$, where $r := \theta_{k-1}(q)$ again denotes the number of points respectively hyperplanes, then the solutions $\binom{x}{y}$ with $x_j \in \{0,1\}$ and $y_j \in \{0, \ldots, n-d\}$ of the

system

$$\left(\begin{array}{ccc|ccc} m_{0,0} & \dots & m_{0,r-1} & -1 & & \\ \vdots & & \vdots & & \ddots & \\ m_{r-1,0} & \dots & m_{r-1,r-1} & & & -1 \\ \hline 1 & \dots & 1 & 0 & \dots & 0 \end{array}\right) \cdot \left(\begin{array}{c} x_0 \\ \vdots \\ x_{r-1} \\ \hline y_0 \\ \vdots \\ y_{r-1} \end{array}\right) = \left(\begin{array}{c} 0 \\ \vdots \\ 0 \\ \hline n \end{array}\right)$$

define the projective (n,k)-codes over $\mathbb{F}_q$ with minimum distance greater than or equal to d. The first part x of a solution $\binom{x}{y}$ defines a selection of points which determine the columns of a generator matrix: The point P_j is selected if and only if x_j is 1. Now if we permit values greater than 1 for the components x_j, then the vector x describes a multiset $\mathcal{X}$, containing the point P_j exactly x_j times.

Hence the solutions $\binom{x}{y}$ with $x_j \in \{0,\dots,n\}$ and $y_j \in \{0,\dots,n-d\}$ of the system of Diophantine equations correspond to the nonredundant (n,k)-codes over $\mathbb{F}_q$ with minimum distance greater than or equal to d.

Assume that $\mathcal{X}$ is such a multiset corresponding to a solution $\binom{x}{y}$ and consider $v_j \in \mathbb{F}_q^k \backslash \{0\}$ such that $H_j = H(v_j)$, then $y_j = |\mathcal{X} \downarrow H(v_j)|$. We obtain the weight distribution from 8.1.5:

$$A_i = (q-1) \cdot \left|\{j \in r \mid y_j = n - i\}\right|, \quad \text{for } i > 0.$$

But as with the construction of blocking sets and projective codes the system of equations is still too big for an efficient computation of solutions. Therefore, again we reduce the dimension of the matrix of coefficients by prescribing a group of automorphisms. But first we have to make clear what a prescription of such a group means in the case of multisets and codes.

If $\Gamma = (\gamma_{ij})$ denotes a generator matrix of an (n,k)-code C and

$$\mathcal{X}_\Gamma := \{\!\{P(\gamma_{*,0}),\dots,P(\gamma_{*,n-1})\}\!\}$$

denotes the n-multiset of points in $\mathrm{PG}_{k-1}(q)$ defined by the columns of the generator matrix Γ, then the following holds true for each $M \in GL_k(q)$:

$$M\mathcal{X}_\Gamma := \{\!\{MP(\gamma_{*,0}),\dots,MP(\gamma_{*,n-1})\}\!\} = \mathcal{X}_{M\cdot\Gamma}.$$

Definition (projective automorphism) A *projective automorphism* of a generator matrix Γ of a nonredundant (n,k)-code is an element $M \in \mathrm{GL}_k(q)$ which leaves the multiset $\mathcal{X}_\Gamma$ invariant: **8.4.1**

$$M\mathcal{X}_\Gamma = \mathcal{X}_\Gamma.$$

A group consisting only of projective automorphisms of Γ is called a group of automorphisms of Γ. The largest group with this property is called the *full* group of projective automorphisms and it is abbreviated by $\mathrm{Aut}(\Gamma)$. $\diamond$

