University of Bayreuth
Department of Mathematics

Advanced and current topics in coding theory

apl. Prof. Dr. Sascha Kurz

Winter term 2020/21

—

The present (partial) lecture notes will emerge parallel to the corresponding lecture “Advanced and current topics in coding theory”. If you find any typos or inaccuracies please let me know at sascha.kurz@uni-bayreuth.de.

Bayreuth, 20th December 2020
Sascha Kurz

Table of contents

1. Preliminaries

Let $\mathbb{F}_q^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_q$. The support $\operatorname{supp}(\mathbf{x})$ of a vector $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ is the set of indices of the non-zero coordinates, i.e.,

$$\operatorname{supp}(\mathbf{x}) := \{1 \le i \le n \,:\, x_i \neq 0\}\,, \tag{1.1}$$

where 0 denotes the zero element in $\mathbb{F}_q$. The (Hamming) weight $\operatorname{wt}(\mathbf{x})$ of $\mathbf{x}$ is the cardinality of its support, i.e.,

$$\operatorname{wt}(\mathbf{x}) := \#\operatorname{supp}(\mathbf{x}). \tag{1.2}$$

With this, the Hamming distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q$ is given by

$$d(\mathbf{x}, \mathbf{y}) := \operatorname{wt}(\mathbf{x} - \mathbf{y}). \tag{1.3}$$

The function $d\colon \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}$ indeed defines a metric on $\mathbb{F}_q^n$ and the corresponding metric space is called the q-ary n-dimensional Hamming space. A q-ary code of length n is a non-empty subset $\mathcal{C} \subseteq \mathbb{F}_q^n$. Elements of a code $\mathcal{C}$ are also called codewords. By $\operatorname{supp}(\mathcal{C}) := \cup_{c \in \mathcal{C}} \operatorname{supp}(c)$ we denote the support of a code $\mathcal{C}$, whose cardinality $\#\operatorname{supp}(\mathcal{C})$ is the effective length n_{eff}. If $n_{\text{eff}} = n$, then $\mathcal{C}$ is called spanning. By $d(\mathcal{C})$ we denote the minimum distance of $\mathcal{C}$, i.e.,

$$d(\mathcal{C}) := \min\{d(\mathbf{x}, \mathbf{y}) \,:\, \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}\,, \tag{1.4}$$

where we set $d(\mathcal{C}) = \infty$ whenever $\#\mathcal{C} = 1$. The code $\mathcal{C}$ is called additive if it is closed under addition and linear if $\mathcal{C}$ is a linear subspace of the vector space $\mathbb{F}_q^n$. Note that a linear code $\mathcal{C}$ contains the all-zero vector $\mathbf{0} \in \mathbb{F}_q^n$ and the minimum distance $d(\mathcal{C})$ equals the minimum Hamming weight $\operatorname{wt}(\mathbf{x})$ of the non-zero vectors $\mathbf{x} \in \mathcal{C}\backslash\{\mathbf{0}\}$. Each k-dimensional linear code over $\mathbb{F}_q$, i.e., each q-ary linear code, contains exactly q^k codewords. Since we will mostly consider linear codes, we call a k-dimensional linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with minimum distance d an $[n, k, d]_q$-code. For small values of q we also speak of binary, ternary, and quaternary codes, referring to 2-ary, 3-ary, and 4-ary codes, respectively. If the minimum distance d is irrelevant, we speak of an $[n, k]_q$-code. If we only know that an $[n, k]_q$-code $\mathcal{C}$ has minimum distance at least d, we denote the situation by $[n, k, \ge d]_q$. Similar notations are used for the other parameters.

Given a basis $\mathbf{g}^1, \dots, \mathbf{g}^k \in \mathbb{F}_q^n$ of an $[n, k]_q$-code $\mathcal{C}$ we call the matrix

$$G = \begin{pmatrix} \mathbf{g}^1 \\ \vdots \\ \mathbf{g}^k \end{pmatrix} = \begin{pmatrix} g_1^1 & g_2^1 & \dots & g_n^1 \\ \vdots & \vdots & \ddots & \vdots \\ g_1^k & g_2^k & \dots & g_n^k \end{pmatrix}$$

a generator matrix of $\mathcal{C}$, where $\mathbf{g}^i = \left(g_1^i, \dots, g_n^i\right) \in \mathbb{F}_q^n$ for all $1 \le i \le k$. An example of an $[8, 4]_2$-code $\mathcal{C}$

is given by the generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{1.5}$$

The number of different ordered bases $\left(g^1,\dots,g^n\right)$ of an $[n,k]_q$-code $\mathcal{C}$ can be counted easily. For the codeword $g^1 \in \mathcal{C}$ we have $\#C - 1 = q^k - 1$ choices since $g^1 \neq \mathbf{0}$. Since the vectors have to be linearly independent we have

$$\#\mathcal{C} - \#\left\langle g^1, \dots g^{i-1}\right\rangle_q = q^k - q^{i-1}$$

choices for g^i, where

$$\left\langle \mathbf{x}^1,\dots,\mathbf{x}^k \right\rangle_q := \left\{ \sum_{i=1}^{k} a_i \mathbf{x}^i \,:\, a_1,\dots,a_k \in \mathbb{F}_q \right\} \tag{1.6}$$

denotes the $\mathbb{F}_q$-span of the vectors $\mathbf{x}^1,\dots,\mathbf{x}^k \in \mathbb{F}_q^n$. Thus, there are

$$\prod_{i=0}^{k-1}\left(q^k - q^i\right) = q^{k(k-1)/2} \cdot \prod_{i=1}^{k}\left(q^i - 1\right) = (q-1)^k q^{\binom{k}{2}} \cdot \prod_{i=1}^{k} \frac{q^i - 1}{q-1} = (q-1)^k q^{\binom{k}{2}} \cdot [k]_q! \tag{1.7}$$

different bases of generator matrices for $\mathcal{C}$, where $[x]_q := \left(q^x - 1\right)/(q-1)$ for integral $x \geq 0$, $q > 1$ and $[x]_q! := \prod_{i=1}^{x} [i]_q = \prod_{i=1}^{x}\left(q^i - 1\right)/(q-1)$.

Applying any sequence of row operations of the Gaussian elimination algorithm to G gives another generator matrix of G. For our example the Gaussian elimination algorithm gives the generator matrix

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

Let $\operatorname{Aut}\left(\mathbb{F}_q^n\right)$ be the group of semilinear transformations of $\mathbb{F}_q^n$ that leave the Hamming distance invariant. For each transformation $\mu \in \operatorname{Aut}\left(F_q^n\right)$ we can find a permutation π of the set $\{1,\dots,n\}$, non-zero field elements $a_i \in \mathbb{F}_q \backslash \{0\}$, where $1 \leq i \leq n$, and a field automorphism α of $\mathbb{F}_q$ such that

$$\mu((x_1,\dots,x_n)) = \left(\alpha\left(a_1 x_{\pi(1)}\right), \alpha\left(a_2 x_{\pi(2)}\right), \dots, \alpha\left(a_n x_{\pi(n)}\right)\right) \tag{1.8}$$

for all $(x_1,\dots,x_n) \in \mathbb{F}_q^n$. Two codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^n$ are said to be equivalent or isomorphic if a transformation $\mu \in \operatorname{Aut}\left(F_q^n\right)$ exists such that $\mu(\mathcal{C}) = \mathcal{C}'$. The automorphism group $\operatorname{Aut}(\mathcal{C})$ of a code $C \subseteq \mathbb{F}_q^n$ is the group

$$\operatorname{Aut}(\mathcal{C}) := \left\{\mu \in \operatorname{Aut}\left(\mathbb{F}_q^n\right) \,:\, \mu(\mathcal{C}) = \mathcal{C}\right\}. \tag{1.9}$$

Note that for the binary field we only have to consider permutations of the set $\{1,\dots,n\}$ of coordinate positions. So, by applying row operations and column permutations we can conclude that for each $[n,k]_q$-code $\mathcal{C}$ there exists a generator matrix G of an equivalent code $\mathcal{C}'$ with generator matrix G' whose leftmost part is a $k \times k$ unit-matrix I_k. Such a matrix G' is called systematic generator matrix. In our example, generated by the matrix in Equation (1.5), a systematic generator matrix is given by

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}. \tag{1.10}$$

The orthogonal

$$\mathcal{C}^\perp := \left\{ \mathbf{y} \in \mathbb{F}_q^n \,:\, \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in \mathcal{C} \right\} \tag{1.11}$$

of an $[n,k]_q$-code $\mathcal{C}$, with respect to the standard inner product

$$\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{i=1}^{n} x_i y_i \tag{1.12}$$

is called the dual code of $\mathcal{C}$. Note that $\mathcal{C}^\perp$ is an $[n, n-k]_q$-code and $\operatorname{Aut}(\mathcal{C}) = \operatorname{Aut}\big(\mathcal{C}^\perp\big)$ since $\langle \mu(\mathbf{x}), \mathbf{y} \rangle = \big\langle \mathbf{x}, \mu^{-1}(\mathbf{y}) \big\rangle$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ and all $\mu \in \operatorname{Aut}\big(\mathbb{F}_q^n\big)$. If $\mathcal{C} \subseteq \mathcal{C}^\perp$, then $\mathcal{C}$ is called self-orthogonal and self-dual if $\mathcal{C} = \mathcal{C}^\perp$. We call an $[n,k]_q$-code Δ-divisible if the weights of the codewords all are divisible by Δ. For $(\Delta, q) = (2,2)$, $(4,2)$, and $(8,2)$, those codes are also called even, doubly-even, and triply-even, respectively. Note that doubly-even codes are self-orthogonal. If the weights of the non-zero codewords are contained in a set $\mathcal{W} \subseteq \mathbb{N}$ of admissible weights, we speak of an $[n,k,\mathcal{W}]_q$-code. The dual minimum distance $d^\perp$ is the minimum distance of the dual code. We call a code projective iff $d^\perp \geq 3$.

Let $\mathcal{C}$ be an $[n,k]_q$-code. By $A_w(\mathcal{C}) \in \mathbb{N}_0$ we denote the number of codewords of weight w in $\mathcal{C}$, where $0 \leq w \leq n$. The sequence of all weights can be summarized in the homogeneous weight enumerator

$$\overline{W}_{\mathcal{C}}(x,y) = \sum_{w=0}^{n} A_w(\mathcal{C}) x^w y^{n-w} \tag{1.13}$$

of $\mathcal{C}$. Setting $y = 1$ we obtain the weight enumerator

$$W_{\mathcal{C}}(x) = \sum_{w=0}^{n} A_w(\mathcal{C}) x^w. \tag{1.14}$$

The homogeneous weight enumerator $\overline{W}_{\mathcal{C}}(x,y)$ and the homogeneous weight enumerator $\overline{W}_{\mathcal{C}^\perp}(x,y)$ of its dual are related by the so-called MacWilliams identity [127]

$$\overline{W}_{\mathcal{C}^\perp}(x,y) = |\mathcal{C}|^{-1} \cdot \overline{W}_{\mathcal{C}}(y-x, y+(q-1)x). \tag{1.15}$$

For the (non-homogeneous) weight enumerators we similarly have

$$W_{\mathcal{C}^\perp}(x) = |\mathcal{C}|^{-1} \cdot W_{\mathcal{C}}(1-x, 1+(q-1)x), \tag{1.16}$$

c.f. [126, Theorem 2.8]. So given the complete weight distribution (A_i) of $\mathcal{C}$, the weight distribution (B_i), where $B_i(\mathcal{C}) = A_i(\mathcal{C}^\perp) \in \mathbb{N}_0$, of the dual code $\mathcal{C}^\perp$ is uniquely determined. We also say that it arises by the MacWilliams transform. A non-polynomial variant is stated in Section 1.4.

We are in particular interested in optimizing the possible parameters of $[n,k,d]_q$-codes. To this end we denote by

- $n_q(k,d) := \min\{n : \text{an } [n,k,d]_q\text{-code exists}\}$ the minimum possible length;
- $k_q(n,d) := \max\{k : \text{an } [n,k,d]_q\text{-code exists}\}$ the maximum possible dimension;
- $d_q(n,k) := \max\{d : \text{an } [n,k,d]_q\text{-code exists}\}$ the maximum possible minimum distance.

We say that an $[n,k,d]_q$-code is length-optimal if no $[n-1,k,d]_q$-code exists, dimension-optimal if not $[n,k+1,d]_q$-code exists, and distance-optimal if no $[n,k,d+1]_q$-code exists.

EXERCISE 1.1 Determine the automorphism group of the linear $[8,4]_2$ code with generator matrix G' given by Equation (1.10).

1.1 Finite fields

If p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements. Up to isomorphism it is the unique field with p elements, so that we will write $\mathbb{F}_p$ in the following. To ease the notation we will denote the elements of $\mathbb{F}_p$ by $\{0,1,\dots,p-1\}$. With this, the addition is given by $(a+b) \mod p$ and the multiplication by $(a \cdot b) \mod p$, where we compute over the integers and reduce modulo p, i.e., $a \mod p$ is the unique integer b in $\{0,1,\dots,p-1\}$ with $a \equiv b \pmod p$. For a general finite field $\mathbb{F}_q$ of order q we denote the neutral element of the addition by 0 and the neutral element of the multiplication by 1. Note that we have $0 \neq 1$. The smallest positive number m of 1s summing to 0 is called the characteristic of the field. It can be easily seen that the characteristic is always a prime number p, see Exercise 1.2. The one-element 1 generates a subfield that is isomorphic to $\mathbb{F}_p$ and we use the corresponding notation for the elements. With this, we can consider $\mathbb{F}_q$ as a $\mathbb{F}_p$-vector space which shows that $q = p^r$ for some suitable integer r. Given an irreducible polynomial f of degree r over $\mathbb{F}_p$ we have $\mathbb{F}_q \cong \mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$. Instead of dealing with residue classes we use the polynomial in $\mathbb{F}_p[x]$ with degree strictly less than r as representants. With this, the addition and the multiplication of two elements $a,b \in \mathbb{F}_p[x]$ with degree less than r is given by $(a+b) \mod f(x)$ and by $(a \cdot b) \mod f(x)$, respectively, where $c \mod f(x)$ is the unique polynomial c' with degree less than r that satisfies $c' \equiv c \pmod{f(x)}$ for arbitrary $c \in \mathbb{F}_p[x]$. So, we need an irreducible polynomial, i.e., a polynomial that cannot be written as a product of two polynomials of strictly smaller degree. For $q=2$ and $r=2$ we may simply check all binary polynomials of degree two. Since $x^2 = x \cdot x$, $x^2+1 = (x+1)(x+1)$, and $x^2+x = x(x+1)$ over $\mathbb{F}_2$, the only possibility is $f(x) = x^2+x+1$. In general there are several irreducible polynomials and a standard representation is obtained by choosing the so-called Conway polynomial. These are e.g. given by x^3+x+1 for $q=8$, x^4+x+1 for $q=16$, and x^2+2x+2 for $q=9$. As a finite field with $q=p^r$ elements is also unique up to isomorphism, we will just write $\mathbb{F}_q$ in the following.

EXERCISE 1.2 Show that the characteristic of a finite field is a prime number.

1.2 The geometric description of linear codes

The aim of this section is to describe linear codes from a geometric point of view. To this end, let $V \simeq \mathbb{F}_q^v$ be a v-dimensional vector space over the finite field $\mathbb{F}_q$. We call each i-dimensional linear subspace of V an

i-space, using the geometric terms points, lines, planes, and hyperplanes for 1-, 2-, 3-, and $(v-1)$-spaces, respectively. A $(v-j)$-space is also called a space of codimension j, where $0 \le j \le v$. In the special case of a space of codimension 2, i.e., a $(v-2)$-space, we also speak of hyperlines. The motivation for this geometric language is that any two different points are on precisely on one common line, which is a familiar axiom in the geometry. The truth of the previous statement follows from the fact that two different 1-dimensional subspaces generate a unique 2-dimensional subspace. Observe the shift in dimension, i.e., we view 1-spaces as points, which are 0-dimensional geometric objects, 2-spaces as lines, which are 1-dimensional geometric objects, and in general i-spaces as $(i-1)$-dimensional geometric objects, where $1 \le i \le k$. Here we will always use the algebraic dimension i and not the geometric dimension $i-1$. The only exception is the notion of the $(v-1)$-dimensional projective geometry $\operatorname{PG}(v-1,q)$ associated with $\mathbb{F}_q^v$. There are $v-1$ types of geometric objects ranging from points (1-spaces) to hyperplanes $(v-1)$-spaces. By $\mathcal{P}$ we denote the set of points and by $\mathcal{H}$ we denote the set of hyperplanes whenever the dimension v of the ambient space and the field size q are clear from the context. Each point $P \in \mathcal{P}$ can be written as a 1-space

$$P = \left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_v \end{pmatrix} \right\rangle_q ,$$

where $(x_1,\dots,x_v) \in \mathbb{F}_q^v$, or using projective coordinates $(x_1 : x_2 : \dots : x_v)$, where $(tx_1 : tx_2 : \dots : tx_v) = (x_1 : x_2 : \dots : x_v)$ for all $t \in \mathbb{F}_q \backslash \{0\}$. Since the dual of a $(v-1)$-space is a 1-space, we have similar notations for hyperplanes.

In general we denote by $\begin{bmatrix} V \\ k \end{bmatrix}$ the set of k-spaces in V and by $\begin{bmatrix} v \\ k \end{bmatrix}_q$ their cardinality $\#\begin{bmatrix} V \\ k \end{bmatrix}$. For integers $0 \le k \le v$ we have, see Exercise 1.3,

$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{v-i}-1}{q^{k-i}-1}. \tag{1.17}$$

For other values of k we set $\begin{bmatrix} v \\ k \end{bmatrix}_q = 0$ by convention. Using the notation $[v]_q := \frac{q^v-1}{q-1}$ and $[v]_q! := \prod_{i=1}^{v} [i]_q$ we can write

$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \frac{[v]_q!}{[k]_q! \cdot [v-k]_q!}. \tag{1.18}$$

The numbers $\begin{bmatrix} v \\ k \end{bmatrix}_q$ are also called q-binomial coefficients. Counting the number of k-spaces contained in a v-space they are a q-analogon of the binomial coefficients $\binom{v}{k}$ which count the number of k-sets contained in a v-set, where a t-set is a set of cardinality t. An important special case of Equation (1.17) is given by

$$\#\mathcal{P} = \begin{bmatrix} v \\ 1 \end{bmatrix}_q = \begin{bmatrix} v \\ v-1 \end{bmatrix}_q = \#\mathcal{H} = \frac{q^v-1}{q-1} = [v]_q. \tag{1.19}$$

Note that duality implies

$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \begin{bmatrix} v \\ v-k \end{bmatrix}_q \tag{1.20}$$

in general.

For a fixed hyperplane $H \in \mathcal{H}$ of $\operatorname{PG}(v-1,q)$ the points outside H are called affine points (with respect to H). These $[v]_q - [v-1]_q = q^{v-1}$ points form the $(k-1)$-dimensional[1] affine geometry $\operatorname{AG}(v-1,q)$.

[1] Warning: Again we use the geometric dimension.

Now let us describe the main correspondence between $[n,k]_q$-codes $\mathcal{C}$ with effective length n and (spanning) multisets $\mathcal{M}$ of points in $\operatorname{PG}(k-1,q)$. Given a generator matrix G of $\mathcal{C}$ without zero columns (note the condition on the effective length) we can construct a multiset of points $P_1,\dots,P_n$ in $\operatorname{PG}(k-1,q)$ by assigning to each column $x \in \mathbb{F}_q^k$ of G the point $\langle x\rangle_q \in \mathcal{P}$. In the other direction we can use a generator $x \in \mathbb{F}_q^k \backslash \{\mathbf{0}\}$ of a point $\langle x\rangle_q$ of the multiset as a column of a generator matrix G of $\mathcal{C}$. In order to be rigorous, we write each multiset of points in $\operatorname{PG}(k-1,q)$ as a mapping $\mathcal{M}\colon \mathcal{P} \to \mathbb{N}_0$. This mapping is extended additively to the subsets $\mathcal{Q}$ of $\mathcal{P}$ by $\mathcal{M}(\mathcal{Q}) = \sum_{P\in\mathcal{Q}} \mathcal{M}(P)$. The integer $n := \mathcal{M}(\mathcal{P}) = \sum_{P\in\mathcal{P}} \mathcal{M}(P)$ is called the cardinality of $\mathcal{M}$. We call the non-negative integer $\mathcal{M}(P)$ the multiplicity of the point $P \in \mathcal{P}$, a notion that is also extended to arbitrary subsets $\mathcal{Q}$ of $\mathcal{P}$. For i-spaces $\mathcal{Q}$ of multiplicity m we speak of m-points, m-lines, m-planes, and m-hyperplanes in the case of $i=1$, $i=2$, $i=3$, and $i=k-1$, respectively. The support $\operatorname{supp}(\mathcal{M})$ of a multiset of points $\mathcal{M}$ is the set of points of strictly positive multiplicity. We call $\mathcal{M}$ spanning if the 1-spaces in $\operatorname{supp}(\mathcal{M})$ span $\mathbb{F}_q^k$. In other words if no hyperplane has multiplicity $n = \#\mathcal{M}$.

The idea of the geometric description is to read off the code parameters from the multiset $\mathcal{M}$ of points in $\operatorname{PG}(k-1,q)$. The subsequent theorem shows how to determine the weight distribution of $\mathcal{C}$ from $\mathcal{M}$, see also Lemma 1.7. To this end, we observe that the codewords of $\mathcal{C}$ are the $\mathbb{F}_q$-linear combinations of the rows of a generator matrix G of $\mathcal{C}$. Let $\mathbf{g}^i = \left(g_1^i,\dots,g_n^i\right) \in \mathbb{F}_q^n$ denote the ith row of G, so that each codeword $\mathbf{c} \in \mathcal{C}$ has the form $\mathbf{c} = h_1 g^1 + h_2 g^2 + \cdots + h_k g^k$ and is uniquely determined by $\mathbf{h} = (h_1,\dots,h_k) \in \mathbb{F}_q^k$. For a fixed coordinate $1 \le j \le n$, indexed by the point P_j, when does $\mathbf{c}$ has entry 0 in coordinate j? Exactly if

$$c_j \;=\; h_1 g_j^1 + h_2 g_j^2 + \cdots + h_k g_j^k \;=\; 0. \tag{1.21}$$

The coefficients h_i, collected in $\mathbf{h}$, of this linear equation define a hyperplane $H \in \mathcal{H}$. In other words, we have $c_j = 0$ iff the point P_j is contained in hyperplane H. The above reasoning implies:

THEOREM 1.1 (Correspondence between linear codes and multisets of points)

Let $\mathcal{C}$ be an $[n,k]_q$-code, G be a generator matrix of $\mathcal{C}$ without zero columns, and $\mathcal{M}$ be the corresponding multiset of points in $\operatorname{PG}(k-1,q)$ (as described above). For each non-zero $\mathbf{h} = (h_1,\dots,h_k) \in \mathbb{F}_q^k \backslash \{\mathbf{0}\}$ let $\mathbf{h}^\perp$ be the hyperplane $H \in \mathcal{H}$, which consists of all $\mathbf{y} = (y_1,\dots,y_k)$ with $\langle \mathbf{h},\mathbf{y}\rangle = 0$. Then, the weight of the codeword $\mathbf{c} = \sum_{i=1}^k h_i g^i$ is given by

$$\operatorname{wt}(\mathbf{c}) = \sum_{P\in\mathcal{P}, P\notin H} \mathcal{M}(P) = \mathcal{M}(\mathcal{P}\backslash H) = n - \mathcal{M}(H). \tag{1.22}$$

The minimum Hamming distance is given by

$$d(\mathcal{C}) = \min\{\mathcal{M}(\mathcal{P}\backslash H) \;:\; H \in \mathcal{H}\} = n - \max\{\mathcal{M}(H) \;:\; H \in \mathcal{H}\}. \tag{1.23}$$

In other words, the weight $\operatorname{wt}(\mathbf{c})$ of a codeword $\mathbf{c} \in \mathcal{C}$ equals the number of points of $\mathcal{M}$ that is not contained in the hyperplane $H = \mathbf{h}^\perp$ associated to $\mathbf{c}$. We remark that if we start with a (non-empty) multiset $\mathcal{M}$ of points in $\operatorname{PG}(k-1,q)$, then the corresponding code $\mathcal{C}$ has dimension k iff $\mathcal{M}$ is spanning. The rank of the constructed matrix G would be strictly smaller than k otherwise.

As there are many generator matrices for a given linear code $\mathcal{C}$, we have several descriptions as multisets of points. Of course, we also cannot reconstruct an ordering of the columns of a generator matrix of $\mathcal{C}$ from $\mathcal{M}$.

With respect to $[n, \le k, d]_q$-codes, Equation (1.23) motivates the following geometric notion.

DEFINITION 1.2

A multiset $\mathcal{K}$ of points in $\operatorname{PG}(k-1,q)$ is an (n,s)-arc if

(a) $\mathcal{K}(\mathcal{P}) = n$,

(b) $\mathcal{K}(H) \le s$ for every hyperplane $H \in \mathcal{H}$, and

(c) there exists a hyperplane $H_0 \in \mathcal{H}$ with $\mathcal{K}(H_0) = s$.

We also speak of an $(n,s;k,q)$-arc.[2]

A maximal hyperplane in an (n,s)-arc is an s-hyperplane. Inverting the direction of the inequality in condition 1.2(b) gives a similar definition:

DEFINITION 1.3

A multiset $\mathcal{K}$ of points in $\operatorname{PG}(k-1,q)$ is an (n,s)-blocking set (or (n,s)-minihyper) if

(a) $\mathcal{K}(\mathcal{P}) = n$,

(b) $\mathcal{K}(H) \ge s$ for every hyperplane $H \in \mathcal{H}$, and

(c) there exists a hyperplane $H_0 \in \mathcal{H}$ with $\mathcal{K}(H_0) = s$.

We also speak of an $(n,s;k,q)$-blocking sets and $(n,s;k,q)$-minihypers.

A minimal hyperplane in an (n,s)-blocking set is an s-hyperplane.

The relation between the minimum distance d and s, which is called species by some authors, is $s = n - d$ or $d = n - s$. If we want that the dimension of the linear code equals k, then we have to assume that the arc is spanning. If $s \le n-1$, then the arc is spanning. In the other direction we have that a non-spanning arc contains a hyperplane H with $\mathcal{K}(H) = n$, i.e., all points are contained in a hyperplane. If we cannot guarantee condition (c) in Definition 1.2, then we speak of an $(n, \le s)$- or an $(n, \le s; k, q)$-arc.

[2] While the notation of an arc is a geometric one, we still use the algebraic dimension k – hoping that reduces the amount of typos and does not confuse the reader.

Definition 1.4

Let $\mathcal{K}$ be an $(n, \le s)$-arc in $\mathrm{PG}(k-1,q)$*. The spectrum of $\mathcal{K}$ is the vector $\mathbf{a} = (a_0, \ldots, a_s) \in \mathbb{N}_0^{s+1}$, where*

$$a_i = \#\left\{H \in \mathcal{H} \,:\, \mathcal{K}(H) = i\right\} \tag{1.24}$$

for $0 \le i \le s$.

Note that we can also uniquely define the spectrum by stating the values of a_i for all $0 \le i \le s$ where $a_i \neq 0$. The entries of the spectrum satisfy a set of constraints which are called standard equations:

Lemma 1.5

The spectrum $\mathbf{a} = (a_0, \ldots, a_s)$ of an $(n, \le s)$-arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$*, where $k \ge 2$, satisfies*

$$\sum_{i=0}^{s} a_i = [k]_q \tag{1.25}$$

$$\sum_{i=0}^{s} i a_i = n \cdot [k-1]_q \tag{1.26}$$

$$\sum_{i=0}^{s} \binom{i}{2} a_i = \binom{n}{2} \cdot [k-2]_q + q^{k-2} \cdot \sum_{i \ge 2} \binom{i}{2} \lambda_i, \tag{1.27}$$

where λ_j denotes the number of points $P \in \mathcal{P}$ with $\mathcal{K}(P) = j$ for all $j \in \mathbb{N}$.

Proof. By assumption the multiplicity of each hyperplane $H \in \mathcal{H}$ satisfies $0 \le \mathcal{K}(H) \le s$, so that the left-hand side of Equation (1.25) counts the number $\#\mathcal{H} = [k]_q$ of hyperplanes. Since every point is contained in $[k-1]_q$ hyperplanes, we have

$$n[k-1]_q = \sum_{P \in \mathcal{P}} \sum_{H \in \mathcal{H} \,:\, P \in H} \mathcal{K}(P) = \sum_{H \in \mathcal{H}} \sum_{P \in H} \mathcal{K}(P) = \sum_{H \in \mathcal{H}} \mathcal{K}(H) = \sum_{i=0}^{s} i a_i, \tag{1.28}$$

i.e., Equation (1.26). The right-hand side of Equation (1.27) can be rewritten as

$$\begin{aligned} & \binom{n}{2} \cdot [k-2]_q + q^{k-2} \cdot \sum_{i \ge 2} \binom{i}{2} \lambda_i \\ = \; & [k-2]_q \cdot \frac{\left(\sum_{P \in \mathcal{P}} \mathcal{K}(P)\right) \left(\sum_{P \in \mathcal{P}} \mathcal{K}(P) \; - \; 1\right)}{2} + q^{k-2} \cdot \sum_{P \in \mathcal{P}} \binom{\mathcal{K}(P)}{2} \\ = \; & \frac{[k-2]_q}{2} \cdot \sum_{P, P' \in \mathcal{P} \,:\, P \neq P'} \mathcal{K}(P) \cdot \mathcal{K}(P') + \left([k-2]_q + q^{k-2}\right) \cdot \sum_{P \in \mathcal{P}} \binom{\mathcal{K}(P)}{2}. \end{aligned}$$

Thus, we have

$$\binom{n}{2} \cdot [k-2]_q + q^{k-2} \cdot \sum_{i \ge 2} \binom{i}{2} \lambda_i = \frac{[k-2]_q}{2} \cdot \sum_{P, P' \in \mathcal{P} \,:\, P \neq P'} \mathcal{K}(P) \cdot \mathcal{K}(P') + [k-1]_q \cdot \sum_{P \in \mathcal{P}} \binom{\mathcal{K}(P)}{2}. \tag{1.29}$$

The left-hand side of Equation (1.27) can be rewritten as

$$\sum_{i=0}^{s} \binom{i}{2} a_i = \sum_{H\in\mathcal{H}} \binom{\mathcal{K}(H)}{2}. \tag{1.30}$$

For a specific hyperplane $H \in \mathcal{H}$ we have

$$\binom{\mathcal{K}(H)}{2} = \frac{\left(\sum\limits_{P\in H} \mathcal{K}(P)\right)\left(\sum\limits_{P\in H} \mathcal{K}(P)\; - \;1\right)}{2} = \frac{1}{2}\cdot \sum_{P,P'\in H\,:P\neq P'} \mathcal{K}(P)\cdot\mathcal{K}(P') + \sum_{P\in H}\binom{\mathcal{K}(P)}{2}. \tag{1.31}$$

Since each point P is contained in $[k-1]_q$ hyperplanes and each pair $\{P, P'\}$, where $P \neq P'$ is contained in $[k-2]_q$ hyperplanes (note that $\dim(\langle P, P'\rangle) = 2$), we conclude

$$\sum_{i=0}^{s} \binom{i}{2} a_i = \frac{[k-2]_q}{2}\cdot \sum_{P,P'\in\mathcal{P}\,:P\neq P'} \mathcal{K}(P)\cdot\mathcal{K}(P') + [k-1]_q \sum_{P\in\mathcal{P}}\binom{\mathcal{K}(P)}{2}. \tag{1.32}$$

Plugging in Equation (1.29) yields Equation (1.27). □

REMARK 1.6 While the proof of Lemma 1.5 looks a bit technical, the underlying idea is pretty simple. To this end we write $\mathcal{K}$ as a list of points $(P_1, \ldots, P_n) \in \mathcal{P}^n$, where repetitions are allowed and the order of the points $P_i \in \mathcal{P}$ plays no role. With this, the equations (1.25)-(1.27) just arise by double-counting the incidences of the tuples (H), (P', H), and $(\{P, P'\}, H)$, respectively, where H is a hyperplane and $P \neq P'$ are points of $\mathcal{K}$.

From Equation (1.22) and the fact that $\mathbf{c}$ and $\alpha\mathbf{c}$, where $\alpha \in \mathbb{F}_q\backslash\{0\}$, correspond the the same hyperplane, we directly conclude:

LEMMA 1.7

Let $\mathcal{K}$ be a spanning $(n, \le n)$-arc in $\mathrm{PG}(k-1, q)$ *and $\mathcal{C}$ it corresponding code. Then, we have*

$$A_i = (q-1)a_{n-i} \tag{1.33}$$

for all $1 \le i \le n$, $A_0 = 1$, and $a_n = 0$.

LEMMA 1.8

Let $\mathcal{K}$ be an $(n, \le n)$-arc in $\mathrm{PG}(k-1, q)$ *and $\mathcal{K}'$ be an isomorphic spanning $(n, \le n)$-arc in* $\mathrm{PG}(k'-1, q)$*, where k' is the dimension of the span of the points in $\mathcal{K}$. Then, we have*

$$a_n(\mathcal{K}) = [k-k']_q \tag{1.34}$$

and

$$a_i(\mathcal{K}) = q^{k-k'} \cdot a_i(\mathcal{K}') \tag{1.35}$$

for all $0 \le i < n$.

Proof. Let us denote the span of the points of $\mathcal{K}$ by H', so that $\dim(H') = k'$. Note that H' is contained in $[k-k']_q$ hyperplanes of $\mathrm{PG}(k-1,q)$, which gives Equation (1.34). Each hyperplane S of H' is contained in $[k-k'+1]_q$ hyperplanes of $\mathrm{PG}(k-1,q)$. Since $[k-k']_q$ of these contain H', Equation (1.35) follows from $[k-k'+1]_q - [k-k']_q = q^{k-k'}$. □

Some codes have very nice descriptions using the geometric language. Consider for example the multiset $\mathcal{M}$ in $\mathrm{PG}(k-1,q)$, where $k \geq 2$, defined by $\mathcal{M}(P) = 1$ for all $P \in \mathcal{P}$. It corresponds to the $\left[[k]_q, k, q^{k-1}\right]_q$ simplex code. The minimum distance follows from the fact that each hyperplane $H \in \mathcal{H}$ contains $[k-1]_q = \frac{q^{k-1}-1}{q-1}$ points from $\mathcal{P}$, so that $\mathcal{M}(\mathcal{P}\backslash\mathcal{H}) = [k]_q - [k-1]_q = q^{k-1}$.

Define the sum of two multisets $\mathcal{K}'$ and $\mathcal{K}''$ in the same geometry $\mathrm{PG}(k-1,q)$ by $(\mathcal{K}'+\mathcal{K}'')(P) = \mathcal{K}'(P) + \mathcal{K}''(P)$ for all points $P \in \mathcal{P}$. With the aid of so-called characteristic functions we can describe more sophisticated constructions in a compact manner. So, given a set of points $\mathcal{Q} \subseteq \mathcal{P}$, we denote by $\chi_{\mathcal{Q}}\colon \mathcal{P} \to \{0,1\}$ the characteristic function of $\mathcal{Q}$, i.e., $\chi_{\mathcal{Q}}(P) = 1$ if $P \in \mathcal{Q}$ and $\chi_{\mathcal{Q}}(P) = 0$ otherwise. If X is a j-space in $\mathrm{PG}(k-1,q)$, where $1 \leq j \leq k$, then we write χ_X for the characteristic function of the points contained in X.

Lemma 1.9

Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_l \subseteq \mathcal{P}$ set of points and $m_1, \ldots, m_l \in \mathbb{Q}$. If

$$\sum_{i=1}^{l} m_i \mathcal{Q}_i(P) \in \mathbb{N}_0 \tag{1.36}$$

for each $P \in \mathcal{P}$, then

$$\mathcal{M} = m_1\mathcal{Q}_1 + m_2\mathcal{Q}_2 + \cdots + m_l\mathcal{Q}_l \tag{1.37}$$

defines a multiset of points in $\mathrm{PG}(k-1,q)$.

Example 1.10 Let H be a hyperplane in $V = \mathrm{PG}(k-1,q)$, where $k \geq 2$. Then $\mathcal{K} = \chi_V - \chi_H = \chi_{\mathcal{P}} - \chi_H$ is a $\left(q^{k-1}, q^{k-2}\right)$-arc that corresponds to a $\left[q^{k-1}, k, q^{k-1} - q^{k-2}\right]_q$-code. ◇

We remark that $\mathcal{K}$ is an affine geometry $\mathrm{AG}(k-1,q)$ and that the corresponding code is a first-order Reed-Muller code $\mathrm{RM}_q(k-1,1)$ of length q^{k-1}.

The multiset of points $\mathcal{K}\colon \mathcal{P} \to \mathbb{N}_0$ in $\mathrm{PG}(k-1,q)$ gives rise to a another multiset $\mathcal{K}^\perp\colon \mathcal{H} \to \mathbb{N}_0$, $H \mapsto \mathcal{K}(H)$. Since the domain is the set of hyperplanes instead of the set of points, we may also speak of a multiset of hyperplanes. The mapping $\mathcal{K}^\perp$ is also a multiset of points in the dual geometry $\mathrm{PG}^\perp(k-1,q)$ where the roles of points and hyperplanes are interchanged and the incidence relation is reversed. Note that $\mathrm{PG}^\perp(k-1,q) \cong \mathrm{PG}(k-1,q)$ via the map $F \mapsto F^\perp$, which assigns to every subspace F in $\mathrm{PG}(k-1,q)$ the orthogonal subspace with respect to the standard inner product $\langle \mathbf{x}, \mathbf{y} \rangle$.

$$\mathcal{K}(H) = \sum_{P \in H} \mathcal{K}(P) = \sum_{P \in \mathcal{P}} \mathcal{K}(P) \cdot \chi_H(P)$$

Also $\mathcal{K}(P)$ can be reconstructed from the $\mathcal{K}(H)$:

LEMMA 1.11

Let $\mathcal{K}$ be a multiset of points in $\operatorname{PG}(k-1,q)$*, where* $k \ge 2$*. Then, we have*

$$\mathcal{K}(P) = \sum_{H\in\mathcal{H}\,:\,P\in H} \frac{1}{[k-1]_q}\cdot\mathcal{K}(H) + \sum_{H\in\mathcal{H}\,:\,P\notin H} \frac{1}{q^{k-1}}\cdot\left(\frac{1}{[k-1]_q}-1\right)\cdot\mathcal{K}(H). \tag{1.38}$$

PROOF. Since each point $P' \in \mathcal{P}$ is contained in $[k-1]_q$ of the $\#\mathcal{H} = [k]_q$ hyperplanes and each point $P' \neq P$ is contained in $[k-2]_q$ of the $[k-1]_q$ hyperplanes that contain P, we have

$$\sum_{H\in\mathcal{H}\,:\,P\in H} \mathcal{K}(H) = [k-2]_q\cdot|\mathcal{K}| + \left([k-1]_q-[k-2]_q\right)\mathcal{K}(P) = [k-2]_q\cdot|\mathcal{K}| + q^{k-2}\mathcal{K}(P)$$

so that

$$\sum_{H\in\mathcal{H}\,:\,P\in H} \mathcal{K}(H) - \frac{[k-2]_q}{[k-1]_q}\cdot\sum_{H\in\mathcal{H}}\mathcal{K}(H) = q^{k-2}\mathcal{K}(P)$$

using $[k-1]_q|\mathcal{K}| = \sum_{H\in\mathcal{H}}\mathcal{K}(H)$. Thus, we can conclude the stated formula using

$$\frac{1}{q^{k-2}}\cdot\left(1-\frac{[k-2]_q}{[k-1]_q}\right) = \frac{1}{q^{k-2}}\cdot\frac{[k-1]_q-[k-2]_q}{[k-1]_q} = \frac{1}{[k-1]_q}$$

and

$$-\frac{[k-2]_q}{[k-1]_q\cdot q^{k-2}} = \frac{1-[k-1]_q}{[k-1]_q\cdot q^{k-1}} = \frac{1}{q^{k-1}}\cdot\left(\frac{1}{[k-1]_q}-1\right).$$

□

Note that $\#\{H\in\mathcal{H} : P\in H\} = [k-1]_q$ and $\#\{H\in\mathcal{H} : P\notin H\} = q^{k-1}$. For $k=2$ points and hyperplanes are the same objects, so that interesting constructions arise for $k\ge 3$ only. A generalization of he notion of the dual arc has been introduced by Brouwer and van Eupen [29] for linear codes and formulated for multiarcs by Dodunekov and Simonis [43].

DEFINITION 1.12

Let $\mathcal{K}$ be an arc and σ be a function satisfying $\sigma(\mathcal{K}(H))\in\mathbb{N}_0$ for all hyperplanes $H\in\mathcal{H}$. The arc

$$\mathcal{K}^\sigma\colon \begin{cases} \mathcal{H}\to\mathbb{N}_0 \\ H\mapsto\sigma(\mathcal{K}(H)) \end{cases} \tag{1.39}$$

is called the σ-dual of $\mathcal{K}$.

Note that taking σ as the identity function on $\mathbb{N}_0$ gives the dual arc $\mathcal{K}^\perp$. If σ is linear, then the parameters of $\mathcal{K}^\sigma$ can be easily computed from the parameters of $\mathcal{K}$.

LEMMA 1.13

Let $\mathcal{K}$ be an $(n, \leq s)$-arc in $\mathrm{PG}(v-1, q)$*, where $v \geq 2$, $S_H = \{\mathcal{K}(H) : H \in \mathcal{H}\}$ be the set of attained hyperplane multiplicities and $S_P = \{\mathcal{K}(P) : P \in \mathcal{P}\}$ be the set of attained point multiplicities. For $\alpha, \beta \in \mathbb{Q}$ let $\sigma(x) = \alpha x + \beta$ be a linear function which only takes non-negative integer values for all $x \in S_H$. Then, we have $\#\mathcal{K}^\sigma = \alpha n[v-1]_q + \beta[v]_q$, the possible point multiplicities with respect to $\mathcal{K}^\sigma$ are given by $\{\alpha i + \beta : i \in S_H\}$ and the possible hyperplane multiplicities with respect to $\mathcal{K}^\sigma$ are given by $\left\{\alpha \cdot \left([v-2]_q n + q^{v-2} i\right) + \beta[v-1]_q : i \in S_P\right\}$.*

PROOF. From the first two standard equations, i.e. Equation (1.25) and Equation (1.26), for the spectrum (a_i) of $\mathcal{K}$

$$\sum_{i \in S_H} a_i = [v]_q \quad \text{and} \quad \sum_{i \in S_H} i a_i = \#\mathcal{K} \cdot [v-1]_q$$

we conclude

$$\#\mathcal{K}^\sigma = \sum_{i \in S_H} \sigma(i) a_i = \sum_{i \in S_H} (\alpha i + \beta) a_i = \alpha \cdot \#\mathcal{K} \cdot [v-1]_q + \beta[v]_q$$

and note that the possible point multiplicities with respect to $\mathcal{K}^\sigma$ are given by

$$\{\sigma(i) : i \in S_H\} = \{\alpha i + \beta : i \in S_H\}.$$

For an arbitrary point $P \in \mathcal{P}$ we have

$$\mathcal{K}^\sigma(P) = \sum_{H \in \mathcal{H} \,:\, P \in H} \mathcal{K}^\sigma(H) = \sum_{H \in \mathcal{H} \,:\, P \in H} \sigma(\mathcal{K}(H)) = \alpha \cdot \sum_{H \in \mathcal{H} \,:\, P \in H} \mathcal{K}(H) \; + \; \beta[v-1]_q.$$

Counting points gives

$$\sum_{H \in \mathcal{H} \,:\, P \in H} \mathcal{K}(H) = [v-2]_q \#\mathcal{K} + \left([v-1]_q - [v-2]_q\right) \mathcal{K}(P) = [v-2]_q \#\mathcal{K} + q^{v-2} \mathcal{K}(P),$$

so that the possible hyperplane multiplicities with respect to $\mathcal{K}^\sigma$ are given by

$$\left\{\alpha \cdot \left([v-2]_q n + q^{v-2} i\right) + \beta[v-1]_q : i \in S_P\right\}.$$

□

COROLLARY 1.14

Let $\mathcal{K}$ be an (n, s)-arc in $\mathrm{PG}(v-1, q)$ *and $\alpha, \beta \in \mathbb{Q}$ such that $\sigma(\mathcal{K}(H)) := \alpha \mathcal{K}(H) + \beta \in \mathbb{N}_0$ for all $H \in \mathcal{H}$. Then, $\mathcal{K}^\sigma$ is an (n', s')-arc in* $\mathrm{PG}(v-1, q)$*, where*

$$n' = \alpha n[v-1]_q + \beta[v]_q \tag{1.40}$$

and

$$s' = \max\left\{\alpha \cdot \left([v-2]_q n + q^{v-2} \mathcal{K}(P)\right) + \beta[v-1]_q : P \in \mathcal{P}\right\} \tag{1.41}$$

EXAMPLE 1.15 (Cf. [29]) Consider the unique projective $[16,5,9]_3$-code $\mathcal{C}$ constructed in [74] corresponding to a projective $(16,7)$-arc $\mathcal{K}$ in $\mathrm{PG}(4,3)$. Choosing $\alpha = -\frac{1}{3}$ and $\beta = \frac{7}{3}$ in Lemma 1.13 we obtain a $(69,24)$-arc in $\mathrm{PG}(4,3)$ with hyperplane multiplicities 24 or 15 that corresponds to a $[69,5,45]_3$-code $\mathcal{C}'$ with weight enumerator $W_{\mathcal{C}'}(x) = 1 + 210x^{45} + 32x^{54}$. Since the hyperplane multiplicities of the original arc are 7, 4, and 1 the point multiplicities in the $(69,24)$-arc corresponding to $\mathcal{C}'$ are 0, 1, and 2. If we want to directly map the non-zero weights 9, 12, and 15 of $\mathcal{C}$ to the column multiplicities 0, 1, and 2 of a generator matrix, then we have to replace the mapping $\sigma(x) = (7-x)/3$ by $\overline{\sigma}(x) = \frac{x}{3} - 3$. Note that both codes $\mathcal{C}$ and $\mathcal{C}'$ are distance optimal. With $\alpha = \frac{1}{3}$ and $\beta = -\frac{1}{3}$ we can also construct a $(173,65)$-arc in $\mathrm{PG}(4,3)$, that corresponds to a $[173,5,108]_3$-code, from $\mathcal{K}$. ◇

Let $\mathcal{K}$ be an (n,s)-arc in $\mathrm{PG}(v'-1,q)$ and U be an arbitrary but fixed u-subspace. For a v-space V in $\mathrm{PG}(v'-1,q)$ with $u+v=v'$ and $U \cap V = \emptyset$ we define the projection $\varphi = \varphi_{U,V}$ from U onto V by

$$\varphi_{U,V} \colon \mathcal{P} \backslash U \to V, P \mapsto V \cap \langle U, P \rangle, \tag{1.42}$$

where $\mathcal{P}$ is the point set of $\mathrm{PG}(v'-1,q)$. The induced arc $\mathcal{K}^\varphi$ is defined on the points of V by

$$\mathcal{K}^\varphi \colon \mathcal{P}(V) \to \mathbb{N}_0, P \mapsto \sum_{Q \in \mathcal{P}\backslash U \,:\, \varphi_{U,V}(Q) = P} \mathcal{K}(Q). \tag{1.43}$$

If S is some subspace in V, the $\mathcal{K}^\varphi(S) = \mathcal{K}(\langle\langle S, U \rangle) - \mathcal{K}(U)$. Clearly, $\mathcal{K}^\varphi$ is an $(n - \mathcal{K}(U), \leq s - \mathcal{K}(U))$-arc in $V \cong \mathrm{PG}(v-1,q)$. Similarly, if $\mathcal{K}$ is an (n,s)-blocking set, then $\mathcal{K}^\varphi$ is an $(n - \mathcal{K}(U), \leq s - \mathcal{K}(U))$-blocking set in V. Mostly we will choose V as a hyperplane and U as a point.

EXERCISE 1.3 Verify the equation for the q-binomial coefficient $\begin{bmatrix} v \\ k \end{bmatrix}_q$ in (1.17).

EXERCISE 1.4 Compute

$$\lim_{q \to 1} [i]_q = \lim_{q \to 1} \frac{q^i - 1}{q - 1}$$

for an integer $i \geq 1$.

EXERCISE 1.5 Compute the weight distribution of the code defined in Example 1.10.

EXERCISE 1.6 Let H and H' be two different hyperplanes in $\mathrm{PG}(k-1,q)$, where $k \geq 2$. Compute the weight distribution of the linear code corresponding to the arc $\mathcal{K} = 2\chi_{\mathcal{P}} - \chi_H - \chi_{H'}$.

EXERCISE 1.7 Construct a $(830,205)$-arc $\mathcal{K}$ in $\mathrm{PG}(4,5)$ such that every point has multiplicity at most 2.

EXERCISE 1.8 Let $\mathcal{K}$ be an $(n, \leq s)$-arc in $\mathrm{PG}(v-1,q)$, where $v \geq 3$, and $\sigma(x) = \alpha x + \beta$, where $\alpha, \beta \in \mathbb{Q}$. Determine $\alpha', \beta' \in \mathbb{Q}$ such that that $(\mathcal{K}^\sigma)^{\sigma'} = \mathcal{K}$ for $\sigma'(x) = \alpha' x + \beta'$.

1.3 Code constructions

In this section we summarize a few simple constructions of codes from given codes. To this end let $S := \{1, \ldots, n\}$ be the coordinate index set of $\mathbb{F}_q^n$. For the sake of rigor we identify $\mathbb{F}_q^n$ with $\mathbb{F}_q$-vector space $\mathbb{F}_q^S$

of the mappings $S \to \mathbb{F}_q$. If T is an m-subset of S, then $\mathbb{F}_q^T$, i.e., the $\mathbb{F}_q$-vector space of the mappings from $T \to \mathbb{F}_q$, can be identified with the subspace

$$\left(\mathbb{F}_q^n\right)^T := \left\{\mathbf{x} \in \mathbb{F}_q^n \,:\, \operatorname{supp}(\mathbf{x}) \subseteq T\right\} \subseteq \mathbb{F}_q^n.$$

Any bijection between T and $\{1, \dots, m\}$ induces an isomorphism between $\mathbb{F}_q^T$ and $\mathbb{F}_q^m$. Given a vector $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ and an m-set $T \subseteq S$, we denote by

$$x_T := (x_i)_{i \in T} \in \mathbb{F}_q^m \tag{1.44}$$

the restriction of $\mathbf{x}$ to T. More generally, for each subset $\mathcal{C}$ of $\mathbb{F}_q^n$ the restriction $\mathcal{C}_T$ of $\mathcal{C}$ to T is given by $\{\mathbf{x}_T \,:\, \mathbf{x} \in \mathcal{C}\}$. The utilized bijection between T and $\{1, \dots, m\}$ is not relevant in most applications as long as only one bijection is used for all restrictions that are combined somehow.

DEFINITION 1.16

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$, $T \subseteq \{1, \dots, n\} =: S$, and $\overline{T} := S \backslash T$.

(a) The restriction $\mathcal{C}_T$ of $\mathcal{C}$ to T is said to be obtained by puncturing $\mathcal{C}$ with respect to $\overline{T}$.

(b) The code $\mathcal{C}^T := \{\mathbf{c} \in \mathcal{C} : \operatorname{supp}(\mathbf{c}) \subseteq T\}_T$ is said to be obtained by shortening $\mathcal{C}$ with respect to $\overline{T}$.

Note that $\mathcal{C}_T$ and $\mathcal{C}^T$ both have length $n - m$. If $\mathcal{C}$ is linear so are $\mathcal{C}_T$ and $\mathcal{C}^T$. An easy implication of puncturing is that in an $[n, k, d]_q$-code both the length and the minimum distance can be decreased by 1 if $d \geq 2$.

LEMMA 1.17

If $d \geq 2$, then any $[n, k, d]_q$-code $\mathcal{C}$ gives an $[n-1, k, d-1]_q$-code by puncturing a suitable coordinate.

PROOF. Let $\mathbf{c}$ be a minimum weight codeword in $\mathcal{C}$. Puncturing any coordinate in $\operatorname{supp}(\mathbf{c})$ gives an $[n-1, \leq k, d-1]_q$-code. It remains to check that the dimension does not decrease if $d \geq 2$, see Exercise 1.9. □

Of special importance is the restriction to the complement of $\operatorname{supp}(\mathbf{c})$ for a codeword $\mathbf{c}$:

DEFINITION 1.18

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code, $\mathbf{c} \in \mathcal{C}$ a codeword of weight $\operatorname{wt}(\mathbf{c}) = w$, and $T = \{1 \leq i \leq n \,:\, c_i = 0\} = \{1, \dots, n\} \backslash \operatorname{supp}(\mathbf{c})$. With this, the residual code of $\mathcal{C}$ with respect to $\mathbf{c}$, denoted by $\operatorname{Res}(\mathcal{C}; \mathbf{c})$, is the restriction $\mathcal{C}_T$. If only the weight w of $\mathbf{c}$ is of importance we will denote it by $\operatorname{Res}(\mathcal{C}; w)$.

If $\mathcal{C}$ is an $[n,k]_q$-code with generator matrix G, then $\operatorname{Res}(\mathcal{C};\mathbf{c})$ is an $[n-w,\le k-1]_q$-code with generator matrix G' obtained from G by removing all columns i with $c_i \neq 0$. If $\mathcal{M}$ denotes the multiset of points in $\operatorname{PG}(k-1,q)$ corresponding to $\mathcal{C}$ and $H \in \mathcal{H}$ denotes the hyperplane corresponding to the codeword $\mathbf{c}$, then the residual code $\operatorname{Res}(\mathcal{C};\mathbf{c})$ corresponds to the multiset

$$\mathcal{M}|_H \colon H \to \mathbb{N}_0, P \mapsto \mathcal{M}(P). \tag{1.45}$$

Since $H \simeq \operatorname{PG}(k-2,q)$ we can identify $\mathcal{M}|_H$ with a multiset of points in $\operatorname{PG}(k-2,q)$. The dimension of $\operatorname{Res}(\mathcal{C};\mathbf{c})$ is $k-1$ iff $\mathcal{M}|_H$ is spanning.

Shortening e.g. implies the Singleton bound, see Theorem 1.31.

The inverse process of puncturing is called lengthening. Let $\mathcal{C}$ be an $[n,k,\ge d]_q$-code and $\varphi\colon \mathcal{C} \to \mathbb{F}_q^m$ be an arbitrary linear mapping. Then

$$\mathcal{C}' := \left\{ \left(\mathbf{c}, \varphi(\mathbf{c})\right) \,:\, \mathbf{c} \in \mathcal{C} \right\}, \tag{1.46}$$

is an $[n+m,k,\ge d]_q$-code. Setting $\varphi(\mathbf{c}) = \mathbf{0}$ for all $\mathbf{c} \in \mathcal{C}$ is called trivial lengthening, i.e., each $[n,k,d]_q$ code can be trivially lengthened to an $[n+m,k,d]_q$ code for each positive integer m. Note that minimum distance d does not change in this situation while it can increase in general. If we choose $\varphi(\mathcal{C})$ as an $[m,k \ge e]_q$-code $\mathcal{D}$, then the $[n+m,k,\ge d+e]_q$-code $\mathcal{C}'$ is called the juxtaposition of $\mathcal{C}$ and $\mathcal{D}$.

LEMMA 1.19

Let $\mathcal{C}$ be an $[n,k,d]_2$ code with odd minimum distance d. Then, there exists an even $[n+1,k,d+1]_2$-code $\mathcal{C}'$.

PROOF. Construct $\mathcal{C}'$ by lengthening with $\varphi\colon \mathcal{C} \to \mathbb{F}_2$, $(c_1,\dots,c_n) \mapsto \sum_{i=1}^n c_i$. □

The construction of the proof of Lemma 1.19 is also called adding a parity check bit.

Lemma 1.17 and Lemma 1.19 directly imply:

COROLLARY 1.20

$n_2(k,2e) = n_2(k,2e-1)+1$

LEMMA 1.21

Let $\mathcal{C}$ be an $[n,k,d]_2$ code with even minimum distance d. Then, there also exists an even $[n,k,d]_2$-code $\mathcal{C}'$.

PROOF. Construct $\mathcal{C}'$ by applying Lemma 1.17 and Lemma 1.19 afterwards, i.e., by puncturing and adding a parity check bit. □

LEMMA 1.22
Let $\mathcal{C}$ be an $[n, k, \geq d]_q$-code with dual minimum distance $d^\perp$. Then, there exists an $\left[n - d^\perp, k - d^\perp + 1, \geq d\right]_q$-code $\mathcal{C}'$.

PROOF. Let $G = \left(\mathbf{g}^1, \ldots, \mathbf{g}^n\right)$ be a generator matrix of $\mathcal{C}$, where $\mathbf{g}^i \in \mathbb{F}_q^k$ for all $1 \leq i \leq n$ are the columns. A dual codeword $c' \in \mathcal{C}^\perp$ satisfies

$$\mathbf{0} = \sum_{i=1}^{n} c'_i \mathbf{g}^i = \sum_{i \in \operatorname{supp}(c')} c'_i \mathbf{g}^i.$$

Now we assume that c' has minimum weight $\operatorname{wt}(c') = d^\perp$ and observe that for each proper subset $A \subsetneq \operatorname{supp}(c')$ we have $\sum_{i \in A} c'_i \mathbf{g}^i \neq \mathbf{0}$, i.e., those $d^\perp$ columns with indices in $\operatorname{supp}(c')$ have rank $d^\perp - 1$. Now we can choose suitable row operations to turn $d^\perp - 1$ of those columns into pivot columns. Removing the corresponding $d^\perp - 1$ rows and the all $d^\perp$ columns with indices in $\operatorname{supp}(c')$ gives a generator matrix G' of an $\left[n - d^\perp, k - \left(d^\perp - 1\right)\right]_q$-code $\mathcal{C}'$. Finally, observe that the minimum distance is not decreased by this operations. □

We remark that the construction in the proof of Lemma 1.22 is called Construction Y_1 by some authors.

Given known non-existence results for codes of smaller dimension a lower bound on the dual minimum distance $d^\perp$ can be concluded.

EXAMPLE 1.23 If an $[34, 9, 14]_2$-code exists, then it has dual minimum distance of at least 4, i.e., we have $B_1 = B_2 = B_3 = 0$. To this end, we have to observe that no $[33, 9, 14]_2$-code, no $[32, 8, 14]_2$-code, and no $[31, 7, 14]_2$-code exists. A $[30, 6, 14]_2$-code indeed exists. ◇

EXERCISE 1.9 Let $\mathcal{C}$ be an $[n, k, d]_q$ code and E be the union of the supports of the codewords of weight 1 in $\mathcal{C}$. Prove that puncturing $\mathcal{C}$ at any coordinate not in E gives an $[n-1, k, \geq d-1]_q$-code. (Note that we have $E = \{1, \ldots, n\}$ iff $k = n$.)

1.4 MacWilliams identities and the linear programming method

The polynomial MacWilliams identity, see Equation (1.14), can also be stated in a more explicit form. Given an $[n, k]_q$-code $\mathcal{C}$ we use the abbreviations $A_i = A_i(\mathcal{C})$ and $B_i = B_i(\mathcal{C}) = A_i(\mathcal{C}^\perp)$ for all $0 \leq i \leq n$. We have

$$\sum_{j=0}^{n-i} \binom{n-j}{i} A_j = q^{k-i} \cdot \sum_{j=0}^{i} \binom{n-j}{n-i} B_j \tag{1.47}$$

for all $0 \leq i \leq n$, see e.g. [126, Lemma 2.2]. If we restrict the range of i to $0 \leq i < t$, then we speak of the first t MacWilliams identities. Some authors, see e.g. [134], also call the equations (1.47) and the equivalent representation

$$\sum_{j=i}^{n} \binom{j}{i} A_j = q^{k-i} \sum_{j=0}^{i} (-1)^j B_j (q-1)^{i-j} \binom{n-j}{n-i}, \tag{1.48}$$

where $0 \le i \le n$, see e.g. [126, Lemma 2.9], binomial moments. Solving the equation system for the B_i gives:

THEOREM 1.24 (MacWilliams Equations) [127]

Let $\mathcal{C}$ be an $[n,k,d]_q$-code, $A_i(\mathcal{C})$ and $B_i(\mathcal{C})$ be the number of codewords of weight i in $\mathcal{C}$ and the dual code $\mathcal{C}^\perp$, respectively. Then, we have

$$\sum_{j=0}^{n} K_i(j) A_j(\mathcal{C}) = q^k B_i(\mathcal{C}) \tag{1.49}$$

for $0 \le i \le n$, where

$$K_i(j) := \sum_{s=0}^{i} (-1)^s \binom{n-j}{i-s} \binom{j}{s} (q-1)^{i-s} \tag{1.50}$$

are the Krawtchouck polynomials (here j is considered as variable of a polynomial).

For the binary case $q = 2$ we want to show another equivalent representation of the first 5 MacWilliams identities.

LEMMA 1.25

The weight distributions (A_i) and (B_i) of an $[n,k]_2$-code and its dual satisfy

$$\sum_{i=1}^{n} A_i = 2^k - 1 \tag{1.51}$$

$$\sum_{i=1}^{n} iA_i = 2^{k-1}(n - B_1) \tag{1.52}$$

$$\sum_{i=1}^{n} i^2 A_i = 2^{k-1}(B_2 - nB_1 + n(n+1)/2) \tag{1.53}$$

$$\sum_{i=1}^{n} i^3 A_i = 2^{k-2}\left(3(B_2 n - B_3) - (3n^2 + 3n - 2)/2 \cdot B_1 + n^2(n+3)/2\right) \tag{1.54}$$

$$\begin{aligned}\sum_{i=1}^{n} i^4 A_i = {} & 2^{k-4}\big(4!(B_4 - nB_3) + 4(3n^2+3n-4)B_2 - 4(n^3+3n^2-9n+7)B_1 \\ & + (n^4+6n^3+3n^2-2n)\big).\end{aligned} \tag{1.55}$$

These equations are a special case of the so-called power moments [134]. If we want to start the summations on the left-hand sides from $i = 0$, then the right-hand side of Equation (1.51) has to be replaced by 2^k, since

$A_0 = 1$. Note that the equations further simplify if we know that effective length equals n, i.e., $B_1 = 0$, or the code is known to be projective, i.e., $B_2 = 0$. In most applications we just specify a basis of t variables out of the A_i and B_i, and solve the first t MacWilliams identities for the basis variables. The A_i and B_i all have to be non-negative integers which can be utilized to exclude the existence of linear codes for some parameters. Actually, for $i \neq 0$ the A_i and B_i have to be integral multiples of $q-1$ since the non-zero codewords are partitioned into equivalence classes of size $q-1$ given by the non-zero codewords generated by such a codeword.

EXAMPLE 1.26 No 8-divisible projective $[52, 10]_2$-code exists since solving the first four MacWilliams identities for $\{A_8, A_{16}, A_{24}, A_{32}\}$ gives

$$\begin{aligned} A_8 &= 10 + A_{40} + 4A_{48} + \frac{1}{4}B_3 \\ A_{16} &= -28 - 4A_{40} - 15A_{48} - \frac{3}{4}B_3 \\ A_{24} &= 790 + 6A_{40} + 20A_{48} + \frac{3}{4}B_3 \\ A_{32} &= 251 - 4A_{40} - 10A_{48} - \frac{1}{4}B_3, \end{aligned}$$

so that $A_{16} \le -28 < 0$, which is a contradiction. ◇

In general we can determine lower and upper bounds for any linear combination of the A_i and B_i by using some subset of the MacWilliams identities (usually the first t equations) and linear programming taking $A_i, B_i \ge 0$ (and $A_0 = B_0 = 1$ or some additional constraints) into account. Adding integer rounding cuts sometimes gives tighter bounds.

EXAMPLE 1.27 In this example we want to show that each even $[13, 5, 6]_2$-code satisfies $B_1 = 0$, $B_2 = 0$, $2 \le B_3 \le 4$, $23 \le A_6 \le 24$, $3 \le A_8 \le 6$, $1 \le A_{10} \le 4$, and $0 \le A_{12} \le 1$. To this end we consider the following linear program based on the first 4 MacWilliams identities:

$$\begin{aligned} \max B_1 & \quad \text{subject to} \\ A_6 + A_8 + A_{10} + A_{12} + 16B_1 &= 31 \\ 6A_6 + 8A_8 + 10A_{10} + 12A_{12} &= 208 \\ 36A_6 + 64A_8 + 100A_{10} + 144A_{12} + 208B_1 - 16B_2 &= 1456 \\ 216A_6 + 512A_8 + 1000A_{10} + 1728A_{12} + 2176B_1 - 312B_2 + 24B_3 &= 10816. \end{aligned}$$

The (unique) optimal solution, computed with `Maple`, is given by

$$B_1 = \frac{3}{8}, B_2 = 0, B_3 = 0, A_6 = \frac{109}{4}, A_8 = 0, A_{10} = \frac{13}{4}, A_{12} = \frac{1}{2}$$

so that, in general, $B_1 \le \lfloor \frac{3}{8} \rfloor = 0$, i.e., we can assume $B_1 = 0$. With this additional equation, maximizing B_2, B_3, A_6, A_8, A_{10}, and A_{12} gives $B_2 \le \lfloor \frac{18}{17} \rfloor = 1$, $B_3 \le 4$, $A_6 \le \lfloor \frac{437}{17} \rfloor = 25$, $A_8 \le 6$, $A_{10} \le \lfloor \frac{11}{2} \rfloor = 5$, and $A_{12} \le \lfloor \frac{20}{13} \rfloor = 1$, respectively. Adding the tightened upper bounds, i.e., those for B_2, A_6, A_{10}, and A_{12}, maximizing B_2 again yields $B_2 \leq \left\lfloor \frac{6}{7} \right\rfloor = 0$, so that $B_2 = 0$. Another iteration yields $B_3 \leq 4$, $A_6 \leq 24$, $A_8 \leq 6$, $A_{10} \leq 4$, and $A_{12} \leq 1$. Similarly we obtain $B_3 \geq 2$, $A_6 \geq 23$, $A_8 \geq 3$, $A_{10} \geq 1$, and $A_{12} \geq 0$ by minimizing the variables. All these final lower and upper bounds for the variables can indeed by attained as shown by the integral solutions determined in Remark 1.28. ◇

REMARK 1.28 The non-negative integral solutions $(B_1, B_2, B_3, A_8, A_{10}, A_{12})$ of the first four MacWilliams identities of an even $[13, 5, 6]_2$-code are given by

$$(0, 0, 4, 24, 3, 4, 0) \text{ and } (0, 0, 2, 23, 6, 1, 1)\,.$$

To this end we solve the four equations for $\{B_3, A_6, A_8, A_{10}\}$:

$$\begin{aligned} B_3 &= 4 - 2A_{12} - 8B_1 - 3B_2 \\ A_6 &= 24 - A_{12} + 10B_1 + 2B_2 \\ A_8 &= 3 + 3A_{12} - 12B_1 - 4B_2 \\ A_{10} &= 4 - 3A_{12} + 2B_1 + 2B_2 \end{aligned}$$

From $B_3 \geq 0$ we conclude $B_1 = 0$ and $B_2 \in \{0, 1\}$. If $B_2 = 1$, then $B_3 \geq 0$ implies $A_{12} = 0$, so that $A_8 = -1 < 0$. Thus, we have $B_2 = 0$ and $A_{10} \geq 0$ implies $A_{12} \in \{0, 1\}$, which gives the two solutions stated above. The MacWilliams transforms of the corresponding weight distributions $(A_i)_i$ are given by

$$(B_i)_i = (1, 0, 0, 4, 30, 57, 36, 36, 57, 30, 4, 0, 0, 1)$$

and

$$(B_i)_i = (1, 0, 0, 2, 40, 39, 46, 46, 39, 40, 2, 0, 0, 1).$$

In many situations the strength of the (I)LP method can be improved by restrictions on the number of codewords of large weight:

LEMMA 1.29

Let $\mathcal{C}$ be an $[n, k, \geq d]_q$-code. The we have

- $A_i \in \{0, q-1\}$ *for all* $i > (qn - (q-1)d)/2$*;*
- $A_i > 0$ *implies* $A_j = 0$ *for all* $j > qn - (q-1)d - i$*.*

PROOF. We want the use the geometric description of $\mathcal{C}$. If the effective length of $\mathcal{C}$ is $n' < n$, then the above conditions for n imply the corresponding conditions for n', so that we can assume w.l.o.g. that $\mathcal{C}$

is spanning. Let $\mathcal{K}$ be the corresponding (n,s)-arc in $\operatorname{PG}(k-1,q)$, where $s=n-d$. For an arbitrary hyperline X and the $q+1$ hyperplanes $H_1,\dots,H_{q+1}$ through X we have

$$n=\#\mathcal{K}=\sum_{i=1}^{q+1}\mathcal{K}(H_i)\;-\;q\mathcal{K}(X)\le\mathcal{K}(H_1)+\mathcal{K}(H_2)+(q-1)s,$$

so that

$$n-\mathcal{K}(H_1)\le n-(q-1)s-\mathcal{K}(H_2)=qn-(q-1)d-(n-\mathcal{K}(H_2))\,.$$

The second statement follows by assuming $n-\mathcal{K}(H_2)=i$ and $n-\mathcal{K}(H_1)=j$, the first by assuming $n-\mathcal{K}(H_1)=n-\mathcal{K}(H_2)=i$, noting that $A_i/(q-1)\in\mathbb{N}_0$. □

In the context of the linear programming method, the second part may be modeled by the additional constraints $A_i+A_j\le q-1$ for all indices i,j satisfying $i+j>qn-(q-1)d$.

EXERCISE 1.10 Show that no projective 2^2-divisible $[19,9]_2$-code exists.

1.5 Bounds for general block codes

Although we are mainly interested in bounds for linear codes, we some times also use bounds for general q-ary code of length n.

THEOREM 1.30 (Hamming bound)

$$A_q(n,d)\le\frac{q^n}{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i}\quad\textit{where } t:=\left\lfloor\frac{d-1}{2}\right\rfloor.^{3}\tag{1.56}$$

PROOF. Let C be a q-ary code of length n with minimum Hamming distance d. For every codeword $c\in C$ the sphere

$$\left\{c'\in\mathbb{F}_q^n\,:\,d(c,c')\le t\right\}$$

of radius t around c has cardinality $\sum\limits_{i=0}^{t}\binom{n}{i}(q-1)^i$ and all those spheres are disjoint, so that

$$\#C\cdot\left(\sum_{i=0}^{t}\binom{n}{i}(q-1)^i\right)\le\#\mathbb{F}_q^n=q^n.$$

□

[3] Note that the Hamming bound is also true for integers q that are not powers of a prime, if we consider q-ary codes of length n over general alphabets of size q.

Another name for the Hamming bound is sphere packing bound or (less common) volume bound.

THEOREM 1.31 (Singleton bound)

$$A_q(n,d) \leq q^{n-d+1} \tag{1.57}$$

PROOF. Let $\mathcal{C}$ be a q-ary code of length n with minimum Hamming distance d. Shortening $\mathcal{C}$ with respect to $T = \{1, \ldots, d-1\}$ (or any other $d-1$ coordinates) gives a q-ary code $\mathcal{C}^T$ of length $n-d+1$, minimum Hamming distance at least 1, and cardinality

$$\#\mathcal{C} = \#\mathcal{C}^T \leq \#\mathbb{F}_q^{n-d+1} = q^{n-d+1}.$$

□

An interesting variant of codes over $\mathbb{F}_q$ are constant-weight codes where all codewords have the same Hamming weight. For weight w we denote their maximum cardinality by $A_q(n,d;w)$, see e.g. Exercise 1.11 for the so called Johnson bound(s).

EXERCISE 1.11 Prove the inequalities $A_2(n,d;w) \leq \lfloor nA_2(n-1,d;w-1)/w \rfloor$ and $A_2(n,d;w) \leq \lfloor nA_2(n-1,d;w)/(n-w) \rfloor$.

2. Residual codes and the Griesmer bound

The aim of this chapter is to prove a lower bound on the minimum length $n_q(k,d)$ of an $[n,k,d]_q$-code, the so-called Griesmer bound. It originates from an observation about a lower bound for the minimum distance of an residual code with respect to a minimum weigh codeword. Having parametric applications of the Griesmer bound in mind, see e.g. Chapter 3 we also present several results that go beyond numerical evaluations of the Griesmer bound. The presented approach is mainly geometrical, but we will also reformulate the main insights in terms of linear codes. The Griesmer bound for binary codes can be traced back to [57].

LEMMA 2.1

The maximum multiplicity of a hyperline, i.e., a subspace of codimension 2, in an m-hyperplane of an $(n,\le s;k,q)$-arc $\mathcal{K}$ is at most $\lfloor (sq+m-n)/q\rfloor = s-\lceil (n-m)/q\rceil \le s-\lceil (n-s)/q\rceil$.

PROOF. Let S be an arbitrary hyperline and $H_0,\dots,H_q$ the $q+1$ hyperplanes through S. With this and $\mathcal{K}(H_0)=m$ we have

$$n=\sum_{i=0}^{q}\mathcal{K}(H_i)-q\cdot\mathcal{K}(S)\le m+q\cdot s-q\cdot\mathcal{K}(S),$$

so that

$$\mathcal{K}(S)\le\frac{qs+m-n}{q}.$$

Note that $\mathcal{K}(S)$ is a non-negative integer and $m\le s$. □

We remark that even for $(n,s;k,q)$-arcs and $m=s$ we cannot expect that the upper bound of Lemma 2.1 is always attained with equality for some hyperline S. If we e.g. choose $n=s+1$, then we get $\mathcal{K}(S)\le s-1$. However, for most parameters $(s,\le s-2;k-1,q)$-arcs indeed exist. As an example for the application of Lemma 2.1 we state that the maximum multiplicity of a line in a 10-plane in a $(104,22;4,5)$-arc is at most 3. A similar counting approach as in the proof of Lemma 2.1 also gives upper bounds on the multiplicities of subspaces of larger codimension:

LEMMA 2.2

Let $\mathcal{K}$ be an $(\widehat{\gamma}_k,\le\widehat{\gamma}_{k-1})$-arc in $\operatorname{PG}(k-1,q)$. For $1\le j\le k$ the maximum multiplicity of a j-space is at most $\widehat{\gamma}_j$, where

$$\widehat{\gamma}_j:=\left\lfloor\frac{[k-j]_q\widehat{\gamma}_{j+1}-\widehat{\gamma}_k}{[k-j]_q-1}\right\rfloor=\widehat{\gamma}_{j+1}-\left\lceil\frac{\widehat{\gamma}_k-\widehat{\gamma}_{j+1}}{[k-j]_q-1}\right\rceil. \tag{2.1}$$

for $j=k-2,\dots,1$.

PROOF. We prove Inequality (2.2) by induction for $j = k-2, \ldots, 1$. So, let X be an arbitrary j-space and $Y_1, \ldots, Y_l$ the $l := [k-j]_q$ subspaces of dimension $j+1$ that contain X. Thus, we conclude

$$\#\mathcal{K} = \sum_{i=1}^{l} \mathcal{K}(Y_i) \;-\; (l-1)\mathcal{K}(X) \leq l \cdot \widehat{\gamma}_{j+1} - (l-1)\mathcal{K}(X)$$

from the induction hypothesis, so that $\mathcal{K}(X) \in \mathbb{N}_0$ and $\#\mathcal{K} = \widehat{\gamma}_k$ imply

$$\mathcal{K}(X) \leq \left\lfloor \frac{l\widehat{\gamma}_{j+1} - \widehat{\gamma}_k}{l-1} \right\rfloor .$$

□

EXAMPLE 2.3 For a $(1010, 204)$-arc in $\mathrm{PG}(4,5)$ we have $\widehat{\gamma}_5 = 1010$, $\widehat{\gamma}_4 = 204$, $\widehat{\gamma}_3 = 42$, $\widehat{\gamma}_2 = 9$, $\widehat{\gamma}_1 = 2$. For a $(513, 205)$-arc in $\mathrm{PG}(4,5)$ we have $\widehat{\gamma}_5 = 513$, $\widehat{\gamma}_4 = 205$, $\widehat{\gamma}_3 = 143$, $\widehat{\gamma}_2 = 130$, $\widehat{\gamma}_1 = 127$. ◇

Setting $\widehat{\gamma}_k = n$ and $\widehat{\gamma}_{k-1} = s$ we can rewrite the recursive definition of $\widehat{\gamma}_j$ in Equation (2.1) to

$$\widehat{\gamma}_j = \left\lfloor \frac{\left\lfloor \begin{matrix} \left\lfloor \frac{\left\lfloor \frac{s\cdot[2]_q-n}{[2]_q-1} \right\rfloor \cdot [3]_q - n}{[3]_q-1} \right\rfloor & \\ & \ddots \end{matrix} \right\rfloor \cdot [k-j]_q - n}{[k-j]_q - 1} \right\rfloor \tag{2.2}$$

For the special case $m = s$ Lemma 2.2 is a generalization of Lemma 2.1. We can also rewrite Lemma 2.1 for $[n, k, \geq d]_q$-codes instead of $(n, \leq s)$-arcs:

LEMMA 2.4

If an $[n, k, \geq d]_q$-code $\mathcal{C}$ contains a codeword c of weight w with $w < \frac{dq}{q-1}$, then the residual code $\mathrm{Res}(\mathcal{C}; c)$ *of $\mathcal{C}$ with respect to c is an $\left[n-w, k-1, \geq d - w + \left\lceil \frac{w}{q} \right\rceil\right]_q$-code.*

PROOF. W.l.o.g. we assume that $\mathcal{C}$ is spanning. Let $\mathcal{M}$ be the $(n, \leq n-d)$-arc in $\mathrm{PG}(k-1, q)$ corresponding to $\mathcal{C}$ and $\mathcal{M}'$ the $(n-w, s)$-arc in $\mathrm{PG}(k-2, q)$ corresponding to $\mathrm{Res}(\mathcal{C}; c)$. From Lemma 2.1 we conclude

$$s \leq n - d - \left\lceil \frac{w}{q} \right\rceil .$$

Thus, the minimum Hamming distance d' of the $[n-w, \leq k-1]_q$-code $\mathrm{Res}(\mathcal{C}; c)$ satisfies

$$d' = (n-w) - s \geq d - w + \left\lceil \frac{w}{q} \right\rceil .$$

Since $w < \frac{dq}{q-1}$ we have

$$n - w > n - d - \frac{w}{q} \geq s,$$

i.e., the arc $\mathcal{M}'$ is spanning and the dimension of $\operatorname{Res}(\mathcal{C}, c)$ is $k-1$. □

We remark that the non-existence of $\left[n-w, k-1, \geq d-w+\left\lceil\frac{w}{q}\right\rceil\right]_q$-code, given $w < \frac{dq}{q-1}$, implies that an $[n,k,d]_q$-code (or an $[n,k,\geq d]_q$-code) cannot contain a codeword of weight w. This application of Lemma 2.4 is also called residual code argument. Note that $w < \frac{dq}{q-1}$ is satisfied for $w = d$.

EXAMPLE 2.5 A $[13,5,6]_2$-code $\mathcal{C}$ cannot contain a codeword of weight 10, since no $[3,4,1]_2$-code exists. From this the non-existence of $[12,5,5]_2$- and $[13,5,6]_2$-codes can be easily concluded see Remark 1.28. ⋄

If no $\left[n-d, k-1, \left\lceil\frac{d}{q}\right\rceil\right]_q$-code exists, then we say that the non-existence of an $[n,k,d]_q$-code follows from Lemma 2.4 using $w = d$. In this case we also speak of a one-step Griesmer (argument).

EXAMPLE 2.6 Since no $[9,5,4]_2$-code exists, the one-step Griesmer argument yields that no $[17,6,8]_2$-code exists. The non-existence of the former follows from the non-existence of $[8,5,3]_2$-codes, which is implied by the Hamming bound, see Theorem 1.30. ⋄

Of course, we can also consider the residual residual code $\operatorname{Res}(\mathcal{C}; c)$ if c has large weight, i.e., $w \geq \frac{dq}{q-1}$. So, removing the assumption $w < \frac{dq}{q-1}$ from Lemma 2.4 we have:

LEMMA 2.7

If an $[n,k,\geq d]_q$-code $\mathcal{C}$ contains a codeword c of weight w, then the residual code $\operatorname{Res}(\mathcal{C}; c)$ of $\mathcal{C}$ with respect to c is an $\left[n-w, \tilde{k}, \geq d-w+\left\lceil\frac{w}{q}\right\rceil\right]_q$-code, where

$$\tilde{k} = k - \dim\left(\mathcal{C}^{\operatorname{supp}(c)}\right). \tag{2.3}$$

PROOF. The length and the stated lower bound on the minimum distance of $\operatorname{Res}(\mathcal{C}; c)$ follows as in the proof of Lemma 2.4. Now let $k' = \dim\left(\mathcal{C}^{\operatorname{supp}(c)}\right)$ and $G = \left(\mathbf{g}^1, \dots, \mathbf{g}^k\right)^\top$ a generator matrix of $\mathcal{C}$, where we assume w.l.o.g. that the last k' rows of G constitute a generator matrix of $\mathcal{C}^{\operatorname{supp}(c)}$. Next we set $T = \{1, \dots, n\} \setminus \operatorname{supp}(c)$ and $\bar{\mathbf{g}}^i = \mathbf{g}^i_T$ for all $1 \leq i \leq k-k'$. By construction, the $\tilde{k} = k - k'$ vectors $\bar{\mathbf{g}}^1, \dots, \bar{\mathbf{g}}^{k-k'}$ span $\operatorname{Res}(\mathcal{C}; c)$. Suppose there exists a vector $\mu \in \mathbb{F}_q^{k-k'} \setminus \mathbf{0}$ with $\sum_{i=1}^{k-k'} \mu_i \bar{\mathbf{g}}^i = \mathbf{0}$, then $\sum_{i=1}^{k-k'} \mu_i \mathbf{g}^i$ is contained in $\mathcal{C}^{\operatorname{supp}(c)}$, which contradicts the assumption that $\mathbf{g}^{k-k'+1}, \dots, \mathbf{g}^k$ is a basis of $\mathcal{C}^{\operatorname{supp}(c)}$. Thus, the $\bar{\mathbf{g}}^i$ give a basis of $\operatorname{Res}(\mathcal{C}; c)$ and $\dim(\operatorname{Res}(\mathcal{C}; c)) = k - k'$. □

EXAMPLE 2.8 If $\mathcal{C}$ is a $[41, 6, \{20, 24, 26, 40\}]_2$-code, then $A_{40} = 0$. To this end we remark that for a codeword c of weight 40 the residual code $\operatorname{Res}(\mathcal{C}; c)$ is an $[1, \le 1]_2$-code and $\mathcal{C}^{\operatorname{supp}(c)}$ is a $[40, \le 4]_2$-code, see Exercise 2.3. ◇

Repeated application of Lemma 2.4 with w chosen as the minimum Hamming distance implies:

THEOREM 2.9 (Griesmer bound)
Each $[n, k, \ge d]_q$-code $\mathcal{C}$ satisfies

$$n \ \ge \ \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil . \tag{2.4}$$

PROOF. Set $d' = d(\mathcal{C}) \ge d$. We proof the statement by induction on k. For $k = 1$ the corresponding inequality $n \ge d$ is trivially satisfied. For $k > 1$ using Lemma 2.4 with a minimum weight codeword gives the existence of a residual $\left[n - d', k - 1, \ge \left\lceil \frac{d'}{q} \right\rceil\right]$-code $\mathcal{C}'$. Eventually applying trivial lengthening we can assume the existence of an $\left[n - d, k - 1, \ge \left\lceil \frac{d}{q} \right\rceil\right]$-code $\mathcal{C}''$. Applying the induction hypothesis to $\mathcal{C}''$ gives

$$n - d \ge \sum_{i=0}^{k-2} \left\lceil \frac{\left\lceil \frac{d}{q} \right\rceil}{q^i} \right\rceil = \sum_{i=0}^{k-2} \left\lceil \frac{d}{q^{i+1}} \right\rceil = \sum_{i=1}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil ,$$

which implies Inequality (2.4). □

EXAMPLE 2.10 No $[103, 4, 82]_5$ code exists. If we apply Theorem 2.9 with $d = 82$, $k = 4$, and $q = 5$, we obtain

$$n \ge \left\lceil \frac{82}{5^0} \right\rceil + \left\lceil \frac{82}{5^1} \right\rceil + \left\lceil \frac{82}{5^2} \right\rceil + \left\lceil \frac{82}{5^3} \right\rceil = 82 + 17 + 4 + 1 = 104,$$

which is a contradiction. ◇

DEFINITION 2.11
An $[n, k, d]_q$-code whose parameters satisfy Inequality (2.4) with equality is called a Griesmer code. The corresponding $(n, n - d; k, q)$-arcs are called a Griesmer arcs.

EXERCISE 2.1 Let $\mathcal{K}$ be an $(n, \le s)$-arc in $\operatorname{PG}(k - 1, q)$. For an arbitrary subspace X of codimension j let $H_1, \ldots, H_l$ denote the $l := [j]_q$ hyperplanes containing X. Deduce an upper bound for $\mathcal{K}(X)$ based on the equation

$$[j - 1]_q \cdot \#\mathcal{K} = \sum_{i=1}^{l} \mathcal{K}(H_i) \ - \ q^{j-1} \cdot \mathcal{K}(X).$$

Can there be instances where this bound is strictly better than $\mathcal{K}(X) \le \widehat{\gamma}_{k-j}$ from Lemma 2.2?

EXERCISE 2.2 Let $\mathcal{K}$ be an arc of cardinality n in $\mathrm{PG}(k-1,q)$ such that every y-space Y satisfies $\mathcal{K}(Y) \le s'$, where $2 \le y \le k-1$ is an arbitrary but fixed parameter. Give an upper bound for $\mathcal{K}(J)$, where J is an arbitrary j-space with $1 \le j \le y-1$.

EXERCISE 2.3 Let $\mathcal{C}$ be a $[40, k, \{20, 24, 26, 40\}]_2$-code that contains a codeword of weight 40. Show that $k \le 4$.

EXERCISE 2.4 Construct $(513, 205)$-arcs $\mathcal{K}$ and $\mathcal{K}'$ in $\mathrm{PG}(4,5)$ such that $\gamma_3(\mathcal{K}) \le 62$ and $\gamma_1(\mathcal{K}') \ge 100$. *Hint:* Look at Exercise 1.7 for $\mathcal{K}$ and use the existence of a (quasi-cyclic) $[52, 5, 39]_5$-code, see [37, Theorem 1], for $\mathcal{K}'$.

EXERCISE 2.5 Show that the, up to equivalence, unique $[7, 4, \{1, 2, 4, 5, 6, 7\}]_3$ code $\mathcal{C}$ is given by the generator matrix

$$\begin{pmatrix} 1100000 \\ 0011000 \\ 0000110 \\ 0101011 \end{pmatrix}$$

and has weight enumerator $W_{\mathcal{C}}(x) = x^0 + 6x^2 + 28x^4 + 24x^5 + 20x^6 + 2x^7$.

2.1 Parameterization of the length and the minimum distance of Griesmer arcs

LEMMA 2.12

Let $k \ge 1$ and d be positive integers. Write d as

$$d = \sigma q^{k-1} - \sum_{i=0}^{k-2} \varepsilon_i q^i, \tag{2.5}$$

where $\sigma \in \mathbb{N}_0$ and the $0 \le \varepsilon_i < q$ are integers for all $0 \le i \le k-2$. Then, Inequality (2.4) is satisfied with equality iff

$$n = \sigma[k]_q - \sum_{i=0}^{k-2} \varepsilon_i [i+1]_q, \tag{2.6}$$

which is equivalent to

$$n - d = \sigma[k-1]_q - \sum_{i=1}^{k-2} \varepsilon_i [i]_q. \tag{2.7}$$

Moreover, for each integer $0 \le j \le k-1$ we have

$$\sum_{i=j}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = \sigma[k-j]_q - \sum_{i=j}^{k-2} \varepsilon_i [i-j+1]_q. \tag{2.8}$$

PROOF. From Equation (2.5) and

$$0 \le \sum_{i=0}^{h-1} \varepsilon_i q^i \le (q-1) \cdot \sum_{i=0}^{h-1} q^i = q^h - 1 < q^h$$

we conclude

$$\left\lceil \frac{d}{q^h} \right\rceil = \sigma q^{k-1-h} - \sum_{i=h}^{k-2} \varepsilon_i q^{i-h} \tag{2.9}$$

for all $0 \le h \le k-1$. With this we have

$$\begin{aligned} \sum_{h=j}^{k-1} \left\lceil \frac{d}{q^h} \right\rceil &= \sigma \sum_{h=j}^{k-1} q^{k-1-h} - \sum_{h=j}^{k-1} \sum_{i=h}^{k-2} \varepsilon_i q^{i-h} \\ &= \sigma \sum_{h=0}^{k-1-j} q^h - \sum_{i=j}^{k-2} \varepsilon_i \sum_{h=j}^{i} q^{i-h} \\ &= \sigma [k-j]_q - \sum_{i=j}^{k-2} \varepsilon_i \sum_{h=0}^{i-j} q^h \\ &= \sigma [k-j]_q - \sum_{i=j}^{k-2} \varepsilon_i [i-j+1]_q \end{aligned}$$

for $j = 0, \ldots, k-1$. The case $j = 0$ implies that the value for n, such that Inequality (2.4) is satisfied with equality, is given by Equation (2.6). The case $j = 1$ gives the equivalent condition for $n - d$. □

In other words a Griesmer code has parameters n and d satisfying Equation (2.6) and Equation (2.5), respectively. Note that each positive integer d admits a representation as in Equation (2.5), see Exercise 2.6. The parameters n and $s = n - d$ of a Griesmer arc are specified by Equation (2.6) and Equation (2.7), repespectively. Note that not every positive integer s admits a representation as in Equation (2.7), satisfying the conditions for σ and the ε_i, see Exercise 2.6. The expressions in (2.8) equal $\widehat{\gamma}_{k-j}$ and are indeed attained for Griesmer arcs.

LEMMA 2.13

For an integer $k \ge 3$ let σ and $0 \le \varepsilon_i < q$, where $0 \le i \le k-2$, be non-negative integers. If

$$n = \sigma [k]_q - \sum_{i=0}^{k-2} \varepsilon_i [i+1]_q \tag{2.10}$$

and

$$s = \sigma [k-1]_q - \sum_{i=1}^{k-2} \varepsilon_i [i]_q, \tag{2.11}$$

then we have

$$\widehat{\gamma}_j = \sigma [j]_q - \sum_{i=k-j}^{k-2} \varepsilon_i [i-k+j+1]_q \tag{2.12}$$

for each (n,s)-arc $\mathcal{K}$ in $\operatorname{PG}(k-1,q)$ and for all $1 \le j \le k$. Moreover, each j-space X with $\mathcal{K}(X) = \widehat{\gamma}_j$ contains a $(j-1)$-space Y with $\mathcal{K}(Y) = \widehat{\gamma}_{j-1}$, where $2 \le j \le k$.

PROOF. First we proof Equation (2.12) by induction for $j = k, k-1, \dots, 1$. The case $j = k$ is given by Equation (2.10) and the case $j = k-1$ is given by Equation (2.11). Note that we have $[a]_q - [b]_q = q^b[a-b]_q$ and $[b]_q - 1 = q[b-1]_q$ for integers $1 \le b \le a$. With this we compute

$$\begin{aligned} \frac{\widehat{\gamma}_k - \widehat{\gamma}_{j+1}}{[k-j]_q - 1} &= \frac{\sigma\left([k]_q - [j+1]_q\right) - \sum\limits_{i=k-j-1}^{k-2} \varepsilon_i \left([i+1]_q - [i+1-k+j+1]_q\right) - \sum\limits_{i=0}^{k-j-2} \varepsilon_i [i+1]_q}{q \cdot [k-j-1]_q} \\ &= \sigma q^j - \sum_{i=k-j-1}^{k-2} \varepsilon_i q^{i-k+j+1} - \frac{\sum\limits_{i=0}^{k-j-2} \varepsilon_i [i+1]_q}{[k-j]_q - 1}, \end{aligned}$$

where $1 \le j \le k-2$. Since

$$0 \le \sum_{i=0}^{k-j-2} \varepsilon_i [i+1]_q \le \sum_{i=0}^{k-j-2} \left(q^{i+1} - 1\right) = \left([k-j]_q - 1\right) - (k-j-1) < [k-j]_q - 1$$

we conclude

$$\left\lceil \frac{\widehat{\gamma}_k - \widehat{\gamma}_{j+1}}{[k-j]_q - 1} \right\rceil = \sigma q^j - \sum_{i=k-j-1}^{k-2} \varepsilon_i q^{i-k+j+1}.$$

Plugging into Equation (2.1) gives

$$\begin{aligned} \widehat{\gamma}_j &= \widehat{\gamma}_{j+1} - \left\lceil \frac{\widehat{\gamma}_k - \widehat{\gamma}_{j+1}}{[k-j]_q - 1} \right\rceil = \sigma\left([j+1]_q - q^j\right) - \sum_{i=k-j-1}^{k-2} \varepsilon_i \left([i+1-k+j+1]_q - q^{i-k+j+1}\right) \\ &= \sigma[j]_q - \sum_{i=k-j-1}^{k-2} \varepsilon_i [i+1-k+j]_q = \sigma[j]_q - \sum_{i=k-j}^{k-2} \varepsilon_i [i+1-k+j]_q, \end{aligned}$$

so that Equation (2.12) is satisfied.

For the final statement note that $\mathcal{K}|_X$ is a $(\widehat{\gamma}_j, \le \widehat{\gamma}_{j-1})$-arc in $\operatorname{PG}(j-1,q)$. Observe that the arc is spanning, due to $\widehat{\gamma}_j > \widehat{\gamma}_{j-1}$, and the non-existence of a hyperplane Y in X with $\mathcal{K}(Y) = \widehat{\gamma}_{j-1}$ contradicts the Griesmer bound, i.e., Inequality (2.4). □

COROLLARY 2.14

Griesmer arcs and codes are spanning. Let $\sigma \in \mathbb{N}$ such that $(\sigma-1)[k]_q < n \le \sigma[k]_q$, or, equivalently, $(\sigma-1)q^{k-1} < d \le \sigma q^{k-1}$, for a Griesmer arc or code. Then, we have $\gamma_1 = \sigma$ for the maximum point multiplicity. In the special case where $\sigma = 1$, i.e., $1 \le n \le [k]_q$ or $1 \le d \le q^{k-1}$, the arc or code is is projective.

PROOF. Using Lemma 2.13 we compute $\gamma_1 = \sigma$. □

Taking up again Example 2.3 we remark

$$\begin{aligned}
1010 &= 2 \cdot 781 - 3 \cdot 156 - 2 \cdot 31 - 3 \cdot 6 - 4 \cdot 1 \\
204 &= 2 \cdot 156 - 3 \cdot 31 - 2 \cdot 6 - 3 \cdot 1 \\
42 &= 2 \cdot 31 - 3 \cdot 6 - 2 \cdot 1 \\
9 &= 2 \cdot 6 - 3 \cdot 1 \\
2 &= 2 \cdot 1
\end{aligned}$$

for a $(1010, 204)$-arc in $\mathrm{PG}(4, 5)$.