If Γ and Γ' denote two generator matrices of the same (n,k)-code C, then there is an element $N \in \mathrm{GL}_k(q)$ such that $\Gamma' = N \cdot \Gamma$. Now if M is a projective automorphism of Γ, i.e $M\mathcal{X}_\Gamma = \mathcal{X}_\Gamma$, then the conjugate element $N \cdot M \cdot N^{-1}$ defines a projective automorphism of Γ', since

$$N \cdot M \cdot N^{-1}\mathcal{X}_{N\cdot\Gamma} = N \cdot M\mathcal{X}_{N^{-1}\cdot N\cdot\Gamma} = N \cdot M\mathcal{X}_\Gamma = N\mathcal{X}_\Gamma = \mathcal{X}_{N\cdot\Gamma},$$

i.e. the conjugate group

$$NGN^{-1} := \left\{ N \cdot M \cdot N^{-1} \mid M \in G \right\}$$

is a group of projective automorphisms of $N \cdot \Gamma$. The set of matrices $N \cdot \Gamma$, where $N \in \mathrm{GL}_k(q)$, contains all the generator matrices of C, and thus all the conjugates NGN^{-1} of G are groups of projective automorphisms, so that we can introduce the following notion of type of a code:

8.4.2 Definition (stabilizer type of a code) Let G be a subgroup of $\mathrm{GL}_k(q)$. An (n,k)-code C over $\mathbb{F}_q$ has as *stabilizer type* the conjugacy class

$$\widetilde{G} := \left\{ NGN^{-1} \mid N \in \mathrm{GL}_k(q) \right\}$$

if there is a generator matrix Γ of C such that Γ has G as a group of projective automorphisms. $\diamond$

This concept allows us to formulate the following important consequence:

8.4.3 Theorem *Let G be a subgroup of $\mathrm{GL}_k(q)$ with orbits $\omega_0, \ldots, \omega_{r-1}$ on the set $\mathcal{U}(k,1,q)$ of points and orbits $\Omega_0, \ldots, \Omega_{r-1}$ on the set $\mathcal{U}(k,k-1,q)$ of hyperplanes. Consider representatives $H_i \in \Omega_i$ and put*

$$m_{ij}^G := \left| \left\{ P \in \omega_j \mid P \subseteq H_i \right\} \right|.$$

There is a bijection between the set of all linear (n,k)-codes over $\mathbb{F}_q$ with minimum distance at least d and type $\widetilde{G}$ and the set of vectors $\binom{x}{y}$ with $x_i \in \{0, \ldots, \lfloor n/|\omega_i| \rfloor\}$ and $y_i \in \{0, \ldots, n-d\}$, $i \in r := |G\backslash\backslash\mathcal{U}(k,1,q)|$, solving the linear system of equations:

$$\left(\begin{array}{ccc|ccc} m_{0,0}^G & \ldots & m_{0,r-1}^G & -1 & & \\ \vdots & & \vdots & & \ddots & \\ m_{r-1,0}^G & \ldots & m_{r-1,r-1}^G & & & -1 \\ \hline |\omega_0| & \ldots & |\omega_{r-1}| & 0 & \ldots & 0 \end{array}\right) \cdot \left(\begin{array}{c} x_0 \\ \vdots \\ x_{r-1} \\ \hline y_0 \\ \vdots \\ y_{r-1} \end{array}\right) = \left(\begin{array}{c} 0 \\ \vdots \\ 0 \\ \hline n \end{array}\right)$$

If $\binom{x}{y}$ is a solution of this system, then the first part x defines an n-multiset $\mathcal{X}$ of points as follows

$$\mathcal{X} = \bigcup_{i:x_i>0} \bigcup_{j=1}^{x_i} \omega_j,$$

where $\cup$ means the union of multisets. Representatives of the points of $\mathcal{X}$, written column by column in a matrix, yield a generator matrix of an (n,k,d,q)-code C. Furthermore, the weight distribution $W_C(x,y) = y^n + \sum_{i=1}^{n} A_i x^i y^{n-i}$ is given by

$$A_i = (q-1) \sum_{j:y_j=n-i} |\Omega_j|. \qquad \square$$

Example Suppose we are now looking for a linear $(14,3,9)$-code over $\mathbb{F}_3$. Such a code is optimal. First note that a code with these parameters cannot be projective, since there are exactly 13 points in $\mathrm{PG}_2(3)$, i.e. at least one point has to occur twice in a generator matrix of such a code. The parameters $q = 3$ and $k = 3$ are the same as in example 8.3.6 and we also prescribe the group $M_3(3)$ as a group of automorphisms. The orbits on the points and hyperplanes are also shown in 8.3.6. The corresponding system of equations is **8.4.4**

$$\left(\begin{array}{ccc|ccc} 2 & 2 & 0 & -1 & 0 & 0 \\ 1 & 1 & 2 & 0 & -1 & 0 \\ 0 & 3 & 1 & 0 & 0 & -1 \\ \hline 3 & 6 & 4 & 0 & 0 & 0 \end{array}\right) \cdot \left(\begin{array}{c} x_0 \\ x_1 \\ x_2 \\ \hline y_0 \\ y_1 \\ y_2 \end{array}\right) = \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ \hline 14 \end{array}\right),$$

where $x_0 \in \{0,1,2,3,4\}$, $x_1 \in \{0,1,2\}$, $x_2 \in \{0,1,2,3\}$ and $y_i \in \{0,1,2,3,4,5\}$, see also 7.7.11. A solution of this system is $(0,1,2;2,5,5)^\top$, which means that the orbit ω_1 occurs once in the corresponding multiset $\mathcal{X}$ and the orbit ω_2 occurs twice in $\mathcal{X}$. Thus we obtain the following multiset

$$\begin{aligned} \mathcal{X} &= \omega_1 \cup \omega_2 \cup \omega_2 \\ &= \{\!\{P_2, P_3, P_5, P_6, P_7, P_{10}, P_8, P_9, P_{11}, P_{12}, P_8, P_9, P_{11}, P_{12}\}\!\} \end{aligned}$$

and finally the generator matrix

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

of an optimal $(14,3,9)$-code. For the weight distribution we obtain:

$$W_C(x,y) = y^{14} + 20x^9y^5 + 6x^{12}y^3,$$

since $A_9 = (3-1)\cdot(|\Omega_1| + |\Omega_2|) = 20$ and $A_{12} = (3-1)\cdot|\Omega_0| = 6$. $\diamond$

8.5

8.5 Numerical Results

On the following pages we present new codes obtained with the proposed method. Applying the modifications to these codes described in the second chapter all in all we got more than 400 new codes (see [32]).

For each pair of values (q,k) we show a table with parameters n,d,G,r of 8.4.3. A row in such a table means that we have constructed a code over $\mathbb{F}_q$ with dimension k, with length n, minimum distance d and type $\widetilde{G}$. The number r is the number of orbits of the corresponding group G on the set of points $\mathcal{U}(k,1,q)$. A bold minimum distance d means, that the (n,k,d)-code is optimal.

For the finite field $\mathbb{F}_q = \mathbb{F}_{p^m}$ we use the additive representation, i.e. the elements of $\mathbb{F}_{p^m} = \mathbb{F}_p/I(f)$ which are cosets $k_0 + k_1x + \ldots + k_{m-1}x^{m-1} + I(f)$ are coded as numbers $k_0 + k_1p + \ldots + k_{m-1}p^{m-1}$. The corresponding irreducible polynomials can be found in Table 3.3.

Table 8.1 Linear codes for $q = 2$ and $k = 10$

n	d	G	r
177	**84**	$\left\langle \begin{pmatrix} 1010100100 \\ 1100001000 \\ 1011000100 \\ 1011110100 \\ 1100000010 \\ 0010001111 \\ 1101010011 \\ 1011010110 \\ 0010110000 \\ 1010101100 \end{pmatrix} \right\rangle$	51