DEFINITION 2.15

Let $\mathcal{K}$ be an arc in $\mathrm{PG}(k-1, q)$. For $j = 1, \ldots, k$ we denote by γ_j the maximum multiplicity of a j-space, i.e.,

$$\gamma_j = \max_{S \in \begin{bmatrix} \mathbb{F}_q^k \\ j \end{bmatrix}} \mathcal{K}(S). \tag{2.13}$$

From Lemma 2.13 we directly conclude:

PROPOSITION 2.16

Each Griesmer arc in $\mathrm{PG}(k-1, q)$ satisfies $\gamma_j = \widehat{\gamma}_j$ for $1 \leq j \leq k$ and (γ_j, γ_{j-1}) are the parameters of a Griesmer arc in $\mathrm{PG}(j-1, q)$ for $2 \leq j \leq k$.

EXAMPLE 2.17 For an $(104, 22; 4, 5)$-arc $\mathcal{K}$ we have $\gamma_4 = 104$, $\gamma_3 = 22$, $\gamma_2 = 5$, and $\gamma_1 = 1$. In other words the arc is projective, i.e., $\gamma_1 = 1$, and each line has multiplicity at most $5 = \gamma_2$, where equality is indeed attained for at least one line in every 22-plane. Of course, also every 5-lines contains at least a 1-point. ◇

EXERCISE 2.6 Show that for positive integers d, k, and q, with $q \geq 2$, Equation (2.5) admits a unique solution $(\varepsilon_0, \ldots, \varepsilon_{k-2}, \sigma)$.

EXERCISE 2.7 Let $\mathcal{K}$ be a $(204, 42)$-arc in $\mathrm{PG}(3, 5)$. Apply direct counting to show that:

(a) the maximum multiplicity of a line is 9 and the maximum multiplicity of a point is 2;

(b) each 42-plane contains a 9-line and that each 9-line contains a 2-point.

2.2 Cases where the Griesmer bound can be attained

DEFINITION 2.18

By $n_q(k,d)$ we denote the minimum possible length n of an $[n,k,d]_q$-code and set

$$g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil . \tag{2.14}$$

Given the Griesmer bound, i.e., Theorem 2.9, the question arises whether $n_q(k,d) = g_q(k,d)$ can be attained, i.e., for which parameters Griesmer codes exist. Our next aim is to show that this is indeed always the case if d is sufficiently large. To this end we start with the construction of Solomon and Stiffler [144]:

LEMMA 2.19

Let

$$n = \sigma[k]_q - \sum_{i=0}^{k-2} \varepsilon_i [i+1]_q$$

and

$$n - d = \sigma[k-1]_q - \sum_{i=1}^{k-2} \varepsilon_i [i]_q,$$

where $\sigma \in \mathbb{N}_0$ and $\varepsilon_i \in \mathbb{N}_0$ for all $0 \le i \le k-2$. If there exist subspaces $S_1, \dots, S_l$ in $\operatorname{PG}(k-1,q)$ such that

$$\#\left\{1 \le j \le l \,:\, \dim(S_j) = i\right\} = \varepsilon_{i+1} \tag{2.15}$$

for $1 \le i \le k-1$ and

$$\#\left\{1 \le j \le l \,:\, P \in S_j\right\} \le \sigma \tag{2.16}$$

for each point P in $\operatorname{PG}(k-1,q)$, then an $[n,k,\ge d]_q$-code exists.

PROOF. The statement is trivial for $n = 0$, so that we assume $n \ge 1$, which implies $n - d < n$. Using the abbreviation $V = \operatorname{PG}(k-1,q)$ we define an $(n, \le n-d)$-arc $\mathcal{K}$ in V via

$$\mathcal{K} = \sigma \cdot \chi_V - \sum_{i=j}^{l} \chi_{S_j}. \tag{2.17}$$

Note that $\mathcal{K} = n$ and $\mathcal{K}(P) \in \mathbb{N}_0$ for each point P in V. For every hyperplane H we have $\#\left(H \cap S_j\right) \ge [\dim(S_j) - 1]_q$ for all $1 \le j \le l$, so that

$$\mathcal{K}(H) = \sigma \# H - \sum_{j=1}^{l} \#\left(H \cap S_j\right) \le \sigma[k-1]_q - \sum_{i=0}^{k-2} \varepsilon_i [i]_q = n - d.$$

Since $n > n - d$ the arc $\mathcal{K}$ is spanning, so that it corresponds to an $[n,k,\ge d]_q$-code. □

Equation (2.15) just says that there are exactly ε_{i+1} subspaces of dimension i among the S_j and Inequality (2.16) that each point is covered at most σ times by the S_j. Of course we can choose such subspaces $S_1, \dots, S_l$ arbitrary if $\sum_{i=0}^{k-2} \varepsilon_i \le \sigma$.

LEMMA 2.20

If $\mathbf{e} = (e_1, \dots, e_{k-1}) \in \mathbb{N}_0^{k-1}$ *and there are* t *vectors* $\mathbf{x}^i = \left(x_1^i, \dots, x_{k-1}^i\right) \in \mathbb{N}_0^{k-1}$ *with*

$$\sum_{j=1}^{k-1} j x_j^i \le k \tag{2.18}$$

for all $1 \le i \le t$ *and*

$$\sum_{i=1}^{t} x_j^i = e_j \tag{2.19}$$

for all $1 \le j \le k-1$*, then there exist subspaces* $S_1, \dots, S_l$ *with*

$$\#\left\{1 \le h \le l \,:\, \dim(S_h) = j\right\} = e_j \tag{2.20}$$

for all $1 \le j \le k-1$*, such that*

$$\#\left\{1 \le h \le k-1 \,:\, P \in S_h\right\} \le t \tag{2.21}$$

for every point P *in* $\mathrm{PG}(k-1, q)$*.*

PROOF. It suffices to prove the statement for $t = 1$ where we can use

$$\mathbb{F}_q^k = \mathbb{F}_q^{k_1'} \times \cdots \times \mathbb{F}_q^{k_{l-1}'} \times \mathbb{F}_q^{\left(k - \sum\limits_{h=1}^{l-1} k_h'\right)}$$

to choose the disjoint subspaces $S_1, \dots, S_l$. (The integers $0 \le k_h' = \dim((S_h) \le k$, where $1 \le h \le l-1$, satisfying $k - \sum\limits_{h=1}^{l-1} k_h' = \dim(S_l) \ge 0$ exist due to Inequality (2.18).) □

More handy, but more coarse, criteria have been determined in the literature, see e.g. Exercise 2.8 and :

PROPOSITION 2.21

For

$$d \ge (q-1)\left\lceil \frac{k-1}{2} \right\rceil q^{k-1} \tag{2.22}$$

we have

$$n_q(k, d) = g_q(k, d).$$

PROOF. The statement is obvious for $k = 1$ so that we assume $k \geq 2$ in the following. Write

$$d = \sigma q^{k-1} - \sum_{i=0}^{k-2} \varepsilon_i q^i,$$

where $\sigma \in \mathbb{N}_0$ and the $0 \leq \varepsilon_i < q$ are integers for all $0 \leq i \leq k-2$, so that $\sigma \geq (q-1)\left\lceil \frac{k-1}{2} \right\rceil$. Consider the $\left\lceil \frac{k-1}{2} \right\rceil$ vectors $\mathbf{x}^i = \left(x_1^i, \dots, x_{k-1}^i\right) \in \mathbb{N}_0^{k-1}$ with $x_j^i = 1$ if $j \in \{i, k-i\}$ and $x_j^i = 0$ otherwise, where $1 \leq i \leq \left\lceil \frac{k-1}{2} \right\rceil$. Taking $q-1$ copies of these they satisfy the criterion of Lemma 2.20 for $\mathbf{e} = (q-1, \dots, q-1) \geq (\varepsilon_0, \dots, \varepsilon_{k-2}) = \varepsilon$. So, after eventually reducing some of the entries of the vectors $\mathbf{x}$ we can apply the construction of Solomon and Stiffler, i.e., Lemma 2.19. □

For $q = 2$ this is the main theorem of [17]. With a bit more effort the right-hand side of Inequality (2.22) can be further reduced. Indeed, for $q = 2$ and $k \leq 4$ we always have $n_q(k, d) = g_q(k, d)$, see Exercise 2.9. Note that we e.g. have $n_2(5, 3) > g_2(5, 3) = 8$ and $n_2(6, 3) > g_2(6, 3) = 9$ due to the Hamming bound, see Theorem 1.30.

PROPOSITION 2.22

For $d \leq 2$ we have $n_q(k, d) = g_q(k, d)$.

PROOF. Consider the generator matrices $G = (I_k)$ and $G' = (I_k|\mathbf{1})$ over $\mathbb{F}_q$, where $\mathbf{1}$ is the all-one vector. They generate $[k, k, 1]_q$- and $[k+1, k, 2]_q$-codes, respectively. □

PROPOSITION 2.23

For $k \leq 2$ we have $n_q(k, d) = g_q(k, d)$.

PROOF. For $k = 1$ we choose $\sigma = d$ and for $k = 2$ we uniquely write $d = \sigma q - \varepsilon_0$, where $\sigma \in \mathbb{N}_0$ and $\varepsilon \in \{0, 1, \dots, q-1\}$. We can easily apply the construction of Solomon and Stiffler since the projective line contains $q+1$ points so that $\varepsilon_0 < q \leq q+1$ pairwise disjoint sets S_i can be chosen. □

Of course, for $k = 1$ the construction of Solomon and Stiffler just corresponds to a generator matrix consisting of a single row with d ones. Also for $k = 2$ the corresponding (n, s)-arcs in $\mathrm{PG}(1, q)$ are easily constructed directly. Just increase the point multiplicities up to s until cardinality n is reached.

Note that we have $n_3(3, 3) > g_3(3, 3) = 5$ since there is no $(5, 2)$-arc in $\mathrm{PG}(2, 3)$.

Of course we can also apply the construction of Solomon and Stiffler in the case of non-Griesmer codes.

EXAMPLE 2.24 An $[41, 6, 19]_2$-code can be obtained from Lemma 2.19. To this end write

$$41 = 1 \cdot [6]_2 - 3 \cdot [3]_2 - 1 \cdot [1]_2 = 63 - 21 - 1 = 41$$

and

$$41-19=1\cdot[5]_2-3\cdot[2]_2=31-9=22.$$

In other words, we choose $\sigma=1$, $\varepsilon_0=1$, $\varepsilon_2=3$, and $\varepsilon_i=0$ for all other $0\le i\le 4$. Observe that we can easily choose four disjoint planes in $\mathrm{PG}(5,2)$ and replace one plane by a contained point. ◇

Note that easy numerical conditions like Lemma 2.20 do not always answer the question if a collection of ε_i $(i+1)$-spaces, where $0\le i\le k-2$, can be arranged in $\mathrm{PG}(k-1,q)$ such that every point is contained in at most σ elements. In the case $\sigma=1$ those configurations can be extended to so-called vector space partitions, see Section 17.3, by adding further points.

EXAMPLE 2.25 (C.f. [17].) In $\mathrm{PG}(5,2)$ there cannot exist subspaces with dimensions 4, 3, 2, and 1, such that every point is covered at most once, since the 4-space and the 3-space have at least one point in common. Note that

$$1\cdot[6]_2-1\cdot[4]_2-1\cdot[3]_2-1\cdot[2]_2-1\cdot[1]_2=37$$

and

$$1\cdot2^5-1\cdot2^3-1\cdot2^2-1\cdot2^1-1\cdot2^0=17$$

i.e., such a configuration would be needed for the Solomon-Stieffler construction of a $[37,6,17]_2$ Griesmer code. Such a code exists nevertheless, see e.g. [57]. ◇

EXERCISE 2.8 Let $d=\beta_0q^{k-1}-\sum_i\beta_iq^{l_i-1}$, where the β_i and l_i are integers with $0\le\beta_i\le\beta_0$ and $\sum_i l_i\le k$. Then, we have $n_q(d,k)=g_q(d,k)$. (C.f. [144, Theorem 2']).)

EXERCISE 2.9 Prove $n_2(d,k)=g_2(d,k)$ for all $k\le 4$.

EXERCISE 2.10 Construct a $[72,6,35]_2$-code using the method of Solomon and Stiffler.

3. Length optimal binary codes for small parameters

In this chapter we are interested in the minimum possible length $n = n_q(k,d)$ of a $[n,k,d]_q$-code. We restrict our attention to the binary case $q = 2$ and small parameters. The Griesmer bound $n_q(k,d) \ge g_q(k,d))$ in Theorem 2.9 is known to be tight if d, depending on q and k, is sufficiently large, see e.g. Proposition 2.21. In Exercise 2.9 we have shown $n_2(k,d) = g_2(k,d)$ for all dimensions $k \le 4$. In other words, we have constructed $[g_2(k,d),k,d]_2$-codes for all parameters with $k \le 4$. To shorten the subsequent discussion we only give proofs for the lower bounds for $n_2(k,d)$ and refer to e.g. `codetables.de` for the existence of attaining codes, see also Exercise 3.1 for a recursive construction.

For $k \le 6$ the values of $n_2(k,d)$ have been completely determined already in 1973 by Baumert and McEliece [17]. The parameters where $n_2(k,d) > g_2(k,d)$ are listed in Table 3.1. For the sake of completeness we give theoretic proofs for the improved lower bounds, noting that some of these where obtained with the aid of computer searches in [17].

k	d	$g_2(k,d)$	$n_2(k,d)$	k	d	$g_2(k,d)$	$n_2(k,d)$
5	3	8	9	5	4	9	10
5	5	12	13	5	6	13	14
6	3	9	10	6	4	10	11
6	5	13	14	6	6	14	15
6	7	16	17	6	8	17	18
6	9	21	22	6	10	22	23
6	11	24	25	6	12	25	26
6	13	28	29	6	14	29	30
6	19	40	41	6	20	41	42

Table 3.1: Parameters where $n_2(k,d) > g_2(k,d)$ for $k \le 6$.

LEMMA 3.1

We have $n_2(5,d) \ge g_2(5,d) + 1$ *for all* $3 \le d \le 6$.

PROOF. For $d = 3$ we apply the Hamming bound (Theorem 1.30). For $d = 6$ we assume the existence of an even $[13,5,6]_2$-code, see Lemma 1.21, and exclude the existence of a codeword of weight 10 by the residual code argument (Lemma 2.4). Then we observe that the first 4 MacWilliams identities do not admit an integral solution, see Remark 1.28. The other two cases $d = 4$ and $d = 5$ follow from Corollary 1.20 (Paritiy check bit construction). □

REMARK 3.2 For the non-existence of $[9,5,4]_2$-codes one may also assume that the code is even and use the residual code argument to conclude that there is no codeword of weight 6, i.e., the non-zero codewords are contained in $\mathcal{W}=\{4,8\}$. With this one, e.g., directly obtains a contradiction from the first two MacWilliams identities.

LEMMA 3.3
We have $n_2(6,d) \ge g_2(6,d)+1$ for all $3 \le d \le 14$ and $d \in \{19,20\}$.

PROOF. Assume $n_2(6,d) \ge g_2(6,d)$. For $d=3$ we apply the Hamming bound (Theorem 1.30). For $d \in \{5,7,9,11\}$ we apply the residual code argument (Lemma 2.4) to deduce the no-existence of a codeword of weight d. Due to Corollary 1.20 it suffices to consider the two remaining cases $d=14$ and $d=20$. We assume that the codes are projective and even, see Corollary 2.14 and Lemma 1.21. Appyling the residual code argument (Lemma 2.4) we conclude that the possible non-zero weights are contained in $\mathcal{W}=\{14,28\}$ and $\mathcal{W}=\{20,24,26,40\}$, respectively. In the first case the first four MacWilliams identities do not admit a solution and in the second case they give

$$\begin{aligned} B_3 &= \frac{470}{3}-\frac{280}{3}A_{40} \\ A_{20} &= \frac{158}{3}-\frac{28}{3}A_{40} \\ A_{24} &= 5+35A_{40} \\ A_{26} &= \frac{16}{3}-\frac{80}{3}A_{40}. \end{aligned}$$

However, $A_{26} \ge 0$ implies $A_{40}=0$, so that $A_{26}=\frac{16}{3}\notin \mathbb{N}_0$, which is a contradicition. □

For the "first gap" in the sequence of distances d with $n_2(k,d)=g_2(k,d)$ can be described in general.

THEOREM 3.4 ([124])
If $3 \le d \le 2^{k-2}-2$, then $n_2(k,d) \ge g_2(k,d)+1$.

PROOF. We prove the statement by induction over the dimension k. Let d be an integer in the specified range, so that $k \ge 5$. Due to Lemma 3.1 we can assume $k \ge 6$. For $d=3$ we apply the Hamming bound (Theorem 1.30) and for $d=4$ we apply Corollary 1.20, so that we can assume $d \ge 5$. Now asume that $\mathcal{C}$ is a $[g_2(k,d),k,d]_2$-Griesmer code with $5 \le d \le 2^{k-2}-4$. From Lemma 2.4 we conclude the existence of a $\left[g_2(k-1,\left\lceil\frac{d}{2}\right\rceil),k-1,\ge\left\lceil\frac{d}{2}\right\rceil\right]_2$-Griesmer code, where $3 \le \left\lceil\frac{d}{2}\right\rceil \le 2^{k-3}-2$, so that we can apply the induction hypothesis to obtain a contradiction. Due to Corollary 1.20 it remains to consider the case $d=2^{k-2}-2=2^{k-1}-2^{k-2}-2^1$, where

$$g_2(k,d)=\left(2^k-1\right)-\left(2^{k-1}-1\right)-\left(2^2-1\right)=2^{k-1}-3=:n.$$

Now assume the existence of an even $[n,k,d]_2$-code $\mathcal{C}$. For an even integer $d+2 \le w \le n-3$ the residual code with respect to a codeword of weight w is an $\left[n-w, k-1, \ge d-\frac{w}{2}\right]_2$-code, see Lemma 2.4. We write $w = d+2l$, where $1 \le l \le 2^{k-3}-2$ and note that we have $n' := n-w = 2^{k-2}-1-2l$ and

$$d' := d-w+\left\lceil \tfrac{w}{2}\right\rceil = \tfrac{d}{2}-l = 2^{k-3}-1-l = 2^{k-2}-2^{k-3}-1-l.$$

Next we want to compute $g_2(k-1,d')$. To this end we write

$$l = \sum_{i=0}^{k-4} \varepsilon_i 2^i,$$

where $\varepsilon_i \in \{0,1\}$ for all $1 \le i \le k-4$. Let $r \ge -1$ the largest integer such that $\varepsilon_0,\dots,\varepsilon_r$ all are equal to 1 and $s = \sum\limits_{i=r+1}^{k-4} \varepsilon_i = \sum\limits_{i=r+2}^{k-4} \varepsilon_i$. (Due to the choice of r we have $\varepsilon_{r+1} = 0$.) Note that $r \le k-5$ since $l \le 2^{k-3}-2$. Thus, we have

$$d' = 2^{k-2}-2^{k-3}-\sum_{i=r+1}^{k-4} \varepsilon_i 2^i \;-\; 2^{r+1}$$

and

$$\begin{aligned} g_2(k-1,d') &= 2^{k-1}-\sum_{i=r+1}^{k-4} \varepsilon_i\left(2^{i+1}-1\right)-\left(2^{r+2}-1\right) \\ &= 2^{k-1}-s-2\cdot\sum_{i=r+1}^{k-4}\varepsilon_i 2^i-2\cdot\sum_{i=0}^{r}\varepsilon_i 2^i \;-\;1 \\ &= 2^{k-1}-s-1-2l \le 2^{k-1}-1-2l = n'. \end{aligned}$$

So, if $s \ge 1$ we can apply the Griesmer bound, see Theorem 2.9, to conclude that no codeword of weight w exists. If $s=0$, then we have $l \le 2^{k-4}-1$, so that $4 \le 2^{k-4} \le d' \le 2^{k-3}-2$ and we can apply the induction hypothesis to conclude that no codeword of weight w exists. Thus, the non-zero weights of $\mathcal{C}$ are contained in $\mathcal{W} = \{d, 2d\}$. Using $n = 2d+1$, $2^k-1 = 4d+7$, and $2^{k-1}-1 = 2d+3$ the first two MacWilliams identites read

$$\begin{aligned} A_d + A_{2d} &= 4d+7 \\ (d+1)A_d + A_{2d} &= (2d+1)(2d+3), \end{aligned}$$

so that

$$\begin{aligned} A_d &= 4d+4-\frac{1}{d} \\ A_{2d} &= 3+\frac{4}{d}. \end{aligned}$$

Since we have $d>1$ the count A_d is not an integer, which is a contradiction. □

While the the proof of Theorem is a bit technical the underlying idea is pretty simple. For all but the last entry of the specified range the one-step Griesmer argument gives a direct contradiction to the assumption that the Griesmer bound can be attained. In the last case, assuming an even weight code, the residual code argument eleminates all weights except d and $2d$ from where many ways lead to an easy contradiction. So looking at a specific numeric instance, it is very easy to conclude the non-existence of the code.

Also the "second gap" in the sequence of distances d with $n_2(k, d) = g_2(k, d)$ can be described in general.

THEOREM 3.5 ([147, Theorem 3.3])
If $2^{k-2} + 3 \le d \le 2^{k-1} - 2^{k-3} - 4$, *then* $n_2(k, d) \ge g_2(k, d) + 1$.

PROOF. We prove the statement by induction over the dimension k. Let d be an integer in the specified range, so that $k \ge 6$. Due to Lemma 3.3 we can assume $k \ge 7$. Using Corollary 1.20, it suffices to restrict our analysis to even values of d. Now, we assume that $\mathcal{C}$ is an even $[g_2(k, d), k, d]_2$ Griesmer code.

If $2^{k-2}+6 \le d \le 2^{k-1}-2^{k-3}-8$, then Lemma 2.4, applied to a codeword of weight d, yields the existence of a $\left[g_2(k-1, \lceil \frac{d}{2} \rceil), k-1, \ge \lceil \frac{d}{2} \rceil\right]_2$-Griesmer code, so that we can apply the induction hypothesis. It remains to exclude the three cases:

(a) $d = 2^{k-2} + 4$;

(b) $d = 2^{k-1} - 2^{k-3} - 6$;

(c) $d = 2^{k-1} - 2^{k-3} - 4$.

Since the argument is quite lengthy and involved we refer to [147] for the details. □

Note the range is empty if $k \le 5$. For $k = 6$ the values $d \in \{19, 20\}$ are affected and for $k = 7$ the excluded range is given by $\{35, 36, \dots, 44\}$. (We remark that [147, Theorem 3.3] contains a small typo for the lower bound and there even are two theorems numbered as 3.3.)

REMARK 3.6 In [147] the three special cases (a), (b), and (c) were excluded by first classifying three parametric classes of Griesmer codes and showing their uniqueness. E.g., for case (a) the uniqueness of the $\left[2^{k-1} + k, k, 2^{k-2} + 2\right]_2$-codes for $k \ge 6$ is used, see Exercise 3.1 for a construction. The residual code argument excludes quite some weights in case (a), see Exercise 3.2, and also the "large" weights can be excluded easily, see Exercise 3.2.

For $k = 7$ all distances d where $n_2(7, d) > g_2(7, d)$ are covered by Theorem 3.4 and Theorem 3.5. However, also the case $n_2(7, d) = g_2(7, d) + 2$ can occur, as we will see in the next four propositions.

PROPOSITION 3.7 ([149, Theorem 3.2])

$$n_2(7, 14) \ge g_2(7, 14) + 2 = 32.$$

PROOF. Assume that $\mathcal{C}$ is an even $[31,7,14]_2$-code. The residual code argument excludes the weights $w \in \{18,22,26\}$. From Lemma 1.22 we conclude that $\mathcal{C}$ is projective, i.e., we have $B_1 = B_2 = 0$. (Otherwise an $[29,6,\geq 14]_2$-code would exist, which is not the case.) Solving the first four MacWilliams identities for $\{A_{14}, A_{16}, A_{20}, B_3\}$ gives

$$\begin{aligned}
A_{14} &= 80 - \frac{8}{3}A_{24} - 8A_{28} - \frac{35}{3}A_{30},\\
A_{16} &= 19 + 5A_{24} + 14A_{28} + 20A_{30},\\
A_{20} &= 28 - \frac{10}{3}A_{24} - 7A_{28} - \frac{28}{3}A_{30},\\
B_3 &= 15 - \frac{10}{3}\cdot A_{24} - 14A_{28} - \frac{70}{3}\cdot A_{30}.
\end{aligned}$$

Since $B_3 \geq 0$ we have $A_{30} = 0$ and $A_{28} \leq 1$. If c is a codeword of weight 28, then $C^{\operatorname{supp}(c)}$ is a $[28,\leq 3,\{14,28\}]_2$-code and $\operatorname{Res}(\mathcal{C};c)$ is a $[3,\leq 3]_2$-code, so that Lemma 2.7 yields a contradiction. Thus, we have $A_{28} = 0$ and $B_3 \in \mathbb{N}_0$ implies $A_{24} \in \{0,3\}$. Assume $A_{24} = 3$ for a moment. If c, c' are two arbitrary codewords of weight 24, then $\#\left(\operatorname{supp}(c) \cap \operatorname{supp}(c')\right) = 17$, so that the sum of three codewords of weight 24 has weight at most $31 - 3\cdot(24-17) = 10$, which contradicts the minimum distance. Thus, we can assume that the weight distribution of $\mathcal{C}$ is given by $A_{14} = 80$, $A_{16} = 19$, and $A_{20} = 28$. Now let c be a specific codeword of weight 20. The weight enumerator of the possible 2-dimensional subcodes containing c and the weight of the corresponding residual codeword, with respect to c, are given by:

$1+2x^{14}+x^{20}$	4	$1+2x^{16}+x^{20}$	6	$1+x^{16}+2x^{20}$	8
$1+x^{14}+x^{16}+x^{20}$	5	$1+x^{14}+2x^{20}$	7	$1+3x^{20}$	10

Let (A'_i) be the weight distribution of the residual code $\operatorname{Res}(\mathcal{C};c)$. Counting codewords via the 2-dimensional subcodes containing c gives

$$\begin{aligned}
80 = A_{14} &= 2A'_4 + A'_5 + A'_7,\\
19 = A_{16} &= A'_5 + 2A'_6 + A'_8,\\
28 = A_{20} &= 1 + A'_7 + A'_8 + 2A'_{10}.
\end{aligned}$$

Additionally using the first three MacWilliams identities for $\operatorname{Res}(\mathcal{C};c)$ and solving for $\{A'_4, A'_5, A'_6, A'_{10}\}$ gives

$$\begin{aligned}
A'_4 &= -70 + 4A'_7 + 2A'_8,\\
A'_5 &= 220 - 9A'_7 - 4A'_8,\\
A'_6 &= -\frac{201}{2} + \frac{9}{2}A'_7 + \frac{3}{2}A'_8,\\
A'_{10} &= \frac{27}{2} - \frac{1}{2}A'_7 - \frac{1}{2}A'_8.
\end{aligned}$$

From $A'_4 \geq 0$ and $A'_{10} \geq 0$ we may conclude $A'_7 > 0$. However, if $A'_7 > 0$, then the residual code with respect to the codeword of weight 14 is a $[17,6,\geq 7]_2$-code, which contains a codeword of weight 13. Considering the corresponding residual code yields an $[4,5]_2$-code, which obviously cannot exist. Thus, we have $A'_7 = 0$ and $A'_4 \geq 0$ implies $A'_8 \geq 35$, so that A'_{10} would be negative, which is a contradiction. □

REMARK 3.8 In the proof of [149, Theorem 3.2], in different notation, $A'_8 = 0$ was shown by a direct argument. Our approach is actually an instance of the LP method based on the 2-dimensional subcodes, see Section 4.1 and especially Remark 4.1 for a detailed discussion.

PROPOSITION 3.9 ([149, Theorem 3.3])

$$n_2(7,16) \geq g_2(7,16) + 2 = 35.$$

PROPOSITION 3.10 ([148])

$$n_2(7,26) \geq g_2(7,26) + 2 = 56.$$

REMARK 3.11 In [149, Theorem 3.6] the result was mentioned, but due to a lengthy proof involving many adhoc arguments the reader was refered to [148]. The enumeration of all $[56,7,26]_2$-codes makes some trouble, see [25].

PROPOSITION 3.12 ([149, Theorem 3.7])

$$n_2(7,28) \geq g_2(7,28) + 2 = 59.$$

Summarizing the previously obtained lower bounds for $n_2(7,d)$ and taking the existence of attaining codes into account, we state:

THEOREM 3.13 (Length-optimal 7-dimensional binary codes)
For $d \geq 455$ we have $n_2(7,d) = g_2(7,d)$ and the other values are given by:

d	$n_2(7,d) - g_2(7,d)$	d	$n_2(7,d) - g_2(7,d)$	d	$n_2(7,d) - g_2(7,d)$
1–2	*0*	*17–24*	*1*	*31–34*	*0*
3–12	*1*	*25–28*	*2*	*35–44*	*1*
13–16	*2*	*29–30*	*1*		

Based on the work of many authors the determination of $n_2(8,d)$ was completed in [26]:

THEOREM 3.14 (Length-optimal 8-dimensional binary codes)
For $d \geq 105$ *we have* $n_2(8,d) = g_2(8,d)$ *and the other values are given by:*

d	$n_2(8,d) - g_2(8,d)$	d	$n_2(8,d) - g_2(8,d)$	d	$n_2(8,d) - g_2(8,d)$
1–2	*0*	*25–32*	*3*	*63–66*	*0*
3–8	*1*	*33–58*	*2*	*67–92*	*1*
9–20	*2*	*59–60*	*3*	*93–98*	*0*
21–24	*1*	*61–62*	*1*	*99–104*	*1*

The determination of $n_2(9,k)$ is still incomplete. A recent result is $n_2(9,20) = g_2(9,20) + 2 = 46$ with a unique attaining code, see [109].

EXERCISE 3.1 Show for $k \geq 3$, $s \in \mathbb{N}$, and $1 \leq d \leq sq^{k-2}$ the existence of an

$$\left[sq^{k-1} + n_q(k-1,d), k, sq^{k-2}(q-1) + d\right]_q\text{-code.}$$

Construct a $\left[2^{k-1} + k, k, 2^{k-2} + 2\right]_2$-code for each $k \geq 3$.
Hint: Consider the Reed-Muller code $\mathrm{RM}_q(k-1,1)$ from the geometric point of view.

EXERCISE 3.2 Let $\mathcal{C}$ be a projective even $[2d + k - 5, k, d]_2$-code without codewords of weight $d + 2$, where $d = 2^{k-2} + 4$ and $k \geq 6$. Show that $\mathcal{C}$ does not contain codewords of weight at least $2d$.

EXERCISE 3.3 For $k \geq 7$ let $d = 2^{k-2} + 4$. Use the residual code argument to exclude as many weights as possible in an even $[g_2((k,d),k,d]_2$-code $\mathcal{C}$. Especially show that weight $d + 2$ cannot occur and give an explicit list for $k = 7$.

4. Enhancing the linear programming method and variants

In this chapter we want to consider variants of “the” linear programming method. Actually, the general underlying idea behind the integer linear programming method is to count some objects using variables $x_i \in \mathbb{N}_0$ and relate them by linear equations or constraints. If the corresponding ILP has an empty solution set, then the described combinatorial object does not exist. In some cases we only can ensure that our variables are non-negative, which still leaves us the possibility to apply linear programming. So, while there is no general linear programming method, e.g. each association scheme comes with a natural linear programming formulation, see e.g. [41]. Even in the case where the constraints are not all linear similar methods from optimization can be applied. Here we mention semi-definite programming and refer the interested reader e.g. to [8, 9, 10].

In this chapter we consider a linear programming method based on 2-dimensional subcodes, see Section 4.1, and the partition weight enumerator where the coordinates are partitioned into subsets, see Section 4.2. In the extreme case where each coordinate forms its own set this yields an exact ILP formulation for arcs. There are also several ways how to enhance an (integer) linear programming formulation by additional constraints using theoretic insights. As an example we mention a few classification results for linear codes in Section 4.3.

4.1 The linear programming method based on 2-dimensional subcodes

The linear programming method based on the MacWilliams identities uses counting variables A_i for the number of codewords of weight i in an $[n,k]_q$-code $\mathcal{C}$. The non-negativity (and the integrality) of the corresponding B_i in the weight distribution of the dual code then gives some restrictions for the A_i. Each non-zero codeword $c \in \mathcal{C}$ spans a 1-dimensional subcode $\langle c\rangle$ with $q-1$ codewords of weight $\operatorname{wt}(c)$ and the zero codeword. These 1-dimensional subcodes partition the non-zero codewords in $\mathcal{C}$ and the number $\frac{A_i}{q-1}$ counts the 1-dimension subcodes $\mathcal{C}'$ with weight enumerator $W_{\mathcal{C}}(x) = 1 + (q-1)x^i$. This reformulation allows straightforward generalizations. Instead of 1-dimensional subcodes we may consider 2-dimensional subcodes. If we want to have a similar kind of partition property, then we have to fix a non-zero codeword $c \in \mathcal{C}$. With this, the set of all 2-dimensional subcodes of $\mathcal{C}$ that contain the codeword c partition the set of codewords in $\mathcal{C}\backslash\langle c\rangle$. Geometrically this corresponds to the fact that for a given hyperplane H every hyperplane $H' \neq H$ intersects H in a unique hyperline S. So, having fixed the codeword c, we call $(w_1, \dots, w_q)$, where $w_1 \le \dots \le w_q$, the weight-type of a 2-dimensional subcode $\mathcal{C}'$ of $\mathcal{C}$ containing the codeword c if

$$W_{\mathcal{C}'}(x) = 1 + (q-1)x^{\operatorname{wt}(c)} + \sum_{i=1}^{q} (q-1)x^{w_i}. \tag{4.1}$$

By $\mathcal{T}_c$ (or $\mathcal{T}_{\operatorname{wt}(c)}$) we denote the set of admissible weight-types, generalizing the set $\mathcal{W}$ of admissible non-zero weights. For an $[31,7]_2$-code $\mathcal{C}$ with $\mathcal{W} = \{14,16,20\}$ and a codeword c of weight 20 we have

$$\mathcal{T}_c = \mathcal{T}_{20} = \Big\{(14,14),(14,16),(16,16),(14,20),(16,20),(20,20)\Big\}. \qquad (4.2)$$

If $x_t \in \mathbb{N}_0$ counts the number of occurrences of weight-type $t \in \mathcal{T}$, then the weight distribution (A_i) of $\mathcal{C}$ is given by

$$A_w = \sum_{t=(w_1,\dots,w_q)\in\mathcal{T}_c} x_t \cdot (q-1) \cdot \#\{1 \le i \le q \,:\, w_i = w\} \qquad (4.3)$$

for all $w \in \mathcal{W}\backslash\operatorname{wt}(c)$ and

$$A_w = (q-1) + \sum_{t=(w_1,\dots,w_q)\in\mathcal{T}_c} x_t \cdot (q-1) \cdot \#\{1 \le i \le q \,:\, w_i = w\} \qquad (4.4)$$

for $w = \operatorname{wt}(c)$. Let the residual code $\operatorname{Res}(\mathcal{C},c)$ with respect to c be an $[n-\operatorname{wt}(c),k']_q$-code and (A'_i) its weight distribution. Noting that the codewords c' in the residual code $\operatorname{Res}(\mathcal{C}';c)$ have weight

$$\operatorname{wt}(c') = \frac{\sum\limits_{i=1}^{q} w_i \;-\; \operatorname{wt}(c)}{q},$$

where $\mathcal{C}'$ is a 2-dimensional subcode of $\mathcal{C}$ containing c of weight-type $(w_1,\dots,w_q)$, we have

$$q^{k-k'} \cdot A'_i = q^{k-k'} \cdot A_i(\operatorname{Res}(\mathcal{C};c)) = \sum_{t=(w_1,\dots,w_q)\in\mathcal{T}\,:\,\left(\sum_{i=1}^q w_i - \operatorname{wt}(c) = iq\right)} q(q-1)\cdot x_t \qquad (4.5)$$

for $i \in \mathbb{N}$ and

$$q^{k-k'} - q = \sum_{t=(w_1,\dots,w_q)\in\mathcal{T}\,:\,\left(\sum_{i=1}^q w_i = \operatorname{wt}(c)\right)} q(q-1)\cdot x_t. \qquad (4.6)$$

For the A_i and the A'_i we can use the corresponding MacWilliams identities and obtain a variant of the (I)LP method, since we have a set of constraints for a set of non-negative (integer) variables. We call this the (I)LP method based on 2-dimensional subcodes. Of course there a several degrees of freedom which need to be specified in a concrete usage. To avoid misunderstandings, we also speak of the (I)LP method based on 1-dimensional subcodes referring to our initial approach of Section 1.4 or the equivalent reformulation stated at the beginning of this section.

In some situation the weight distribution (A_i) of $\mathcal{C}$ is given, see e.g. the proof of Proposition 3.7, where $A_{14} = 80$, $A_{16} = 19$, and $A_{20} = 28$.

Of course we can use different techniques to further restrict the set $\mathcal{T}_c$ of admissible weight-types, as we also use e.g. the residual code argument to restrict the set $\mathcal{W}$ of feasible non-zero weights. In the proof of Proposition 3.7 the weight-type $(14,20)$ is excluded, so that the LP method yields an empty polyhedron. (Note that the counting variables x_t do not explicitly occur in the proof of Proposition 3.7, since for each possible non-zero weight in the residual code there is a a unique weight-type.)

REMARK 4.1 In the process of finding a non-existence proof for a linear code with certain parameters, one can utilize the LP method based on 2-dimensional subcodes by first starting with some set $\mathcal{W}$ of admissible weights. In the example of Proposition 3.7 we have $\mathcal{W} = \{14, 16, 20\}$. One can try to further restrict $\mathcal{W}$ by applying the LP method based on 2-dimensional subcodes for a codeword of weight $w \in \mathcal{W}$ and start with some initial set $\mathcal{T}_w$. In our example we choose $w = 20$ and $\mathcal{T}_w$ as specified in Equation (4.2). If maximizing x_t yields a target value strictly smaller than one, then we can remove the weight-type t from $\mathcal{T}_w$. If minimizing x_t yields a target value strictly larger than 0, which is the case in our example for $t = (14, 20)$, then excluding weight-type t by some separate argument allows us to remove w from $\mathcal{W}$. In our example we end up with $\mathcal{W} = \{14, 16\}$, which is infeasible (for the "original" LP method based on 1-dimensional subcodes, see Section 1.4). Note that we have already used these techniques to ensure or exclude weights, see Section 1.4.

Of course, the above approach can also be formulated in the geometric language. So, let $\mathcal{K}$ be an (n, s)-arc in $\mathrm{PG}(k-1, q)$ and H be an arbitrary but fixed hyperplane. Let (a'_i) be the spectrum of the restriction $\mathcal{K}|_H$ to the hyperplane H. For each hyperline S in $\mathrm{PG}(k-1, q)$ that is contained H, i.e., a hyperplane of H, let $H_0^S, \dots, H_q^S$ denote the $q+1$ hyperplanes containing S, where we assume $H_0^S = H$ w.l.o.g. Counting points gives

$$\#\mathcal{K} = \sum_{i=0}^{q} \mathcal{K}\big(H_i^S\big) \; - \; q\mathcal{K}(S).$$

We say that S has type $(m_1, \dots, m_q)$ (with respect to H), where $m_1 \le \dots \le m_q$ and $m_j = \mathcal{K}\Big(H_{\pi(j)}^S\Big)$ for all $1 \le j \le q$ and a bijection π on $\{1, \dots, q\}$. In other words, $(m_1, \dots, m_q)$ is just the sorted vector of the multiplicities of the hyperplanes through S except H. With this, we have

$$\mathcal{K}(S) = \frac{\mathcal{K}(H) + \sum\limits_{i=1}^{q} \mathcal{K}\big(H_i^S\big) \; - \; \#\mathcal{K}}{q} = \frac{\mathcal{K}(H) + \sum\limits_{i=1}^{q} m_i \; - \; \#\mathcal{K}}{q}. \tag{4.7}$$

By $\mathcal{T}_H$ (or $\mathcal{T}_{\mathcal{K}(H)}$) we denote a set of admissible types and by $x_t \in \mathbb{N}_0$ the number of occurrences of hyperlines S, that are contained in H, of type $t \in \mathcal{T}_H$. Counting gives

$$a_i = \sum_{t=(m_1,\dots,m_q)\in\mathcal{T}_H} x_t \cdot \#\left\{1 \le j \le q \,:\, m_j = i\right\} \tag{4.8}$$

for all $i \in \mathbb{N}_0 \backslash \{\mathcal{K}(H)\}$ and

$$a_i = 1 + \sum_{t=(m_1,\dots,m_q)\in\mathcal{T}_H} x_t \cdot \#\left\{1 \le j \le q \,:\, m_j = i\right\} \tag{4.9}$$

for $i = \mathcal{K}(H)$. The only difference to the situation for linear codes is the factor $q-1$, which goes in line with the fact that hyperplanes correspond to $q-1$ codewords. For the spectrum (a'_i) of the restricted arc $\mathcal{K}|_H$ we obtain

$$a'_i = \sum_{t=(m_1,\dots,m_q)\in\mathcal{T}_H \,:\, \mathcal{K}(H)+\sum\limits_{j=1}^{q} m_j \,-\, \#\mathcal{K}=iq} x_t \tag{4.10}$$

for all $i \in \mathbb{N}_0$. Note that the scaling factor, that occured in the case of linear codes, is hidden in the spectrum (a'_i), i.e., if $\mathcal{K}|_H$ is not spanning than all a'_i are divisible by a suitable power of q. Moreover, no case differentiation is necessary, since the zero codeword does not correspond to a hyperplane.

EXAMPLE 4.2 We want to apply the above technique in order to show that no $(12, \le 3)$-arc in $\mathrm{PG}(2,5)$ exists. Assume, to the contrary, that $\mathcal{K}$ is a $(12, \le 3)$-arc in $\mathrm{PG}(2,5)$. Applying Lemma 2.1 for $0 \le m \le 3$ yields that $\mathcal{K}$ is projective, i.e., $\mathcal{K}(P) \in \{0,1\}$ for all $P \in \mathcal{P}$. Moreover, in each 1-line each point has a maximum multiplicity of at most 0, which is absurd. Thus, we have $a_1 = 0$. Consider a 2-line H. Since $\mathcal{K}$ is projective the spectrum of $\mathcal{K}|_H$ is given by $a'_0 = 4$, $a'_1 = 2$. The possible types are given by

$$\mathcal{T}_H = \Big\{(3,3,3,3,3),(2,2,2,2,2),(0,2,2,3,3)\Big\}.$$

From Equation (4.10) we conclude

$$\begin{aligned} 4 = a'_0 &= x_{(2,2,2,2,2)} + x_{(0,2,2,3,3)}, \\ 2 = a'_1 &= x_{(3,3,3,3,3)} \end{aligned}$$

and equations (4.8)-4.9) give

$$\begin{aligned} a_0 &= x_{(0,2,2,3,3)}, \\ a_2 &= 1 + 5x_{(2,2,2,2,2)} + 2x_{(0,2,2,3,3)}, \\ a_3 &= 2x_{(0,2,2,3,3)} + 5x_{(3,3,3,3,3)}, \end{aligned}$$

so that $a_3 \le 2 \cdot 4 + 5 \cdot 2 = 18$. However, the standard equations for $\mathcal{K}$ imply $a_0 = 5$, $a_2 = 6$, and $a_3 = 20 > 18$. Framed differently, $x_{(2,2,2,2,2)}$ has to be strictly negative. (In our case, there is a unique solution of the linear equation system consisting of the standard equations and the above five equations including the x_t: $x_{(2,2,2,2,2)} = -1$, $x_{(0,2,2,3,3)} = 5$, $x_{(3,3,3,3,3)} = 2$, $a'_0 = 4$, $a'_1 = 2$, $a_0 = 5$, $a_2 = 6$, and $a_3 = 20$.) Note that we have $a_2 > 0$. Otherwise the above contradiction would only imply that there is no 2-line. ◇

In general the number of possible types, and so the number of variables x_t, can become quite large. So, we want to conclude a more handy necessary criterion for the existence of arcs from the described technique. The starting point are the standard equations for the arc $\mathcal{K}$.

COROLLARY 4.3

The spectrum (a_i) of an (n,s)-arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ with $\lambda_j = \#\{P \in \mathcal{P} : \mathcal{K}(P) = j\}$ satisfies

$$\sum_{H\in\mathcal{H}} \binom{s-\mathcal{K}(H)}{2} = \binom{s}{2} \cdot [k]_q - n(s-1)\cdot[k-1]_q + \binom{n}{2}\cdot[k-2]_q + q^{k-2}\cdot\sum_{i\ge 2}\binom{i}{2}\lambda_i. \qquad (4.11)$$

PROOF. From Lemma 1.5 we conclude

$$\sum_{i=0}^{s} \binom{s-i}{2} = a_i\binom{s}{2} \cdot [k]_q - n(s-1)\cdot[k-1]_q + \binom{n}{2}\cdot[k-2]_q + q^{k-2}\cdot\sum_{i\ge 2}\binom{i}{2}\lambda_i$$

and replace the left-hand side by $\sum_{H\in\mathcal{H}}\binom{s-\mathcal{K}(H)}{2}$. □

Our next aim to upper bound the left-hand side of Equation (4.11) in terms of some structural information.

DEFINITION 4.4

Let $\mathcal{K}$ be an (n,s)-arc in $\mathrm{PG}(k-1,q)$, where $k \ge 3$, and H_0 a hyperplane: For each hyperline S (i.e., a subspace of co-dimension 2) contained in H_0 let $H_1^S,\dots,H_q^S$ denote the other q hyperplanes through S. With this we set

$$\eta_i(H_0) = \max_{S\,:\,\mathcal{K}(S)=i, S\le H_0, \dim(S)=k-2} \sum_{h=1}^{q} \binom{s-\mathcal{K}(H_h^S)}{2}. \tag{4.12}$$

If here exists no hyperlines S with $\mathcal{K}(S)=i$, then we set $\eta_i(H_0)=0$. We abbreviate $\eta_i(H_0)$ as η_i whenever the hyperplane H_0 is clear from the context.

LEMMA 4.5

Let $\mathcal{K}$ be an (n,s)-arc in $\mathrm{PG}(k-1,q)$, where $k\ge 3$, H_0 be a hyperplane, (a_i') be the spectrum of the restriction $\mathcal{K}|_{H_0}$, and $\widehat{\eta}_i$ some numbers satisfying $\eta_i \le \widehat{\eta}_i$ for all $i\in\mathbb{N}_0$. Then, we have

$$\begin{aligned}\sum_i a_i'\widehat{\eta}_i + \binom{s-\mathcal{K}(H_0)}{2} \;&\ge\; \binom{s}{2}\cdot[k]_q - n(s-1)\cdot[k-1]_q + \binom{n}{2}\cdot[k-2]_q + q^{k-2}\cdot\sum_{i\ge 2}\binom{i}{2}\lambda_i \\ &\ge\; \binom{s}{2}\cdot[k]_q - n(s-1)\cdot[k-1]_q + \binom{n}{2}\cdot[k-2]_q, \end{aligned}\tag{4.13}$$

where $\lambda_j = \#\{P\in\mathcal{P} : \mathcal{K}(P)=j\}$.

PROOF. We have

$$\sum_{H\in\mathcal{H}} \binom{s-\mathcal{K}(H)}{2} \le \sum_i a_i'\cdot\widehat{\eta}_i + \binom{s-\mathcal{K}(H_0)}{2}, \tag{4.14}$$

so that Equation (4.11) implies the first inequality. The second inequality follows from $\lambda_i \ge 0$. □

Note that the right-hand side of Inequality (4.13) depends only on the parameters of $\mathcal{K}$. Given a set $\mathcal{T}_{H_0}$ of admissible types, we can easily compute $\widehat{\eta}_i$ by taking the maximum of $\sum_{h=1}^{q}\binom{s-m_h}{2}$ over all types $t=(m_1,\dots,m_q)\in\mathcal{T}_H$ with $\mathcal{K}(H_0)+\sum_{h=1}^{q} m_h - \#\mathcal{K} = iq$. In Example 4.2 we compute $\widehat{\eta}_0=3$ and $\widehat{\eta}_1=0$, so that

$$\sum_i a_i'\widehat{\eta}_i + \binom{s-\mathcal{K}(H_0)}{2} = 4\cdot 3 + 2\cdot 0 + 0 = 12$$

and

$$\binom{s}{2}\cdot[k]_q - n(s-1)\cdot[k-1]_q + \binom{n}{2}\cdot[k-2]_q = 3\cdot 31 - 12\cdot 2\cdot 6 + 66\cdot 2 = 15$$

give a contradiction. Note that the last inequality in (4.13) is satisfied with equality iff $\mathcal{K}$ is projective, i.e., if $\mathcal{K}(P)\in\{0,1\}$ for all points $P\in\mathcal{P}$.