Table 8.2 Linear codes for $q = 3$ and $k = 6$

n	d	G	r
191	**126**	$\left\langle \begin{pmatrix} 100000 \\ 001000 \\ 000010 \\ 000001 \\ 000100 \\ 010000 \end{pmatrix}, \begin{pmatrix} 001000 \\ 000100 \\ 000001 \\ 100000 \\ 000010 \\ 010000 \end{pmatrix} \right\rangle$	20
202	132	$\left\langle \begin{pmatrix} 100000 \\ 001000 \\ 000010 \\ 000001 \\ 000100 \\ 010000 \end{pmatrix}, \begin{pmatrix} 001000 \\ 000100 \\ 000001 \\ 100000 \\ 000010 \\ 010000 \end{pmatrix} \right\rangle$	20
219	**144**	$\left\langle \begin{pmatrix} 000001 \\ 100002 \\ 010001 \\ 001002 \\ 000102 \\ 000012 \end{pmatrix} \right\rangle$	23

Table 8.3 Linear codes for $q = 3$ and $k = 7$

n	d	G	r
202	129	$\left\langle \begin{pmatrix} 2211010 \\ 1011220 \\ 1211220 \\ 0022000 \\ 0201010 \\ 0212120 \\ 0000001 \end{pmatrix} \right\rangle$	35
222	144	$\left\langle \begin{pmatrix} 0000010 \\ 1000010 \\ 0100000 \\ 0010010 \\ 0001000 \\ 0000120 \\ 0000001 \end{pmatrix} \right\rangle$	45

Table 8.4 Linear codes for $q = 3$ and $k = 8$

n	d	G	r
64	37	$\left\langle \begin{pmatrix} 00000010 \\ 00010000 \\ 00000100 \\ 10000000 \\ 01000000 \\ 00001000 \\ 00100000 \\ 00000001 \end{pmatrix}, \begin{pmatrix} 01000000 \\ 00001000 \\ 00000100 \\ 00000001 \\ 00010000 \\ 10000000 \\ 00000010 \\ 00100000 \end{pmatrix} \right\rangle$	72
224	141	$\left\langle \begin{pmatrix} 00000100 \\ 10000000 \\ 01000200 \\ 00100200 \\ 00010100 \\ 00001000 \\ 00000010 \\ 00000001 \end{pmatrix} \right\rangle$	69
228	144	$\left\langle \begin{pmatrix} 00000100 \\ 10000000 \\ 01000200 \\ 00100200 \\ 00010100 \\ 00001000 \\ 00000010 \\ 00000001 \end{pmatrix} \right\rangle$	69

Table 8.5 Linear codes for $q = 4$ and $k = 5$

n	d	G	r
56	**40**	$\left\langle \begin{pmatrix} 00001 \\ 00010 \\ 01000 \\ 10000 \\ 00100 \end{pmatrix} \right\rangle$	69
70	**50**	$\left\langle \begin{pmatrix} 01133 \\ 13012 \\ 03012 \\ 32022 \\ 13311 \end{pmatrix} \right\rangle$	33
99	**72**	$\left\langle \begin{pmatrix} 10000 \\ 00010 \\ 00001 \\ 01000 \\ 00100 \end{pmatrix}, \begin{pmatrix} 10000 \\ 02000 \\ 00100 \\ 00030 \\ 00002 \end{pmatrix} \right\rangle$	31
137	**100**	$\left\langle \begin{pmatrix} 22101 \\ 33213 \\ 31331 \\ 00020 \\ 13032 \end{pmatrix} \right\rangle$	33
163	**120**	$\left\langle \begin{pmatrix} 33221 \\ 21332 \\ 31212 \\ 21333 \\ 10013 \end{pmatrix} \right\rangle$	21
177	130	$\left\langle \begin{pmatrix} 00010 \\ 00100 \\ 10000 \\ 00001 \\ 01000 \end{pmatrix}, \begin{pmatrix} 00100 \\ 10000 \\ 00001 \\ 00010 \\ 01000 \end{pmatrix} \right\rangle$	25