EXERCISE 4.1 Show that no $(5s-3,s)$-arc exists in $\mathrm{PG}(2,5)$ for $1\le s\le 4$.

EXERCISE 4.2 Show that a $(104,22)$-arc in $\mathrm{PG}(3,5)$, which does not contain a 16-plane or a 17-plane, cannot contain a 0-plane.

4.2 Partition weight enumerator

The weight enumerator of a linear $[n,k]_q$ code $\mathcal{C}$ can be refined to a so-called partition weight enumerator, see e.g. [142, 85] To this end let $r \ge 1$ be an integer and $\cup_{j=1}^{r} P_j$ be a partition of the coordinates $\{1,\dots,n\}$. By $I = (i_1,\dots,i_r)$ we denote a multi-index, where $0 \le i_j \le p_j$ and $p_j = \#P_j$ for all $1 \le j \le r$. With this, $a_I \in \mathbb{N}_0$ denotes the number of codewords c such that $\#\left\{h \in P_j \,:\, c_h \neq 0\right\} = i_j$ for all $1 \le j \le r$, which generalizes the notion of the counts a_i. By $a_I^* \in \mathbb{N}_0$ we denote the corresponding counts for the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$. The generalized relation between the a_I^* and the a_I is given by:

$$\begin{aligned}&\sum_{I=(i_1,\dots,i_r)} a_I^* \prod_{j=1^r} z_j^{i_j}\\ =\ & \frac{1}{2^k} \cdot \sum_{I=(i_1,\dots,i_r)} a_I \prod_{j=1}^{r} \left(1+z_j\right)^{n-i_j} \left(1-z_j\right)^{i_j} \qquad (4.15)\end{aligned}$$

The partition weight enumerator with respect to a codeword c is given by Equation (4.15), where we choose $r = 2$, $P_2 = \operatorname{supp}(c)$, and $P_1 = \{1,\dots,n\}\backslash P_2$, so that restricting to the coordinates in P_1 gives the residual code. The case $r = 1$ corresponds to the usual (integer) linear programming method based on the MacWilliams identities, see Section 1.4. In the extreme case $r = n$ each coordinate forms its own set.

Based on the geometric representation of linear codes as arcs we can also state an exact ILP formulation. To this end, let $\mathcal{P}$ denote the set of points in $\operatorname{PG}(k-1,q)$ and $\mathcal{H}$ denote the set of hyperplanes. An $(n,\le s)$-arc $\mathcal{K}$ in $\operatorname{PG}(k-1,q)$ is modeled by non-negative integer variables x_P for all $P \in \mathcal{P}$. With this the cardinality $\#\mathcal{K}$ is given by

$$n = \sum_{P\in\mathcal{P}} x_P \qquad (4.16)$$

and the condition on the species s can be ensured by

$$\sum_{P\in\mathcal{P}\cap H} x_P \le s \qquad (4.17)$$

for each hyperplane $H \in \mathcal{H}$. If we choose fixed values for n and s, then the question is if there exists a feasible solution. We may also maximize n for a given value of n or minimize s for a given value of s. For blocking sets we have just to change the direction of the inequalities in (4.17). If we are interested in Δ-divisible arcs we can replace (4.17) by

$$\sum_{P\in\mathcal{P}\cap H} x_P = n - \Delta y_H, \qquad (4.18)$$

where $y_H \in \mathbb{N}_0$ for all $H \in \mathcal{H}$. Lower and upper bounds for the occurring weights can be formulated directly as lower and upper bounds for y_H. The ILP approach is very flexible so that nearly any condition can be modeled by introducing further integer or binary variables, see e.g. Exercise 4.3.

Since each point is contained in $[k-1]_q$ hyperplanes, summing Inequality (4.17) over all hyperplanes $H \in \mathcal{H}$ gives $[k-1]_q n \le [k-1]_q s$, so that $[k]_q(n-s) \le \left([k]_q - [k-1]_q\right) n = q^{k-1}n$, which is equivalent to

$$n \ge \frac{q^k-1}{(q-1)q^{k-1}} \cdot d \qquad (4.19)$$

for the length of an $[n, k, \geq d]_q$-code. This bound is tight if d is divisible by q^{k-1} and can be obtained from the Griesmer bound by ignoring the ceilings.

EXERCISE 4.3 Formulate an ILP model for an $(n, \leq s)$-arc $\mathcal{K}$ in $\operatorname{PG}(k-1, q)$ such that either $\mathcal{K}(H) = s$ or $\mathcal{K}(H) \leq s'$ for all hyperplanes H.

4.3 Classification of linear codes

PROPOSITION 4.6

Let $\mathcal{K}$ be an $(n, \leq s)$-arc in $\operatorname{PG}(k-1, q)$ such that every hyperplane $H \in \mathcal{H}$ has multiplicity $\mathcal{K}(H) = s$. Then, there exists an integer t such that $n = t[k]_q$ and $\mathcal{K}(P) = t$ for all $P \in \mathcal{P}$. If $k \geq 2$, then we additionally have $s = t[k-1]_q$.

PROOF. If $k = 1$, then we can choose $t = n$. The unique point P then satisfies $\mathcal{K}(P) = \#\mathcal{K} = n = t$. Since there is no hyperplane at all, s can be chosen arbitrarily.

Now assume $k \geq 2$. Using the standard equations from Lemma 1.5 we will first determine the spectrum (a_i) of $\mathcal{K}$. From Equation (1.25) we conclude $a_2 = [k]_q$, so that Equation (1.26) gives $s[k]_q = n[k-1]_q$. If $k = 2$, then we have $\mathcal{K}(P) = s = t[k-1]_q = t$ for every point $P \in \mathcal{P}$ since every hyperplane is a point for $k = 2$. For $k \geq 3$ let P be an arbitrary but fix point and $H_1, \dots, H_l$ be the $l := [k-1]_q$ hyperplanes through P. From

$$\begin{aligned}
&(t[k]_q - \mathcal{K}(P))[k-2]_q = (n - \mathcal{K}(P))[k-2]_q = (\#\mathcal{K} - \mathcal{K}(P))\,[k-2]_q \\
= &\sum_{i=1}^{l} (\mathcal{K}(H_i) - \mathcal{K}(P)) = l(s - \mathcal{K}(P)) = [k-1]_q(t[k-1]_q - \mathcal{K}(P))
\end{aligned}$$

we deduce

$$\begin{aligned}
q^{k-2}\mathcal{K}(P) &= t \cdot ([k-1]_q[k-1]_q - [k]_q[k-2]_q) \\
&= t \cdot ([k-1]_q\,(q[k-2]_q + 1) - (q[k-1]_q + 1)\,[k-2]_q) \\
&= t \cdot ([k-1]_q - [k-2]_q) = q^{k-2}t,
\end{aligned}$$

so that $\mathcal{K}(P) = t$. □

EXERCISE 4.4 Let $k \geq 2$ and $\ell \geq 0$ be integers and $\mathcal{C}$ be a $\left[2^{k-1} + \ell\left(2^k - 1\right), k, (2\ell+1)2^{k-2}\right]_2$-code and $\mathcal{K}$ be the corresponding arc in $\operatorname{PG}(k-1, 2)$. Show that $\mathcal{K}(P) \in \{\ell, \ell+1\}$ for the point multiplicity of every point $P \in \mathcal{P}$. Determine the geometric structure of the points with multiplicity ℓ.

5. Lengths of divisible codes

In this chapter we will consider the possible effective lengths of q^r-divisible linear codes. As an application we might consider the following question: Can we pack 20 solids, i.e., 4-spaces, and 30 planes in $\mathbb{F}_2^9$ so that their pairwise intersection is trivial? Counting the points gives

$$\begin{bmatrix}9\\1\end{bmatrix}_2 - 20 \cdot \begin{bmatrix}4\\1\end{bmatrix}_2 - 30 \cdot \begin{bmatrix}3\\1\end{bmatrix}_2 = 1 > 0,$$

so that we do not obtain a direct contradiction. However, it will turn out that the non-existence of a 2^2-divisible binary linear code of effective length 1 implies the non-existence of such a configuration of planes and solids. Mainly based on [90] we will completely characterize the possible effective lengths of q^r-divisible linear codes over $\mathbb{F}_q$ for every positive integer r.

The so-called divisible code bound, see e.g. [151, 153], gives an upper bound on the dimension of a divisible code. Here we focus on the lengths of q^r-divisible $\mathbb{F}_q$-linear codes, without any restriction on the dimension. As the length of a divisible code can always be increased by adding an arbitrary number of all-zero coordinates, it is natural to look at the effective length. So, in order to ease the notation, whenever we speak of the length of a code in this chapter, then we refer to the effective length. A multiset $\mathcal{M}$ of points in $\operatorname{PG}(v-1,q)$ is called Δ-divisible if the corresponding linear code is Δ-divisible. In [152, Theorem 1] it was shown that for $\Delta = p^e t$, where p is the characteristic of the base field $\mathbb{F}_q$, $e \in \mathbb{N}_0$, and p is comprime to $t \in \mathbb{N}$, each full-length Δ-divisible $\mathbb{F}_q$-linear code is the t-fold repetition of a p^e-divisible $\mathbb{F}_q$-linear code. So, it is sufficient to study q^r-divisible codes where $r \in \mathbb{Q}_{\ge 0}$ such that $q^r = p^e$ for some integer e. Note that in some cases we restrict to $r \in \mathbb{N}_0$. As a shorthand, a q^r-divisible code will always be a q^r-divisible linear code over $\mathbb{F}_q$. The conditions for a q^r-divisible multiset $\mathcal{M}$ of points in $\operatorname{PG}(v-1,q)$ are equivalent to $\#\mathcal{M} \equiv \mathcal{M}(H) \pmod{q^r}$ for every hyperplane H if $v \ge 2$ and to $\#\mathcal{M} \equiv 0 \pmod{q^r}$ if $v = 1$. For every subspace U and every multiset of points $\mathcal{M}$ we also write $\mathcal{M} \cap U$ for the restriction of $\mathcal{M}$ to U, i.e., $(\mathcal{M} \cap U)(P) = \mathcal{M}(P)$ and 0 otherwise. With this, the above condition can also be written as $\#\mathcal{M} \equiv \#(\mathcal{M} \cap H) \pmod{q^r}$ for all $H \in \mathcal{H}$. Note that a q^r-divisible multiset $\mathcal{M}$ of points is $q^{r'}$-divisible for all $0 \le r' \le r$. We also use the notation $\mathcal{M}_1 + \mathcal{M}_2$ and $\lambda \cdot \mathcal{M}$ for the sum of two multisets of points $\mathcal{M}_1, \mathcal{M}_2$ and the λ-fold repetition of a multiset of points $\mathcal{M}$. More precisely, we have $(\mathcal{M}_1 + \mathcal{M}_2)(P) = \mathcal{M}_1(P) + \mathcal{M}_2(P)$ and $(\lambda \cdot \mathcal{M})(P) = \lambda \cdot \mathcal{M}(P)$ for all $P \in \mathcal{P}$. Here, we do not require $\lambda \in \mathbb{N}$ but only that the values $\mathcal{M}(P)$ of a multiset of points are non-negative integers. Intermediate results in a more complicated expression defining a multiset of points may be fractional or negative. If we speak of a q^r-divisible multiset $\mathcal{M}$ of points without specifying the ambient space V or its dimension v, then we assume that the points in $\mathcal{M}$ are contained in an ambient space V of a suitably large finite dimension v. This is justified by the following lemma.

LEMMA 5.1

Let $V_1 < V_2$ be $\mathbb{F}_q$-vector spaces and $\mathcal{M}$ a multiset of points in V_1. Then $\mathcal{M}$ is q^r-divisible in V_1 if and *only if $\mathcal{M}$ is q^r-divisible in V_2 (using the natural continuation of the characteristic function $\mathcal{M}(P) = 0$ for all $P \in V_2 \backslash V_1$).*

Proof. Assume that $\mathcal{M}$ is q^r-divisible in V_1. Let H be a hyperplane of V_2. Then $\#(\mathcal{M} \cap H) = \#(\mathcal{M} \cap (H \cap V_1))$, where $H \cap V_1$ is either V_1 or a hyperplane in V_1. In the first case, the expression equals $\#\mathcal{M}$, and in the second case, it is congruent to $\#\mathcal{M} \pmod{q^r}$ by q^r-divisibility of $\mathcal{M}$ in V_1.

Now assume that $\mathcal{M}$ is q^r-divisible in V_2, and let H' be a hyperplane of V_1. There is a hyperplane H in V_2 such that $H \cap V_1 = H'$. So $\#(\mathcal{M} \cap H') = \#(\mathcal{M} \cap H) \equiv \#\mathcal{M} \pmod{q^r}$ by q^r-divisibility of $\mathcal{M}$ in V_2. □

There are a few very basic constructions for q^r-divisible multisets of points:

Lemma 5.2

(i) Let U be a q-vector space of dimension $k \geq 1$. The set $\begin{bmatrix} U \\ 1 \end{bmatrix}$ of $[k]_q$ points contained in U is q^{k-1}-divisible.

(ii) For q^r-divisible multisets $\mathcal{M}$ and $\mathcal{M}'$ in V, the sum (or multiset union) $\mathcal{M} + \mathcal{M}'$ is q^r-divisible.

(iii) The q-fold repetition of a q^r-divisible multiset $\mathcal{M}$ is q^{r+1}-divisible.

Proof. For part (i), we take the ambient space $V = U$. Let H be a hyperplane of V. Then $U \cap H$ is a $(k-1)$-space and therefore

$$\#(\begin{bmatrix} U \\ 1 \end{bmatrix} \cap H) = [k-1]_q \equiv [k]_q = \#\begin{bmatrix} U \\ 1 \end{bmatrix} \pmod{q^{k-1}}.$$

Parts (ii) and (iii) are clear from looking at the characteristic functions. □

A subspace $U \leq V$ is commonly identified with the set $\begin{bmatrix} U \\ 1 \end{bmatrix}$ of points covered by U. With that identification, Lemma 5.2(i) simply states that every k-subspace is q^{k-1}-divisible. The corresponding linear code is the q-ary simplex code of dimension k. In the case $\langle \mathcal{M} \rangle_{\mathbb{F}_q} \cap \langle \mathcal{M}' \rangle_{\mathbb{F}_q} = \{\mathbf{0}\}$, the multiset union in Lemma 5.2(ii) corresponds to the direct sum of linear codes, and in the case $\langle \mathcal{M} \rangle_{\mathbb{F}_q} = \langle \mathcal{M}' \rangle_{\mathbb{F}_q}$ it corresponds to the juxtaposition. The construction in Lemma 5.2(iii) corresponds to the q-fold repetition of a linear code.

Note that for a multiset of points $\mathcal{M}_1$ in V_1 and a multiset of points $\mathcal{M}_2$ in V_2 we can consider their embeddings $\mathcal{M}_1', \mathcal{M}_2'$ in $V_1 \times V_2$ and consider the sum $\mathcal{M}_1' + \mathcal{M}_2'$ in the ambient space $V_1 \times V_2$. Applying Lemma 5.2(ii) we have:

Lemma 5.3

The set of possible cardinalities of q^r-divisible multisets of points is closed under addition.

For each integer r and each dimension $1 \le i \le r+1$ the q^{r+1-i}-fold repetition of an i-space is a q^r-divisible multiset of cardinality $q^{r+1-i} \cdot [i]_q$. So, for a fixed prime power q, a non-negative integer r and $i \in \{0, \ldots, r\}$, we define

$$s_q(r,i) := q^i \cdot [r-i+1]_q = \frac{q^{r+1}-q^i}{q-1} = \sum_{j=i}^{r} q^j = q^i + q^{i+1} + \ldots + q^r \tag{5.1}$$

and state:

Lemma 5.4

For each $r \in \mathbb{N}_0$ and each $i \in \{0, \ldots, r\}$ there is a q^r-divisible multiset of points of cardinality $s_q(r,i)$.

As a consequence of Lemma 5.3 and Lemma 5.4 all $n = \sum_{i=0}^{r} a_i s_q(r,i)$ with $a_i \in \mathbb{N}_0$ are realizable cardinalities of q^r-divisible multisets of points. Later on we will prove that these integers are indeed the only possibilities. As $s_q(r,r) = q^r$ and $s_q(r,0) = 1 + q + q^2 + \ldots + q^r$ are coprime, for fixed q and r there is only a finite set of cardinalities which is not realizable as a q^r-divisible multiset. Note that the number $s_q(r,i)$ is divisible by q^i, but not by q^{i+1}. This property allows us to create kind of a positional system upon the sequence of base numbers

$$S_q(r) := (s_q(r,0), s_q(r,1), \ldots, s_q(r,r)).$$

Our next aim is to show that each integer n has a unique $S_q(r)$-adic expansion

$$n = \sum_{i=0}^{r} a_i s_q(r,i) \tag{5.2}$$

with $a_0, \ldots, a_{r-1} \in \{0, \ldots, q-1\}$ and leading coefficient $a_r \in \mathbb{Z}$. The idea is to consider Equation (5.2) modulo $q, q^2, \ldots, q^r$ which gradually determines $a_0, a_1, \ldots, a_{r-1} \in \{0, \ldots, q-1\}$, using that $s_q(r,i)$ is divisible by q^i, but not by q^{i+1}. For the existence part, we give an algorithm that computes the $S_q(r)$-adic expansion.

Algorithm 5.5

```
Input: $n \in \mathbb{Z}$, field size $q$, exponent $r \in \mathbb{N}_0$
Output: representation $n = \sum_{i=0}^{r} a_i s_q(r,i)$ with $a_0, \ldots, a_{r-1} \in \{0, \ldots, q-1\}$ and $a_r \in \mathbb{Z}$
$m \leftarrow n$
For $i \leftarrow 0$ To $r-1$
    $a_i \leftarrow m \bmod q$
    $m \leftarrow \frac{m - a_i \cdot [r-i+1]_q}{q}$
$a_r \leftarrow m$
```

LEMMA 5.6

Let $n \in \mathbb{Z}$ and $r \in \mathbb{N}_0$. Algorithm 5.5 computes the unique $S_q(r)$-adic expansion of n.

PROOF. First, we check that Algorithm 5.5 computes indeed an $S_q(r)$-adic expansion of n. Note that in the i-th loop run ($i \in \{0, \dots, r-1\}$) after the execution of "$a_i \leftarrow m \bmod q$" we have $m \equiv a_i \pmod{q}$, so that the updated value of m in the subsequent line is always an integer, and thus $a_r \in \mathbb{Z}$ at the end of the algorithm. The line "$a_i \leftarrow m \bmod q$" provides $a_i \in \{0, \dots, q-1\}$ for all $i \in \{0, \dots, r-1\}$. After the i-th loop run, we have $n = q^{i+1}m + \sum_{j=0}^{i} q^j [r-j+1]_q$, which one shows by induction. Therefore, at the end of the algorithm

$$n = q^r a_r + \sum_{j=0}^{r-1} q^j [r-j+1]_q = \sum_{j=0}^{r} a_j s_q(r,j).$$

For uniqueness, assume that there is a different representation $n = \sum_{i=0}^{r} b_i s_q(r,i)$ with $b_0, \dots, b_{r-1} \in \{0, \dots, q-1\}$ and $b_r \in \mathbb{Z}$. Let t be the smallest index i with $a_i \neq b_i$. Then $\sum_{i=0}^{t-1} a_i s_q(r,i) = \sum_{i=0}^{t-1} b_i s_q(r,i)$ and thus

$$\underbrace{(a_t - b_t)}_{\neq 0} s_q(r,t) = \sum_{i=t+1}^{r} (b_i - a_i) s_q(r,i).$$

As $s_q(r,i)$ is divisible by q^i but not by q^{i+1}, the right hand side is divisible by q^{t+1}, but the left hand side is not, which is a contradiction. □

DEFINITION 5.7

Let $n \in \mathbb{Z}$ and $n = \sum_{i=0}^{r} a_i s_q(r,i)$ be its unique $S_q(r)$-adic expansion. The number a_r will be called the leading coefficient and the number $\sigma = \sum_{i=0}^{r} a_i$ will be called the cross sum of the $S_q(r)$-adic expansion of n.

EXAMPLE 5.8 For $q = 3$, $r = 3$, we have $S_3(3) = (40, 39, 36, 27)$. For $n = 137$, Algorithm 5.5 computes

$$\begin{aligned}
m &\leftarrow 137,\\
a_0 &\leftarrow 137 \bmod 3 = 2,\\
m &\leftarrow (137 - 2 \cdot [4]_3)/3 = (137 - 2 \cdot 40)/3 = 19,\\
a_1 &\leftarrow 19 \bmod 3 = 1,\\
m &\leftarrow (19 - 1 \cdot [3]_3)/3 = (19 - 1 \cdot 13)/3 = 2,\\
a_2 &\leftarrow 2 \bmod 3 = 2,\\
m &\leftarrow (2 - 2 \cdot [2]_3)/3 = (2 - 2 \cdot 4)/3 = -2,\\
a_3 &\leftarrow -2.
\end{aligned}$$

Therefore, the $S_3(3)$-adic expansion of 137 is

$$137 = 2 \cdot 40 + 1 \cdot 39 + 2 \cdot 36 + (-2) \cdot 27.$$

The leading coefficient is $a_3 = -2$, and the cross sum is $2 + 1 + 2 + (-2) = 3$. ◇

For $\lambda \in \mathbb{N}_0$ and a multiset $\mathcal{M}$ of points with maximum point multiplicity at most λ, i.e., $\gamma_1(\mathcal{M}) \le \lambda$, we define the λ-complementary multiset $\mathcal{M}^{\complement_\lambda}$ by $\mathcal{M}^{\complement_\lambda}(P) = \lambda - \mathcal{M}(P)$ for all $P \in \mathcal{P}$. For $\lambda = \gamma_1$ we just write $\mathcal{M}^{\complement}$ instead of $\mathcal{M}^{\complement_{\gamma_1}}$.

An important observation is that the restriction $\mathcal{M}|_H = \mathcal{M} \cap H$ of a q^r-divisible multiset of points $\mathcal{M}$ to a hyperplane $H \in \mathcal{H}$ is q^{r-1}-divisible, provided that $r \ge 1$.

LEMMA 5.9

Let $\mathcal{M}$ be a q^r-divisible multiset of points in V and $U \neq \langle \mathbf{0} \rangle$ a subspace of V of codimension $0 \le j \le r$. Then, the restriction $\mathcal{M}|_U = \mathcal{M} \cap U$ is a q^{r-j}-divisible multiset in U.

PROOF. The case $j = 0$ is trivial. By induction, it suffices to consider the case $j = 1$. Let W be a hyperplane of U, that is a subspace of V of codimension 2. There are $q+1$ hyperplanes $H_1, \ldots, H_{q+1}$ in V containing W (U being one of them). From the q^r-divisibility of $\mathcal{M}$ we get

$$(q+1)\#\mathcal{M} \equiv \sum_{i=1}^{q+1} \#(\mathcal{M} \cap H_i) = q \cdot \#(\mathcal{M} \cap W) + \#\mathcal{M} \pmod{q^r}.$$

Hence $q \cdot \#(\mathcal{M} \cap W) \equiv q \cdot \#\mathcal{M} \equiv q \cdot \#(\mathcal{M} \cap U) \pmod{q^r}$ and thus

$$\#(\mathcal{M} \cap W) \equiv \#(\mathcal{M} \cap U) \pmod{q^{r-1}}.$$

□

Note that the restriction of a multiset of points to a hyperplane H corresponds to the residual of a linear code in a codeword associated with H. In the latter form, Lemma 5.9 can be found in [154, Lemma 13].

From the first two standard equations or a corresponding averaging argument we can conclude the existence of a hyperplane containing not too many points of $\mathcal{M}$.

LEMMA 5.10

Let $\mathcal{M}$ be a non-empty multiset of points. Then, there exists a hyperplane H with $\#(\mathcal{M} \cap H) < \frac{\#\mathcal{M}}{q}$.

PROOF. Let V be a suitable ambient space of $\mathcal{M}$ of finite dimension $v \ge 1$. Summing over all hyperplanes H gives $\sum_{H\mathcal{H}} \#(\mathcal{M} \cap H) = \#\mathcal{M} \cdot [v-1]_q$, so that we obtain on average

$$\frac{\#\mathcal{M} \cdot [v-1]_q}{[v]_q} = \frac{\#\mathcal{M} \cdot [v-1]_q}{q[v-1]_q + 1} = \#\mathcal{M} \cdot \frac{1}{q + \frac{1}{[v-1]_q}} < \frac{\#\mathcal{M}}{q}$$

points of $\mathcal{M}$ per hyperplane. Choosing a hyperplane H that minimizes $\#(\mathcal{M} \cap H)$ completes the proof. □

The coding counterpart of Lemma 5.10 is the well-known existence of a codeword of weight $> \frac{q-1}{q} n_{\text{eff}}$, where n_{eff} denotes the effective length of C.

THEOREM 5.11 (Lengths of q^r-divisible codes)
Let $n \in \mathbb{Z}$ and $r \in \mathbb{N}_0$. The following are equivalent:

(i) There exists a full-length q^r-divisible linear code of length n over $\mathbb{F}_q$.

(ii) The leading coefficient of the $S_q(r)$-adic expansion of n is non-negative.

PROOF. We are going to show the geometric version of the theorem. That is, we replace statement (i) by the geometric counterpart "There exists a q^r-divisible multiset of points over $\mathbb{F}_q$ of size n".

The implication "(ii) ⇒ (i)" follows from Lemma 5.4 and Lemma 5.3.

The main part of the proof is the verification of "(i) ⇒ (ii)". The statement is clear for $r = 0$ or $n \leq 0$, so we may assume $r \geq 1$ and $n \geq 1$.

Let $\mathcal{M}$ be a q^r-divisible multiset of points of size $n = \#\mathcal{M} \geq 1$. Let $n = \sum_{i=0}^{r} a_i s_q(r, i)$ with $a_0, \ldots, a_{r-1} \in \{0, 1, \ldots, q-1\}$ and $a_r \in \mathbb{Z}$ be the $S_q(r)$-adic expansion of n (see Lemma 5.6) and $\sigma = \sum_{i=0}^{r} a_i$ its cross sum.

Let $H \in \mathcal{H}$ be a hyperplane in V and $m = \#(\mathcal{M} \cap H)$. From the q^r-divisibility of $\mathcal{M}$ we conclude $n - m = \tau q^r$ with $\tau \in \mathbb{Z}$. Using $s_q(r, i) = s_q(r-1, i) + q^r$, we get

$$\begin{aligned} m = n - \tau q^r &= \sum_{i=0}^{r-1} a_i (s_q(r-1, i) + q^r) + a_r q^r - \tau q^r \\ &= \sum_{i=0}^{r-1} a_i s_q(r-1, i) + (\sigma - \tau) q^r \qquad (5.3) \\ &= \sum_{i=0}^{r-2} a_i s_q(r-1, i) + (a_{r-1} + q(\sigma - \tau)) q^{r-1}. \qquad (5.4) \end{aligned}$$

By Lemma 5.9, $\mathcal{M} \cap H$ is a q^{r-1}-divisible multiset of size m, and line (5.4) is the $S_q(r-1)$-adic expansion of m. Hence by induction over r, we get that $a_{r-1} + q(\sigma - \tau) \geq 0$. So $q(\sigma - \tau) \geq -a_{r-1} > -q$, implying that $\sigma - \tau > -1$ and thus $\sigma \geq \tau$.

Using Lemma 5.10, we may choose H such that $m < \frac{n}{q}$. Thus, combining the expression for m from line (5.3) together with $qs_q(r-1,i) = s_q(r,i+1)$ and $s_q(r,i) - s_q(r,i+1) = q^i$ gives

$$\begin{aligned}
0 < n - qm &= \sum_{i=0}^{r} a_i s_q(r,i) - \sum_{i=0}^{r-1} a_i s_q(r,i+1) - (\sigma-\tau)q^{r+1} \\
&= \sum_{i=0}^{r-1} a_i q^i + a_r q^r - (\sigma-\tau)q^{r+1} \le \sum_{i=0}^{r-1} (q-1)q^i + a_r q^r \\
&= (q^r - 1) + a_r q^r < (1 + a_r)q^r.
\end{aligned}$$

Therefore $1 + a_r > 0$ and finally $a_r \ge 0$. □

The statement of the theorem covers code lengths $n \le 0$, with the usual convention that the length of a code is never negative, and that there exists a single code of length 0, which is linear of dimension 0, contains only the empty word of weight 0 and is full-length.

REMARK 5.12 By Theorem 5.11, the $S_q(r)$-adic expansion of n provides a certificate not only for the existence, but remarkably also for the non-existence of a q^r-divisible multiset of size n.

For instance, the $S_3(3)$-adic expansion $137 = 2\cdot 40 + 1\cdot 39 + 2\cdot 36 + (-2)\cdot 27$ with leading coefficient -2 from Example 5.8 implies immediately that there is no 27-divisible ternary linear code of effective length 137.

REMARK 5.13 The proof of Theorem 5.11 uses the q^r-divisibility of $\mathcal{M}$ only in two places: For the hyperplane H containing less than the average number of points, and for invoking Lemma 5.9, telling us that the restriction of $\mathcal{M}$ to this hyperplane H is q^{r-1}-divisible. Restricting the requirements to what was actually needed in the proof, let us call a multiset $\mathcal{M}$ of points weakly q^r-divisible if $r = 0$ or if there is a hyperplane H such that $\#(\mathcal{M}\cap H) < \frac{\#\mathcal{M}}{q}$ and $\#\mathcal{M} \equiv \#(\mathcal{M}\cap H) \pmod{q^r}$, and $\mathcal{M}\cap H$ is weakly q^{r-1}-divisible. The statement of Theorem 5.11 is still true for weakly q^r-divisible multisets of points.

There are many more weakly q^r-divisible multisets of points than q^r-divisible ones. As an example, any multiset $\mathcal{M}$ of points of size $\#\mathcal{M} = q$ in the projective line $\mathrm{PG}(1,q)$ is weakly q-divisible: Since $[2]_q = q+1 > q$, the projective line contains a point P not contained in $\mathcal{M}$ which provides a suitable hyperplane H for the definition. The only q-divisible multiset of this type is a single point of multiplicity q.

As a byproduct of the proof of Theorem 5.11, we get the following theorem on the maximum weight of a divisible code:

THEOREM 5.14 (Maximum weight of a q^r-divisible code)

Let C be a q^r-divisible code of effective length n. Then the maximum weight of C is at most σq^r, where σ denotes the cross-sum of the $S_q(r)$-adic expansion of n.

PROOF. The proof of Theorem 5.11 shows that if $\mathcal{M}$ is a non-empty q^r-divisible multiset of size n and σ is the cross sum of the $S_q(r)$-adic expansion of n, we have $\#\mathcal{M} - \#(\mathcal{M} \cap H) = \tau q^r$ with $\tau \leq \sigma$ for every hyperplane H. In other words, the maximum weight of a full-length q^r-divisible linear code of length n over $\mathbb{F}_q$ is at most σq^r. □

EXAMPLE 5.15 The $S_2(3)$-adic expansion of $n = 59$ is $1 \cdot 15 + 0 \cdot 14 + 1 \cdot 12 + 4 \cdot 8$, with cross sum $\sigma = 1+0+1+4 = 6$. Therefore by Theorem 5.14, the codewords of an 8-divisible code of effective length 59 are of weight at most $6 \cdot 8 = 48$. This reasoning is the first step in the proof that there is no projective 8-divisible binary linear code of length 59 in [82]. ◇

EXAMPLE 5.16 In algebraic geometry, a nodal surface is a surface in the complex projective space whose only singularities are nodes. An old problem asks for the maximum number $\mu(s)$ of nodes a nodal surface of given degree s can have [16]. This problem has been solved only for $s \leq 6$. The answer in the largest settled case is $\mu(6) = 65$. The lower bound $\mu(6) \geq 65$ is realized by Barth's sextic [15] and the sextics in the 3-parameter series in [133, Theorem 5.5.9].

The proof of the upper bound $\mu(6) \leq 65$ is based on a coding theoretic argument. Each nodal surface comes with its even sets of nodes, which are the codewords of a certain binary linear code C assigned to the nodal surface. The length n of C is the number of nodes, and C is known to be 4-divisible if s is odd and 8-divisible if s is even. In the case $s = 6$, additionally $\dim(C) \geq n - 53$, and the nonzero weights of the 8-divisible code C are contained in $\{24, 32, 40, 56\}$ [32]. For $n = 66$, we get $\dim(C) \geq 13$, which has been shown to be impossible [86].

The unique code that arise from a nodal sextic having the record number 65 of nodes was recently characterized [101]. The $S_2(3)$-adic expansion of 65 is $1\cdot15+1\cdot14+1\cdot12+3\cdot8$ with cross sum $\sigma = 1+1+1+3 = 6$. If C is full-length, by Theorem 5.14 the weights in C are at most $6 \cdot 8 = 48$. So in this case, weight 56 is not possible and hence all nonzero weights of C are contained in $\{24, 32, 40\}$. ◇

In analogy to the Frobenius Coin Problem, cf. [27], we define $\mathrm{F}_q(r)$ as the smallest integer such that a q^r-divisible multiset of cardinality n exists for all integers $n > \mathrm{F}_q(r)$. In other words, $\mathrm{F}_q(r)$ is the largest integer which is not realizable as the size of a q^r-divisible multiset of points over $\mathbb{F}_q$. If all non-negative integers are realizable then $\mathrm{F}_q(r) = -1$, which is the case for $r = 0$.

PROPOSITION 5.17

For every prime power q and $r \in \mathbb{N}_0$ we have

$$\mathrm{F}_q(r) = r \cdot q^{r+1} - [r+1]_q = rq^{r+1} - q^r - q^{r-1} - \ldots - 1.$$

PROOF. By Theorem 5.11, $\mathrm{F}_q(r)$ is the largest integer n whose $S_q(r)$-adic expansion $n = \sum_{i=0}^{r-1} a_i s_q(r,i) + a_r q^r$ has leading coefficient $a_r < 0$. Clearly, this n is given by $a_0 = \ldots = a_{r-1} = q-1$ and $a_r = -1$, such that

$$\mathrm{F}_q(r)=\sum_{i=0}^{r-1}(q-1)s_q(r,i)-q^r=\sum_{i=0}^{r-1}(q^{r+1}-q^i)-q^r=rq^{r+1}-\frac{q^{r+1}-1}{q-1}.$$

□

5.1 Applications

As a preparation for the applications in Galois geometries, we introduce the following notions of sharpened rounding, which are based on the existence of certain divisible codes.

DEFINITION 5.18

For $a\in\mathbb{Z}$ and $b\in\mathbb{Z}\setminus\{0\}$ let $\llbracket a/b\rrbracket_{q^r}$ be the maximal $n\in\mathbb{Z}$ such that there exists a q^r-divisible $\mathbb{F}_q$-linear code of effective length $a-nb$. If no such code exists for any n, we set $\llbracket a/b\rrbracket_{q^r}=-\infty$. Similarly, let $\lceil\!\lceil a/b\rceil\!\rceil_{q^r}$ denote the minimal $n\in\mathbb{Z}$ such that there exists a q^r-divisible $\mathbb{F}_q$-linear code of effective length $nb-a$. If no such code exists for any n, we set $\lceil\!\lceil a/b\rceil\!\rceil_{q^r}=\infty$

REMARK 5.19

(i) Note that the symbols $\llbracket a/b\rrbracket_{q^r}$ and $\lceil\!\lceil a/b\rceil\!\rceil_{q^r}$ encode the four values a, b, q and r. Thus, the fraction a/b is a formal fraction, and the power q^r is a formal power.

(ii) We have

$$\llbracket 0/b\rrbracket_{q^r}=\lceil\!\lceil 0/b\rceil\!\rceil_{q^r}=0$$

and

$$\begin{aligned}&\ldots\le\llbracket a/b\rrbracket_{q^2}\le\llbracket a/b\rrbracket_{q^1}\le\llbracket a/b\rrbracket_{q^0}=\lfloor a/b\rfloor\\&\le a/b\le\lceil a/b\rceil=\lceil\!\lceil a/b\rceil\!\rceil_{q^0}\le\lceil\!\lceil a/b\rceil\!\rceil_{q^1}\le\lceil\!\lceil a/b\rceil\!\rceil_{q^2}\le\ldots\end{aligned}$$

LEMMA 5.20

Let $\lambda\in\mathbb{N}_0$ and $\mathcal{M}$ a multiset of points in $\mathrm{PG}(v-1,q)$ of maximum point multiplicity at most λ. Let $0\le r\le v-1$ such that q^r is a power of the characteristic of the field. Then, $\mathcal{M}$ is q^r-divisible if and only its λ-complement $\mathcal{M}^{\complement_\lambda}$ is.

PROOF. By Lemma 5.2(i), the (multi-)set of points $\mathcal{P}$ is q^{v-1}-divisible. Since $r\le v-1$, it is q^r-divisible. So, the result follows from the equation $\mathcal{M}+\mathcal{M}^{\complement_\lambda}=\lambda\cdot\mathcal{P}$. □

The connection between divisible codes and Galois geometries is based on the following lemmas.

LEMMA 5.21

Let $\mathcal{U}$ be a multiset of subspaces of V and $\mathcal{M} = \biguplus_{U\in\mathcal{U}} \begin{bmatrix} U \\ 1 \end{bmatrix}$ the associated multiset of points.[1] *Let k be the smallest dimension among the subspaces in $\mathcal{U}$. If $k \geq 1$, then the multiset $\mathcal{M}$ is q^{k-1}-divisible.*

PROOF. Apply Lemma 5.2(i) and (ii). □

Lemma 5.21 can be applied in many contexts. Existence conditions for q-analogs of group divisible designs are e.g. concluded in [30].

LEMMA 5.22

Let $k \in \mathbb{Z}_{\geq 1}$ and $\mathcal{U}$ be a multiset of k-spaces in $\operatorname{PG}(v-1,q)$.

(i) If every point in $\mathcal{P}$ is covered by at most λ elements of $\mathcal{U}$, then

$$\#\mathcal{U} \leq \llfloor \lambda \cdot [v]_q/[k]_q \rrfloor_{q^{k-1}}.$$

(ii) If every point in $\mathcal{P}$ is covered by at least λ elements in $\mathcal{U}$, then

$$\#\mathcal{U} \geq \llceil \lambda \cdot [v]_q/[k]_q \rrceil_{q^{k-1}}.$$

PROOF. By Lemma 5.21, the associated multiset $\mathcal{M} = \sum_{U\in\mathcal{U}} \begin{bmatrix} U \\ 1 \end{bmatrix}$ of points is q^{k-1}-divisible.

Part (i): Let $\mathcal{M}^{\complement_\lambda}$ be the λ-complementary multiset as in Lemma 5.20. Then $\#\mathcal{M}^{\complement_\lambda} = \lambda \cdot [v]_q - \#\mathcal{U} \cdot [k]_q$ and by Lemma 5.21 and Lemma 5.20, $\mathcal{M}^{\complement_\lambda}$ is q^{k-1}-divisible.

Part (ii): Let $\mathcal{M}'$ arise from $\mathcal{M}$ by reducing the multiplicity of every point by λ, i.e. $\mathcal{M}' = \mathcal{M} - \lambda\begin{bmatrix} V \\ 1 \end{bmatrix}$. By Lemma 5.2(i), $\begin{bmatrix} V \\ 1 \end{bmatrix}$ is q^{v-1}-divisible, and by $k \leq v$, it is q^{k-1}-divisible. So $\mathcal{M}'$ is q^{k-1}-divisible of size $\#\mathcal{U} \cdot [k]_q - \lambda \cdot [v]_q$. □

EXAMPLE 5.23 What is the maximum number of planes in $\operatorname{PG}(7,2)$ such that every point is covered at most three times? Counting points gives

$$\left\lfloor \frac{3 \cdot [8]_2}{[3]_2} \right\rfloor = \left\lfloor 109 + \tfrac{2}{7} \right\rfloor = 109$$

[1] In the expression $\biguplus_{U\in\mathcal{U}}$, the subspace U is repeated according to its multiplicity in the multiset $\mathcal{U}$.

as upper bound, while Lemma 5.22(i) gives

$$\leq \left\lfloor\!\!\left\lfloor \frac{3 \cdot [8]_2}{[3]_2} \right\rfloor\!\!\right\rfloor_{2^2} = 107$$

since no 2^2-divisible code of length 9 exists over $\mathbb{F}_2$. This bound is indeed tight, see [48, 49] where also more general packings of k-spaces are studied. ◇

In order to answer our initial question whether there exists a configuration of 20 solids and 30 planes in $\mathbb{F}_2^9$ with pairwise trivial intersection we apply Lemma 5.21 to conclude the existence of a 2^2-divisible set $\mathcal{M}$ of points in $\mathbb{F}_2^9$ of cardinality 510. Due to Lemma 5.20 the 1-complement $\mathcal{M}^{\complement_1}$ is a 2^2-divisible multiset of points in $\mathbb{F}_2^9$ of cardinality 1 and maximum point multiplicity 1. As mentioned in the introduction, no 2^2-divisible multiset of points exists over $\mathbb{F}_2$.

As it is the case in the initial example, we typically have some extra information for a q^r-divisible multiset of points $\mathcal{M}$. E.g., in our example, we know that $\mathcal{M}$, which is 2^2-divisible, can be embedded in $\operatorname{PG}(v-1,2)$, where $v \leq 9$. However, if we have $r = k-1$ and we get q^r-divisibility from the existence of some k-spaces, then we automatically have $v \geq k$ and observe that we can construct q^{k-1}-divisible multisets of each possible cardinality in $\operatorname{PG}(k-1,q)$. So, upper bounds for the dimension of the ambient space do not give further restrictions. Note that the mentioned construction can require large point multiplicities. So, it makes sense to incorporate an upper bound on the point multiplicity in Definition 5.18

DEFINITION 5.24

For $a \in \mathbb{Z}$ and $b \in \mathbb{Z}\backslash\{0\}$ let $\llfloor a/b \rrfloor_{q^r,\widehat{\gamma}}$ be the maximal $n \in \mathbb{Z}$ such that there exists a q^r-divisible multisets of points in $\operatorname{PG}(v-1,q)$ for suitably large v with maximum point multiplicity $\gamma_1 \leq \widehat{\gamma}$ and cardinality $a-nb$. If no such multiset exists for any n, we set $\llfloor a/b \rrfloor_{q^r,\widehat{\gamma}} = -\infty$.

Of course we may similarly define $\llceil a/b \rrceil_{q^r,\widehat{\gamma}}$. Note however, that Lemma 5.22(i) gives the natural upper bound $\lambda \geq \gamma_1$ while Lemma 5.22(ii) does not imply an upper bound. In Exercise 5.2 we will show that there exists a 2^3-divisible multiset of cardinality 12 with maximum point multiplicity 4 while there is none for smaller maximum point multiplicities. As another application we mention the following important refinement of Lemma 5.22(i).

LEMMA 5.25

Let $\mathcal{U}$ be a set of k-spaces in $\operatorname{PG}(v-1,q)$, where $1 \leq k \leq v$, with pairwise trivial intersection. Then, we have

$$\#\mathcal{U} \leq \llfloor [v]_q/[k]_q \rrfloor_{q^{k-1},1}. \tag{5.5}$$

We remark that the sets $\mathcal{U}$ in Lemma 5.25 are called partial spreads and the tightest known upper bounds on the maximum size of a partial spread, see e.g. [95], are implied by Inequality (5.5). However, the evaluation currently is a non-trivial task. It corresponds to the classification of the possible lengths of projective q^r-divisible codes, see e.g. [65, 67, 79, 82, 106] and Chapter 10 for partial results. In Section 15.1 we collect a few parametric bounds for partial spreads.

If the dimension v is not important or sufficiently large, then for each integer r all possible cardinalities of q^r-divisible multisets of points can be realized with maximum point multiplicity at most q^r. The cases $1 < \widehat{\gamma} < q^r$ are widely untouched and deserve to be studied in detail. If the maximum point multiplicity is restricted by an upper bound than also upper bounds on the dimension of the ambient space further restrict the existence of such divisible arcs. Of course the analysis gets even messier.

EXERCISE 5.1 Let $v = tk + r$ with $r \in \{1, \dots, k-1\}$ and $\mathcal{U}$ be a multiset of k-spaces in $\operatorname{PG}(v-1, q)$ such that every point is covered at most $\lambda \in \mathbb{N}$ times. Show

$$\#\mathcal{U} \le \lambda \cdot \left(1 + \sum_{i=1}^{t-1} q^{ik+r}\right) + 1 = \lambda \cdot \left(\frac{q^v - q^{k+r}}{q^k - 1} + 1\right) < \lambda \frac{[v]_q}{[k]_q}$$

for $k > \lambda [r]_q$.
Hint: As always, it might be helpful to start with special cases, e.g., $\lambda = 1$, $q = 2$, $r = 2$, $k = 4$, and $t = 2$; cf. also Example 5.23.

EXERCISE 5.2 Show that a 2^3-divisible multiset of points of cardinality 12 is a 4-fold line.

EXERCISE 5.3 Let $\mathcal{U}$ be a multiset of k-spaces in $\operatorname{PG}(v-1, q)$ that covers each point at least once. Show

$$\#\mathcal{U} \ge \left\lceil \frac{[v]_q}{[k]_q} \right\rceil$$

and determine for the case of equality the structure of the (multi-)set of points that is covered more than once.
Hint: For the second part a generalization of Exercise 5.2 is needed.

EXERCISE 5.4 Let $\mathcal{U}$ be a multiset of 4-spaces in $\operatorname{PG}(6, 2)$ that covers every 2-space at least once. Show $\#\mathcal{U} > 77$.
Hint: Exercise 5.2 might be useful.

EXERCISE 5.5 Determine the possible lengths of 4^r-divisible multisets of points in $\operatorname{PG}(v-1, 4)$, where $r \in \left\{\frac{1}{2}, \frac{3}{2}\right\}$ and v is sufficiently large.

6. Parametric results obtained from the linear programming method

The aim of this chapter is to draw some parametric conclusions from the linear programming method. Our first example is an alternative version of Lemma 5.10. Given an arc $\mathcal{K}$ in $\operatorname{PG}(v-1,q)$ let $\mathcal{T}(\mathcal{K}) := \{0 \le i \le \#\mathcal{K} : a_i > 0\}$ denote the set of attained hyperplane multiplicities, where a_i is the number of hyperplanes H with $\#(\mathcal{K} \cap H) = i$.

LEMMA 6.1

For integers $u \in \mathbb{Z}$, $m \ge 0$ and $\Delta \ge 1$ let $\mathcal{K}$ in be a Δ-divisible arc in $\operatorname{PG}(v-1,q)$ of cardinality $n = u + m\Delta \ge 0$. Then, we have

$$(q-1) \cdot \sum_{h \in \mathbb{Z}, h \le m} h a_{u+h\Delta} = (u + m\Delta - uq) \cdot \frac{q^{v-1}}{\Delta} - m, \tag{6.1}$$

where we set $a_{u+h\Delta} = 0$ if $u + h\Delta < 0$.

PROOF. Rewriting the standard equations from Lemma 1.5 yields

$$(q-1) \cdot \sum_{h \in \mathbb{Z}, h \le m} a_{u+h\Delta} = q \cdot q^{v-1} - 1$$

and

$$(q-1) \cdot \sum_{h \in \mathbb{Z}, h \le m} (u + h\Delta) a_{u+h\Delta} = (u + m\Delta)(q^{v-1} - 1).$$

u times the first equation minus the second equation gives Δ times the stated equation. □

COROLLARY 6.2

For integers $u, m \ge 0$ and $\Delta \ge 1$ let the arc $\mathcal{K}$ in $\operatorname{PG}(v-1,q)$ satisfy $\#\mathcal{K} = u + m\Delta$ and $\mathcal{T}(\mathcal{K}) \subseteq \{u, u+\Delta, \dots, u+m\Delta\}$. Then, $u < \frac{m\Delta}{q-1}$ or $u = m = 0$.

LEMMA 6.3

For integers $u \in \mathbb{Z}$, $m \ge 0$, and $\Delta \ge 1$ let $\mathcal{K}$ be a Δ-divisible arc of cardinality $n = u + m\Delta \ge 0$ in $\operatorname{PG}(v-1,q)$. Then, we have

$$(q-1) \cdot \sum_{h \in \mathbb{Z}, h \le m} h(h-1) a_{u+h\Delta} = \tau_q(u, \Delta, m) \cdot \frac{q^{v-2}}{\Delta^2} - m(m-1),$$

where we set

$$\tau_q(u,\Delta,m)=m(m-q)\Delta^2+\big(q^2u-2mqu+mq+2mu-qu-m\big)\,\Delta+(q-1)^2u^2+(q-1)u \quad (6.2)$$

and $a_{u+h\Delta}=0$ *if* $u+h\Delta<0$.

PROOF. Rewriting the standard equations from Lemma 1.5 yields

$$\begin{aligned}(q-1)\cdot\sum_{h\in\mathbb{Z},h\le m}a_{u+h\Delta}&=q^2\cdot q^{v-2}-1,\\(q-1)\cdot\sum_{h\in\mathbb{Z},h\le m}(u+h\Delta)a_{u+h\Delta}&=(u+m\Delta)(q\cdot q^{v-2}-1),\\(q-1)\cdot\sum_{h\in\mathbb{Z},h\le m}(u+h\Delta)(u+h\Delta-1)a_{u+h\Delta}&=(u+m\Delta)(u+m\Delta-1)(q^{v-2}-1).\end{aligned}$$

$u(u+\Delta)$ times the first equation minus $(2u+\Delta-1)$ times the second equation plus the third equation gives Δ^2 times the stated equation. □

COROLLARY 6.4

For integers $u\in\mathbb{Z}$ *and* $\Delta,m\ge 1$ *let* $\mathcal{K}$ *be* Δ*-divisible arc of cardinality* $n=u+m\Delta\ge 0$ *in* $\operatorname{PG}(v-1,q)$. *If one of the following conditions hold, then* $(q-1)\cdot\sum_{i=2}^m i(i-1)x_i\notin\mathbb{N}_0$, *which is impossible.*

(a) $\tau_q(u,\Delta,m)<0$;

(b) $\tau_q(u,\Delta,m)\cdot q^{v-2}$ *is not divisible by* Δ^2;

(c) $m\ge 2$ *and* $\tau_q(u,\Delta,m)=0$.

We have the following special cases:

$$\begin{aligned}\tau_q(u,q^r,m)&=\big(m(m-q)q^r-2mqu+q^2u+mq+2mu-qu-m\big)\cdot q^r\\&\quad+\big(q^2u^2-2qu^2+qu+u^2-u\big)\,,\\\tau_2(u,2^r,m)&=(m(m-2)2^r-2mu+m+2u)\cdot 2^r+\big(u^2+u\big)\,.\end{aligned}$$

LEMMA 6.5

Given a positive integer m, *we have* $\tau_q(u,\Delta,m)\le 0$ *iff*

$$\begin{aligned}&(q-1)u-(m-q/2)\Delta+\frac{1}{2}\\\in&\left[-\frac{1}{2}\cdot\sqrt{q^2\Delta^2-4qm\Delta+2q\Delta+1},\frac{1}{2}\cdot\sqrt{q^2\Delta^2-4qm\Delta+2q\Delta+1}\right].\end{aligned}\qquad(6.3)$$

The last interval is non-empty, i.e., the radicand is non-negative, iff $1\le m\le\lfloor(q\Delta+2)/4\rfloor$. *We have* $\tau_q(u,\Delta,1)=0$ *iff* $u=(\Delta-1)/(q-1)$.

PROOF. Solving $\tau_q(u, \Delta, m) = 0$ for u yields the boundaries for u stated in Inequality (6.3). Inside this interval we have $\tau_q(u, \Delta, m) \le 0$. Now, $q^2\Delta^2 - 4qm\Delta + 2q\Delta + 1 \ge 0$ is equivalent to $m \le \frac{q\Delta}{4} + \frac{1}{2} + \frac{1}{4q\Delta}$. Rounding down the right hand side, while observing $\frac{1}{4q\Delta} < \frac{1}{4}$ yields $\lfloor (q\Delta + 2)/4 \rfloor$. □

We remark that [23, Theorem 1.B] is quite similar to Lemma 6.3 and its implications. For the use of a quadratic non-negative polynomial over the integers see Inequality (3.2). The multipliers used in the proof of Lemma 6.3 can be directly read off from the following observation.

LEMMA 6.6

For pairwise different non-zero numbers a, b, c the inverse matrix of

$$\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 - a & b^2 - b & c^2 - c \end{pmatrix}$$

is given by

$$\begin{pmatrix} bc(c-b) & -(c+b-1)(c-b) & (c-b) \\ -ac(c-a) & (c+a-1)(c-a) & -(c-a) \\ ab(b-a) & -(b+a-1)(b-a) & (b-a) \end{pmatrix} \cdot \big((c-a)(c-b)(b-a)\big)^{-1}$$

As we have remarked before, the standard equations correspond to the first three MacWilliams identities. By additionally considering the fourth MacWilliams identity we obtain a further criterion. Before we state the general result, we illustrate it by a concrete example

LEMMA 6.7

No 2^3-divisible arc in $\mathrm{PG}(v-1, 2)$ *of cardinality* 52 *exists* .

PROOF. Using the abbreviation $y = 2^{v-3}$ the first four MacWilliams identities, see Equation (1.47), are given by

$$\begin{aligned} A_0 + A_8 + A_{16} + A_{24} + A_{32} &= 8y \cdot A_0^\perp \\ \binom{52}{1}A_0 + \binom{44}{1}A_8 + \binom{36}{1}A_{16} + \binom{28}{1}A_{24} + \binom{20}{1}A_{32} &= 4y \cdot 52A_0^\perp \\ \binom{52}{2}A_0 + \binom{44}{2}A_8 + \binom{36}{2}A_{16} + \binom{28}{2}A_{24} + \binom{20}{2}A_{32} &= 2y \cdot \binom{52}{2}A_0^\perp \\ \binom{52}{3}A_0 + \binom{44}{3}A_8 + \binom{36}{3}A_{16} & \\ +\binom{28}{3}A_{24} + \binom{20}{3}A_{32} &= y \cdot \left(\binom{52}{3}A_0^\perp + A_3^\perp\right) \end{aligned}$$

Plugging in $A_0 = A_0^\perp = 1$ and substituting $x = yA_3^\perp$ yields

$$\begin{aligned} A_8 &= -4 + A_{40} + 4A_{48} + \frac{1}{512}x + \frac{7}{64}y \\ A_{16} &= 6 - 4A_{40} - 15A_{48} - \frac{3}{512}x - \frac{17}{64}y \\ A_{24} &= -4 + 6A_{40} + 20A_{48} + \frac{3}{512}x + \frac{397}{64}y \\ A_{32} &= 1 - 4A_{40} - 10A_{48} - \frac{1}{512}x + \frac{125}{64}y. \end{aligned}$$

With this we compute

$$A_{16} + \frac{31}{20}A_8 = -\frac{1}{5} - \frac{49}{20}A_{40} - \frac{44}{5}A_{48} - \frac{123}{1280}y - \frac{29}{10240}x,$$

which contradicts $A_8, A_{16}, A_{40}, A_{48}, x, y \geq 0$. □

We remark that the non-existence of a 2^3-divisible set of cardinality $n = 52$ implies several upper bounds for partial spreads, e.g., $129 \leq A_2(11, 8; 4) \leq 132$, $2177 \leq A_2(15, 8; 4) \leq 2180$, and $34945 \leq A_2(19, 8; 4) \leq 34948$. The underlying idea of the proof of Lemma 6.7 can be generalized:

LEMMA 6.8

For $t \in \mathbb{Z}$ be an integer and $\mathcal{K}$ be Δ-divisible arc of cardinality $n > 0$ in $\operatorname{PG}(v-1, q)$. Then, we have

$$\sum_{i \geq 1} \Delta^2 (i-t)(i-t-1) \cdot (g_1 \cdot i + g_0) \cdot A_{i\Delta} \ + qhx = n(q-1)(n - t\Delta)(n - (t+1)\Delta) g_2,$$

where $g_1 = \Delta q h$, $g_0 = -n(q-1)g_2$, $g_2 = h - (2\Delta qt + \Delta q - 2nq + 2n + q - 2)$ and

$$h = \Delta^2 q^2 t^2 + \Delta^2 q^2 t - 2\Delta n q^2 t - \Delta n q^2 + 2\Delta n q t + n^2 q^2 + \Delta n q - 2n^2 q + n^2 + nq - n.$$

PROOF. We slightly rewrite the first four MacWilliams identities to

$$\begin{aligned} \sum_{i=1}^{s} A_{i\Delta} \ - q^3 y &= -1 \\ \sum_{i=1}^{s} (n - i\Delta) \cdot A_{i\Delta} \ - nq^2 y &= -n \\ \sum_{i=1}^{s} (n - i\Delta)(n - i\Delta - 1) \cdot A_{i\Delta} \ - 2\binom{n}{2} qy &= -2\binom{n}{2} \\ \sum_{i=1}^{s} (n - i\Delta)(n - i\Delta - 1)(n - i\Delta - 2) \cdot A_{i\Delta} \ - 6\binom{n}{3} y - x &= -6\binom{n}{3}, \end{aligned}$$

where s is suitably large, $k = \dim(\langle\mathcal{C}\rangle)$, $y = q^{k-3}$, and $x = y \cdot A_3^\perp$. We consider a linear combination of those equations with multipliers

$$\begin{aligned}
f_1 &= (bcq^2 - bnq - bq^2 - cnq - cq^2 + bq + cq + n^2 + 3nq + q^2 - 3n - 3q + 2)bcn \\
f_2 &= -b^2c^2q^3 + b^2cq^3 + bc^2q^3 + b^2n^2q + bcn^2q - bcq^3 + c^2n^2q - b^2nq - bcnq \\
&\quad -bn^3 - 3bn^2q - c^2nq - cn^3 - 3cn^2q + 3bn^2 + 3bnq + 3cn^2 + 3cnq + n^3 \\
&\quad +2n^2q - 2bn - 2cn - 3n^2 - 2nq + 2n \\
f_3 &= b^2cq^3 + bc^2q^3 - b^2nq^2 - bcnq^2 - 3bcq^3 - c^2nq^2 + 3bnq^2 + 3cnq^2 + n^3 \\
&\quad -2nq^2 - 3n^2 + 2n \\
f_4 &= -(bcq^2 - bnq - cnq + n^2 + nq - n)q,
\end{aligned}$$

where $b = n - t\Delta$ and $c = n - (t+1)\Delta$.

For the coefficient of $A_{i\Delta}$ we have

$$\begin{aligned}
& f_1 + f_2 \cdot (n - i\Delta) + f_3 \cdot (n - i\Delta)(n - i\Delta - 1) \\
& +f_4 \cdot (n - i\Delta)(n - i\Delta - 1)(n - i\Delta - 2) \\
= \; & \Delta^2(i - t)(i - t - 1) \cdot (g_1 \cdot i + g_0).
\end{aligned}$$

The coefficient of y vanishes, i.e., $-q^3f_1 - nq^2f_2 - n(n-1)qf_3 - n(n-1)(n-2)f_4 = 0$. The coefficient of x is given by $(bcq^2 - bnq - cnq + n^2 + nq - n)q = qh$. The right hand side is given by $-f_1 - nf_2 - n(n-1)f_3 - n(n-1)(n-2)f_4 = n(q-1)(n-t\Delta)(n-(t+1)\Delta)g_2$. □

COROLLARY 6.9

Using the notation of Lemma 6.8, if $n/\Delta \notin [t, t+1]$, $h \ge 0$, and $g_2 < 0$, then there exists no Δ-divisible arc $\mathcal{K}$ of cardinality n in $\mathrm{PG}(v-1, q)$.

PROOF. First we observe $(i-t)(i-t-1) \ge 0$, $(n-t\Delta)(n-(t+1)\Delta) > 0$, and $g_1 \ge 0$. Since $g_2 < 0$, we have $g_0 \ge 0$ so that $g_1 i + g_0 \ge 0$. Thus, the entire left hand side is non-negative and the right hand side is negative –a contradiction. □

Applying Corollary 6.9 with $t = 3$ gives Lemma 6.7. For the somehow related use of a cubic polynomial over the integers in a related context see [23, Section 4], especially Inequality (4.1). In the proof of Lemma 6.8 we are essentially solving the linear equation system, given by the first four MacWilliams identities,for $A_{s\Delta}, A_{t\Delta}, A_{(t+1)\Delta}$ and y. The corresponding multipliers are given by:

LEMMA 6.10

For pairwise different numbers a, b, c, n and $q, y \neq 0$ let

$$M = \begin{pmatrix} 1 & 1 & 1 & -q^3y \\ a & b & c & -nq^2y \\ a(a-1) & b(b-1) & c(c-1) & -n(n-1)qy \\ a(a-1)(a-2) & b(b-1)(b-2) & c(c-1)(c-2) & -n(n-1)(n-2)y \end{pmatrix}.$$

With this, the entries of the first row of $\frac{1}{(b-c)y}\cdot\det(M)\cdot M^{-1}$ *are given by* f_1*,* f_2*,* f_3*, and* f_4 *as stated in the proof of Lemma 6.8.*

PROOF. Just insert the expression into a computer algebra system like e.g. `Maple`. □

As a further example we consider the parameters $q = 2$, $\Delta = 2^4 = 16$, and $n = 235$. The condition $n/\Delta \notin [t, t+1]$ excludes $t \in \{14, 15\}$. The condition $h \geq 0$ is satisfied for all integers t since the excluded interval $(6.700, 6.987)$ contains no integer. The condition $g_2 < 0$ just allows to choose $t = 7$, which also satisfies $qh \geq -g_0$.

We can perform a closer analysis in order to develop computational cheap checks. We have $g_2 < 0$ iff

$$n \in \left(\frac{\Delta qt + \frac{\Delta q}{2} - \frac{3}{2} - \frac{1}{2}\cdot\sqrt{\omega}}{q-1}, \frac{\Delta qt + \frac{\Delta q}{2} - \frac{3}{2} + \frac{1}{2}\cdot\sqrt{\omega}}{q-1}\right),$$

where $\omega = \Delta^2 q^2 - 4qt\Delta - 2\Delta q + 4q + 1$. Thus, $\omega > 0$, i.e., we have

$$t \leq \left\lfloor \frac{q\Delta - 2}{4} + \frac{1}{\Delta} + \frac{1}{4q\Delta} \right\rfloor.$$

We have $h \geq 0$ iff

$$n \notin \left(\frac{\Delta qt + \frac{\Delta q}{2} - \frac{1}{2} - \frac{1}{2}\cdot\sqrt{\omega - 4q}}{q-1}, \frac{\Delta qt + \frac{\Delta q}{2} - \frac{1}{2} + \frac{1}{2}\cdot\sqrt{\omega - 4q}}{q-1}\right).$$

The most promising possibility, if not the only at all, seems to be

$$n \in \Big(\frac{\Delta qt + \frac{\Delta q}{2} - \frac{3}{2} - \frac{1}{2}\cdot\sqrt{\omega}}{q-1}, \frac{\Delta qt + \frac{\Delta q}{2} - \frac{1}{2} - \frac{1}{2}\cdot\sqrt{\omega - 4q}}{q-1}\Big],$$

which allows the choice of at most one integer n. In our example $q = 2$, $\Delta = 2^4 = 16$ the possible n for $t = 1, \ldots, 7$ correspond to $33, 66, 99, 132, 166, 200, 235$, respectively. The two other conditions are automatically satisfied.

We close this section by a few more general results. If we use the representation of the MacWilliams identities in terms of power moments, then we end up with so-called Vandermonde matrices whose determinant is well known.

LEMMA 6.11

The determinant of the Vandermonde matrix

$$V(x_1, \ldots, x_n) = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix} \tag{6.4}$$

is given by

$$\prod_{1\le i<j\le n} (x_j - x_i)\,. \tag{6.5}$$

Let us give the inverse matrix and the basis solution for the case of the first three MacWilliams identities solve for three primal weights.

LEMMA 6.12

For pairwise different $w_1, w_2, w_3 \in \mathbb{R}$ *the inverse matrix of*

$$\begin{pmatrix} 1 & 1 & 1 \\ w_1 & w_2 & w_3 \\ w_1^2 & w_2^2 & w_3^2 \end{pmatrix}$$

is given by

$$\begin{pmatrix} \frac{w_2w_3}{(w_1-w_2)(w_1-w_3)} & \frac{-(w_2+w_3)}{(w_1-w_2)(w_1-w_3)} & \frac{1}{(w_1-w_2)(w_1-w_3)} \\ \frac{w_1w_3}{(w_2-w_1)(w_2-w_3)} & \frac{-(w_1+w_3)}{(w_2-w_1)(w_2-w_3)} & \frac{1}{(w_2-w_1)(w_2-w_3)} \\ \frac{w_1w_2}{(w_3-w_1)(w_3-w_2)} & \frac{-(w_1+w_2)}{(w_3-w_1)(w_3-w_2)} & \frac{1}{(w_3-w_1)(w_3-w_2)} \end{pmatrix}.$$

LEMMA 6.13

Solving the first three MacWilliams identities of a projective $[n,k]_2$*-code for* $\{A_{w_1}, A_{w_2}, A_{w_3}\}$*, where* w_1, w_2, w_3 *are pairwise different, yields*

$$\begin{aligned} (w_1-w_2)(w_1-w_3)\cdot A_{w_1} &= w_2w_3\left(2^k-1\right) - (w_2+w_3)\cdot 2^{k-1}n + 2^{k-2}n(n+1) \\ &\quad - \sum_{i\in\mathbb{N}\setminus\{w_1,w_2,w_3\}} (i-w_2)(i-w_3)\cdot A_i \end{aligned}$$

EXERCISE 6.1 Proof the formula for the determinant of the Vandermonde matrix, see Lemma 6.11.

EXERCISE 6.2 Show that no projective 2^5-divisible $[n,k]_2$-code with

$$n \in \{325, 390, 456, 521, 587, 652, 718, 784, 850, 917, 985\}$$

exists.

7. The cylinder conjecture

Originally the cylinder conjecture was motivated by the classification sets of p^2 points in $\mathrm{AG}(3,p)$ that determine few directions, where p is a prime, see e.g. [13, 38]. This line of research continues the study of similar questions in $\mathrm{AG}(2,p)$ dating back to [135, 125]. Here we will go along the way of trying to classify the isomorphism types of q^r-divisible sets of q^{r+1} points and generalize the cylinder conjecture to that end. For surveys on q^r-divisible sets of points or divisible codes we refer the reader to [79] and [151].

In $\mathrm{AG}(3,p)$ a cylinder is a set of p parallel full affine lines, i.e., p-lines. In its strong version the cylinder conjecture states that each set of p^2 points in $\mathrm{AG}(3,p)$ such that every hyperplane contains $0 \pmod p$ of these points is a cylinder. Here, we phrase the problem in $\mathrm{PG}(3,q)$, where we call a set of q affine lines $L_1\backslash F,\dots,L_q\backslash F$, that intersect in the same point F, a cylinder. With this, we can more generally state the conjecture that each q-divisible set of q^2 points in $\mathrm{PG}(3,q)$ is a cylinder. As mentioned before, we want to be even more general and are interested in the classification of q^r-divisible sets of q^{r+1} points in $\mathrm{PG}(v-1,q)$, where $r\ge 1$ is an arbitrary integer. To this end we generalize the notion of a cylinder.

Definition 7.1

Let r be a positive integer. An r-cylinder is a multiset of q^r points in $\mathrm{PG}(v-1,q)$ that arises as the union of the points of q affine r-subspaces $L_1\backslash F$, …, $L_q\backslash F$, where the L_i are r-spaces and F is a $(r-1)$-space that is contained in all L_i.

We remark that our definition of a 2-cylinder matches the definition of a cylinder in [38] and the one stated above. By convention a 1-cylinder is just a multiset of q points. As those affine subspaces will appear more often, we denote by $A(S,B)$ the affine subspace $\langle S,B\rangle\backslash B$, where S is a point and B and arbitrary subspace. Note that we have $\dim(A(S,B)) = \dim(B)+1$. Next, we observe that r-cylinders can be constructed easily starting from a multiset of q points.

Construction 7.2

Let r and v' be a non-negative integer, and consider a v'-space V' and a disjoint r-space F in $V=\mathbb{F}_q^{v'+r}$. If $\mathcal{M}'$ is a multiset of q points in V', we can associate to every point in $\mathcal{M}'$ the $(r+1)$-space spanned by F and the point. For the ease of notation we enumerate these $(r+1)$-spaces as $L_1,\dots,L_q$. With this, the multiset $\mathcal{M}$ consists of the points of $L_i\backslash F$, where $1\le i\le q$.

In other words we construct the multiset of points $\mathcal{M}$ corresponding to the union of $A(M,F)$ over all $M\in\mathcal{M}'$. Obviously, Construction 7.2 gives an r-cylinder. In the other direction, if we start from an r-cylinder $L_1\backslash F$, …, $L_q\backslash F$, then we can choose M_i arbitrary in $L_i\backslash F$ for $1\le i\le q$. If we set $\mathcal{M}'=$

$\{M_i : 1 \le i \le q\}$ and apply Construction 7.2, then we obtain the r-cylinder we started with. It remains to observe that the multiset of points corresponding to an r-cylinder is q^{r-1}-divisible.

PROPOSITION 7.3

The multiset of points of an r-cylinder is q^{r-1}-divisible.

PROOF. We use the notation of Definition 7.1 for a given r-cylinder. The statement is trivial for $r = 1$ so that we assume $r \ge 2$. Each hyperplane H intersects F either in dimension $r-1$ or $r-2$. In the first case we have $\#\left(L_i \backslash F \cap H\right) \in \left\{0, q^{r-1}\right\}$. In the second case we have $\#\left(L_i \backslash F \cap H\right) = q^{r-2}$ for all $1 \le i \le q$. With this, we have $\#(\mathcal{M} \cap H) \equiv 0 \pmod{q^{r-1}}$ for the corresponding multiset of points $\mathcal{M}$ of the r-cylinder. □

So, r-cylinders yield q^{r-1}-divisible multiset of q^r points and the question arises if there are other isomorphism types. Indeed there are. Any multiset of q (possibly equal) points with multiplicity q^{r-1} each is q^{r-1}-divisible. For that reason we will consider sets of points instead of multisets in the remaining part. We remark that studying multisets of points with restricted point multiplicity might be an interesting problem, but we will not go into this here. It will also depend on the dimension whether other isomorphism types exist. Since each set $\mathcal{S}$ of points in $\operatorname{PG}(v-1,q)$ can be embedded in $\operatorname{PG}(v'-q,q)$ for $v' > v$ we will always assume that $\mathcal{S}$ is spanning in $\operatorname{PG}(v-1,q)$. We observe that, In Construction 7.2, $\mathcal{M}$ is spanning iff $\mathcal{M}'$ is spanning and $\mathcal{M}$ is a set iff $\mathcal{M}'$ is a set. We call an $(r+1)$-cylinder spanning or projective if the corresponding multiset of points is.

LEMMA 7.4

There exists a spanning projective $(r+1)$-cylinder in $\operatorname{PG}(v-1,q)$ iff $r+2 \le v \le r+q$.

PROOF. Due to the above observations it suffices to remark that $2 \le \dim(\langle \mathcal{M}' \rangle) \le q$ and all dimensions in that range can indeed be attained. □

We say that the cylinder conjecture is true for the tuple $(q,r,v) \in \mathbb{N}_0^3$ if all q^r-divisible spanning sets of q^{r+1} points in $\operatorname{PG}(v-1,q)$ are $(r+1)$-cylinders. If $r = 0$, then the cylinder conjecture is trivially true for (q,r,v). The strong cylinder conjecture from [38] corresponds to the special case $(p,1,4)$, where p is a prime. (We will see shortly that it makes no difference if we consider point sets in affine or projective geometries.)

In Lemma 5.9 we have seen that the restriction $\mathcal{K}|_H$ of a q^r-divisible arc $\mathcal{K}$ in $\operatorname{PG}(v-1,q)$ to a hyperplane H is q^{r-1}-divisible. We will see shortly that if $\#\mathcal{K} = q^{r+1}$, then there are many hyperplanes H so that $\#\mathcal{K}|_H = q^r$, i.e., we can apply inductive arguments. Indeed, it will turn out that the cylinder conjecture is true for (q,r,v) iff it is true for $(q,1,v-r+1)$, see Corollary 7.17. If q is a proper prime power, i.e., not a prime, then there exist counter examples for suitable dimensions which are e.g. based on subgeometries, see Lemma 7.24. In Section 7.1 we will consider the cylinder conjecture for the general case (q,r,v) and especially show the equivalence to the cylinder conjecture for $(q, 1, v-r+1)$. It turns out that the cylinder conjecture is true for $q \in \{2, 3, 5\}$, for $(4, 1, 3)$ and $(4, 1, 4)$, but not for $(4, 1, 5)$. The special case $(q, 1, 4)$ is treated in detail in Section 7.2, where the case $q = 7$ is fully resolved. Although our numerical data is still rather limited, we state:

CONJECTURE 7.5

The cylinder conjecture is true for $(q, r, r+3)$ and for (p, r, v) if p is a prime.

7.1 Generalized cylinder conjecture

We first want to draw some conclusions from the standard equations, see Lemma 1.5.

LEMMA 7.6

Let $\mathcal{S}$ be a q^r-divisible spanning set of q^{r+1} points in $\operatorname{PG}(v-1, q)$ and let a_i be the number of hyperplanes in $\operatorname{PG}(v-1, q)$ containing exactly i points of $\mathcal{S}$, where $0 \le i \le n$. Then we have

$$(q-1) \cdot \sum_{i=0}^{q-1} a_{i\Delta} = q^2 y - 1, \tag{7.1}$$

$$(q-1) \cdot \sum_{i=0}^{q-1} i a_{i\Delta} = q(qy-1), \tag{7.2}$$

$$(q-1) \cdot \sum_{i=0}^{q-1} i(i\Delta - 1) a_{i\Delta} = q(q\Delta - 1) \cdot (y-1), \tag{7.3}$$

where $\Delta = q^r$ and $y = q^{v-2}$.

PROOF. We use the equations from Lemma 1.5. Multiplying them by $q-1$, using $n = q\Delta$, $y = q^{v-2}$, and taking divisibility into account gives

$$(q-1) \cdot \sum_{i=0}^{q} a_{i\Delta} = q^2 y - 1, \tag{7.4}$$

$$(q-1) \cdot \sum_{i=0}^{q} i\Delta a_{i\Delta} = q\Delta \cdot (qy-1), \tag{7.5}$$

$$(q-1) \cdot \sum_{i=0}^{q} \binom{i\Delta}{2} a_{i\Delta} = \binom{q\Delta}{2} \cdot (y-1). \tag{7.6}$$

Finally, dividing Equation (7.5) by Δ, Equation (7.6) by $\Delta/2$, and taking $a_{q\Delta} = 0$ into account gives the stated result. □

LEMMA 7.7

Let $\mathcal{S}$ be a q^r-divisible spanning set of q^{r+1} points in $\operatorname{PG}(v-1,q)$. *Then, the number a_{q^r} of hyperplanes with the smallest non-zero number of points is at least* $\frac{q^v-1}{q-1} - \left(q^{v-r-1}+1-q\right)$.

PROOF. Using the notation from Lemma 7.6, Equation (7.3) minus $2\Delta-1$ times Equation (7.2) gives

$$(q-1)\cdot\sum_{i=0}^{q-1}\Delta\cdot i(i-2)a_{i\Delta} = -\Delta\cdot\left((q^2y-1-(q-1)qy/\Delta+(q-1)^2\right).$$

Since $i(i-2)\ge 0$ and $a_{i\Delta}\ge 0$ for all $2\le i\le q-1$ and i=1, we conclude $(q-1)a_{\Delta}\ge q^2y-1-(q-1)\cdot(qy/\Delta+1-q)$. □

In other words, almost all hyperplanes contain exactly q^r points. For these hyperplanes we might apply induction, i.e., we can assume that they are r-cylinders.

LEMMA 7.8

Let $\mathcal{S}$ be a q^r-divisible spanning set of q^{r+1} points in $PG(v-1,q)$. Then, the number a_0 of empty hyperplanes is at most $\left(q^{v-r-1}+2-q\right)/2$.

PROOF. Using the notation from Lemma 7.6, 2Δ times Equation (7.1) minus $3\Delta-1$ times Equation (7.2) plus Equation (7.3) gives

$$(q-1)\cdot\sum_{i=0}^{q-1}\Delta\cdot(i-1)(i-2)a_{i\Delta} = \Delta(q-1)\cdot(qy/\Delta+2-q)\,.$$

Since $(i-1)(i-2)\ge 0$ and $a_{i\Delta}\ge 0$ for all $0\le i\le q-1$, we conclude $2a_0\le qy/\Delta+2-q$. □

LEMMA 7.9

Let $\mathcal{S}$ be a q^r-divisible spanning set of q^{r+1} points in $\operatorname{PG}(v-1,q)$. *Then, the number a_0 of empty hyperplanes is at least* $\frac{q^{v-r-1}-1}{q-1}$.

PROOF. Using the notation from Lemma 7.6, $\Delta(q-1)$ times Equation (7.1) minus $q\Delta-1$ times Equation (7.2) plus Equation (7.3) gives

$$(q-1)\cdot\sum_{i=0}^{q-1}\Delta\cdot(i-1)(i-q+1)a_{i\Delta} = (qy-\Delta)(q-1).$$

Since $(i-1)(i-q+1)\le 0$ and $a_{i\Delta}\ge 0$ for all $1\le i\le q-1$, we conclude $(q-1)a_0\ge qy/\Delta-1 = q^{v-r-1}-1$. □

COROLLARY 7.10

Every q^r-divisible spanning set of q^{r+1} points in $\mathrm{PG}(v-1,q)$ contains at least one empty hyperplane.

PROOF. Since $\mathrm{PG}(v-1,q)$ contains $[v]_q = q^{v-1} + q^{v-2} + \cdots + 1$ points, we have $v \geq r+2$, so that Lemma 7.9 gives the stated result. □

Thus, it makes no difference if we speak about point sets in $\mathrm{AG}(v-1,q)$ or $\mathrm{PG}(v-1,q)$.

In Table 7.1 we give a few examples for linear programming bounds for the a_i and mention that the bounds of the above lemmas are attained with equality.

r	v	$a_0 \geq$	$a_0 \leq$	$a_{5^r} \geq$
1	3	1	1	30
1	4	6	11	135
1	5	31	61	660
1	6	156	311	3285
2	4	1	1	155
2	5	6	11	760
2	6	31	61	3785
2	7	156	311	18910

Table 7.1: Linear programming bounds for 5^r-divisible sets of 5^{r+1} points in $\mathrm{PG}(v-1,5)$.

Another implication of Corollary 7.10 is that the cylinder conjecture is true for small dimensions:

PROPOSITION 7.11

Let $\mathcal{S}$ be a q^r-divisible spanning set of q^{r+1} points in $\mathrm{PG}(v-1,q)$. If $v \leq r+2$, then $v = r+2$ and $\mathcal{S} \simeq \mathrm{AG}(v-1,q)$.

PROOF. As in the proof of Corollary 7.10 we conclude $v \geq r+2$, so that $v = r+2$. A single empty hyperplane leaves only q^{r+1} possible points, which all have be to contained in $\mathcal{S}$. □

In other words, the cylinder conjecture is true for all (q,r,v), where $v \leq r+2$. So, the classification of q^r-divisible spanning sets of q^{r+1} points in $\mathrm{PG}(v-1,q)$ is *challenging* for $v \geq r+3$ only.

Our next goal is to transfer many of the insights of [38] to our more general situation.

LEMMA 7.12 (Cf. [38, Lemma 1])

Let $\mathcal{S}$ be a q^r-divisible spanning set of q^{r+1} points in $\mathrm{PG}(v-1,q)$. Let K be a subspace of codimension 2 in $\mathrm{PG}(v-1,q)$. Assume that $|\mathcal{S} \cap K| = kq^{r-1}$ for some integer $0 < k < q$. Then, any hyperplane containing K contains at most kq^r points from $\mathcal{S}$.

PROOF. Since every hyperplane containing K contains at least kq^{r-1} points, it should contain at least q^r points. Therefore, counting the number of points on hyperplanes containing K, we find at least $(q+1)\left(q^r - kq^{r-1}\right) + kq^{r-1} = q^{r+1} - (k-1)q^r$ points. Hence, there are $(k-1)q^r$ points left, which implies that a single hyperplane contains at most kq^r points. □

COROLLARY 7.13 (Cf. [38, Corollary 1])

Let $\mathcal{S}$ be a q^r-divisible spanning set of q^{r+1} points in $\operatorname{PG}(v-1,q)$. Suppose the hyperplane H contains kq^r points of $\mathcal{S}$, where $0 < k < q$, then every hyperplane K of H, i.e., $K \le H$ is a subspace of codimension 2 in $\operatorname{PG}(v-1,q)$, contains either 0 or at least kq^{r-1} points of $\mathcal{S}$. Moreover, $|\mathcal{S} \cap K| \equiv 0 \pmod{q^{r-1}}$.

PROOF. The congruence $|\mathcal{S} \cap K| \equiv 0 \pmod{q^{r-1}}$ follows from Lemma 5.9. Suppose that K contains lq^{r+1} points for some integer $0 < l < k$. Then, by Lemma 7.12, every hyperplane H in $\operatorname{PG}(v-1,q)$ containing K contains at most $lq^r < kq^r$ points, which is a contradiction. □

We remark that Lemma 7.12 can be generalized to the situation where $\mathcal{S}$ contains λq^r points, see Exercise 7.1.

THEOREM 7.14 (Full affine line; cf. [38, Theorem 2])

Let $\mathcal{K}$ be a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(v-1,q)$. If $\mathcal{K}$ contains a q-line L, then $\mathcal{K}$ is a 2-cylinder.

PROOF. Due to Proposition 7.11 we can assume $v \ge 4$. Let Q be the unique 0-point on L, R be an arbitrary 1-point not contained in L, and H be a hyperplane containing L and R. We may assume $\mathcal{K}(H) = kq$ with $1 < k < q$. For a 1-point P on L let $K_1, \ldots, K_l$ denote the $l := q^{v-3}$ $(v-2)$-spaces that contain P but not Q and are contained in H. Since every point in $H \backslash L$ is contained in exactly q^{v-4} of these subspaces, we have

$$\sum_{i=1}^{l} |\mathcal{S} \cap K_i \backslash P| = |\mathcal{S} \cap H \backslash L| \cdot q^{v-4} = q^{v-3}(k-1).$$

From Corollary 7.13 we conclude $|\mathcal{S} \cap K_i \backslash P| \ge k-1$, so that $\mathcal{K}(K_i) = k$ for all $1 \le i \le l$.

Now let L' be the line $\langle R, Q\rangle$ and $K_1', \ldots, K_l'$ denote the $l = q^{v-3}$ $(v-2)$-spaces that contain R but not Q and are contained in H. Since K_i' does not contain Q it meets L in a 1-point P, so that $|\mathcal{S} \cap K_i' \backslash R| = k-1$ for all $1 \le i \le l$. Similar as before, counting points yields

$$\sum_{i=1}^{l} \left|\mathcal{S} \cap K_i' \backslash R\right| = \left|\mathcal{S} \cap H \backslash L'\right| \cdot q^{v-4},$$

so that $\mathcal{K}(L') = q$. In other words, every point of $\mathcal{S}$ is contained on a q-line through the 0-point Q, i.e., $\mathcal{S}$ is a 2-cylinder. □

We can also generalize Theorem 7.14 to situations of q^r-divisible point sets of cardinality q^{r+1} where $r > 1$, see Exercise 7.2. However, it is sufficient to consider the cylinder conjecture for (q, r, v) in the special case $r = 1$ as we will show next.

PROPOSITION 7.15

If the cylinder conjecture is true for $(q, r + 1, v + 1, q)$*, then it is true for* (q, r, r).

PROOF. If the cylinder conjecture is false for (q, r, v), then we can apply the following construction to a corresponding counterexample and obtain a counterexample for $(q, r + 1, v + 1)$.

Consider a q^r-divisible set $\mathcal{S}$ of q^{r+1} points in $V := PG(v-1, q)$. For a point P outside of the ambient space we consider the new ambient space $V' := \langle \mathrm{PG}(v - 1, q), P\rangle$ and set $\mathcal{S}' = \{\langle S, P\rangle\backslash\{P\} : S \in \mathcal{S}\}$. By construction $\dim(V') = v+1$ and $\mathcal{S}'$ is a set of q^{r+2} points in V'. Now let H' by a hyperplane of V'. Either $H' = V$ or $H := H'\cap V$ is a hyperplane of V. In the first case the have $\mathcal{S}'\cap H' = \mathcal{S}$, which is of cardinality q^{r+1}. In the second case we have $|\mathcal{S} \cap H| \equiv 0 \pmod{q^r}$. If $P \le H'$, then $|\mathcal{S}' \cap H'| = q \cdot |\mathcal{S} \cap H| \equiv 0 \pmod{q^{r+1}}$. If P is not contained in H' then each of the q^{r+1} affine lines $\langle S, P\rangle\backslash\{P\}$ is met by H' in a single point not equal to P, so that $|\mathcal{S}' \cap H'| = q^{r+1}$. Thus, $\mathcal{S}'$ is q^{r+1}-divisible and one can see that it is not a cylinder, if $\mathcal{S}$ is not. □

THEOREM 7.16 (Increase r)

If the cylinder conjecture is true for $(q, 1, v)$*, then it is true for all* $(q, r, v + r - 1)$, $r \ge 1$.

PROOF. Due to Proposition 7.11 we can assume $v \ge 4$. We will prove by induction on r. So, assume that the cylinder conjecture is true for $(q, r - 1, v + r - 2)$. Let $\mathcal{S}$ be a spanning q^r-divisible set of q^{r+1} points in $\mathrm{PG}(v' - 1, q)$, where $v' = v + r - 1$ and $r \ge 2$. Now let $\mathcal{F}$ be the set of points F such that there exists a point $S \in \mathcal{S}$ with $A(S, F) \subseteq \mathcal{S}$.

We will structure our proof into some intermediate results:

(1) For each point $S \in \mathcal{S}$ there exists an $(r - 1)$-space B such that $A(S, B) \subseteq \mathcal{S}$.

(2) $\dim(\langle\mathcal{F}\rangle) \in \{r - 1, r\}$.

(3) For each $S_1, S_2 \in \mathcal{S}$ there exists an $(r - 1)$-space B such that $A(S_1, B)$ and $A(S_2, B)$ are both contained in $\mathcal{S}$.

(4) Let $S \in \mathcal{S}$ be a point such that there exist $(r - 1)$-spaces $B_1 \ne B_2$ with $A(S, B_1), A(S, B_2) \subseteq \mathcal{S}$. Then, we have $A(S, \langle\mathcal{F}\rangle) \subseteq \mathcal{S}$.

(5) $\mathcal{S}$ is an $(r + 1)$-cylinder.

For (1) we use Lemma 7.7 to conclude that there are at most $q^{v'-r-1}+1-q$ hyperplanes that do not contain exactly q^r points from $\mathcal{S}$. Thus, for each point $S \in \mathcal{S}$ at least one of the $\frac{q^{v'-1}-1}{q-1}$ hyperplanes containing S contains exactly q^r points from $\mathcal{S}$. If H is such a hyperplane, we can apply induction for H and conclude that $\mathcal{S} \cap H$ can be partitioned into $\cup_{i=1}^{q} A(S_i, B)$ for some $(r-1)$-space B and q points $S_i \in \mathcal{S}$. Of course there exists an index $1 \le j \le q$ with $S \in A(S_j, B)$ and hence $A(S,B) = A(S_j, B)$.

For (2) we note that every point $F \in \mathcal{F}$ is contained in every empty hyperplane, as F is the only point in $A(S,F)$ not in $\mathcal{S}$, so that $\langle \mathcal{F} \rangle$ is contained in the intersection of all empty hyperplanes. Since there are exactly $\frac{q^{v'-\dim(\langle \mathcal{F} \rangle)}-1}{q-1}$ hyperplanes containing $\langle \mathcal{F} \rangle$ we conclude from Lemma 7.9 that $\dim(\langle \mathcal{F} \rangle) \le r+1$ and moreover if equality holds then every hyperplane containing $\langle \mathcal{F} \rangle$ is empty. Since $\mathcal{S} \neq \emptyset$, this is only possible if $\langle \mathcal{F} \rangle$ is a hyperplane itself, i.e., $v' = r+2$ and $v = 3$. Thus, we have $\dim(\langle \mathcal{F} \rangle) \le r$. If B is a subspace according to (1), then $B \subseteq \mathcal{S}$ so that $\dim(\langle \mathcal{F} \rangle) \ge r-1$.

For (3) we can apply the same idea as in (1). Consider the line $L = \langle S_1, S_2 \rangle$, then L is contained in $\frac{q^{v'-2}-1}{q-1} > q^{v'-r-1}+1-q$ hyperplanes (using $r \ge 2$). So, we can use Lemma 7.7 to conclude the existence of a hyperplane H with $L \le H$ and $|\mathcal{S} \cap H| = q^r$. Induction on this hyperplane then gives the existence of an $(r-1)$-space B such that $A(S,B) \subseteq \mathcal{S} \cap H$ for all $S \in \mathcal{S} \cap H$.

For (4) we note that $B_1, B_2 \subseteq \mathcal{F}$ imply $\dim(\langle \mathcal{F} \rangle) \ge r$, so that (2) gives $\dim(\langle \mathcal{F} \rangle) = r$. If $r = 2$, then take a point F on the line $\langle \mathcal{F} \rangle$ and a point $S \in \mathcal{S}$. We will directly prove that $A(S,F) \subseteq \mathcal{S}$. We know that there are at most $q^{v'-3}-q+1$ hyperplanes not intersecting $\mathcal{S}$ in q^2 points by Lemma 7.7, so out of the q^{v-3} hyperplanes through $\langle S, F \rangle$ intersecting $\langle \mathcal{F} \rangle$ in only F, there must be at least $q-1$ hyperplanes containing exactly q^2 points. So take one such hyperplane, apply induction and find that $A(S,F) \subseteq \mathcal{S}$. It follows that $A(S, \langle \mathcal{F} \rangle) \subseteq S$ for all $S \in \mathcal{S}$, i.e., (4) is valid for $r = 2$.

Now assume $r \ge 3$. We can find a point $S \in \mathcal{S}$ and distinct $(r-1)$-spaces B_1, B_2 such that $A(S, B_1)$ and $A(S, B_2)$ both are contained in $\mathcal{S}$. Now, take a point $F \in \langle \mathcal{F} \rangle \setminus \{B_1, B_2\}$, and consider any 3-space π through $\langle S, F \rangle$ not intersecting $B_1 \cap B_2$. Then this 3-space π intersects B_1 and B_2 each in a point, say F_1 and F_2. There are $\frac{q^{v'-3}-1}{q-1}$ hyperplanes through this 3-space, which is more than $q^{v'-r-1}-q+1$ if $r \ge 3$. We again conclude by induction that there must be a $(r-1)$-space B such that $A(S,B) \subseteq \mathcal{S}$. As F_1 and F_2 must be contained in B, we conclude that F must also be and hence $A(S,F) \subseteq \mathcal{S}$. It follows that $A(S, \langle \mathcal{F} \rangle) \subseteq S$ for all $S \in \mathcal{S}$, i.e., (4) is valid

For the final step (5) we assume that there exists a point $S \in \mathcal{S}$ such that for all $(r-1)$-spaces B_1, B_2 with $A(S, B_1), A(S, B_2) \subseteq \mathcal{S}$ we have $B_1 = B_2$. From (3) we then conclude $A(S', B_1) \subseteq \mathcal{S}$ for all $S' \in \mathcal{S}$, so that modulo B_1 we obtain a set $\mathcal{S}'$ of q^2 points that is q-divisible and has dimension $v - r + 1 = v'$. For this set $\mathcal{S}'$ we can apply the cylinder conjecture for $(v', 1, q)$, i.e., $\mathcal{S}' = \cup_{i=1}^{q} A(S_i'', B)$ for some points S_i'' and B. By construction, we then have $\mathcal{S} = \cup_{i=1}^{q} A(S_i'', \langle B, B_3 \rangle)$, i.e., $\mathcal{S}$ is an $(r+1)$-cylinder. Note that this case indeed has to occur too if $\dim(\langle \mathcal{F} \rangle) = r-1$. Otherwise, i.e., if no such point $S \in \mathcal{S}$ exists such that B_1 is unique, we can apply (4) to conclude $A(S, \langle \mathcal{F} \rangle) \subseteq \mathcal{S}$ for all $S \in \mathcal{S}$. Again, we conclude that $\mathcal{S}$ is an $(r+1)$-cylinder. □

Corollary 7.17

The cylinder conjecture is true for (q, r, v) iff it is true for $(q, 1, v - r + 1)$.

Our next aim is to show that the cylinder conjecture is true for all parameters (q, r, v) where $q \in \{2, 3\}$.

LEMMA 7.18

Let $\mathcal{S}$ be a spanning set of q^{r+1} points in $\operatorname{PG}(v-1, q)$. If every hyperplane of $\operatorname{PG}(v-1, q)$ contains either q^r or no point from $\mathcal{S}$, then $v = r+2$ and $\mathcal{S} \simeq \operatorname{AG}(v-1, q)$.

PROOF. Setting $\Delta = q^r$, the standard equations give $v = r + 2$, so that we can apply Proposition 7.11. □

COROLLARY 7.19

The cylinder conjecture is true for $(2, r, v)$, i.e., for all cases where $q = 2$.

PROPOSITION 7.20

Let $\mathcal{K}$ be a 3-divisible projective $(9, \le 6)$-arc in $\operatorname{PG}(v-1, 3)$. Then, $\mathcal{K}$ is a 2-cylinder.