Table 8.6 Linear codes for $q = 4$ and $k = 5$

n	d	G	r
182	134	$\left\langle \begin{pmatrix} 00010 \\ 00100 \\ 10000 \\ 00001 \\ 01000 \end{pmatrix}, \begin{pmatrix} 00100 \\ 10000 \\ 00001 \\ 00010 \\ 01000 \end{pmatrix} \right\rangle$	25
189	**140**	$\left\langle \begin{pmatrix} 20200 \\ 31231 \\ 00022 \\ 30003 \\ 32102 \end{pmatrix} \right\rangle$	21
194	**144**	$\left\langle \begin{pmatrix} 10210 \\ 32020 \\ 30110 \\ 20000 \\ 00001 \end{pmatrix} \right\rangle$	21
226	**168**	$\left\langle \begin{pmatrix} 00010 \\ 00100 \\ 10000 \\ 00001 \\ 01000 \end{pmatrix}, \begin{pmatrix} 00100 \\ 10000 \\ 00001 \\ 00010 \\ 01000 \end{pmatrix} \right\rangle$	25
236	**176**	$\left\langle \begin{pmatrix} 00010 \\ 00100 \\ 10000 \\ 00001 \\ 01000 \end{pmatrix}, \begin{pmatrix} 00100 \\ 10000 \\ 00001 \\ 00010 \\ 01000 \end{pmatrix} \right\rangle$	25

Table 8.7 Linear codes for $q = 4$ and $k = 6$

n	d	G	r
102	72	$\left\langle \begin{pmatrix} 200000 \\ 002000 \\ 000200 \\ 000002 \\ 020000 \\ 000020 \end{pmatrix}, \begin{pmatrix} 002000 \\ 200000 \\ 020000 \\ 000002 \\ 000200 \\ 000020 \end{pmatrix} \right\rangle$	51
108	76	$\left\langle \begin{pmatrix} 000100 \\ 100000 \\ 000001 \\ 001000 \\ 000010 \\ 010000 \end{pmatrix}, \begin{pmatrix} 000001 \\ 000100 \\ 100000 \\ 000010 \\ 010000 \\ 001000 \end{pmatrix} \right\rangle$	51
134	96	$\left\langle \begin{pmatrix} 000100 \\ 100000 \\ 000001 \\ 001000 \\ 000010 \\ 010000 \end{pmatrix}, \begin{pmatrix} 000001 \\ 000100 \\ 100000 \\ 000010 \\ 010000 \\ 001000 \end{pmatrix} \right\rangle$	51
140	100	$\left\langle \begin{pmatrix} 010000 \\ 000010 \\ 000100 \\ 000001 \\ 100000 \\ 001000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 000010 \\ 001000 \\ 100000 \\ 010000 \\ 000001 \end{pmatrix} \right\rangle$	51
146	104	$\left\langle \begin{pmatrix} 010000 \\ 000010 \\ 000100 \\ 000001 \\ 100000 \\ 001000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 000010 \\ 001000 \\ 100000 \\ 010000 \\ 000001 \end{pmatrix} \right\rangle$	51

Table 8.8 Linear codes for $q = 4$ and $k = 6$

n	d	G	r
161	115	$\left\langle \begin{pmatrix} 000030 \\ 000300 \\ 300000 \\ 000003 \\ 003000 \\ 030000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 000001 \\ 100000 \\ 010000 \\ 000010 \\ 001000 \end{pmatrix} \right\rangle$	51
165	118	$\left\langle \begin{pmatrix} 010000 \\ 000010 \\ 000100 \\ 000001 \\ 100000 \\ 001000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 000010 \\ 001000 \\ 100000 \\ 010000 \\ 000001 \end{pmatrix} \right\rangle$	51
175	126	$\left\langle \begin{pmatrix} 001130 \\ 233003 \\ 322120 \\ 331110 \\ 103301 \\ 011332 \end{pmatrix} \right\rangle$	17
180	130	$\left\langle \begin{pmatrix} 010000 \\ 000010 \\ 000100 \\ 000001 \\ 100000 \\ 001000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 000010 \\ 001000 \\ 100000 \\ 010000 \\ 000001 \end{pmatrix} \right\rangle$	51
185	134	$\left\langle \begin{pmatrix} 010000 \\ 000010 \\ 000100 \\ 000001 \\ 100000 \\ 001000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 000010 \\ 001000 \\ 100000 \\ 010000 \\ 000001 \end{pmatrix} \right\rangle$	51

Table 8.9 Linear codes for $q = 4$ and $k = 6$

n	d	G	r
191	138	$\left\langle \begin{pmatrix} 010000 \\ 000010 \\ 000100 \\ 000001 \\ 100000 \\ 001000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 000010 \\ 001000 \\ 100000 \\ 010000 \\ 000001 \end{pmatrix} \right\rangle$	51
195	141	$\left\langle \begin{pmatrix} 010000 \\ 000010 \\ 000100 \\ 000001 \\ 100000 \\ 001000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 000010 \\ 001000 \\ 100000 \\ 010000 \\ 000001 \end{pmatrix} \right\rangle$	51
201	145	$\left\langle \begin{pmatrix} 000100 \\ 001000 \\ 000010 \\ 010000 \\ 100000 \\ 000001 \end{pmatrix}, \begin{pmatrix} 010000 \\ 001000 \\ 100000 \\ 000010 \\ 000001 \\ 000100 \end{pmatrix} \right\rangle$	51
205	148	$\left\langle \begin{pmatrix} 000100 \\ 001000 \\ 000010 \\ 010000 \\ 100000 \\ 000001 \end{pmatrix}, \begin{pmatrix} 010000 \\ 001000 \\ 100000 \\ 000010 \\ 000001 \\ 000100 \end{pmatrix} \right\rangle$	51
210	152	$\left\langle \begin{pmatrix} 000010 \\ 010000 \\ 100000 \\ 001000 \\ 000001 \\ 000100 \end{pmatrix}, \begin{pmatrix} 010000 \\ 000001 \\ 000010 \\ 001000 \\ 000100 \\ 100000 \end{pmatrix} \right\rangle$	51

Table 8.10 Linear codes for $q = 4$ and $k = 6$

n	d	G	r
220	160	$\left\langle \begin{pmatrix} 000010 \\ 010000 \\ 100000 \\ 001000 \\ 000001 \\ 000100 \end{pmatrix}, \begin{pmatrix} 010000 \\ 000001 \\ 000010 \\ 001000 \\ 000100 \\ 100000 \end{pmatrix} \right\rangle$	51
226	163	$\left\langle \begin{pmatrix} 000100 \\ 001000 \\ 000010 \\ 010000 \\ 100000 \\ 000001 \end{pmatrix}, \begin{pmatrix} 010000 \\ 001000 \\ 100000 \\ 000010 \\ 000001 \\ 000100 \end{pmatrix} \right\rangle$	51
232	168	$\left\langle \begin{pmatrix} 000010 \\ 010000 \\ 100000 \\ 001000 \\ 000001 \\ 000100 \end{pmatrix}, \begin{pmatrix} 010000 \\ 000001 \\ 000010 \\ 001000 \\ 000100 \\ 100000 \end{pmatrix} \right\rangle$	51
237	172	$\left\langle \begin{pmatrix} 000010 \\ 010000 \\ 100000 \\ 001000 \\ 000001 \\ 000100 \end{pmatrix}, \begin{pmatrix} 010000 \\ 000001 \\ 000010 \\ 001000 \\ 000100 \\ 100000 \end{pmatrix} \right\rangle$	51
242	176	$\left\langle \begin{pmatrix} 000010 \\ 010000 \\ 100000 \\ 001000 \\ 000001 \\ 000100 \end{pmatrix}, \begin{pmatrix} 010000 \\ 000001 \\ 000010 \\ 001000 \\ 000100 \\ 100000 \end{pmatrix} \right\rangle$	51