PROOF. Assume, to the contrary, that $\mathcal{K}$ is not a 2-cylinder, so that Proposition 7.11 implies $v \ge 4$. Since the maximum multiplicity of a hyperplane is 6, each subspace of multiplicity 6 is a hyperplane. Assume that K is a subspace of multiplicity 4, so that $\dim(K) \le v - 2$. We denote the codimension $v - \dim(K)$ of K by x, i.e. $x \ge 2$. Since there are $[x]_3$ hyperplanes through K, every 1-point outside of K is contained in $[x-1]_3$ hyperplanes, and every hyperplane through K has multiplicity 6, we have $2[x]_3 = 5[x-1]_3$, so that $3^{x-1} = -3$, which is impossible. Thus, no subspace can have a multiplicity of exactly 4. From the standard equations we compute $a_0 = \left(3^{v-2} - 1\right)/2$, $a_3 = \left(7 \cdot 3^{v-2} + 3\right)/2$, and $a_6 = \left(3^{v-2} - 3\right)/2$, so that $a_6 \ge 3$. Let H be such a hyperplane with $\mathcal{K}(H) = 6$. Since $\mathcal{K}|_H$ is spanning, we have $\dim(H) \le 6$. If $\dim(H) = 6$, then we can assume w.l.o.g. that the 1-points in H are given by $\langle e_1 \rangle, \ldots, \langle e_6 \rangle$, where the e_i denote the unit vectors. With this, the subspace $\langle e_1, \ldots, e_4 \rangle$ would have multiplicity 4, which is a contradiction. Now assume $\dim(H) = 5$ and that the 1-points in H are given by $\langle e_1 \rangle, \ldots, \langle e_5 \rangle$ and a sixth point P. Consider the subspace $\langle e_1, \ldots, e_4 \rangle$. Since it does not contain e_5 and there is no subspace of multiplicity four, it has to contain P, i.e., the fifth coordinate of the vectors in P are zero. The same is true if we consider the subspace $\langle \{e_1, \ldots, e_5\} \backslash e_i \rangle$, i.e., we can conclude that the i-th coordinate of the vectors in P are zero for all $1 \le i \le 5$, which is a contradiction. Thus, there remain the possibilities $\dim(H) \in \{3, 4\}$, i.e., $v \in \{4, 5\}$. From Theorem 7.14 we conclude that the maximum line multiplicity γ_2 is at most 2. So, if $\dim(H) = 3$, then $\mathcal{K}|_H$ would be a $(6, \le 2)$-arc in $\operatorname{PG}(2, 3)$, which does not exist. Thus, we have $\dim(H) = 4$ and $v = 5$. Using Corollary 7.13 we conclude that every plane π in H has a multiplicity in $\{0, 2, 3, 5\}$. Since there is no $(5, \le 2)$-arc in $\operatorname{PG}(2, 3)$, we have $\mathcal{K}|_\pi \ne 5$. For the spectrum (a'_i) of $\mathcal{K}|_H$ the standard equations yield the unique solution $a'_0 = 8$, $a'_2 = 18$, $a'_3 = 14$. Now consider the subspaces spanned by one of the $\binom{6}{3} = 20$ triples of 1-points in H. Since the arc is projective and there is no 3-line all these subspaces are pairwise different planes, i.e., $a'_3 \ge 20$, which is a contradiction. □

Corollary 7.17 directly implies:

COROLLARY 7.21

The cylinder conjecture is true for $(3, r, v)$, i.e., for all cases where $q = 3$.

An interesting implication is that the dimension k of every 3^r-divisible projective $\left[3^{r+1}, k\right]_3$-code is at most $r + 3$ for every positive integer r. We remark that Ward's upper bound on the dimension of divisible codes, see e.g. [151] and Exercise 7.3, is not strong enough to give this result. Using the software package `LinCode` [98] we have computationally checked that there is no 3-divisible $[9, \ge 5]_3$-code, no 9-divisible $[27, \ge 6]_3$-code, and no 27-divisible $[81, \ge 7]_3$-code, i.e., it might not be necessary to assume that the arc is projective to obtain the stated upper bound for the dimension.

We remark that the truth of the cylinder conjecture for $(2, 1, 4)$ and $(3, 1, 4)$ was also proven in [38].

In principle it is possible to enumerate all projective q^r-divisible $\left[q^{r+1}, v\right]_q$ codes and to check whether the corresponding point sets are r-cylinders for given finite parameters. However, given the currently available software for the exhaustive enumeration of linear codes, this approach is limited to rather small parameters. Nevertheless we report our corresponding findings here. The last step, i.e., checking whether all resulting point sets are $(r + 1)$-cylinders, can be replaced by a counting argument. The numbers of projective linear codes over $\mathbb{F}_5$ of effective lengths $n = 5$ ordered by their dimension k are given by $2^1 3^4 4^3 5^1$, as can be easily enumerated using the software package `LinCode` [98] – even a classification by hand is possible. So, Construction 7.2 yields $3^1 4^4 5^3 6^1$, again ordered by their dimension k, 5-divisible projective linear codes over $\mathbb{F}_5$ of effective lengths $n = 25$. Using `LinCode` we verified that there are no further 5-divisible projective linear codes over $\mathbb{F}_5$ of effective length $n = 25$. Thus, we have computationally proven that the cylinder conjecture is true for $(5, 1, v)$, where the dimension v is arbitrary. This covers the special case $(5, 1, 4)$ that we treat in the subsequent section. From Corollary 7.17 we conclude:

COROLLARY 7.22

The cylinder conjecture is true for $(5, r, v)$, i.e., for all cases where $q = 5$.

For $q \in \{2, 3, 4\}$ we can perform the same computation. The cases $q = 2, 3$ verify our theoretical findings for $(q, 1, v)$. The number of projective linear codes over $\mathbb{F}_4$ of effective lengths $n = 4$ ordered by their dimension k are given by $2^1 3^2 4^1$. The number of 4-divisible projective linear codes over $\mathbb{F}_4$ of effective lengths $n = 16$ ordered by their dimension k are given by $3^1 4^2 5^2$. In other words, the cylinder conjecture is true for $(4, 1, 3)$ and $(4, 1, 4)$ but not for $(4, 1, 5)$. For $v \ge 6$ there do not exist projective 4-divisible $[16, v]_4$-codes so that the cylinder conjecture is true for $(4, 1, v)$, where $v \ge 6$, by convention. So, Corollary 7.17 gives:

COROLLARY 7.23

The cylinder conjecture is true for $(4, r, v)$ iff $v \neq r + 4$.

Of the two linear codes in dimension 5, the one that does not correspond to a 2-cylinder has a generator matrix given by

$$\begin{pmatrix} 0110101101110000 \\ 1101100011101000 \\ 1100011111000100 \\ 1111111000000010 \\ 0111010110100001 \end{pmatrix}.$$

The code has weight enumerator $W(z) = 1z^0 + 90z^8 + 840z^{12} + 93z^{16}$ and an automorphism group of order 1935360. Considered over $\mathbb{F}_2$ the stated generator matrix gives a linear $\mathbb{F}_2$ code with weight enumerator $W(z) = 1z^0 + 30z^8 + 1z^{16}$, i.e., the code is an affine 5-space, which is 2^3-divisible.

Computationally we also verified that the cylinder conjecture is true for $(4, 2, 5)$, which also follows from Theorem 7.16. Due to the counter example for $(4, 1, 5)$ there is also a counter example for $(4, 2, 6)$, see Proposition 7.15 . We have computationally checked that this counter example is unique.

In order to generalize the above counter example to the cylinder conjecture for $(4, 1, 5)$ we remark that for each integer $h \geq 2$ the field $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^h}$, so that $\mathbb{F}_{q^h}^v \cong \mathbb{F}_q^{vh}$. Using this isomorphism we can we can embed every multiset of points $\mathcal{M}'$ in $\mathbb{F}_q^v$ as a multiset of points $\mathcal{M}$ (of the same cardinality) in $\mathbb{F}_{q^h}^v$. Moreover, every k-space in $\mathbb{F}_{q^h}^v$ corresponds to a kh-space in $\mathbb{F}_q^{vh}$.

LEMMA 7.24

Let $\mathcal{S}'$ be a spanning projective $2h$-cylinder in $\mathbb{F}_q^v$, where $h \geq 2$. Then the corresponding embedding $\mathcal{S}$ in $\mathbb{F}_{q^h}^v \cong \mathbb{F}_q^{vh}$ is a spanning projective q^h-divisible $\left(\left(q^h\right)^2, < q^{2h}\right)$-arc in $\mathrm{PG}\left(v-1, q^h\right)$ that is not a 2-cylinder

PROOF. First we observe $\#\mathcal{S} = \#\mathcal{S}' = q^{2h} = \left(q^h\right)^2$. Since $\mathcal{S}'$ is spanning and projective, the same applies to $\mathcal{S}$. Assume that $\mathcal{S}$ is a 2-cylinder and let L be one of the q^h-lines. Consider to 1-points P_1, P_2 on L and denote by P_1', P_2' be the corresponding points in $\mathcal{S}'$. The lines $L' = \langle P_1', P_2' \rangle$ has multiplicity at most q in $\mathcal{S}'$, so that L has a multiplicity of at most q in $\mathcal{S}$, which is a contradiction due to $h \geq 2$. An arbitrary hyperplane H in $\mathbb{F}_{q^h}^v$ has dimension $(v-1)h$ over $\mathbb{F}_q$. Since $\mathbb{F}_q^v$ has dimension v over $\mathbb{F}_q$, there exists a subspace K in $\mathbb{F}_q^v$ of dimension at least $v - h$ such that $|\mathcal{S} \cap H| = |\mathcal{S}' \cap K|$. Note that $\mathcal{S}'$ is q^{2h-1}-divisible, so that $|\mathcal{S}' \cap K| \equiv 0 \pmod{q^h}$ due to Lemma 5.9. Thus, $\mathcal{S}$ is q^h-divisible. □

COROLLARY 7.25

For each integer $h \geq 2$ the cylinder conjecture is wrong for $\left(q^h, r, v\right)$, where $2h + r \leq v \leq 2h + r + q - 2$.

PROOF. From Lemma 7.24 and Lemma 7.4 we conclude that the cylinder conjecture is wrong for $\left(q^h, 1, v\right)$, where $2h + 1 \leq v \leq 2h - 1 + q$, so that Corollary 7.17 gives the general statement. □

If $v = 2h + r$, then the point set $\mathcal{S}'$ in Lemma 7.24 is an affine geometry, so that $\mathcal{S}$ is an affine subgeometry. For the special case $h = 2$ one also speaks of a Baer (sub-) geometry. In general, our construction is an instance of the technique of the so-called field reduction, which yields a lot of non-trivial constructions and characterizations of geometric and algebraic structures, see e.g. [121]. Of course one might conjecture that every projective q^r-divisible $\left(q^{r+1}, \le (q-1)q^r\right)$-arc in $\operatorname{PG}(v-1, q)$ is either an $(r+1)$-cylinder or arises from a cylinder over a subfield.

EXERCISE 7.1 Let $\mathcal{S}$ be a q^r-divisible spanning set of λq^r points in $\operatorname{PG}(v-1, q)$. Let K be a subspace of codimension 2 in $\operatorname{PG}(v-1, q)$. Assume that $|\mathcal{S} \cap K| = kq^{r-1}$ for some integer $0 < k < q$. Show that any hyperplane containing K contains at most $(\lambda - q + k)q^r$ points from $\mathcal{S}$.

EXERCISE 7.2 Let $\mathcal{S}$ be a q^r-divisible spanning set of q^{r+1} points in $\operatorname{PG}(v-1, q)$, where $v = r + 3$. Show that if $\mathcal{S}$ contains a full affine $(r+1)$-space, then $\mathcal{S}$ is an $(r+1)$-cylinder.

EXERCISE 7.3 Use Ward's upper bound on the dimension of divisible codes, see e.g. [151, Theorem 6], to conclude an upper bound on the dimension k of a 3^r-divisible $\left[3^{r+1}, k\right]_3$-code. Also compute the upper bound for the case where weight 3^r does not occur.

7.2 The cylinder conjecture for $\mathbf{r} = 1$ and $\mathbf{v} = 4$

In this section we want to consider the cylinder conjecture for $(q, 1, 4)$. Instead of a 2-cylinder we well just speak of a cylinder. From Corollary 7.10 we conclude that each q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(3, q)$ satisfies $a_0 \ge 1$, i.e., it can be embedded in $\operatorname{AG}(3, q)$. From Corollary 7.13 and the existence of an empty hyperplane we conclude:

LEMMA 7.26
Let $\mathcal{K}$ be a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(3, q)$. Then, the multiplicity of each line L in a kq-plane H is contained in $\{0, k, k+1, \dots, q\}$.

Since each q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(v-1, q)$ that contains a q-line is a cylinder, see Theorem 7.14, we have:

LEMMA 7.27
Let $\mathcal{K}$ be a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(3, q)$ that is not a cylinder. Then, the maximum multiplicity of line satisfies $\gamma_2 \le q - 1$.

LEMMA 7.28
Let $\mathcal{K}$ be a projective $(q(q-1), \le q-1)$-arc in $\operatorname{PG}(2, q)$. Then, there exists a line with a multiplicity not in $\{0, q-1\}$.

PROOF. Otherwise the first two standard equations would give $a_0 = 1$ and $a_{q-1} = q^2 + q$, so that the third yields the contradiction

$$\binom{q-1}{2} a_{q-1} = \frac{q(q-1)(q^2-q-2)}{2} < \frac{q(q-1)(q^2-q-1)}{2} = \binom{q(q-1)}{2}.$$

□

COROLLARY 7.29

Let $\mathcal{K}$ be a q-divisible projective $\big(q^2, \le q^2 - q\big)$-arc in $\mathrm{PG}(3,q)$. *If $\mathcal{K}$ is not a cylinder, then there is no $(q-1)q$-plane.*

PROOF. If H is a $q(q-1)$-plane, then lemmas 7.26, 7.27, and 7.28 yield a contradiction. □

COROLLARY 7.30

Let $\mathcal{K}$ be a q-divisible projective $\big(q^2, \le q^2 - q\big)$-arc in $\mathrm{PG}(3,q)$, *where $q \in \{2,3\}$. Then, $\mathcal{K}$ is a cylinder.*

PROOF. Assume that $\mathcal{K}$ is not a cylinder, so that Corollary 7.29 implies $a_{q(q-1)} = 0$. For $q = 2$ this means that all points of $\mathcal{K}$ are contained in 0-planes, which is absurd. For $q = 3$ solving the first two standard equations give $a_0 = 1$ and $a_3 = 39$. The third implies the contradiction

$$\binom{3}{2} a_3 = 117 < 144 = \binom{9}{2} \cdot (3+1)\,.$$

□

REMARK 7.31 The argumentation of the proof of Corollary 7.30, i.e., the first three standard equations combined with Corollary 7.29, would give the unique spectrum $a_0 = 7$, $a_1 = 72$, and $a_2 = 6$ for $q = 4$.

LEMMA 7.32

Let $\mathcal{K}$ be a projective $(q(q-2), \le q-1)$-arc in $\mathrm{PG}(2,q)$, *where $q \ge 4$. Then, there exists a line with a multiplicity not in $\{0, q-2, q-1\}$.*

PROOF. Otherwise the first two standard equations would give $a_{q-1} = a_0(q-2) - (q-2)$ and $a_{q-2} = q^2 + 2q - 1 - a_0(q-1)$, so that the third yields

$$0 = a_{q-2}\binom{q-2}{2} + a_{q-1}\binom{q-1}{2} - \binom{q(q-2)}{2} = \frac{(q-2)(a_0(q-1) - 3q + 1)}{2},$$

which implies

$$a_0 = \frac{3q-1}{q-1} = 3 + \frac{2}{q-1} \notin \mathbb{N}_0.$$

□

REMARK 7.33 In the proof of Lemma 7.32 the third standard equation is needed since e.g. $(a_0, a_{q-2}, a_{q-1}) = (2, 17, 2)$ satisfies the first two standard equations for $q = 4$.

COROLLARY 7.34

Let $\mathcal{K}$ be a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(3, q)$. *If $\mathcal{K}$ is not a cylinder, then there is no $(q-2)q$-plane.*

PROOF. Due to Corollary 7.30 we can assume $q \ge 4$. If H is a $(q-2)$-plane, then lemmas 7.26, 7.27, and 7.32 yield a contradiction. □

COROLLARY 7.35

Let $\mathcal{K}$ be a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(3, q)$*, where $q = 4$. Then, $\mathcal{K}$ is a cylinder.*

PROOF. Assume that $\mathcal{K}$ is not a cylinder, so that Corollary 7.29 and Corollary 7.34 imply $a_{q(q-1)} = 0$ and $a_{q(q-2)} = 0$. For $q = 4$ solving the first two standard equations give $a_0 = 1$ and $a_4 = 84$. The third implies the contradiction

$$\binom{4}{2} a_4 = 504 < 600 = \binom{16}{2} \cdot (4+1)\,.$$

□

We might continue in the vein of Lemma 7.32 and consider projective $(q(q-3), \le q-1)$-arc in $\operatorname{PG}(2, q)$ whose line multiplicities are contained in $\{0, q-3, q-2, q-1\}$. Due to to Corollary 7.30 and Corollary 7.35 we are only interested in the cases where $q \ge 5$. It turns out that he unique possibility is given by $q = 5$ and a spectrum given by $a_0 = 6$, $a_2 = 15$, $a_3 = 10$, and $a_4 = 0$, see Exercise 7.4. So, similar to Corollary 7.34, we can conclude that a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc $\mathcal{K}$ in $\operatorname{PG}(3, q)$ that not a cylinder does not contain a $(q-3)q$-plane unless $q = 5$.

PROPOSITION 7.36

Let $\mathcal{K}$ be a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(3, q)$*, where $q = 5$. Then, $\mathcal{K}$ is a cylinder.*

PROOF. Assume that $\mathcal{K}$ is not a cylinder, so that Corollary 7.29 and Corollary 7.34 imply $a_{q(q-1)} = 0$ and $a_{q(q-2)} = 0$. With this, the standard equations for $\mathcal{K}$ yield the unique spectrum $a_0 = 11$, $a_5 = 135$, and $a_{10} = 10$. Now let H be a 10-plane with spectrum (b_i), where $b_i = 0$ for $i \notin \{0, 2, 3, 4\}$. From the standard equations we conclude $b_2 = 51 - 6b_0$, $b_3 = -38 + 8b_0$, and $b_4 = 18 - 3b_0$, so that $b_4 \ge 0$ implies $b_0 \le 6$ and $b_3 \ge 0$, $b_0 \in \mathbb{N}_0$ imply $b_0 \ge \left\lceil \frac{19}{4} \right\rceil = 5$. Assume $b_0 = 5$ and note that two 4-lines cannot share a common 1-point P since otherwise counting points on the lines $L_1, \ldots, L_6$ through P would yield the contradiction

$$10 = \#\mathcal{K}|_H = \sum_{i=1}^{6} \mathcal{K}(L_i) - 5\mathcal{K}(P) \ge 2 \cdot 4 + 4 \cdot 2 - 5 = 11$$

using $\mathcal{K}(L_i) \ge 2$ for all $1 \le i \le 6$. Thus, the 4-lines are pairwise disjoints, so that $10 = \#\mathcal{K}|_H \ge a_4 \cdot 4 = 12$, which is a contradiction. Thus, we have $b_0 = 6$, $b_2 = 15$, $b_3 = 10$, and $b_i = 0$ otherwise for the spectrum (b_i) of $\mathcal{K}|_H$.

For a line L of multiplicity 3 in H denote the other 5 hyperplanes by $H_1, \dots, H_5$. Since $\mathcal{K}(H_i) \in \{5, 10\}$ for all $1 \le i \le 5$ and $\#\mathcal{K} = 25$, there exists an index $1 \le i \le 5$ with $\mathcal{K}(H_i) = 10$. Due to $1 + b_3 \cdot 1 = 11$, there are at least eleven 10-planes, which contradicts $a_{10} = 10$. □

REMARK 7.37 Indeed, there exists a unique projective $[10, 3, \{6, 7, 8, 10\}]_5$ code $\mathcal{C}$ with generator matrix

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

c.f. [146, Section 2.4]. This code has an automorphism group of order 480 and weight enumerator $W_{\mathcal{C}}(x) = 1x^0 + 40x^7 + 60x^8 + 24x^{10}$. We remark that the existence of the above code was excluded in the proof of [38, Theorem 4], i.e., the proof is flawed. More precisely, in the last sentence of the proof where 2 further 0-line (secant) are constructed it can happen that they (partially) coincide with the four 0-lines (secants) found before.

LEMMA 7.38

Let $\mathcal{K}$ be a q-divisible projective $(q^2, \le q^2 - q)$-arc in $\mathrm{PG}(3, q)$ that is not a cylinder. Then, we have $\gamma_2 \le q - 2$ for the maximum line multiplicity.

PROOF. Due to Corollary 7.30 and Corollary 7.35 we can assume $q \ge 5$. Lemma 7.27 states that the maximum line multiplicity γ_2 is at most $q - 1$. Assume that L is a line of multiplicity $q - 1$ and denote by Q_1, Q_2 the two 0-points on L. Now let H be an arbitrary hyperplane containing L, where we have $\mathcal{K}(H) = kq$ for an integer $1 \le k < q$.

For each 1-point P on L let $L_1, \dots, L_q$ denote the q lines trough P in H that are not equal to L. Note that Lemma 7.26 implies $\mathcal{K}(L_i) \ge k$ for all $1 \le i \le q$. From

$$kq = \mathcal{K}(H) = \mathcal{K}(L) + \sum_{i=1}^{k} \mathcal{K}(L_i) - q\mathcal{K}(P) \ge q - 1 + qk - q = kq - 1$$

we conclude that $q - 1$ of the L_i, where $1 \le i \le q$, have multiplicity k and one has multiplicity $k + 1$.

Now let M be a line through Q_1 or Q_2 that is not equal L. Since $\mathcal{K}(M) \le q - 1$ there exists a 0-point R on M that is not contained in L. Let L'_i be the lines through R and Q_i in H, where $1 \le i \le 2$. By $L'_3, \dots, L'_{q+1}$ we denote the remaining $q - 1$ lines through R in H. Note that the L'_i meet the line L in a 1-points, so that $\mathcal{K}(L'_i) \in \{k, k + 1\}$ for $3 \le i \le q + 1$. From

$$kq = \mathcal{K}(H) = \sum_{i=1}^{q+1} \mathcal{K}(L'_i) - q\mathcal{K}(R) \ge \mathcal{K}(L'_1) + \mathcal{K}(L'_2) + (q - 1)k$$

we conclude $\mathcal{K}(L_1') + \mathcal{K}(L_2') \le k$, so that $\mathcal{K}(L_1'), \mathcal{K}(L_2') \in \{0, k\}$ due to Lemma 7.26. Thus, for $1 \le i \le 2$ the $q+1$ lines through Q_i in H are given by the $(q-1)$-lines L, $\frac{q-1}{k}$ lines of multiplicity 0, and $\left(q - \frac{q-1}{k}\right)$ lines of multiplicity k. Now we are ready to determine the spectrum (a_i) of H:

$$\begin{aligned} a_0 &= 2 \cdot \frac{q-1}{k} \\ a_k &= (q-1)\cdot(q-1) + 2 \cdot \left(q - \frac{q-1}{k}\right) \\ a_{k+1} &= (q-1)\cdot 1 \\ a_{q-1} &= 1 \end{aligned}$$

and $a_i = 0$ for all $i \notin \{0, k, k+1, q-1\}$. If $k = q-1$ or $k+1 = q-1$, then we would have to take the sum of both values or different , but we suppress this technical subtlety for the ease of notation. From the third standard equation we conclude

$$0 = \binom{k}{2} a_k + \binom{k+1}{2} a_{k+1} + \binom{q-1}{2} a_{q-1} - \binom{kq}{2} = q \cdot \frac{(k-1)(k-q+1)}{2},$$

so that $k \in \{1, q-1\}$.

So, considering the $q+1$ hyperplanes through L in $\mathrm{PG}(3,q)$ we conclude that q have multiplicity q and one has multiplicity $q(q-1)$, where the latter contradicts Corollary 7.29. □

LEMMA 7.39

Let $\mathcal{K}$ be a projective $(q(q-3), \le q-2)$-arc in $\mathrm{PG}(2,q)$, where $q \ge 7$. Then, there exists a line with a multiplicity not in $\{0, q-3, q-2\}$.

PROOF. Otherwise the first two standard equations would give $a_{q-2} = a_0(q-3) - (q-3)$ and $a_{q-3} = q^2 + 2q - 2 - a_0(q-2)$ so that the third yields

$$0 = a_{q-3}\binom{q-3}{2} + a_{q-2}\binom{q-2}{2} - \binom{q(q-3)}{2} = \frac{(q-3)(a_0(q-2) - 4q + 2)}{2}$$

which implies

$$a_0 = \frac{4q-2}{q-2} = 4 + \frac{6}{q-2}.$$

Since $a_0 \in \mathbb{N}_0$, we have $q \in \{3, 4, 5, 8\}$. Due to our assumption $q \ge 7$ it remains to exclude the case $q = 8$, where $a_0 = 5$, $a_5 = 48$, and $a_6 = 20$. Consider a 6-line L. The only possibility for the distribution of the multiplicities of the lines through a 0-point on L is given by $0^2 5^2 6^5$, so that there are $3 \cdot 2 = 6$ 0-lines. This contradicts $a_0 = 5$. □

The assumption $q \ge 7$ in Lemma 7.39, see Remark 7.37 for $q = 5$ and the generator matrix

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

for $q = 4$.

COROLLARY 7.40

Let $\mathcal{K}$ be a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\operatorname{PG}(3, q)$*. If $\mathcal{K}$ is not a cylinder, then there is no $(q-3)q$-plane.*

PROOF. Due to Corollary 7.30, Corollary 7.35, and Proposition 7.36 we can assume $q \ge 7$. Lemma 7.38 implies that the maximum line multiplicity γ_2 is at most $q - 2$. If H is a $(q-3)$-plane, then Lemma 7.26 and Lemma 7.39 yield a contradiction. □

LEMMA 7.41

Let $\mathcal{K}$ be a projective $(q(q-4), \le q-2)$-arc in $\operatorname{PG}(2, q)$ *with line multiplicities contained in $\{0, q-2, q-3, q-4\}$. Then, we have $q \le 13$.*

PROOF. Solving the standard equations gives

$$\begin{aligned}
a_{q-2} &= \frac{(q-4)(5q-3)}{2} - \frac{(q-3)(q-4)}{2}a_0 \\
a_{q-3} &= -(q-4)(5q-2) + (q-2)(q-4)a_0 \\
a_{q-4} &= \frac{7q^2 - 19q + 6}{2} - \frac{(q-2)(q-3)}{2}a_0,
\end{aligned}$$

so that $a_{q-2} \ge 0$ implies

$$a_0 \le \frac{5q-3}{q-3} = 6 - \frac{q-15}{q-3}$$

and $a_{q-3} \ge 0$ implies

$$a_0 \ge \frac{5q-2}{q-2} = 5 + \frac{8}{q-2}.$$

So, for $q \ge 16$ we have $a_0 \notin \mathbb{N}_0$, which is a contradiction. □

REMARK 7.42 In the proof of Lemma 7.41 the only possible choices for a_0 are given by

- $q = 7$: $a_0 \in \{7, 8\}$, where $(a_0, a_{q-4}, a_{q-3}, a_{q-2}) = (7, 38, 6, 6)$ or $(8, 28, 21, 0)$;
- $q = 8$: $a_0 = 7$, where $(a_0, a_{q-4}, a_{q-3}, a_{q-2}) = (7, 46, 16, 4)$;
- $q = 9$: $a_0 = 7$, where $(a_0, a_{q-4}, a_{q-3}, a_{q-2}) = (7, 54, 30, 0)$;
- $q = 11$: $a_0 = 6$, where $(a_0, a_{q-4}, a_{q-3}, a_{q-2}) = (6, 106, 7, 14)$;
- $q = 13$: $a_0 = 6$, where $(a_0, a_{q-4}, a_{q-3}, a_{q-2}) = (6, 141, 27, 9)$.

This list can be further reduced, see Exercise 7.5.

LEMMA 7.43

Let $\mathcal{K}$ be a projective $(21,5)$-arc in $\operatorname{PG}(2,7)$, whose line multiplicities are contained in $\{0,3,4,5\}$. Then the spectrum is given by $a_0=8$, $a_3=28$, $a_4=21$, and $a_i=0$ otherwise.

PROOF. Given the prove of Lemma 7.41 it remains to exclude the possible spectrum $a_0=7$, $a_3=38$, $a_4=6$, and $a_5=6$. Consider a 4-line L. Through each of the four 0-points on L there go at least two 0-lines, since otherwise $1\cdot 0+6\cdot 3+1\cdot 4=22>21=\#\mathcal{K}$. However, this gives at least $4\cdot 2=8>7=a_0$ 0-lines, which is a contradiction. □

REMARK 7.44 An arc with parameters and spectrum as specified in Lemma 7.43 indeed exists.

LEMMA 7.45

No 7-divisible projective $(49,21)$-arc in $\operatorname{PG}(3,7)$ with $\gamma_2\le 5$ exists.

PROOF. Assume, to the contrary, the existence of such an arc $\mathcal{K}$ and let H be a 21-plane. From Lemma 7.43 we conclude that the spectrum (b_i) of $\mathcal{K}|_H$ satisfies $b_0=8$, $b_3=28$, $b_4=21$, and $b_i=0$ otherwise. Consider the possible hyperplane distributions through a 0-line in H: $0^5 7^1 21^2$, $0^5 14^2 21^1$, $0^4 7^2 14^1 21^1$, and $0^3 7^4 21^1$. In each case there are at least three 0-planes through a 0-line in H, so that there are at least $3b_0=24$ 0-planes in total. However, solving the standard equations for $\{a_0,a_7,a_{14}\}$ gives $a_0=22-a_{21}$, $a_7=357+3a_{21}$, and $a_{14}=21-3a_{21}$, so that $a_0\le 22$. □

LEMMA 7.46

Let $\mathcal{K}$ be a 7-divisible projective $(49,42)$-arc in $\operatorname{PG}(3,7)$. Either $\mathcal{K}$ is a cylinder or the spectrum is given by $a_0=22$, $a_7=357$, $a_{14}=21$ and there exists a hyperplane H such that $\mathcal{K}|_H$ is a projective $(14,5)$-arc in $\operatorname{PG}(2,7)$ whose line multiplicities are contained in $\{0,2,3,4,5\}$.

PROOF. Assume that $\mathcal{K}$ is not a cylinder. Due to Corollary 7.29, Corollary 7.34, and Corollary 7.40 the multiplicities of the hyperplanes are contained in $\{0,7,14,21\}$. Lemma 7.38 gives $\gamma_2\le 5$, so that Lemma 7.45 yields $a_{21}=0$. With this, the standard equations have the stated solution. So, let H be one of the 14-planes. From Lemma 7.26 we finally conclude that $\mathcal{K}|_H$ does not contain a 1-line. □

REMARK 7.47 After 1671 seconds of computation time `QextNewEdition` claims that there are no projective $(14,\le 5)$-arcs in $\operatorname{PG}(2,7)$ without lines of multiplicity 1. If we additionally assume that there is no line of multiplicity 5, then 908 seconds of computation time are needed. Using Lemma 7.46 this implies the truth of the cylinder conjecture for $(7,1,4)$.

In the following we want to give an alternative, computer-free proof of the cylinder conjecture for $(7,1,4)$.

LEMMA 7.48

Let $\mathcal{K}$ be a projective $(14, 5)$-arc in $\mathrm{PG}(2, 7)$, whose line multiplicities are contained in $\{0, 2, 3, 4, 5\}$. Then, the possible spectra $(a_0, a_2, a_3, a_4, a_5)$ are either $(10, 37, 2, 8, 0)$, $(11, 31, 10, 5, 0)$, $(12, 25, 18, 2, 0)$, $(11, 30, 13, 2, 1)$, or $(10, 36, 5, 5, 1)$.

PROOF. Solving the standard equations for $\{a_0, a_2, a_3\}$ gives

$$\begin{aligned} a_0 &= \frac{38}{3} - a_5 - \frac{1}{3}a_4 \\ a_2 &= 21 + 5a_5 + 2a_4 \\ a_3 &= \frac{70}{3} - 5a_5 - \frac{8}{3}a_4 \end{aligned}$$

From $a_0 \in \mathbb{N}_0$ we conclude $a_4 \equiv 2 \pmod 3$, so that especially $a_4 \geq 2$. With this, $a_3 \in \mathbb{N}_0$ yields $a_4 \leq 8$ and $a_5 \leq 3$.

In order to show $a_5 \leq 1$ we consider a 5-line L. Now, let P be an arbitrary 1-point on L and Q be an arbitrary 0-point on L. Counting the points on the lines $L, L_1, \dots, L_7$ through P gives

$$14 = \#\mathcal{K} = \mathcal{K}(L) + \sum_{i=1}^{7} \mathcal{K}(L_i) - 7\mathcal{K}(P) = \mathcal{K}(L_1) + \sum_{i=2}^{7} \mathcal{K}(L_i) - 2 \geq \mathcal{K}(L_1) + 6 \cdot 2 - 2 = \mathcal{K}(L_1) + 10,$$

so that there is no 5-line through P besides L. Now assume that M is a 5-line through Q and let R be a 0-point on M not equal to Q. By $L'_0, \dots, L'_7$ we denote the lines through R, where we assume $L'_0 = M$. Since five of the lines $L'_1, \dots, L'_7$ hit L in a point they have multiplicity at least 2, which yields at least $5 + 5 \cdot 2 = 15 > 14$ points in $\mathcal{K}$, which is a contradiction. Thus, there is also no 5-line through Q besides L, so that a_5 is at most 1.

To sum up, if $a_5 = 0$, then $a_3 \in \mathbb{N}_0$ implies $a_4 \in \{2, 5, 8\}$, and if $a_5 = 1$, the $a_3 \in \mathbb{N}_0$ implies $a_4 \in \{2, 5\}$. Plugging into the above equations give the five stated spectra. □

Note that we have applied the same "technique" to conclude $a_5 \leq 1$ as the one used in the proof of Lemma 7.38.

LEMMA 7.49

Let $\mathcal{K}$ be a projective $(14, \leq 5)$-arc in $\mathrm{PG}(2, 7)$, whose line multiplicities are contained in $\{0, 2, 3, 4, 5\}$. Then, we have $(a_4, a_5) \neq (8, 0)$.

PROOF. Assume that $(a_4, a_5) = (8, 0)$, so that $a_0 = 10$, $a_2 = 37$, and $a_3 = 2$. Let L be a 4-line and P be a 1-point on L. Since there is no 5-line at all, at least one 3-line must go through P. (The possible distributions of the line multiplicities are $4^1 3^3 2^4$ and $4^2 3^1 2^5$.) This gives $a_3 \geq 4$, which contradicts $a_3 = 2$. □

LEMMA 7.50

Let $\mathcal{K}$ be a projective $(14, \le 5)$-arc in $\operatorname{PG}(2,7)$, whose line multiplicities are contained in $\{0,2,3,4,5\}$. Then, we have $a_5 = 0$.

PROOF. Let L be a 5-line and Q_1, Q_2, and Q_3 be the 0-points on L. Define $\mathcal{K}'$ by $\mathcal{K}'(Q_i) = 2$ for all $1 \le i \le 3$ and $\mathcal{K}'(P) = \mathcal{K}(P)$ for all other points P. Noting that all 0-lines of $\mathcal{K}$ have to intersect L in one of the points Q_i, we observe that $\mathcal{K}'$ is a double-blocking set of cardinality 20 that contains the full line L. Setting $\mathcal{K}''(P) = \mathcal{K}'(P) - 1$ for all $P \in L$ and $\mathcal{K}''(P) = \mathcal{K}'(P)$ otherwise, we observe that $\mathcal{K}''$ is a non-trivial blocking set, i.e., it contains no full line. In [19] it was shown that a non-trivial blocking set in $\operatorname{PG}(2,p)$ has cardinality at least $3(p+1)/2$, which is met with equality in our situation. In that case every 1-point is contained on exactly $(p-1)/2$ 1-lines, see [19]. Blocking sets of cardinality 12 in $\operatorname{PG}(2,7)$ have been classified in [20]. Besides the projective triangle, see [125] for a classification for Rédei types, there exists a unique sporadic example of non-Rédei type. So, we may invert the above construction by interchanging 0- and 1-points on a 3-line of the blocking set $\mathcal{K}''$ in order to obtain all possibilities. In the sporadic case the line multiplicities through a 1-point are given by $1^3 2^2 4^3$, i.e., there is no line of multiplicity 3. In the case of the projective triangle let R_1, R_2, R_3 be the corners of the triangle, i.e., those 1-points P where the multiplicities of the lines through P are given by $1^3 2^3 5^2$. For the other nine points the line multiplicities of the lines through the 1-point are given by $1^3 2^1 3^3 5^1$. So, let L_1 be the line connecting R_2 and R_3, L_2 the line connecting R_1 and R_3, and L_3 the line connecting R_1 and R_2. By P_1, P_2, P_3 we denote the 1-points on a 3-line L', where we assume w.l.o.g. that the point P_i is on the line L_i. We obtain $\mathcal{K}$ by inverting the point multiplicities on L', i.e., by setting $\mathcal{K}(P') = 1 - \mathcal{K}''(P')$ for all points P' on L'. Note that the line trough P_1 and R_1 is a 1-line in $\mathcal{K}$ – contradiction. (The latter can be deduced less explicitly by considering the multiplicities of the lines through P_1. We have the 5-line L', the 4-line L_1, and exactly three 0-lines, since in $\mathcal{K}''$ every 1-point is contained in exactly three 1-lines. Thus, one of the remaining three lines through P_1 has to be a 1-line.) □

In order to exclude the existence of a $(14,4)$-arc $\mathcal{K}$ in $\operatorname{PG}(2,7)$ with spectrum $(a_0, a_1, a_2, a_3, a_4) = (11, 0, 31, 10, 5)$, we consider the dual arc $\mathcal{K}^\perp$. The number $\lambda_i(\mathcal{K}^\perp)$ of i-points of the dual arc $\mathcal{K}^\perp$ equals the number $a_i(\mathcal{K})$ of hyperplanes with multiplicity i with respect to $\mathcal{K}$. For the other direction, 1-points in $\mathcal{K}$ correspond to 21-lines in $\mathcal{K}^\perp$ and 0-points in $\mathcal{K}$ correspond to 14-lines in $\mathcal{K}^\perp$. If $m_1, \dots, m_8$ are the multiplicities of the points on a given line and $m_1 \ge \dots \ge m_8$, then we call $(m_1, \dots, m_8)$ the type of the line. Due to the above considerations, we can assume $\lambda_5(\mathcal{K}^\perp) = a_5(\mathcal{K}) = 0$ in the following, so that the possible line types of a line L in $\mathcal{K}^\perp$ are given as follows:

$\mathcal{K}^\perp(L)$	type of L	name	exponent notation
14	$(4,4,4,2,0,0,0,0)$	A_1	$4^3 2^1 0^4$
	$(4,4,2,2,2,0,0,0)$	A_2	$4^2 2^3 0^3$
	$(4,2,2,2,2,2,0,0)$	A_3	$4^1 2^5 0^2$
	$(2,2,2,2,2,2,2,0)$	A_4	$2^7 0^1$
	$(4,4,3,3,0,0,0,0)$	A_5	$4^2 3^2 0^4$
	$(4,3,3,2,2,0,0,0)$	A_6	$4^1 3^2 2^2 0^3$
	$(3,3,2,2,2,2,0,0)$	A_7	$3^2 2^4 0^2$
	$(3,3,3,3,2,0,0,0)$	A_8	$3^4 2^1 0^3$
21	$(4,4,3,2,2,2,2,2)$	B_1	$4^2 3^1 2^5$
	$(4,3,3,3,2,2,2,2)$	B_2	$4^1 3^3 2^4$
	$(3,3,3,3,3,2,2,2)$	B_3	$3^5 2^3$

LEMMA 7.51

No $(14,4)$*-arc* $\mathcal{K}$ *in* $\mathrm{PG}(2,7)$ *with spectrum* $(a_0,a_1,a_2,a_3,a_4) = (11,0,31,10,5)$ *exists.*

PROOF. Assume the contrary. Instead of $\mathcal{K}$ we consider its dual $\mathcal{K}^\perp$. The number λ_i of i-points is given by $\lambda_0 = 11$, $\lambda_1 = 0$, $\lambda_2 = 31$, $\lambda_3 = 10$, and $\lambda_4 = 5$. There are fourteen 21-lines and forty-three 14-lines.

Assume that L is a line of type B_3. Let P_3 be a 3-point on L. The five 14-lines through P_3 use at least five further 3-points. Thus, the two 21-lines through P_3 that are not equal to L have P_3 as their unique 3-point, i.e., they are of type B_1. Counting 4-points then gives that the distribution of the types of the lines through P_3 is given by $A_6A_7^4B_1^2B_3$. Now let Q_3 be a 3-point outside of L. Each of the three 21-lines through Q_3 meets L in a 2-point since the only 21-line through a 3-point of L that contains at least two 3-points is L. Each of the five 3-points on L is incident with two lines of type B_1, so that there are at least ten lines of type B_1 meeting L in a 3-point. Since the pairs of five 4-points span at most $\binom{5}{2} = 10$ lines, each of these lines has type B$_1$ and each line through a 2-point on L contains at most one 4-point. So, the three 21-lines through Q_3, that meet L in a 2-point, each contain at least two further 3-points. Together with the five 3-points on L that are too many. Thus, in the following we assume that there is no line of type B_3.

Let P_3 be an arbitrary 3-point. The five 14-lines through P_3 contain at least five further 3-points, so that not all three 21-lines through P_3 can be of type B_2 due to $\lambda_3 = 10$. From $\lambda_4 = 5$ we conclude that not all three 21-lines through P_3 can be of type B_1. So, the possibilities are $B_1^2B_2$ or $B_1B_2^2$. In the latter case each 14-line through P_3 contains exactly two 3-points and one of these line contains a 4-point. In the first case there is no 4-point on a 14-line through P_3 and one of these lines contains exactly four 3-points. In other words, the two possible patterns of the types of the lines through P_3 are given by $A_7^4A_8B_1^2B_2$ and $A_6A_7^4B_1B_2^2$.

So, each 3-point is contained in at least one line of type B_1. Such a line contains exactly one 3-point, so that the number of lines of type B_1 is at least $\lambda_3 = 10$. Since there are $\binom{5}{2} = 10$ pairs of 4-points, there can be at most 10 lines of type B_1. So, there are exactly ten lines of type B_1 and the pattern of the types of the lines through each of the ten 3-points is $A_6A_7^4B_1B_2^2$. Counting the number of lines of type B_2 via the 3-points gives $10 \cdot 2/3 = 20/3$, which is not an integer. □

PROPOSITION 7.52

Let $\mathcal{K}$ be a q-divisible projective $\left(q^2, \le q^2 - q\right)$-arc in $\mathrm{PG}(3, q)$, where $q = 7$. Then, $\mathcal{K}$ is a cylinder.

PROOF. Assume that $\mathcal{K}$ is not a cylinder. Due to Lemma 7.46, there exists a hyperplane H so that $\mathcal{K}|_H$ is a projective $(14, 5)$-arc in $\mathrm{PG}(2, 7)$ whose line multiplicities are contained in $\{0, 2, 3, 4, 5\}$. From Lemma 7.48, Lemma 7.49, Lemma 7.50, and Lemma 7.51 the spectrum of $\mathcal{K}|_H$ is given by $(b_0, b_2, b_3, b_4, b_5) = (12, 25, 18, 2, 0)$. Note that every j-line in H, where $j \ge 2$, is contained in $(j - 1)$ planes of multiplicity 14 and $(9 - j)$ planes of multiplicity 7 in $\mathrm{PG}(3, 7)$. Thus $\mathcal{K}$ contains at least $b_3 + 2b_4 = 18 + 2 \cdot 2 = 22$ planes of multiplicity 14, which contradicts $a_{14} = 21$. □

While our computer-free proof of the cylinder conjecture for $(7, 1, 4)$ is rather lengthy, most parts are more or less systematic and might be generalized to larger field sizes. A big obstacle is that we cannot prove the truth of the observation in Remark 7.47 directly. Actually, we do not have a complete proof of this specific nonexistence result for a $(14, 4)$-arc in $\mathrm{PG}(2, 7)$ without 1-lines and just sailed around the remaining open case in the proof of Proposition 7.52. Maybe other methods are more suitable for this kind of problems in $\mathrm{PG}(2, q)$. Of course, allowing computer enumerations drastically reduces the length of the argumentation. Starting from Lemma 7.26 and Lemma 7.27 we can computationally exclude many possibilities for the restriction $\mathcal{K}|_H$ of a projective q-divisible $\left(q^2, \le q^2 - q\right)$-arc to $\mathcal{K}$ that is not a cylinder to a hyperplane H. In other words, the possible multiplicities for the weights $\mathcal{K}(H)$ for the hyperplanes can be restricted by enumeration results for 3-dimensional codes over $\mathbb{F}_q$. By considering a subcode of the 4-dimensional projective code corresponding to $\mathcal{K}$ we obtain a q^2-divisible $\left[q^2 - 1, 3\right]_q$-code C with a restricted set of weights that might also be enumerated computationally. For our example we remark that there are 54 non-isomorphic $[48, 3, \{21, 28, 35, 42\}]_7$-codes and 46 non-isomorphic $[48, 3, \{28, 35, 42\}]_7$-codes. Moreover, the information that $\mathcal{K}$ does not contain a full affine line restricts the possible residual codes of codewords in C. By that criterion 6 of of the 46 non-isomorphic $[48, 3, \{28, 35, 42\}]_7$-codes can be excluded. Similar restrictions can arise from the previously mentioned classification of projective $[kq, 3, \{(k - 1)q + 1, \ldots, k(q - 1), kq\}]_q$-codes. E.g., as also theoretically proven, all projective $[21, 3, \{15, 16, 17, 18, 21\}]7$-codes do not contain codewords of weight 15 or 16. So, in the residual code of a codeword of weight 28 in C the weights 15 and 16 cannot occur. This excludes 12 further codes. For the remaining twenty-eight $[48, 3, \{28, 35, 42\}]_7$-codes we can computationally check whether an extension to a projective $[49, 4, \{28, 35, 42\}]_7$-code exists. To this end we can utilize and ILP formulation and an ILP solver, see Section 4.2. We remark that the tightest ILP instance needed 1 238 996 branch&bound nodes and 28.75 hours of computation time. At the very least, this approach gives a computational verification of Proposition 7.52.

Let us finish with some conclusions for the cylinder conjecture for $q = 8$. Assume that $\mathcal{K}$ is an 8-divisible projective $(64, \le 56)$-arc in $\mathrm{PG}(3, q)$ that is not a cylinder. From Corollary 7.29, Corollary 7.34, Corollary 7.40, Lemma 7.41, Remark 7.42, and Exercise 7.5 we conclude that the hyperplane multiplicities with respect to $\mathcal{K}$ are contained in $\{0, 8, 16, 24\}$. Solving the standard equations for the spectrum (a_i) of $\mathcal{K}$ gives

$$\begin{aligned} a_0 &= 29 - a_{24} \\ a_8 &= 528 + 3a_{24} \\ a_{16} &= 28 - 3a_{24}, \end{aligned}$$

so that $a_0 \le 29$. How assume that H is a 24-plane and consider the spectrum (b_i) of $\mathcal{K}|_H$. Solving the standard equations for $\{b_3, b_5, b_6\}$ gives

$$\begin{aligned} b_3 &= 97 - \frac{b_4}{3} - 5b_0 \\ b_5 &= -69 - b_4 + 9b_0 \\ b_6 &= 45 - 5b_0 + \frac{b_4}{3}, \end{aligned}$$

so that $b_5 \ge 0$ implies $b_0 \ge \left\lceil \frac{69}{9} \right\rceil = 8$. Since through every 0-line in H there are at least three 0-planes, $a_0 \le 29$ implies $b_0 \le \left\lfloor \frac{29}{3} \right\rfloor = 9$. For $b_0 = 8$ we have $b_3 = 62 - b_6$, $b_4 = -15 + 3b_6$, and $b_5 = 18 - 3b_6$, so that either

$$(b_0, b_3, b_4, b_5, b_6) \in \{(8, 57, 0, 3, 5), (8, 56, 3, 0, 6)\}$$

or

$$(b_0, b_3, b_4, b_5, b_6) = (9, 52 - b_6, 3b_6, 12 - 3b_6, b_6)\,,$$

where $0 \le b_6 \le 4$. Consider a 4-line L. Through each of the five 0-points on L there are at least two incident 0-lines, so that $b_0 \ge 5 \cdot 2 = 10$. Thus, we conclude

$$(b_0, b_3, b_4, b_5, b_6) \in \{(8, 57, 0, 3, 5), (9, 52, 0, 12, 0)\}\,.$$

For the second case consider a 1-point P. Since all lines through P have to be 3- or 5-lines, we have $\#\mathcal{K} \equiv 1 \pmod 2$, which is a contradiction. For the first case we consider a 5-line L and observe that the unique possibility for the distribution of the multiplicities of the lines through a 1-point on L is given by $3^7 5^1 6^1$. Thus, besides L, there remain eight 0-lines, twenty-two 3-lines, and two 5-lines for the four 0-points on L. The only possibility for a 0-point, using only 0-, 3-, and 5-lines, is $0^3 3^3 5^3$ for the distribution of the multiplicities of the incident lines. This case cannot occur four times, so that we finaly conclude $a_{24} = 0$, which leaves the unique spectrum $(a_0, a_8, a_{16}) = (29, 528, 28)$ for $\mathcal{K}$. The above considerations are elementary and easy, but a bit adhoc. As for $q = 7$, we are again in a situation where it seems that we are missing the right tools to tackle the problem in an elegant way. (Possibly results on sets of points without tangents, see e.g. [21, 22], might be generalized to our situation.) Of course, it is very likely that the cylinder conjecture is true for $q = 8$.