Table 8.11 Linear codes for $q = 4$ and $k = 7$

n	d	G	r
126	88	$\langle \begin{pmatrix} 3001233 \\ 2212232 \\ 0010311 \\ 2230310 \\ 1310312 \\ 1110332 \\ 2303023 \end{pmatrix} \rangle$	89
158	110	$\langle \begin{pmatrix} 1000010 \\ 0010001 \\ 0011000 \\ 1000000 \\ 1101000 \\ 1010111 \\ 0010100 \end{pmatrix} \rangle$	181
161	112	$\langle \begin{pmatrix} 1000010 \\ 0010001 \\ 0011000 \\ 1000000 \\ 1101000 \\ 1010111 \\ 0010100 \end{pmatrix} \rangle$	181
189	132	$\langle \begin{pmatrix} 1331321 \\ 1330022 \\ 2230231 \\ 0322221 \\ 2000032 \\ 3200131 \\ 2201032 \end{pmatrix} \rangle$	89

Table 8.12 Linear codes for $q = 5$ and $k = 5$

n	d	G	r
53	**40**	$\langle \begin{pmatrix} 41233 \\ 22240 \\ 13413 \\ 32040 \\ 40040 \end{pmatrix} \rangle$	61
92	70	$\langle \begin{pmatrix} 00002 \\ 10002 \\ 01001 \\ 00104 \\ 00010 \end{pmatrix} \rangle$	45
100	76	$\langle \begin{pmatrix} 00002 \\ 10002 \\ 01001 \\ 00104 \\ 00010 \end{pmatrix} \rangle$	45
110	85	$\langle \begin{pmatrix} 12344 \\ 31144 \\ 20332 \\ 34344 \\ 43110 \end{pmatrix} \rangle$	71

Table 8.13 Linear codes for $q = 5$ and $k = 6$

n	d	G	r
50	34	$\left\langle \begin{pmatrix} 212000 \\ 042000 \\ 023000 \\ 000130 \\ 000100 \\ 000001 \end{pmatrix} \right\rangle$	173
70	50	$\left\langle \begin{pmatrix} 010000 \\ 001000 \\ 100000 \\ 000010 \\ 000001 \\ 000100 \end{pmatrix}, \begin{pmatrix} 100000 \\ 010000 \\ 003000 \\ 000300 \\ 000010 \\ 000002 \end{pmatrix} \right\rangle$	35
73	52	$\left\langle \begin{pmatrix} 100000 \\ 000100 \\ 000010 \\ 000001 \\ 010000 \\ 001000 \end{pmatrix}, \begin{pmatrix} 001000 \\ 000100 \\ 000001 \\ 000010 \\ 010000 \\ 100000 \end{pmatrix} \right\rangle$	110

Table 8.14 Linear code for $q = 7$ and $k = 4$ with generator matrix

$$\Gamma := \begin{pmatrix} 0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&1&2&3&3&6&0&0&2&4&4&6&0&2&4&5&5&6&1&1&2&5&5&6&2 \\ 0&3&6&5&0&6&0&1&2&2&1&5&6&4&4&6&1&5&2&4&5&3&3&6&4&6 \\ 1&6&1&5&6&2&1&4&1&2&4&4&5&4&6&1&1&5&1&2&6&6&4&1&4&0 \end{pmatrix}$$

n	d	G	r
26	**20**	$\left\langle \begin{pmatrix} 0010 \\ 1030 \\ 0110 \\ 0001 \end{pmatrix} \right\rangle$	74

Table 8.15 Linear codes for $q = 7$ and $k = 5$

n	d	G	r
28	20	$\left\langle \begin{pmatrix} 00100 \\ 00010 \\ 10000 \\ 01000 \\ 00001 \end{pmatrix}, \begin{pmatrix} 10000 \\ 03000 \\ 00300 \\ 00060 \\ 00002 \end{pmatrix} \right\rangle$	147
34	25	$\left\langle \begin{pmatrix} 53000 \\ 25000 \\ 00300 \\ 00001 \\ 00050 \end{pmatrix} \right\rangle$	189
48	36	$\left\langle \begin{pmatrix} 66240 \\ 44440 \\ 46200 \\ 10450 \\ 00001 \end{pmatrix} \right\rangle$	131