EXERCISE 7.4 Let $\mathcal{K}$ be a projective $(q(q-3), \le q-1)$-arc in $\mathrm{PG}(2, q)$, where $q \ge 5$, whose line multiplicities are contained in $\{0, q-3, q-2, q-1\}$. Show that $q = 5$ and that the spectrum is given by $a_0 = 6$, $a_2 = 15$, $a_3 = 10$, and $a_4 = 0$.

EXERCISE 7.5 Exclude some possibilities from Remark 7.42.

EXERCISE 7.6 Let $\mathcal{K}$ be a projective $(14, 4)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, 7)$ with spectrum $(a_0, a_1, a_2, a_3, a_4) = (12, 0, 25, 18, 2)$. Show that the counts of the number of lines per types of the dual arc $\mathcal{K}^\perp$ are given by one of the following three possibilities:

A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	B_1	B_2	B_3
0	0	2	2	1	4	28	6	0	8	6
0	1	0	3	0	6	27	6	0	8	6
0	0	0	3	0	8	27	5	1	6	7

EXERCISE 7.7 Reformulate the proof of Lemma7.51 without using the dual arc $\mathcal{K}^\perp$.

8. Extendability results and $(\mathbf{t} \mod \mathbf{q})$-arcs

DEFINITION 8.1

An (n,s)-arc in $\mathrm{PG}(k-1,q)$ $\mathcal{K}$ is called t-extendable if there exists an $(n+t,s)$-arc $\mathcal{K}'$ in $\mathrm{PG}(k-1,q)$ with $\mathcal{K}'(P) \geq \mathcal{K}(P)$ for all $P \in \mathcal{P}$. An arc is called extendable if it is 1-extendable.

DEFINITION 8.2

An (n,s)-blocking set $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ is called reducible if there exists an $(n-1,s)$-blocking set $\mathcal{K}'$ in $\mathrm{PG}(k-1,q)$ with $\mathcal{K}'(P) \leq \mathcal{K}(P)$ for all $P \in \mathcal{P}$. A blocking set is irreducible if it is not reducible.

DEFINITION 8.3

*An (n,s)-arc with spectrum (a_i) is said to be divisible with divisor $\Delta \in \mathbb{N}$ (**also allowed** $\Delta = 1$), or Δ-divisible, if $a_i = 0$ for all $i \not\equiv n \pmod{\Delta}$.*

Alternative: An (n,s)-arc with spectrum (a_i) is said to be divisible with divisor $\Delta \in \mathbb{N}$, or Δ-divisible, if $a_i > 0$ implies $i \equiv n \pmod{\Delta}$.

In other words an arc $\mathcal{K}$ is Δ-divisible if the corresponding linear code $\mathcal{C}$ is Δ-divisible, i.e., if the weight of every codeword is divisible by Δ.

DEFINITION 8.4

An (n,s)-arc in $\mathrm{PG}(k-1,q)$ with $s \equiv n+t \pmod{\Delta}$ and spectrum (a_i) is called t-quasidivisible with divisor $\Delta \in \mathbb{N}$ (or t-quasidivisible modulo Δ) if $a_i = 0$ for all $i \not\equiv n, n+1, \ldots, n+t \pmod{\Delta}$, $1 \leq t \leq q-1$. If we speak of a t-quasidivisible arc, then Δ is assumed to be equal to the field size q.

For a t-quasidivisible arc a special σ-dual arc is of importance:

DEFINITION 8.5

Let $\mathcal{K}$ be a t-quasidivisible (n,s)-arc with divisor q in $\mathrm{PG}(k-1,q)$, where $1 \leq t < q$. By $\widetilde{K}$ we denote the σ-dual of $\mathcal{K}$ in the dual geometry $\mathrm{PG}^{\perp}(k-1,q)$, where $\sigma(x) = n+t-x \mod q$. In other words, we have

$$\widetilde{K} : \begin{cases} \mathcal{H} \rightarrow \{0,1,\ldots,t\} \\ H \mapsto \widetilde{K}(H) \equiv n+t-\mathcal{K}(H) \pmod{q} \end{cases} \tag{8.1}$$

In other words, hyperplanes of multiplicity congruent to $n + a \pmod q$ become $(t - a)$-points in the dual geometry. In particular, s-hyperplanes become 0-points with respect to $\widetilde{K}$. In general, the cardinality of $\widetilde{\mathcal{K}}$ cannot be obtained from the parameters of $\mathcal{K}$.

THEOREM 8.6 (E.g. [119, Theorem 1])

Le $\mathcal{K}$ be an (n, s)-arc in $\mathrm{PG}(k-1, q)$, which is t-quasidivisible modulo q with $1 \leq t < q$. Let $\widetilde{K}$ defined by Equation (8.1). If

$$\widetilde{K} = \sum_{i=1}^{c} \chi_{\widetilde{P}_i} + \widetilde{\mathcal{K}}' \tag{8.2}$$

for some multiset $\widetilde{\mathcal{K}}'$ in $\mathrm{PG}^{\perp}(k-1, q)$ and c not necessarily different hyperplanes $\widetilde{P}_1, \ldots, \widetilde{P}_c$ in $\mathrm{PG}^{\perp}(k-1, q)$, then $\mathcal{K}$ is c-extendable. In particular, if $\widetilde{\mathcal{K}}$ contains a hyperplane in its support, then $\mathcal{K}$ is extendable.

PROOF. We prove by induction on c. Since all maximal hyperplanes, i.e., w-hyperplanes, correspond to 0-points in the dual geometry, the condition of the theorem is that there exist a point $P \in \mathcal{P}$ which is not incident with maximal hyperplanes. So the arc $\mathcal{M}$ defined by $\mathcal{M}(P) = \mathcal{K}(P) + 1$ and $\mathcal{M}(P') = \mathcal{K}(P')$ for all $P' \in \mathcal{P}\backslash\{P\}$ is an $(n+1, w)$-arc in $\mathrm{PG}(k-1, q)$. If we increase the multiplicity of P by 1, we also increase the multiplicity of all hyperplanes through P by 1. Hence, the multiplicity of all points in the hyperplane $\widetilde{P}$ in the dual geometry is decreased by 1. W.l.o.g. we assume $\widetilde{P} = \widetilde{P}_1$, so that

$$\widetilde{\mathcal{M}} = \widetilde{\mathcal{K}} - \chi_{\widetilde{P}} = \sum_{i=2}^{c} \chi_{\widetilde{P}_i} + \widetilde{\mathcal{K}}'. \tag{8.3}$$

From the induction hypothesis we conclude that $\mathcal{M}$ is $(c-1)$-extendable. Thus, $\mathcal{K}$ is c-extendable, as claimed. □

Let us note that the condition of Theorem 8.6 is sufficient, but not necessary, since 0-points in $\mathrm{PG}^{\perp}(k-1, q)$ with respect to $\widetilde{K}$ can correspond to hyperplanes in $\mathrm{PG}(k-1, q)$ that are not of the maximum possible multiplicity with respect to the (n, s)-arc $\mathcal{K}$. However, in some situations $\mathcal{K}(H) \equiv s \pmod q$, where $H \in \mathcal{H}$, implies $\mathcal{K}(H) = s$.

In the remaining part of this chapter, for an (n, s)-arc $\mathcal{K}$ in $\mathrm{PG}(k-1, q)$, by $\widetilde{\mathcal{K}}$ we always denote the multiset in $\mathrm{PG}^{\perp}(k-1, q)$ defined by Equation (8.1).

By Theorem 8.6, the extendability of an t-quasidivisible arc $\mathcal{K}$ is linked with the structure of the multiset $\widetilde{K}$ in the dual geometry. It turns out that this multiset is highly divisible.

LEMMA 8.7

Let $\mathcal{K}$ be an arc in $\mathrm{PG}(k-1, q)$. If we have $\mathcal{K}(L) \equiv t \pmod q$ for every line L in $\mathrm{PG}(k-1, q)$ and a fixed integer t, then we have $\mathcal{K}(S) \equiv \pmod q$ for every subspace S in $\mathrm{PG}(k-1, q)$ with $\dim(S) \geq 2$. ▪

PROOF. Set $y = \dim(S)$ and assume $y \geq 3$. For a fixed point P in S let $L_1, \dots, L_l$ be the $l = [y-1]_q$ lines through P in S. With this, we compute

$$\mathcal{K}(S) = \sum_{i=1}^{l} \mathcal{K}(L_i) - (l-1) \cdot \mathcal{K}(P) \equiv [y-1]_q \cdot t - q[y-2]_q \cdot \mathcal{K}(P) \equiv t \pmod{q}.$$

□

THEOREM 8.8 (E.g. [119, Theorem 2])
Let $\mathcal{K}$ be an (n,s)-arc in $\mathrm{PG}(k-1,q)$ which is t-quasidivisible modulo q with $1 \leq t < q$. For every subspace $\widetilde{S}$, with $\dim\left(\widetilde{S}\right) \geq 2$, in the dual geometry $\mathrm{PG}^{\perp}(k-1,q)$ we have

$$\widetilde{\mathcal{K}}\left(\widetilde{S}\right) \equiv t \pmod{q}. \tag{8.4}$$

PROOF. Due to Lemma 8.7 it suffices to consider an arbitrary line $\widetilde{S}$ in the dual geometry $\mathrm{PG}^{\perp}(k-1,q)$. It corresponds to a subspace S of codimension 2 in $\mathrm{PG}(k-1,q)$. Let $H_0, \dots, H_q$ the $q+1$ hyperplanes through S. Reducing both sides of

$$n = \sum_{i=0}^{q} \mathcal{K}(H_i) - q \cdot \mathcal{K}(S)$$

modulo q, using $\mathcal{K}(H_i) \equiv n + t - \widetilde{\mathcal{K}}(H_i) \pmod{q}$ for $0 \leq i \leq q$, gives

$$n \equiv (q+1)(n+t) - \sum_{i=0}^{q} \widetilde{\mathcal{K}}(H_i)\,,$$

so that

$$\widetilde{\mathcal{K}}\left(\widetilde{S}\right) = \sum_{i=0}^{q} \widetilde{\mathcal{K}}(H_i) \equiv t \pmod{q}.$$

□

So, the multiset $\widetilde{\mathcal{K}}$ has the following properties: the multiplicity of each point is at most t; the multiplicity of each y-subspace, where $2 \leq y \leq k$, is at least $t[y]_q$ and congruent to t modulo q.

DEFINITION 8.9
An arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ is called a $(t \mod q)$-arc, where $t \in \mathbb{N}$, if we have $\mathcal{K}(S) \equiv t \pmod{q}$ for all subspace S with $\dim(S) \geq 2$ and $\mathcal{K}(P) < q$ for all points $P \in \mathcal{P}$. If there is no restriction on the point multiplicities, then we speak of a free $(t \mod q)$-arc and of a strong $(t \mod q)$-arc if the maximum point multiplicity is at most t

REMARK 8.10

- Due to Lemma 8.7, an equivalent version of Definition 8.9 is to require the condition $\mathcal{K}(S) \equiv t \pmod q$ just for all lines S in $\mathrm{PG}(k-1,q)$.
- Note that increasing or decreasing (if the point multiplicity is at least q) converts a free $(t \mod q)$-arc into another $(t \mod q)$-arc, so that we are mostly not interested in free $(t \mod q)$-arcs.
- In a few papers $(t \mod q)$-arcs are indeed strong $(t \mod q)$-arcs, so that one should carefully check the assumptions when using results from the literature.

The importance of $(t \mod q)$-arcs is due to the fact that every t-quasidivisible arc $\mathcal{K}$ gives a unique strong $(t \mod q)$-arc $\widetilde{K}$.

COROLLARY 8.11
If $\mathcal{K}$ is a t-quasidivisible arc in $\mathrm{PG}(k-1,q)$, then $\widetilde{K}$, defined by Equation (8.1), is a strong $(t \mod q)$-arc.

Note that this correspondence is not injective, i.e., different t-quasidivisible arcs can produce the same strong $(t \mod q)$-arc. The mapping $^\sim$ is also not surjective since strong $(t \mod q)$-arcs without 0-points and $1 \le t < q$ cannot be obtained by (8.1) from t-quasidivisible arcs. However, it is not clear whether all strong $(t \mod q)$-arcs with 0-points and $1 \le t < q$ come from t-quasidivisible arcs.

8.1 Constructions for $(\mathbf{t} \mod \mathbf{q})$-arcs

A few constructions for $(t \mod q)$-arcs are known.

PROPOSITION 8.12
If H is a hyperplane in $\mathrm{PG}(k-1,q)$, then χ_H is a strong $(1 \mod q)$-arc $\mathcal{K}$.

PROOF. Surely, we have $\mathcal{K}(P) \le 1$ for all $P \in \mathcal{P}$. For every subspace S with $\dim(S) \ge 2$ in $\mathrm{PG}(k-1,q)$ we have $\dim(S \cap H) \in \{\dim(S), \dim(S)-1\}$. Noting that $[x]_q \equiv [x-1]_q \equiv 1 \pmod q$ for every integer $x \ge 2$, we conclude $\mathcal{K}(S) \equiv 1 \pmod q$. □

PROPOSITION 8.13
Let $\mathcal{K}_1$ be a $(t_1 \mod q)$-arc and $\mathcal{K}_2$ be a $(t_2 \mod q)$-arc in $\mathrm{PG}(k-1,q)$. If $t = t_1 + t_2$, then $\mathcal{K}_1 + \mathcal{K}_2$ is a $(t \mod q)$-arc in $\mathrm{PG}(k-1,q)$. If $\mathcal{K}_1$ and $\mathcal{K}_2$ are strong, then $\mathcal{K}_1 + \mathcal{K}_2$ is also strong.

PROOF. The conditions of Definition 8.9 are directly verified. □

In particular, the sum of $t \in \mathbb{N}$ (not necessarily different) hyperplanes is a $(t \mod q)$-arc.

COROLLARY 8.14

Let $\mathcal{K}$ and $\mathcal{K}'$ be $(0 \mod p)$-arcs in $\mathrm{PG}(k-1,p)$, where p is a prime. Then, $\mathcal{K}+\mathcal{K}'$ and $\alpha\mathcal{K}$, where $\alpha \in \{0,\dots,p-1\}$, are also $(0 \mod p)$-arcs. In particular, the set of all $(0 \mod p)$-arcs in $\mathrm{PG}(k-1,p)$ is a vector space over $\mathbb{F}_p$.

PROPOSITION 8.15 (E.g. [136, Theorem 2])

Let $\mathcal{K}_0$ be a $(t \mod q)$-arc in a hyperplane $H \cong \mathrm{PG}(k-2,q)$ of $\mathrm{PG}(k-1,q)$, where $k \ge 2$. For a fixed point P in $\mathrm{PG}(k-1,q)$, not incident with H, we define an arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ as follows:

- *$\mathcal{K}(P)=t$;*
- *for each point $Q \neq P$ in $\mathcal{P}$ we set $\mathcal{K}(Q)=\mathcal{K}_0(R)$, where $R=\langle P,Q\rangle \cap H$.*

Then, $\mathcal{K}$ is a $(t \mod q)$-arc in $\mathrm{PG}(k-1,q)$ of cardinality $q \cdot \#\mathcal{K}_0 + t$. If $\mathcal{K}_0$ is strong, so is $\mathcal{K}$.

PROOF. Let $L_1,\dots,L_l$ denote the $l=[k-1]_q$ lines through P and $R_i = L_i \cap H$ for $1 \le i \le l$. First we observe

$$\begin{aligned}\#\mathcal{K} &= \sum_{i=1}^{l}\mathcal{K}(L_i)-(l-1)\cdot\mathcal{K}(P)=\sum_{i=1}^{l}(1\cdot\mathcal{K}(R_i)+\mathcal{K}(P))-(l-1)\cdot\mathcal{K}(P)\\ &= q\cdot\sum_{i=1}^{l}\mathcal{K}_0(R_i)+\mathcal{K}(P)=q\cdot\mathcal{K}_0(H)+\mathcal{K}(P)=q\cdot\#\mathcal{K}_0+t.\end{aligned}$$

Using Lemma 8.7, it is sufficient to show $\mathcal{K}(S)\equiv t \pmod q$ for every line S in $\mathrm{PG}(k-1,q)$. If S contains P, then $S=\langle R,P\rangle$ for a point R in H, so that $\mathcal{K}(S)=q\cdot\mathcal{K}(R)+\mathcal{K}(P)\equiv\mathcal{K}(P)=t \pmod q$. If S does not contain P, then we set $S' := \langle S,P\rangle \cap H$ and compute $\mathcal{K}(S)=\mathcal{K}(S')=\mathcal{K}_0(S')\equiv t \pmod q$.

For the last statement assume that $\mathcal{K}_0$ is strong. From the construction we conclude $\mathcal{K}(P)\le t$ and $\mathcal{K}(Q)=\mathcal{K}_0(R)\le t$ for all points $Q \neq P$ in $\mathcal{P}$. □

We call the $(t \mod q)$-arcs obtained from Proposition 8.15 lifted arcs and the point P the lifting point. It is possible that a lifted arc can be obtained from several different lifting points.

LEMMA 8.16

Let $\mathcal{K}$ be a lifted arc. If P,Q are lifting points for $\mathcal{K}$, then any point in $\langle P,\rangle$ is a lifting point. In particular, the lifting points of $\mathcal{K}$ form a subspace.

PROOF. Assume $P \neq Q$ and let $L = \langle P, Q \rangle$. Due to the assumption, all points on L are t-points. Let π be an arbitrary plane containing L. Choose an arbitrary point R in $\pi \backslash L$ and set $a = \mathcal{K}(R)$. Since P is a lifting point all points on the line $L' = \langle P, R \rangle$ except P are a-points. Since Q is a lifting point, for every point R' in $L' \backslash P$ all points on the line $\langle Q, R' \rangle$ except Q are a-points. Thus, all points in $\pi \backslash L$ have the same multiplicity $(a(\pi))$ and all points on L have multiplicity t. This proves the lemma. □

REMARK 8.17 We can have a more general notion of lifted arcs by replacing the (lifting) point P by a subspace U. To this end, let $\mathcal{K}_0$ be a $(t \mod q)$-arc in a subspace $S \cong \mathrm{PG}(k-1-\dim(U), q)$ of $\mathrm{PG}(k-1, q)$ of codimension U that is disjoint to U. With this, we define an arc $\mathcal{K}$ in $\mathrm{PG}(k-1, q)$ as follows:

- $\mathcal{K}(P) = t$ for every point P in U;
- for each point Q in $\mathcal{P} \backslash U$ we set $\mathcal{K}(Q) = \mathcal{K}_0(R)$, where $R = \langle U, Q \rangle \cap S$.

We can easily check that $\mathcal{K}$ is a $(t \mod q)$-arc in $\mathrm{PG}(k-1, q)$ of cardinality $q^{\dim(U)} \cdot \#\mathcal{K}_0 + [\dim(U)]_q t$. If $\mathcal{K}_0$ is strong, so is $\mathcal{K}$. However, due to Lemma 8.16, $\mathcal{K}$ is also an lifted arc with lifting point P, where P is an arbitrary point of U.

REMARK 8.18 For quite some time the only known strong $(t \mod q)$-arcs in $\mathrm{PG}(k-1, q)$, where $k \geq 4$, where lifted arcs. We present a non-lifted $(3 \mod 5)$-arc in $\mathrm{PG}(3, 5)$ in Theorem 8.58.

In the plane case, i.e., in $\mathrm{PG}(2, q)$, non-trivial strong $(t \mod q)$-arcs can be constructed as σ-duals of certain blocking sets.

PROPOSITION 8.19 ([118, Theorem 10])

A strong $(t \mod q)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$ of cardinality $mq + t$ exists if and only if there exists an $((m - t)q + m, \geq m - t)$-blocking set $\mathcal{B}$ with line multiplicities contained in $\{m - t, m - t + 1, \ldots, m\}$.

PROOF. Let $\mathcal{K}$ be a strong $(t \mod q)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$ of cardinality $mq + t$. Then, we choose $\mathcal{B}$ in the dual plane $\mathrm{PG}^{\perp}(k-1, q)$ as $\mathcal{K}^{\sigma}$, where $\sigma(x) = (x - t)/q$, and apply Lemma 1.13 (with $\alpha = \frac{1}{q}$ and $\beta = -\frac{t}{q}$). In our situation the set of attained point multiplicities of $\mathcal{K}$ is given by $S_P = \{0, \ldots, t\}$ and the set of occurring hyperplane multiplicities, i.e. line multiplicities, is given by $S_H = \{iq + t : 0 \leq i \leq t\}$, since $\mathcal{K}(L) \equiv 3 \pmod q$ for every line L and $\gamma_1(\mathcal{K}) \leq t$. Thus, we have $\#\mathcal{B} = \#\mathcal{K}^{\sigma} = (m - t)q + m$, $\gamma_1(\mathcal{B}) \leq t$, and the line multiplicities with respect to $\mathcal{B}$ are contained in $\{m - t, \ldots, m\}$.

For the other direction we start from $\mathcal{B}$ and construct $\mathcal{K} = \mathcal{B}^{\sigma}$ with $\sigma(x) = x - m + t$. From Lemma 1.13 we conclude $\#\mathcal{K} = mq + t$, $\gamma_1(\mathcal{K}) \leq t$, and $\mathcal{K}(L) \equiv t \pmod q$ for every line L, i.e., $\mathcal{K}$ is a strong $(t \mod q)$-arc in $\mathrm{PG}(2, q)$ with cardinality $mq + t$. □

8.2 Classification of $(\mathbf{t} \mod \mathbf{q})$-arcs

First we consider strong $(t \mod q)$-arcs $\mathcal{K}$, where t is small. If $t=0$, then only the trivial empty arc with $\#\mathcal{K}=0$ is possible. For $t=1$ the possibilities are given by the characteristic function of a hyperplane or the entire ambient space, see Exercise 8.1. In both cases it contains a complete hyperplane, which implies that every 1-quasidivisible arc is extendable. The $(2 \mod q)$-arcs for odd field sizes $q \ge 5$ were (indirectly) characterized in [128]. Explicit classifications are also mentioned in e.g. [136, 118, 116, 128]. We will give a self-contained proof and a slight extension in the following. Prior to that, we briefly introduce some basic notation and fact from finite geometry, see e.g. [75]. For odd field sizes q a $(q+1,2)$-arc in $\operatorname{PG}(2,q)$ is called oval. The 1-lines through these 1-points are called tangents. The remaining points, i.e., the 0-points, are either contained on two or on zero tangents. The first case occurs $\frac{q(q+1)}{2}$ times and on speaks of external points. The remaining $\frac{q(q-1)}{2}$ 0-points are called internal points.

LEMMA 8.20

Let $\mathcal{K}$ be a q-divisible arc in $\operatorname{PG}(2,q)$ whose cardinality n is congruent to 2 modulo q. For $q \ge 5$ we have one of the following possibilities:

(1) $n=2q+2$, $a_2=q^2+q-1$, $a_{q+2}=2$, $a_{2q+2}=0$, $\lambda_0=q(q-1)$, $\lambda_1=2q$, $\lambda_2=1$;

(2) $n=2q+2$, $a_2=q(q+1)$, $a_{q+2}=0$, $a_{2q+2}=1$, $\lambda_0=q^2$, $\lambda_1=0$, $\lambda_2=q+1$;

(3) $n=q^2+q+2$, $a_2=q$, $a_{q+2}=q^2+1$, $a_{2q+2}=0$, $\lambda_0=q(q-1)/2$, $\lambda_1=2q$, $\lambda_2=1+q(q-1)/2$;

(4) $n=q^2+q+2$, $a_2=q+1$, $a_{q+2}=q^2-1$, $a_{2q+2}=1$, $\lambda_0=q(q+1)/2$, $\lambda_1=0$, $\lambda_2=1+q(q+1)/2$;

(5) $n=q^2+2q+2$, $a_2=i$, $a_{q+2}=q^2+q-2i$, $a_{2q+2}=i+1$, $\lambda_0=iq$, $\lambda_1=q^2-2iq$, $\lambda_2=1+q(i+1)$, *where* $0 \le i \le \left\lfloor \frac{q}{2} \right\rfloor$;

(6) $n=(q+1)(q+2)$, $a_2=0$, $a_{q+2}=q^2-1$, $a_{2q+2}=q+2$, $\lambda_0=q(q-1)/2$, $\lambda_1=0$, $\lambda_2=(q+1)(q+2)/2$;

(7) $n=2\left(q^2+q+1\right)$, $a_2=0$, $a_{q+2}=0$, $a_{2q+2}=q^2+q+1$, $\lambda_0=0$, $\lambda_1=0$, $\lambda_2=q^2+q+1$.

PROOF. Solving the standard equations for the hyperplanes and points

$$\begin{aligned}
a_2+a_{q+2}+a_{2q+2} &= q^2+q+1 \\
2a_2+(q+2)a_{q+2}+(2q+2)a_{2q+2} &= n(q+1) \\
a_2+\frac{(q+2)(q+1)}{2}a_{q+2}+(q+1)(2q+1)a_{2q+2} &= \binom{n}{2}+q\lambda_2 \\
\lambda_0+\lambda_1+\lambda_2 &= q^2+q+1 \\
\lambda_1+2\lambda_2 &= n
\end{aligned}$$

for $\{a_2, a_{q+2}, \lambda_0, \lambda_1, \lambda_2\}$ gives

$$\begin{aligned}
a_2 &= \frac{q^3 + xq - nq + 3q^2 - n + 3q + 2}{q} \\
a_{q+2} &= -\frac{2xq - nq + 2q^2 - n + 2q + 2}{q}, \\
\lambda_0 &= \frac{2xq^2 + nq^2 - n^2 + 2nq - 4q^2 + 4n - 4q - 4}{2q} \\
\lambda_1 &= -\frac{2xq^2 + nq^2 - 2q^3 - n^2 + 3nq - 6q^2 + 4n - 6q - 4}{q} \\
\lambda_2 &= \frac{2xq^2 + nq^2 - 2q^3 - n^2 + 4nq - 6q^2 + 4n - 6q - 4}{2q}
\end{aligned}$$

where we set $x := a_{2q+2}$ as an abbreviation.

First we treat a few special cases. separately. If $n = 2q + 2$, then the above equations simplify to $a_2 = q^2 + x + q - 1$, $a_{q+2} = -2x + 2$, $\lambda_0 = xq + q^2 - q$, $\lambda_1 = 2q(1 - x)$, and $\lambda_2 = xq + 1$. From $\lambda_1 \geq 0$ and $x \in \mathbb{N}_0$ we conclude $x \in \{0, 1\}$, which gives the cases (1) and (2). In the following we assume $n \neq 2q + 2$.

If $n = q^2 + q + 2$, then the above equations simplify to $a_2 = x + q$, $a_{q+2} = q^2 - 2x + 1$, $\lambda_0 = xq + \frac{1}{2}q(q-1)$, $\lambda_1 = 2q(1 - x)$, and $\lambda_2 = 1 + xq + \frac{1}{2}q(q - 1)$. From $\lambda_1 \geq 0$ and $x \in \mathbb{N}_0$ we conclude $x \in \{0, 1\}$, which gives the cases (3) and (4). In the following we assume $n \neq q^2 + q + 2$.

If $n = q^2 + 2q + 2$, then the above equations simplify to $a_2 = x - 1$, $a_{q+2} = q^2 - 2x + q + 2$, $\lambda_0 = (x - 1)q$, $\lambda_1 = q \cdot (q + 2 - 2x)$, and $\lambda_2 = xq + 1$. From $\lambda_0 \geq 0$, $\lambda_1 \geq 0$, and $x \in \mathbb{N}_0$ we conclude $x \in \left\{1, 2, \ldots, 1 + \left\lfloor \frac{q}{2} \right\rfloor\right\}$, which gives the parametric case (5), where $i = x - 1$. In the following we assume $n \neq q^2 + 2q + 2$.

If $n = q^2 + 3q + 2$, then the above equations simplify to $a_2 = x - q - 2$, $a_{q+2} = q^2 - 2x + 2q + 3$, $\lambda_0 = xq - \frac{1}{2}q(q + 5)$, $\lambda_1 = 2q(q + 2 - x)$, and $\lambda_2 = xq - \frac{1}{2}q(q + 1) + 1$. From $a_2 \geq 0$ and $\lambda_1 \geq 0$ we conclude $x = q + 2$, which gives case (6). In the following we assume $n \neq q^2 + 3q + 2$.

Now we are ready to analyze the general situation. From $a_{q+2} \geq 0$ we conclude

$$n \geq \frac{2(xq + q^2 + q + 1}{q + 1} \geq \frac{2(q^2 + q + 1)}{q + 1} > 2q,$$

so that $n \equiv 2 \pmod q$ and $n \neq 2 + 2q$ implies $n \geq 2 + 3q$. The non-negativity of λ_1 gives

$$n \leq 2 + q \cdot \frac{q + 3 - \sqrt{q^2-2q-7+8x}}{2} = 2 + q \cdot \frac{q + 3 - \sqrt{(q-3)^2+4(q-4)+8x}}{2} \underset{q\geq5}{\overset{x\geq0}{<}} 3q + 2$$

or

$$n \geq 2 + q \cdot \frac{q + 3 + \sqrt{q^2 - 2q - 7 + 8x}}{2} = \frac{q^2 + 3q + 4 + q\sqrt{q^2 - 2q - 7 + 8x}}{2} \tag{8.5}$$

where we only need to consider Inequality (8.5), due to $n \geq 2 + 3q$. From $n \equiv 2 \pmod q$, the estimation

$$2 + q \cdot \frac{q + 3 + \sqrt{q^2 - 2q - 7 + 8x}}{2} = 2 + q \cdot \frac{q + 3 + \sqrt{(q-3)^2+4(q-4)+8x}}{2} \underset{q\geq5}{\overset{x\geq0}{>}} q^2 + 2,$$

and $n \notin \{q^2+q+2, q^2+2q+2, q^2+3q+2\}$ we conclude $n \ge q^2+4q+2$. From $a_0 \ge 0$ we conclude

$$n \le \frac{q^3+xq+3q^2+3q+2}{q+1}, \tag{8.6}$$

so that Inequality (8.5) yields

$$\frac{q^3+xq+3q^2+3q+2}{q+1} \ge \frac{q^2+3q+4+q\sqrt{q^2-2q-7+8x}}{2},$$

which implies $x \le q+2$ or $x \ge q^2+q+1$. If $x \ge q^2+q+1$, then $a_2+a_{q+2}+x = q^2+q+1$, and $a_2, a_{q+2} \ge 0$ imply $a_2 = 0$, $a_{q+2} = 0$, and $x = q^2+q+1$, so that $n = 2(q^2+q+1)$. This is case (7). If $x \le q+2$, then Inequality (8.6) implies

$$n \le \frac{q^3+q(q+2)+3q^2+3q+2}{q+1} = q^2+3q+2,$$

a range for n that has been treated before. □

REMARK 8.21 We remark that the cases $q \in \{2,3,4\}$ admit the same solutions of the standard equations and a few more:

$$n = 11, a_2 = 7, a_5 = 6, a_8 = 0, \lambda_0 = 6, \lambda_1 = 3, \lambda_2 = 4$$

for $q = 3$ and

$$n = 14, a_2 = 14, a_6 = 7, a_{10} = 0, \lambda_0 = 14, \lambda_1 = 0, \lambda_2 = 7$$
$$n = 18, a_2 = 9, a_6 = 12, a_{10} = 0, \lambda_0 = 12, \lambda_1 = 0, \lambda_2 = 9$$

for $q = 4$. For $q = 3$ the arc can be described as follow. The four 2-points form an oval, all internal points are 1-points, and all external points are 0-points. A generator matrix of the corresponding code is e.g. given by

$$\begin{pmatrix} 11111111100 \\ 00001111210 \\ 00110011201 \end{pmatrix}.$$

For $q = 4$ we can construct a corresponding projective 2-divisible arc via $\mathcal{K}'(P) = \mathcal{K}(P)/2$ for all $P \in \mathcal{P}$. The corresponding codes are 2-weight codes and examples are given by the parametric families RT1 and RT3 in [31], respectively.

PROPOSITION 8.22

Let $q \ge 5$ be odd. For a strong $(2 \mod q)$-arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$ we have the following possibilities:

(I) A lifted arc from a 2-line with $\#\mathcal{K} = 2q+2$. There exists two possibilities:

(I-1) a double line; or

(I-2) a sum of two different lines.

(II) A lifted arc from a $(q+2)$-line L with $\#\mathcal{K} = q^2 + 2q + 2$ points. The line L has i double points, $q - 2i + 2$ single points, and $i - 1$ 0-points, where $1 \le i \le \frac{q+1}{2}$. We say that such an arc is of type (II-i) if it is lifted from a line with i double points.

(III) A lifted arc from a $(2q+2)$-line, which is the same as two copies of the plane. Such an arc has $2(q^2 + q + 1)$ points.

(IV) An exceptional $(2 \mod q)$-arc for q odd. It consists of the points of an oval, a fixed tangent to this oval, and two copies of each internal point of the oval (c.f. [14]).

PROOF. We apply Lemma 8.20 and first note that the cases (4) and (6) cannot occur for odd field sizes q since $\lambda_1 = 0$ but $a_{q+2} > 0$. First observe that each $(2q+2)$-line is a double line, i.e. each of the $q+1$ points has multiplicity 2, and each $q+2$-line contains at least one 2-point. For case (1) there is a unique 2-point which has to be contained on the two $q+2$-lines, so that the remaining $2q$ points on these two lines are 1-points. This is case (I-2) in the classification. For the case (2) the unique $2q+2$-line, $\lambda_1 = 0$, and $\lambda_2 = q+1$ imply case (I-1). In case (7) all points have multiplicity 2, which corresponds to case (III). For case (5) let us first observe that there are no 0-points for $i = 0$, i.e., setting $\mathcal{K}'(P) = \mathcal{K}(P) - 1$ for all $P \in \mathcal{P}$ gives a strong $(1 \mod q)$-arc of cardinality $q+1$, which is the characteristic function of a line, see Exercise 8.1. The multiset of points given by $\mathrm{PG}(2,q)$ and a line can also be described as in (II-1). For $i \ge 1$ there exist 0-points, so that the distribution of the multiplicities of the lines through a 0-point is given by $2^1(q+2)^q$. Due to the existence of a $(2q+2)$-line, the 2-line through a 0-point contains a 2-point. If $i = 1$ there is a unique such 2-point Q, for $i > 1$ we observe that all such 2-lines through 0-points have to intersect in the same 2-point (that we also call Q). So, through the 2-point Q there are exactly i two-lines, so that counting points give that the remaining lines through Q split into $(i+1)$ lines of multiplicity $2q+2$, which contain all 2-points, and $q - 2i$ lines of multiplicity $q+2$, which then consist of q one-points and Q. This is the situation described in case (II-$(i+1)$). For the remaining case (3) we consider the dual arc $\mathcal{K}^\sigma$ with respect to $\sigma(x) = \frac{q+2-x}{q}$. With this, $\mathcal{K}^\sigma$ is a (projective) $(q,2)$-arc in $\mathrm{PG}(2,q)$ which is extendable. An extension point of $\mathcal{K}^\sigma$ corresponds to a full line in $\mathcal{K}$. After extending $\mathcal{K}^\sigma$ we obtain an oval, which yields the description for $\mathcal{K}$ given in (IV). □

REMARK 8.23 For even field sizes q the case (4) in Lemma 8.20 can be attained. Removing the unique double line from $\mathcal{K}$ and halving all point multiplicities yields a projective $q/2$-divisible arc $\mathcal{K}'$ with cardinality $q(q-1)/2$ and line multiplicities 0 and $q/2$ in $\mathrm{PG}(2,q)$. A corresponding 2-weight code is contained in the family TF2 in [31]. In case (6) halving the point multiplicities yields a projective $q/2$-divisible arc $\mathcal{K}'$ with cardinality $(q+1)(q+2)/2$ and line multiplicities $q(q+1)/2$ and $q(q+2)/2$ in $\mathrm{PG}(2,q)$. Corresponding 2-weight codes are contained in the families TF1d and TF2d in [31].

THEOREM 8.24 ([118, Theorem 11],[136, Theorem 5])
Let $\mathcal{K}$ be a strong $(2 \mod q)$-arc in $\mathrm{PG}(k-1,q)$, where $k \ge 4$. Then, $\mathcal{K}$ is a lifted arc. In particular, for $k \ge 4$ every $(2 \mod q)$-arc in $\mathrm{PG}(k-1,q)$ has a hyperplane in its support.

COROLLARY 8.25

For $k \ge 4$ each 2-quasidivisible arc in $\mathrm{PG}(k-1,q)$ *is extendible.*

For strong $(t \mod q)$-arcs the situation is far more complicated if $t \ge 3$. E.g. for strong $(3 \mod q)$-arcs in $\mathrm{PG}(2,q)$ we have many strong $(3 \mod q)$-arcs obtained as the sum of a strong $(2 \mod q)$- and a strong $(1 \mod q)$-arc, but also some non-trivial indecomposable arcs. As examples we will discuss the possible strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of small cardinality later on. First we state some easy general observations.

LEMMA 8.26

Let $\mathcal{K}$ be a $(t \mod q)$*-arc in* $\mathrm{PG}(k-1,q)$*, where $k \ge 3$. For every hyperplane H in* $\mathrm{PG}(k-1,q)$ *the restricted arc $\mathcal{K}|_H$ is a* $(t \mod q)$*-arc in* $\mathrm{PG}(k-2,q)$*. If $\mathcal{K}$ is strong, so is $\mathcal{K}|_H$.*

PROOF. The conditions of Definition 8.9 are directly verified. □

LEMMA 8.27

Let $\mathcal{K}$ be a $(t \mod q)$*-arc in* $\mathrm{PG}(k-1,q)$*, where $k \ge 2$. Then, we have $\#\mathcal{K} \ge [k-1]_q \cdot t$.*

PROOF. Note that $t < q$. We prove by induction on k. If $k = 2$, then the ambient space is a line L and $\mathcal{K}(L) \equiv t \pmod q$ implies $\#\mathcal{K} = \mathcal{K}(L) \ge t$, since $t < q$. Now let $k \ge 3$. If all points have multiplicity at least 1, then $\#\mathcal{K} \ge [k]_q > [k-1]_q \cdot t$ since $t < q$. So, let P be a 0-point with respect to $\mathcal{K}$. Let $H_1, \dots, H_l$ the $l = [k-1]_q$ hyperplanes through P. Since every point $Q \ne P$ in $\mathcal{P}$ is contained in exactly $[k-2]_q$ of these hyperplanes, we have

$$[k-2]_q \cdot \#\mathcal{K} = \sum_{i=1}^{l} \mathcal{K}(H_i) - (l - [k-2]_q) \cdot \mathcal{K}(P) = \sum_{i=1}^{l} \mathcal{K}(H_i). \tag{8.7}$$

From the induction hypothesis we conclude $\mathcal{K}(H_i) \ge [k-2]_q \cdot t$, so that $\#\mathcal{K} \ge [k-1]_q \cdot t$. □

LEMMA 8.28

If $\mathcal{K}$ is a $(t \mod q)$*-arc in* $\mathrm{PG}(k-1,q)$ *whose support contains a hyperplane H, where $t \ge 1$, then $\mathcal{K}' = \mathcal{K} - \chi_H$ is a* $(t-1 \mod q)$*-arc in* $\mathrm{PG}(k-1,q)$*.*

PROOF. Let L be an arbitrary line in $\mathrm{PG}(k-1,q)$. Since $\mathcal{K}(L) \equiv t \pmod q$ and $\#(L \cap H) \equiv 1 \pmod q$, we have $\mathcal{K}'(L) \equiv t-1$. Obviously, $\mathcal{K}'(P) \le \mathcal{K}(P)$ for all $P \in \mathcal{P}$, so that the last statement follows. □

Note that it may happen that $\mathcal{K}$ is strong while $\mathcal{K}'$ is not strong. This is e.g. the case when $\mathcal{K}$ has full support.

PROPOSITION 8.29

For $k \geq 2$, each $(t \mod q)$-arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ of cardinality $[k-1]_q \cdot t$ is a sum of t hyperplanes.

PROOF. We prove by induction on t. Note that all inequalities in the analysis of the proof of Lemma 8.27 are tight, so that every hyperplane H that contains a 0-point P satisfies $\mathcal{K}(H) = [k-2]_q \cdot t$. Since there are $[k]_q$ hyperplanes in $\mathrm{PG}(k-1,q)$, every points is contained in $[k-1]_q$ hyperplanes, and

$$[k]_q \cdot [k-2]_q \cdot t = \left([k-1]_q + \frac{1}{q}\right) \cdot ([k-1]_q - 1) \cdot t < [k-1]_q \cdot [k-1]_q \cdot t = [k-1]_q \cdot \#\mathcal{K}$$

there exists a hyperplane H' with $\mathcal{K}(P') \geq 1$ for all $P' \in H'$. From Lemma 8.28 and the induction hypothesis we conclude that $\mathcal{K}$ is the sum of t hyperplanes. □

THEOREM 8.30 ([118, Theorem 9]

Let $\mathcal{K}$ be a strong $(t \mod q)$-arc in $\mathrm{PG}(k-1,q)$, where $k \geq 4$, such that the restriction $\mathcal{K}|_H$ to every hyperplane H of $\mathrm{PG}(k-1,q)$ is lifted, then $\mathcal{K}$ itself is a lifted arc.

EXERCISE 8.1 Let $\mathcal{K}$ be a strong $(1 \mod q)$-arc in $\mathrm{PG}(k-1)$, where $k \geq 2$. Show that $\mathcal{K}$ is either the characteristic function of a hyperplane or the characteristic function of the entire ambient space $\mathrm{PG}(k-1,q)$.

EXERCISE 8.2 Show that no $(106, 22)$-arc in $\mathrm{PG}(3,5)$ exists.
Hint: Use the fact that each 1-quasi-divisible arc is extendible, see Theorem 8.8 and Exercise 8.1.

EXERCISE 8.3 Show that each $(5,2)$-arc in $\mathrm{PG}(2,5)$ is extendible.

8.3 Classification of strong $(3 \mod 5)$-arcs in $\mathrm{PG}(3,5)$ with small cardinality

The aim of this section to prove a structure result for strong $(3 \mod 5)$-arcs in $\mathrm{PG}(3,5)$ with relatively small cardinality. To this end we first obtain some results on the structure of the contained hyperplanes, i.e., strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$. So, let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. We know $18 \leq \#\mathcal{K} \leq 3 \cdot [3]_5 = 93$, see Lemma 8.27 for the lower bound, and $\#\mathcal{K} \equiv 3 \pmod 5$. The type of a line L is a vector $(m_0, \ldots, m_5)$, where $m_0 \geq m_1 \geq \cdots \geq m_5$ and the m_i are the multiplicities of the points on L. By assumption we have $m_i \in \{0,1,2,3\}$ for all $0 \leq i \leq 5$. As usual, the total number of i-points is denoted by λ_i and (a_i) is the spectrum. The possible line types are given as follows:

$\mathcal{K}(L)$	type of L	name
3	$(3,0,0,0,0,0)$	A_1
	$(2,1,0,0,0,0)$	A_2
	$(1,1,1,0,0,0)$	A_3
8	$(3,3,2,0,0,0)$	B_1
	$(3,3,1,1,0,0)$	B_2
	$(3,2,2,1,0,0)$	B_3
	$(3,2,1,1,1,0)$	B_4
	$(3,1,1,1,1,1)$	B_5
	$(2,2,2,2,0,0)$	B_6
	$(2,2,2,1,1,0)$	B_7
	$(2,2,1,1,1,1)$	B_8
13	$(3,3,3,3,1,0)$	C_1
	$(3,3,3,2,2,0)$	C_2
	$(3,3,3,2,1,1)$	C_3
	$(3,3,2,2,2,1)$	C_4
	$(3,2,2,2,2,2)$	C_5
18	$(3,3,3,3,3,3)$	D_1

LEMMA 8.31

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\#\mathcal{K} = 18$, then $\mathcal{K}$ is the sum of three lines and the possible line types are A_1, A_2, A_3, B_5, B_8, C_5, and D_1.

PROOF. From Proposition 8.29 we conclude that $\mathcal{K}$ is a sum of three lines. So, if L is a line of type $(m_0, m_1, m_2, m_3, m_4, 0)$, then we have $\sum_{i=0}^{4} b_i = 3$. If $b_0 > 0$, then we can subtract $b_0\chi_L$ from $\mathcal{K}$ and conclude $\sum_{i=0}^{4} b_i - 5b_0 = 3 - b_0$, so that only the stated types remain. (Indeed, all of them can be attained by checking the different arrangements of three lines.) □

By using Proposition 8.19, the classification in Lemma 8.31 is equivalent to the enumeration of $(3,0)$-blocking sets with line multiplicities 0, 1, 2, or 3. Clearly, such blocking sets correspond to three (not necessarily different) points. Next we show that some line types cannot occur in $\mathcal{K}$ if its cardinality is small.

LEMMA 8.32

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\mathcal{K}$ contains a line L of type D_1, then we have $\#\mathcal{K} = 18$ or $\#\mathcal{K} \geq 38$.

PROOF. Let P be point outside of L with $\mathcal{K}(P) > 0$. Note that every line through P hits L in a 3-point so that is has multiplicity at least 8. Thus, we have $\#\mathcal{K} \geq 1 + 6 \cdot (8-1) = 43$ if $\mathcal{K}(P) = 1$ and $\#\mathcal{K} \geq 2 + 6 \cdot (8-2) = 38$. If all points are either 0- or 3-points, then define $\mathcal{K}'$ via $\mathcal{K}'(P) = \mathcal{K}(P)/3$, so that $\mathcal{K}'$ is a strong $(1 \mod 5)$-arc in $\mathrm{PG}(2,5)$. Thus, $\mathcal{K}'$ is either a line or the entire ambient space, so that we conclude $\#\mathcal{K} \in \{18, 93\}$ from $\#\mathcal{K} = 3 \cdot \#\mathcal{K}'$. □

LEMMA 8.33

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\#\mathcal{K} \in \{23,28,33\}$, then we have

$$\begin{aligned}
a_3 &= \frac{248-6\#\mathcal{K}}{5}+a_{13}\\
a_8 &= \frac{6\#\mathcal{K}-93}{5}-2a_{13}\\
\lambda_1 &= \frac{744-\#\mathcal{K}\cdot(56-\#\mathcal{K})}{5}-10a_{13}+3\lambda_3\\
\lambda_2 &= \frac{\#\mathcal{K}\cdot(61-\#\mathcal{K})-744}{10}+5a_{13}-3\lambda_3
\end{aligned}$$

PROOF. From Lemma 8.32 we conclude $a_i=0$ for all $i \in \mathbb{N}_0\backslash\{3,8,13\}$, so that the statement follows from the standard equations and $\lambda_1+2\lambda_2+3\lambda_3=n$. □

LEMMA 8.34

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\mathcal{K}$ contains a line L of type C_1 or C_2, then we have $\#\mathcal{K} \ge 33$.

PROOF. Let P_0 the (unique) 0-point on the 13-line L. Counting the points on the lines through P_0 gives $\#\mathcal{K} \ge 13+5\cdot 3-5\cdot 0=28$. So, we assume $\#\mathcal{K}=28$ in the following.