Table 8.16 Linear codes for $q = 8$ and $k = 4$

n	d	G	r
85	**72**	$\langle \begin{pmatrix} 0010 \\ 1070 \\ 0170 \\ 0001 \end{pmatrix} \rangle$	73
97	82	$\langle \begin{pmatrix} 0010 \\ 1000 \\ 0100 \\ 0001 \end{pmatrix}, \begin{pmatrix} 0001 \\ 1000 \\ 0010 \\ 0100 \end{pmatrix} \rangle$	57
103	**88**	$\langle \begin{pmatrix} 0010 \\ 1000 \\ 0100 \\ 0001 \end{pmatrix}, \begin{pmatrix} 0001 \\ 1000 \\ 0010 \\ 0100 \end{pmatrix} \rangle$	57
108	92	$\langle \begin{pmatrix} 0010 \\ 1000 \\ 0100 \\ 0001 \end{pmatrix}, \begin{pmatrix} 0001 \\ 1000 \\ 0010 \\ 0100 \end{pmatrix} \rangle$	57
117	**100**	$\langle \begin{pmatrix} 0571 \\ 3403 \\ 2247 \\ 1361 \end{pmatrix} \rangle$	45

Table 8.17 Linear codes for $q = 8$ and $k = 5$

n	d	G	r
79	63	$\langle \begin{pmatrix} 00010 \\ 10010 \\ 01040 \\ 00160 \\ 00001 \end{pmatrix} \rangle$	121
98	80	$\langle \begin{pmatrix} 10000 \\ 00100 \\ 01000 \\ 00001 \\ 00010 \end{pmatrix}, \begin{pmatrix} 20000 \\ 03000 \\ 00400 \\ 00030 \\ 00002 \end{pmatrix} \rangle$	61
100	81	$\langle \begin{pmatrix} 10000 \\ 00100 \\ 01000 \\ 00001 \\ 00010 \end{pmatrix}, \begin{pmatrix} 20000 \\ 03000 \\ 00400 \\ 00030 \\ 00002 \end{pmatrix} \rangle$	61
103	84	$\langle \begin{pmatrix} 10000 \\ 00100 \\ 01000 \\ 00001 \\ 00010 \end{pmatrix}, \begin{pmatrix} 20000 \\ 03000 \\ 00400 \\ 00030 \\ 00002 \end{pmatrix} \rangle$	61
119	98	$\langle \begin{pmatrix} 00010 \\ 10010 \\ 01040 \\ 00160 \\ 00001 \end{pmatrix} \rangle$	121
130	107	$\langle \begin{pmatrix} 42000 \\ 56000 \\ 00120 \\ 00140 \\ 00007 \end{pmatrix} \rangle$	81

Table 8.18 Linear code for $q = 9$ and $k = 3$ with generator matrix

$$\Gamma := \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 2 & 2 & 5 & 7 & 5 & 7 & 5 & 7 & 6 & 8 \\ 1 & 1 & 6 & 6 & 5 & 7 & 8 & 5 & 7 & 0 & 0 & 1 & 7 & 8 & 6 & 1 & 8 \end{pmatrix}$$

n	d	G	r
17	**14**	$\langle \begin{pmatrix} 010 \\ 100 \\ 001 \end{pmatrix} \rangle$	51

Table 8.19 Linear codes for $q = 9$ and $k = 4$

n	d	G	r
41	34	$\langle \begin{pmatrix} 8418 \\ 5878 \\ 7312 \\ 0215 \end{pmatrix} \rangle$	20
102	88	$\langle \begin{pmatrix} 1600 \\ 8600 \\ 0006 \\ 0050 \end{pmatrix} \rangle$	46
123	106	$\langle \begin{pmatrix} 0001 \\ 1002 \\ 0100 \\ 0017 \end{pmatrix} \rangle$	20
130	112	$\langle \begin{pmatrix} 0600 \\ 3710 \\ 4130 \\ 0001 \end{pmatrix} \rangle$	50