If L is of type C_1, i.e., $(3,3,3,3,1,0)$, then we have $\lambda_1=1$, since counting the points on the lines through a 1-point outside of L would give $\#\mathcal{K} \ge 4\cdot 8+2\cdot 3-5\cdot 1=33$ otherwise. From Lemma 8.33 we then conclude $\lambda_3=(10a_{13}-1)/3$ and $\lambda_2=14-5a_{13}$, so that $a_{13}=1$ and $\lambda_3=3$. However, there are already four 3-points on L, which is a contradiction.

If L is of type C_2, i.e., $(3,3,3,2,2,0)$, then we have $\lambda_2=2$, since counting the points on the lines through a 2-point outside of L would give $\#\mathcal{K} \ge 5\cdot 8+1\cdot 3-5\cdot 2=33$ otherwise. From Lemma 8.33 we then conclude $\lambda_3=(11+5a_{13})/3$ and $\lambda_1=13-5a_{13}$, so that $a_{13}=2$, $\lambda_1=3$, and $\lambda_3=7$. Now let P_1 be a point outside of L, then counting the points on the lines through P_1 gives $\#\mathcal{K} \ge 3\cdot 8+3\cdot 3-5\cdot 1=28$. Thus, each of the three lines through P_1 and a 3-point of L is an 8-line which contains at least one further 1-point. This contradicts the fact that there are only three 1-points in total. □

LEMMA 8.35

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\mathcal{K}$ contains a line L of type C_3, C_4, or C_5, then we have $\#\mathcal{K} \neq 23$.

PROOF. Assume $\#\mathcal{K} = 23$. If P_3 is a 3-point outside of L, then counting the points on the lines through P_3 gives $\#\mathcal{K} \geq 6 \cdot 8 - 5 \cdot 3 = 33$. Thus, we have $\lambda_3 \leq 3$, so that Lemma 8.33 gives

$$\lambda_1 = 3\lambda_3 - 3 - 10a_{13} \leq 6 - 10a_{13}.$$

So, from $\lambda_1 \geq 0$ we conclude $a_{13} = 0$, which contradicts the existence of the 13-line L. □

LEMMA 8.36

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\#\mathcal{K} = 23$, then we have $\lambda_1 = 6$, $\lambda_2 = 4$, $\lambda_3 = 3$, $a_3 = 22$, and $a_8 = 9$. The number of occurrences of the different line types is given by:

A_1	A_2	A_3	B_2	B_3
6	*12*	*4*	*3*	*6*

The following patterns of lines through a point P occur:

- $\mathcal{K}(P) = 3$: $A_1^2B_2^2B_3^2$ *three times;*
- $\mathcal{K}(P) = 2$: $A_2^3B_3^3$ *four times;*
- $\mathcal{K}(P) = 1$: $A_2^2A_3^2B_2B_3$ *six times;*
- $\mathcal{K}(P) = 0$: $A_1A_2^4B_2$ *six times;*
- $\mathcal{K}(P) = 0$: $A_1^2A_2^2A_3B_3$ *twelve times.*

PROOF. Using Lemma 8.34 and Lemma 8.35 we conclude $a_3 = 22$, $a_8 = 9$, $\lambda_1 = a_3\lambda_3 - 3$, and $\lambda_2 = 13 - 3\lambda_3$ from Lemma 8.33. Since $\lambda_1, \lambda_2 \in \mathbb{N}_0$, we have $\lambda_3 \in \{1,2,3,4\}$.

If $\lambda_3 = 1$, then there are four 8-lines through the unique 3-point P, which is impossible using only 2-points (except P).

If $\lambda_3 = 2$, then let P, P' denote the two 3-points and L denote the line spanned by P and P'. Consider a 0-point P_0 on L. The other five lines through P_0, except L, have to be 3-lines. Since there are no further 3-points, this implies $\lambda_1 \geq 5$, which is a contradiction.

If $\lambda_3 = 4$, then through each of the 6 pairs of 3-points we have an 8-lines, since three 3-points cannot lie on a line (using $a_{13} = a_{18} = 0$). For each 3-point there is an extra 8-line, since there are four 8-lines through each 3-point. This gives at least ten 8-lines, which contradicts $a_8 = 9$.

Thus, we have $\lambda_1 = 6$, $\lambda_2 = 4$, $\lambda_3 = 3$. Again, no three 3-points can be on the same line, so that the nine 8-lines contain either two 3-points (in 3 cases) or one 3-point (in 6 cases). Thus, the line types B_6, B_7, and

B_8 cannot occur. So, especially, no three 2-points can be on the same line. The $\binom{4}{2} = 6$ lines through pairs of 2-points are of type B_3, so that line types B_4 and B_5 cannot occur. Since through each 2-point there are already three 8-lines, line type also B_1 does not occur and type B_2 occurs exactly 3 times. Next we consider one of the six 1-points P_1. The three 3-points split on the two 8-lines through P_1, so that one is of type B_2 and one of type B_3. This used one of the remaining five 1-points, so that the others are split into two 3-lines of type A_3. Thus, there are $6 \cdot 2/3 = 4$ lines of type A_3 in total. Each of the four 2-points is on three 3-lines, which all have to be of type A_2, so that we have 12-lines of type A_2 in total. The missing six 3-lines then have to be of type A_1. Each of the three 3-points is on exactly two 3-lines, which have to be of type A_1. Counting the 3-points on the 8-lines gives that the pattern of the lines through each 3-point is $A_1^2B_2^2B_3^2$. The 3-lines through a 2-point have to be of type A_2 and the 8-lines have to be of type B_3. The two 8-lines through a 1-point have to use all three 3-points, so that one is of type B_2 and one of type B_3. There are two further 2-points left, so that two of the 3-lines through a 1-point are of type A_2 and two are of type A_3. Through each 0-point there is exactly one 8-lines. It can be of type B_2 or of type B_3. Since there are three lines of type B_2 and 6 lines of type B_3, the first case occurs six and the second case occurs twelve times. Counting the remaining 3- and 2-points gives the number of 3-lines of type A_1 and A_2, respectively, so that also the number of 3-lines of type A_3 is uniquely determined. □

REMARK 8.37 Proposition 8.19 links strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 23 to $(9,1)$-blocking sets in $\mathrm{PG}(2,5)$ with line multiplicities contained in $\{1,2,3,4\}$, i.e., (trivial) blocking sets containing a full line are excluded. It is well known that the projective triangle is the only possibility over $\mathbb{F}_5$. So, our reasoning gives a proof for this fact, or we can use this uniqueness result to shorten our analysis. A nice picture of the arc is drawn in [136].

LEMMA 8.38

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\#\mathcal{K} = 28$, then we have $\lambda_1 = 10$, $\lambda_2 = 0$, $\lambda_3 = 6$, $a_3 = 16$, and $a_8 = 15$. The number of occurrences of the different line types is given by:

A_1	A_3	B_2
6	*10*	*15*

The following patterns of lines through a point P occur:

- $\mathcal{K}(P) = 3$: $A_1B_2^5$ *six times;*
- $\mathcal{K}(P) = 1$: $A_3^3B_2^3$ *ten times;*
- $\mathcal{K}(P) = 0$: $A_1^2A_3^2B_2^2$ *fifteen times.*

PROOF. From Lemma 8.33 we conclude $a_3 = 16 + a_{13}$, $a_8 = 15 - 2a_{13}$, $\lambda_1 = 3\lambda_3 - 8 - 10a_{13}$, and $\lambda_2 = 18 + 5a_{13} - 3\lambda_3$. If $a_{13} \geq 2$, then $\lambda_1 \geq 0$ would imply $\lambda_3 \geq 10$, so that $\#\mathcal{K} \geq 30$. If $a_{13} = 1$, then

$\lambda_1, \lambda_2 \ge 0$ imply $\lambda_3 \in \{6,7\}$. If $\lambda_3 = 6$, then $\lambda_1 = 0$ and $\lambda_2 = 5$, so that every line through a 2-point has a multiplicity of at least 8, which gives $\#\mathcal{K} \ge 6 \cdot 8 - 5 \cdot 2 = 38$. So, for $a_{13} = 1$, we have $\lambda_3 = 7$, $\lambda_1 = 3$, $\lambda_2 = 2$, and $a_8 = 13$. Since $\binom{7}{2} = 21 > 14 = a_8 + a_{13}$, there exist a line L that contains strictly more than two 3-points. Since $a_{13} = 1$, such a line is unique. If L contains three 3-points, then the seven 3-points also generate $\binom{6}{2} = 15 > 14 = a_8 + a_{13}$. The only possibility for L is type C_1. But then, counting the points on the lines through a 1-point outside of L would give $\#\mathcal{K} \ge 4 \cdot 8 + 2 \cdot 3 - 5 \cdot 1 = 33$. Thus, we have $a_3 = 16$, $a_8 = 15$, and $a_{13} = 0$.

Using $a_{13} = 0$, the conditions $\lambda_1, \lambda_2 \ge 0$ imply $\lambda_3 \in \{3,4,5,6\}$. If $\lambda_3 = 3$, then $\lambda_1 = 1$ and counting the lines through a 2-point gives $\#\mathcal{K} \ge 5 \cdot 8 + 1 \cdot 3 - 5 \cdot 2 = 33$. Since no three 3-points can be situated on a line and each 3-point is located on five 3-lines, the number of 8-lines containing at least one 3-point is given by $\binom{\lambda_3}{2} + (6 - \lambda_3) \cdot \lambda_3$.

So, for $\lambda_3 = 4$ let L' be this unique 8-line without a 3-point. Note that we $\lambda_1 = 4$ and $\lambda_2 = 6$ in this case. If L' would be of type B_8, then all lines through a 2-point on L' would by 8-lines, which implies $\#\mathcal{K} \ge 6 \cdot 8 - 5 \cdot 2 = 38$. If L' is of type B_6 then consider a 2-point P_2 not on L'. The lines through P_2 have to be 8-lines if they hit a 2-point on L' and 3-lines if they hit a 0-point on L', since otherwise we would have $\#\mathcal{K} > 28$. Since no two 3-points can be contained on those four 8-lines, each of the six lines through P_2 contains a 1-point, which contradicts $\lambda_1 = 4$.

If $\lambda_3 = 5$, then $\lambda_2 = 3$ and each of the fifteen 8-lines contains at least one 3-point. Thus, the three 2-points are not contained on a line. Note that no line has type B_6, B_7, or B_8, since every 8-line contains a 3-point. For an arbitrary 2-point P_2 two from the four 8-lines through P_2 contain another 2-point and so have to be of type B_3. The other two 8-lines through P_2 are of type B_1 and B_4, each indeed occurring, since $\lambda_3 = 5$. Thus, we have at least 3 lines of type B_3 and 3-lines of type B_4, i.e., at least six 8-lines containing a unique 3-point. Together with the $\binom{5}{2} = 10$ 8-lines containing two 3-points, this contradicts $a_8 = 15$.

Finally, only the possibility $\lambda_3 = 6$ remains, so that $\lambda_1 = 10$ and $\lambda_2 = 0$. The fact, that there is no 2-point, eliminates all line types except A_1, A_3, B_2, and B_5. Since each of the six 3-points is on a unique 3-line, type A_1 occurs exactly six times. Since each of the ten 1-points is on exactly three 3-lines, which have to be of type A_3, we have 10 lines of type A_3 in total. Line type B_2 occurs $\binom{6}{2} = 15$ times, so that line type B_5 does not occur at all.

For the patterns through a point P we remark that there are five 8-lines if $\mathcal{K}(P) = 3$, three 8-lines if $\mathcal{K}(P) = 1$, and two 8-lines if $\mathcal{K}(P) = 0$. All of these have to be of type B_2, which is the only occurring type of 8-lines. Counting 3-points and 1-points yields the unique distribution of the 3-lines through P on the two possible types A_1 and A_3 in each case for $\mathcal{K}(P) \in \{0,1,3\}$. □

REMARK 8.39 Proposition 8.19 links strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 28 to $(15,2)$-blocking sets $\mathcal{B}$ in $\mathrm{PG}(2,5)$ with line multiplicities contained in $\{2,3,4,5\}$, i.e. the support of $\mathcal{B}$ cannot contain a full line. It can be shown that $\mathcal{B}$ cannot contain points of multiplicity strictly larger than 1, which is equivalent to the fact that $\mathcal{K}$ does not contain 13-lines, so that it can be obtained as the complement of a $(16,4)$-arc in $\mathrm{PG}(2,5)$, whose classification is well known. A nice picture of the strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ of cardinality 28 is drawn in [136].

LEMMA 8.40

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\#\mathcal{K} = 33$ and there is a line L of type C_1, then we have one of the following two possibilities:

A_1	A_2	A_3	B_1	B_2	B_3	B_6	C_1	λ_1	λ_2	λ_3	a_3	a_8	a_{13}
8	4	0	16	0	0	1	2	1	4	8	12	17	2
4	5	2	5	4	10	0	1	5	5	6	11	19	1

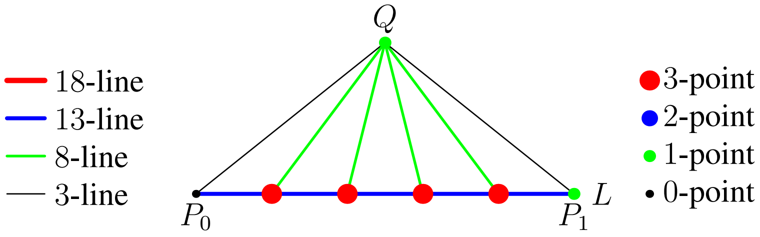
In the case of the first row, the following patterns of lines through a point P occur:

- $\mathcal{K}(P) = 3$: $A_1B_1^4C_1$ *eight times;*
- $\mathcal{K}(P) = 2$: $A_2B_1^4B_6$ *four times;*
- $\mathcal{K}(P) = 1$: $A_2^4C_1^2$ *one time;*
- $\mathcal{K}(P) = 0$, *P on a 13-line:* $A_1^4B_6C_1$ *two times;*
- $\mathcal{K}(P) = 0$: *P not on a 13-line* $A_1^2A_2B_1^3$ *sixteen times.*

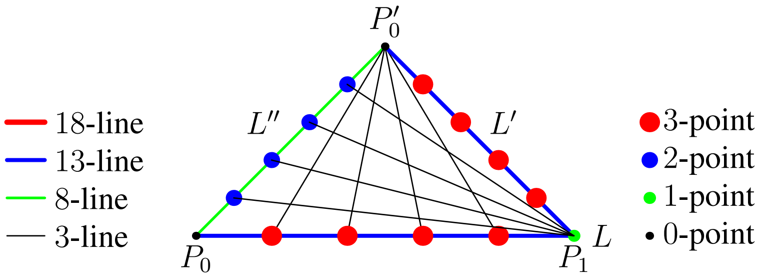
For the second row we have:

- $\mathcal{K}(P) = 3$, *P on L:* $A_1B_1B_2B_3^2C_1$ *four times;*
- $\mathcal{K}(P) = 1$, *P on L:* $A_2A_3^2B_3^2C_1$ *one time;*
- $\mathcal{K}(P) = 0$, *P on L:* $A_2^4B_1C_1$ *one time;*
- $\mathcal{K}(P) = 3$, *P not on L:* $B_1^3B_2^2B_3$ *two times;*
- $\mathcal{K}(P) = 2$: $A_2B_1B_3^4$ *five times;*
- $\mathcal{K}(P) = 1$, *P not on L:* $A_1A_3B_2^2B_3^2$ *four times;*
- $\mathcal{K}(P) = 0$, *P not on L:* $A_1^2A_2B_2B_3^2$ *four times;*
- $\mathcal{K}(P) = 0$, *P not on L:* $A_1A_2^2B_1B_2B_3$ *four times;*
- $\mathcal{K}(P) = 0$, *P not on L:* $A_1A_2A_3B_1^2B_3$ *six times.*

PROOF. Let P_0 be the unique 0-point and P_1 be the unique 1-point on L. Consider another 1-point Q outside of L. Counting points on the lines through Q yields that $\langle Q, P_0\rangle$, $\langle Q, P_1\rangle$ are 3-lines and the other four lines through Q and the 3-points of L are 8-lines. Thus, the lines through P_1 are of type A_2, A_3, B_3, or C_1.

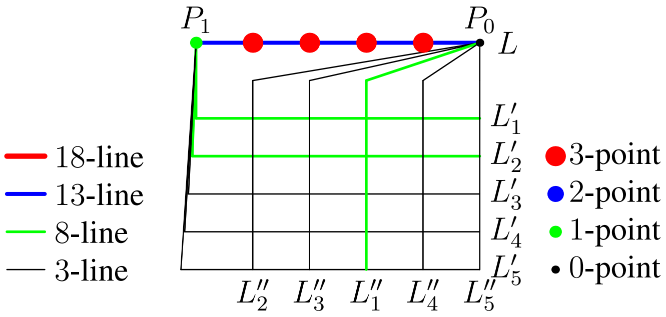


Assume that L' is another line, not equal to L, of type C_1 through P_1. Let P_0' be the unique 0-point on L'. For an arbitrary 3-point P_3 on L counting points on the lines through P_3 yield that the lines meeting L' in one of the four 3-points are 8-lines and the unique line meeting L' in the 0-point P_0' is a 3-line, using that L is a 13-line. Thus, counting the points on the lines through P_0' give that $\langle P_0', P_0\rangle =:= L''$ is an 8-line. So, all points with strictly positive multiplicity are located on the lines L, L', and L''. Thus, the lines through P_1, that are not equal to L or L', meet L'' in a 2-point, i.e., L'' is of type B_6.

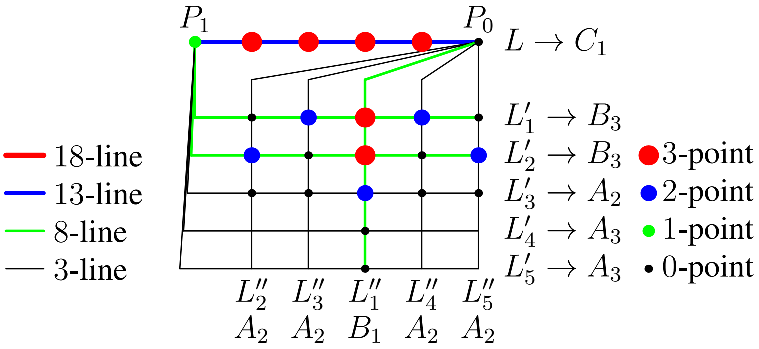


Thus, we have $\lambda_1 = 1$, $\lambda_2 = 4$, and $\lambda_3 = 8$. The pattern of types of the lines through P_0 or P_0' is given by $A_1^4B_1C_1$. Since all 3-points on the 13-line L of type C_1 meet P_0' in a 3-line, which has to be of type A_1, the remaining four lines trough a 3-point on L have to be 8-lines. Since L' is met in a 3-point and L'' is met in a 2-point all of these have to be of type B_1. For the 3-points on L' we can similarly conclude that they for a 3-line of type A_1 with P_0 and that the pattern of types of the incident lines is given by $A_1B_1^4C_1$, just as for the 3-points on L. Each of the four 2-points is located on the line L'' of type B_6. The 3-points are met by four 8-lines of type B_1 and the the unique 1-point P_1 is met by a 3-line of type A_2. For P_1 the pattern $A_2^4C_1^2$ can be directly read off from the above drawing. From this, we can easily complete the data from the first row of the table in our statement. For the remaining $[3]_5 - \lambda_1 - \lambda_2 - \lambda_3 - 2 = 16$ points P not equal to P_0 or P_0' we have $\mathcal{K}(P) = 0$. Since they are not contained on one of the two 13-lines, P is incident with three 3- and three 8-lines. The line $\langle P, P_1\rangle$ has to be a 3-line of type A_2, so that the two remaining 3-lines have to be of type A_1. Since P is not located on L'', the incident 3-lines have to be of type B_1.

If P_1 is not incident with another line of type C_1, then it is incident with two 8-lines L_1', L_2' and three 3-lines L_3', L_4', L_5'. Since the lines through P_1 are of type A_2, A_3, or B_3, as discussed above, the 8-lines are of type B_3 and the 3-lines are of types A_2 and/or A_3. With this, we have $\lambda_3 = 6$ and $4 \le \lambda_2 \le 7$. Lemma 8.33 gives $\lambda_2 = 5a_{13}$, so that $a_{13} \in \mathbb{N}_0$ implies $\lambda_2 = 5$ and $a_{13} = 1$. Plugging into Lemma 8.33 yields $\lambda_1 = 5$, $a_3 = 11$, and $a_8 = 19$. The lines through P_0 are given by L, an 8-line L_1'' and four 3-lines $L_2'', \dots, L_5''$.



The 8-lines L'_1 and L'_2 through P_1 have to be of type B_3 since they cannot contain a 1-point $Q \neq P_1$ outside of L. Similarly, the 8-line L''_1 is of type B_1 or B_6 since it cannot contain a 1-point Q outside of L. It cannot be of type B_6 since otherwise the lines L'_1, L'_2, and L''_1 would contain $6 > 5 = \lambda_2$ points of multiplicity 2, so that L''_1 has type B_1. Since there is a single 2-point that is not on L'_1 or L'_2, the lines through P_1 have the following types: 2 times B_3, 1 times C_1, 1, times A_2, and 2-times A_3. W.l.o.g. we choose the label such that L'_3 has type A_2. Since there are four 2-points not on L''_1, the lines through P_0 have the following types: 1 times C_1, 4 times A_2, and 1 times B_1. W.l.o.g. we assume that the two 2-points on L'_1 are on L''_3 and L''_4. We summarize our findings in the following picture.



Now consider the lines $L, \tilde{L}_1, \dots, \tilde{L}_5$ through a 3-point P_3 on L. Counting points give that exactly one of the $\tilde{L}_i$ has multiplicity 3, say $\tilde{L}_1$, and the others have multiplicity 8. Note that L is the unique line of weight 13. Clearly, $\tilde{L}_1$ has to be of type A_1. Containing a 3-point, the 8-lines $\tilde{L}_2, \dots, \tilde{L}_5$ have one of the types $B_1, \dots, B_5$. Since $L'_3 \backslash P_1$ contains only 0- or 2-points, the line $\tilde{L}$ cannot be of type $B_5 = (3, 1, 1, 1, 1, 1)$. Next we exclude type $B_4 = (3, 2, 1, 1, 1, 0)$. Since $L'_1 \backslash P_1$ and $L'_2 \backslash P_1$ contain no 1-points, $\tilde{L}$ would meet L'_3, L'_4, L'_5 in a 1-point, which is impossible as L'_3 contains no 1-point except P_1. Now we are ready to determine the counts of the types of the lines $\tilde{L}_2, \dots, \tilde{L}_5$. Two of them meet L''_1 in one of its two 3-points and so are of type B_3 using four out of the five 2-points. Thus, type B_1 and B_2 both have to occur exactly once. So the types of the lines incident with a 3-point on L are given by $A_1 B_1 B_2 B_3^2 C_1$. For P_1 and P_0 we have already determined the patterns $A_2 A_3^2 B_3^2 C_1$ and $A_2^4 B_1 C_1$, respectively. Since the patterns of all points on L are known, we can easily complete the second row of the table of the statement.

Now consider one of the two 3-points P'_3 not on L. Since $a_{13} = 1$, all six incident lines have to be 8-lines of types B_1, B_2, or B_3. The line $\langle P'_3, P_0 \rangle$ is of type B_1 and the line $\langle P'_3, P_1 \rangle$ is of type B_3. The remaining four lines have to be of type B_1 or B_2. Counting the number of 1-points gives that two are of type B_1 and two are of type B_2. So, for P_3' we have the pattern $B_1^3B_2^2B_3$. Each 2-point is incident with five 8-lines and a 3-line, which is of type A_2. Counting 3-points gives that four 8-lines have to be of type B_3, so that counting 1-points gives that the remaining 8-line is of type B_1. Each of the four 1-points not on L is incident with two 3-lines and four 8-lines. Counting the 3-points gives that two of the 8-lines are of type B_2 and two are of type B_3. Thus, couting the 1- and 2-points gives that there is one 3-line of type A_1 and one of type A_3. It remains to determine the patterns of the fourteen 0-points that are not on L. First note that the lines incident with such a 0-point split into three of multiplicity 3 and three of multiplicity 8. Let P_0' be one of the four 0-points on L_1' or L_2', which are both of type B_3. The line $\langle P_0', P_1\rangle$ is of type B_3 and the line $\langle P_0', P_0\rangle$ is of type A_2. All other line incident with P_0' meet L in a 3-point, so that there are two 3-lines of type A_1. Counting 3-points gives that the total number of lines through P_0' of type B_3 is two. Counting the number of 1-points gives that the third 8-line through P_0' has type B_2. So, the four 0-points on L_1' or L_2' have pattern $A_1^2A_2B_2B_3^2$. Now let P_0'' be one of the four 0-points on L_3'. The lines $\langle P_0'', P_1\rangle$ and $\langle P_0'', P_0\rangle$ are of type A_2. All other line incident with P_0' meet L in a 3-point, so that the third 3-line through P_0'' is of type A_1. Counting 3-points gives that there is a unique line of type B_3 through P_0''. Counting 2-points yields that there is an $8-$line of type B_1 and one of type B_2 through P_0''. So, the four 0-points on L_3' have pattern $A_1A_2^2B_1B_2B_3$. The remaining six 0-points P_0''' are located on L_4' or L_5'. The line $\langle P_0''', P_1\rangle$ is of type A_3 and the line $\langle P_0''', P_0\rangle$ is of type A_2. All other line incident with P_0''' meet L in a 3-point, so that the third 3-line through P_0''' is of type A_1. Counting 3-points gives that one of the three 8-lines through P_0''' is of type B_3 and counting 2-points then gives that the other two 8-lines are of type B_1. So, the six 0-points on L_4' or L_5' have pattern $A_1A_2A_3B_1^2B_3$. □

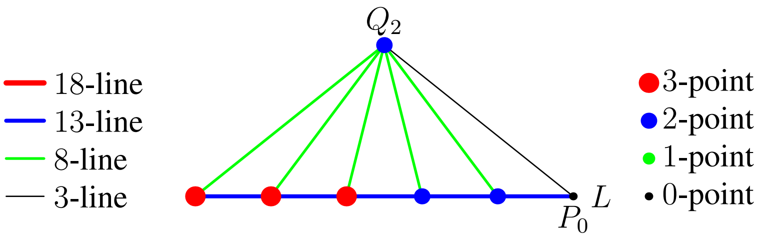
REMARK 8.41 The first case in Lemma 8.40 is case (4) and the second case in Lemma 8.40 is case (3) in [136], where also pictures can be found. The approach is based on Proposition 8.19 and the classification of the corresponding blocking sets. In our situation these are $(21,3)$-blocking sets $\mathcal{B}$ with line multiplicities 3, 4, 5, or 6. Those blocking sets do not have points of cardinality 3 or larger, as the maximum line multiplicity in a strong $(3 \mod 5)$-arc $\mathcal{K}$ in $\mathrm{PG}(2,5)$ of cardinality 33 is 13. Moreover, it can be shown that the number of 2-points in $\mathcal{B}$, corresponding to 13-lines in $\mathcal{K}$, is at most 2. In case (4) we have $\lambda_2 = 2$ and in case (3) we have $\lambda_2 = 1$. Case (2) also satisfies $\lambda_2 = 1$ and we will determine the corresponding arc in Lemma 8.43. The classification of strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ with cardinality 33 that do not contain a 13-line corresponds to the classification of projective blocking sets, i.e., those with $\lambda_2 = 0$. Taking the complement, they correspond to $(10,3)$-arcs, which have been classified in [113]. Instead of repeating the classification of the seven non-isomorphic objects in our context, we will only deduce some partial information, see Lemma 8.45, and show that sever line types cannot occur in strong $(3 \mod 5)$-arcs in $\mathrm{PG}(3,5)$ of cardinality at most 158. We will just describe two remaining possibilities that are counter examples to some (flawed) published results, see Lemma 8.51 and Lemma 8.52.

LEMMA 8.42

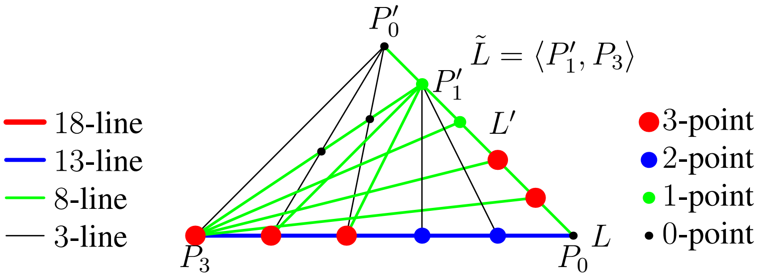
Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. If $\#\mathcal{K} = 33$, then no line is of type C_2, C_3, or C_5.

PROOF. Assume that L is a line of type C_2 and P_0 be the unique 0-point on L. Let L' be the unique 8-line through P_0. Counting points on the lines through an arbitrary 2-point Q_2 outside of L yields that the line $\langle Q_2, P_0\rangle$ is a 3-line and the other five lines through Q_2 are 8-lines. Since L' is an 8-line that contains the

0-point P_0 and no 2-point, it is of type B_2. Since Q_2 cannot be contained in a 13-line, each 13-line not equal to L has to be be of type C_1. From Lemma 8.40 we can conclude $a_{13} = 1$, i.e., L is the unique 13-line. With this, Lemma 8.33 implies $a_3 = 11$, $a_8 = 19$, $\lambda_1 = 3\lambda_3 - 13$, and $\lambda_2 = 23 - 3\lambda_3$.



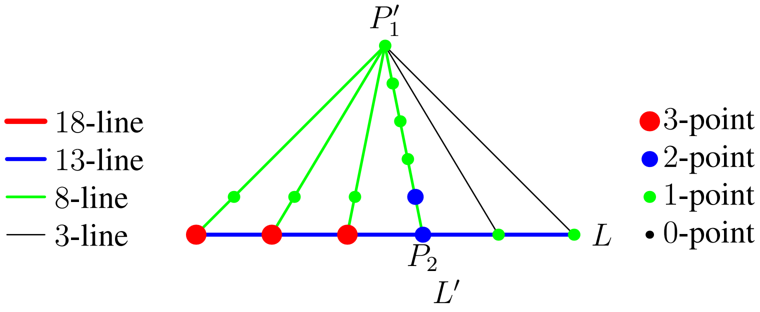
Consider the lines through P_0. The line L has multiplicity 13 and L' has multiplicity 8, so that the other four lines each have multiplicity 3. Thus, we have $2 \le \lambda_2 \le 6$, so that $\lambda_2 = 23 - 3\lambda_3$ and $\lambda_3 \in \mathbb{N}_0$ imply $\lambda_2 = 5$, $\lambda_3 = 6$, and $\lambda_1 = 5$. Let $P_0' \ne P_0$ be the second 0-point on L' and P_3 be one of the three 3-points on L. Counting points on the lines through P_3 gives that those lines meeting L' in a 1- or a 3-point have multiplicity 8 and the line $\langle P_3, P_0' \rangle$ has multiplicity 3. So, if a line through P_0' meets L in a 3-point, then it has multiplicity 3 and is of type A_1. Let P_1' be an arbitrary 1-point on L'. Each line through P_1' that meets L in a 3-point is a 8-line, so that the lines connecting P_1' with a 2-point on L are 3-lines of type A_2. The points with strictly positive multiplicity not on L or L' consist of a 3-point, three 2-points, and three 1-points. Counting yields, that the three 8-lines through P_1' except L' attain the types B_2, B_3, and B_4 exactly once. W.l.o.g. we assume that the line $\tilde{L} := \langle P_1', P_3 \rangle$ has type $B_4 = (3, 2, 1, 1, 1, 0)$. However, the three 3-lines through P_0' of type A_1 enforce at least two 0-points on $\tilde{L}$, which is a contradiction.



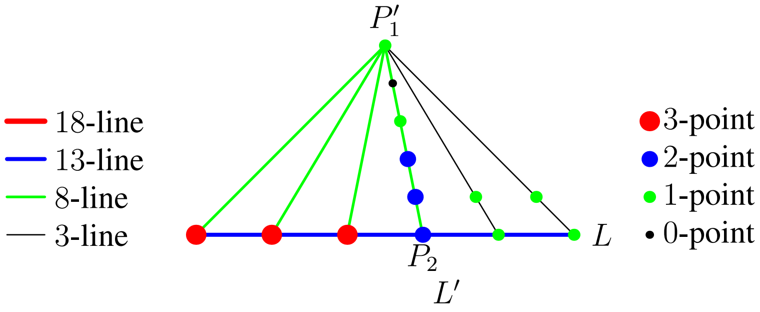
Let L be a line of type C_3 or C_5 and Q_3 be an arbitrary 3-point outside of L. Since every line through Q_3 meets L in a point of strictly positive multiplicity, counting points yields that all these lines are 8-lines. Thus, if there are further 13-lines, besides L, then they are of type C_5 and have to met L in a 3-point. From Lemma 8.33 we conclude $\lambda_1 = -3 - 10a_{13} + 3\lambda_3$ and $\lambda_2 = 18 + 5a_{13} - 3\lambda_3$. Clearly, not all points of strictly positive multiplicity can be 3-points, so that $\lambda_3 \le 10$. With this, $\lambda_1 \ge 0$ implies $a_{13} \le 2$. If $a_{13} = 2$, then $\lambda_1 \ge 0$ and $\lambda_3 \in \mathbb{N}_0$ imply $\lambda_3 \ge 8$, so that $\lambda_2 \le \lfloor (33 - 3\lambda_3)/2 \rfloor \le 4$. Thus, both 13-lines have to be of type C_3, which is a contradiction. So, we conclude $a_{13} = 1$, and Lemma 8.33 yields $a_3 = 11$, $a_8 = 19$, $\lambda_1 = 3\lambda_3 - 13$, and $\lambda_2 = 23 - 3\lambda_3$. Since $\lambda_1, \lambda_2 \ge 0$ and $\lambda_3 \in \mathbb{N}_0$, we have $\lambda_3 \in \{5, 6, 7\}$.

Assume that L is a line of type C_3 and let P_2 be unique 2-point on L. The multiplicities of the lines through P_2 are given by $13^1 8^3 3^2$, where the 3-lines are of type A_2. This gives $\lambda_1 \ge 4$, so that $\lambda_1 \in \{5, 8\}$,

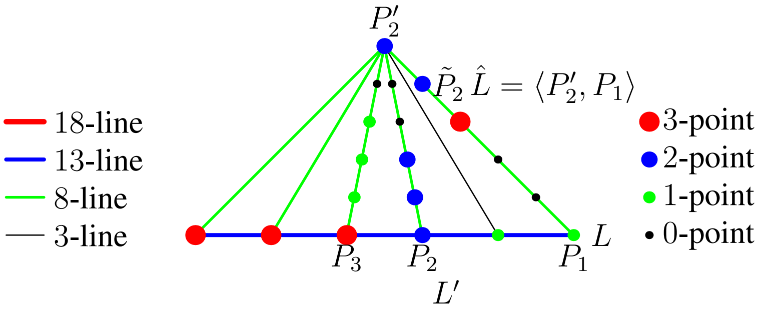
$\lambda_2 \in \{2,5\}$, and $\lambda_3 \in \{6,7\}$. Since $\lambda_2 \geq 2$, we can assume that L' is a line through P_2 containing two 2-points. Assume, for a moment, that L' is of type B_8 and let P_1' be a fix 1-point on L'. On the lines L and L' there are already six 1-points, which implies $\lambda_1 = 8$, $\lambda_2 = 2$, and $\lambda_3 = 7$. Thus, the three lines connecting P_1' and one of the three 3-points on L each contain another 1-point except P_1', since all 2-points are on L'. This gives at least nine 1-points – a contradiction.



Assume, for a moment, that L' is of type B_7 and let P_1' be a fix 1-point on L'. Since the lines L and L' contain four 1-points and three 2-points, we conclude $\lambda_1 = 5$, $\lambda_2 = 5$, and $\lambda_3 = 6$. However, through P_1' there are two 3-lines and four 8-lines. The two 3-lines have to meet L in 1-points, which gives two additional 1-points outside of the lines L and L'. So, there are at least six 1-points – contradiction.



Thus, L' is of type B_3 or B_6. If $\lambda_2 = 2$, then L' is of type B_3 and counting the 3-points on the lines through the unique 3-point on L' give $\lambda_3 \leq 6$, which contradicts $\lambda_3 = 7$. Thus, the only remaining possibility is $(\lambda_1, \lambda_2, \lambda_3) = (5,5,6)$. W.l.o.g. we assume that L' is of type $B_6 = (2,2,2,2,0,0)$ (there cannot be four lines through P_2 of type B_3). By $\tilde{P}_2$ we denote the fifth 2-point not on L'. From the six lines through $\tilde{P}_2$ five have multiplicity 8 and one has multiplicity 3. The later is of type A_2 and meets L' in a 0-point. In four case an 8-line through $\tilde{P}_2$ meets L' in a 2-point. Since there are no further 2 points, these four lines use at least four 1-points. Since $\lambda_1 = 5$, all of them have to be of type $B_3 = (3,2,2,1,0,0)$, so that the fifth 8-line through $\tilde{P}_2$ if of type $B_1 = (3,3,2,0,0,0)$. So, at least one of the four 8-lines through $\tilde{P}_2$ of type B_3, say $\hat{L}$, meets L in a 1-point P_1 and L' in a 2-point P_2'. Now consider the line through P_2'. We have the line L' of type B_6 and the line $\hat{L}$ of type B_3. The unique 3-line through P_2' has to meet L in the other 1-point not equal to P_1. Counting 3-points gives that two of the remaining 8-lines through P_2' are of type B_1, so that the last one, say L'' is of type $B_4 = (3,2,1,1,1,0)$. Let us denote the unique 3-point of L'', which also is on L, by P_3, i.e., we have $L'' = \langle P_2', P_3 \rangle$. Now consider the lines through P_1. The line L is a 13-line and the line $\hat{L}$ is an 8-line. Since there are only two further 2-points not on these two lines, at most two of the lines through P_1 can be of type A_2. Since there are three 3-lines through P_1 there exists a 3-line L''' through P_1 of type A_3. Now, note that L is a line containing two 1-points and L'', L''' are lines that both contain three 1-points. Since there are only five 1-points, this is only possible if the lines L, L'', and L''' pairwise intersect in a 1-point. However, the intersection of L'' and L is the 3-point P_3. Thus, L cannot be of type C_3.



Assume that L is a line of type C_5. Counting the points on the lines through a 2-point Q_2 outside of L would give $\#\mathcal{K} \geq 6 \cdot 8 - 5 \cdot 2 = 38$, so that $(\lambda_1, \lambda_2, \lambda_3) = (5, 5, 6)$. Let P_3 be the unique 3-point on L and Q_3 an arbitrary 3-point not on L. Note that the line $\langle P_3, Q_3 \rangle$ is an 8-line since there are no further 13-lines besides L. Moreover, those 8-lines have to be of type B_2, since there are no 2-points outside of L. Since Q_3 is arbitrary, all five lines through P_3 that are not equal to L are 8-lines. Thus, we obtain the contradiction $\#\mathcal{K} = 5 \cdot 8 + 1 \cdot 13 - 5 \cdot 2 = 43 \neq 33$. □

Lemma 8.43

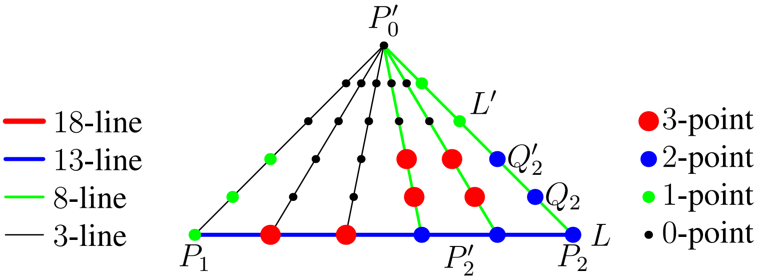
Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$. *If $\#\mathcal{K} = 33$ and there is a line L of type C_4, then we have:*

A_1	A_2	A_3	B_1	B_2	B_3	B_7	C_4	λ_1	λ_2	λ_3	a_3	a_8	a_{13}
2	*8*	*1*	*8*	*6*	*4*	*1*	*1*	*5*	*5*	*6*	*11*	*19*	*1*

Moreover, if P'_0 is the unique 0*-point on the unique line L' of type B_7, then the types of the lines through P'_0 is given by $A_1^2 A_3 B_1^2 B_7$.*

Proof. Let L be a line of type C_4. From Lemma 8.33 we conclude $\lambda_1 = -3 - 10a_{13} + 3\lambda_3$, so that $\lambda_1 \geq 0$ and $a_{13} \geq 1$ imply $\lambda_3 \geq 5$. Let Q_3 be an arbitrary 3-point outside of L. Counting points on the lines through Q_3 yields that all these lines have multiplicity 8. Since only four of those line can contain an additional 3-point, i.e., those that meet L in a point of multiplicity at most 2, we have $\lambda_3 \leq 7$. With this, $\lambda_1 \geq 0$ and the existence of L imply $a_{13} = 1$, so that Lemma 8.33 gives $a_3 = 11$, $a_8 = 19$, $\lambda_1 = 3\lambda_3 - 13$, and $\lambda_2 = 23 - 3\lambda_3$. Since L contains three 2-points we have $\lambda_3 \neq 7$. There are exactly two 3-lines through a 2-point on L. Since there is one 1-point on L, this implies $\lambda_1 \geq 1$ and $\lambda_3 \neq 5$, so that $(\lambda_1, \lambda_2, \lambda_3) = (5, 5, 6)$.

Let Q_2 and Q_2' denote the two other 2-points not on L. The multiplicities of the lines through the unique 1-point on L, which we label as P_1, are given by $13^1 8^2 3^2$. The four 3-points not on L must be located on the two 8-lines, so that they are of type B_2 and use two of the four 1-points not on L. Thus from the three 3-lines two are of type A_2 and one of type A_3. To sum the distribution of the types of the lines through the unique 1-point on L is given by $A_2^2 A_3 B_2^2 C_4$. The multiplicities on the lines through a 3-point on L are given by $13^1 8^4 3^1$. The unique 3-line is of type A_1 and each of the four 8-lines contains exactly one of the four 3-points not on L, so that two are of type B_1 and two are of type B_2. So, the pattern of the lines through a 3-point on L is given by $A_1 B_1^2 B_2^2 C_4$. Thus, the line through the 2-points Q_2 and Q_2' meets L in a 2-point, which we call P_2. In general, the multiplicities of the lines through a 2-point on L are given by $13^1 8^3 3^2$. The two 3-lines are of type A_2. For P_2 the line containing Q_2 and Q_2' has to be of type B_7 since there are no more 2-points. There remain two 8-lines and four 3-points, so that the lines are of type B_1. So, the pattern of the lines through P_2 is given by $A_2^2 B_1^2 B_7 C_4$. Now let P_2' be one of the two other 2-points on L not equal to P_2. Note that Q_2 and Q_2' are on different, so that these two lines have to be 8-lines of type B_3. Counting 3-points yields that the third 8-line through P_2' is of type B_1. With this, the pattern of the lines through P_2' is given by $A_2^2 B_1 B_3^2 C_4$ and we can easily count the occurrences of the total number of lines of different types.



For the last statement, let P_0' be the unique 0-point on the unique 8-line L' of type B_7. The intersection of L and L' is labeled P_2. Since the unique 3-line through a 3-point on L is of type A_1, it meets L' in P_0'. For each 2-point P_2' on L that is not equal to P_2, there is a unique 8-line of type B_1. Since there is no 3-point and a unique 0-point on L', its intersection with L' is P_0'. Thus, the remaining two 1-points that are not on L or L' have to be located on the line $\langle P_1, P_0' \rangle$, which then is a 3-line of type A_3. □

REMARK 8.44 The arc in Lemma 8.43 is case (2) in [136], where also a picture can be found.

LEMMA 8.45

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ of cardinality 33 that does not contain a line of type C_1 or C_4. Then, we have $a_3 = 10$, $a_8 = 21$, $a_{13} = 0$, $\lambda_1 = 3\lambda_3 - 3$, $\lambda_2 = 18 - 3\lambda_3$, and $3 \le \lambda_3 \le 6$. Moreover, there is no 3-line of type A_1.

PROOF. From Lemma 8.42 we conclude $a_{13} = 0$, so that Lemma 8.33 gives $a_3 = 10$, $a_8 = 21$, $\lambda_1 = 3\lambda_3 - 3$, and $\lambda_2 = 18 - 3\lambda_3$. Since $\lambda_1, \lambda_2 \ge 0$, we have $1 \le \lambda_3 \le 6$. Since there are no 13-lines, all six lines through a 3-point have multiplicity 8, so that no 3-line of type A_1 exists. Thus, each 3-line contains at least one 1-point. Since each 1-point is contained on exactly two 3-lines, we have $10 = a_3 \ge 2\lambda_1$, so that $\lambda_1 \ge 5$ and $\lambda_3 \ge 3$. □

line type	name	$\mathcal{K}(H) = 18$	$\mathcal{K}(H) = 23$	$\mathcal{K}(H) = 28$	$\mathcal{K}(H) = 33$
$(3,0,0,0,0,0)$	A_1	✓	✓	✓	✓
$(2,1,0,0,0,0)$	A_2	✓	✓	×	✓
$(1,1,1,0,0,0)$	A_3	✓	✓	✓	✓
$(3,3,2,0,0,0)$	B_1	×	×	×	✓
$(3,3,1,1,0,0)$	B_2	×	✓	✓	✓
$(3,2,2,1,0,0)$	B_3	×	✓	×	✓
$(3,2,1,1,1,0)$	B_4	×	×	×	
$(3,1,1,1,1,1)$	B_5	✓	×	×	
$(2,2,2,2,0,0)$	B_6	×	×	×	✓
$(2,2,2,1,1,0)$	B_7	×	×	×	✓
$(2,2,1,1,1,1)$	B_8	✓	✓	×	
$(3,3,3,3,1,0)$	C_1	×	×	×	✓
$(3,3,3,2,2,0)$	C_2	×	×	×	×
$(3,3,3,2,1,1)$	C_3	×	×	×	×
$(3,3,2,2,2,1)$	C_4	×	×	×	✓
$(3,2,2,2,2,2)$	C_5	✓	×	×	×
$(3,3,3,3,3,3)$	D_1	✓	×	×	×

Table 8.1: Possible line types in a hyperplane H of a strong $(3 \mod 5)$-arc $\mathcal{K}$ with $\#\mathcal{K} \le 158$.

Before we start to exclude some configurations in a strong $(3 \mod 5)$-arc $\mathcal{K}$ in $\mathrm{PG}(3,5)$, we summarize our knowledge on the possible occurrence of line types in a hyperplane H of small multiplicity $\mathcal{K}(H)$, see Table 8.1. We remark that the line types B_4, B_5, and B_8 can indeed occur in 33-planes that do not contain a 13-line. For 33-planes we can refine this information a bit by distinguishing the cases whether a line of type C_1, C_4, or no 13-line at all exists, see Table 8.2. We remark that all types of 8-lines and the types A_2, A_3 can indeed occur in 33-planes that do not contain a 13-line.

LEMMA 8.46

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$. If $\#\mathcal{K} \le 158$, then there is no line of type B_4, B_7, C_2, C_3, or C_4.

PROOF. Assume that L is a 13-line and let $H_0, \dots, H_5$ be the six hyperplanes through L. Since $6 \cdot 38 - 5 \cdot 13 = 163 > \#\mathcal{K}$, there is an index $0 \le i \le 5$ with $\mathcal{K}(H_i) \le 33$. If L is of type C_2, C_3, or C_4, then $\#\mathcal{K}(H_i) = 33$, see Lemma 8.31, Lemma 8.36, and Lemma 8.38. Due to Lemma 8.42 L is of type C_4, so that Lemma 8.43 yields the existence of a line L_1 of type B_7 in $\mathcal{K}|_{H_i}$. Let P be the unique 0-point on L_1. From Lemma 8.43 we further conclude that the other two 8-lines through P in $\mathcal{K}|_{H_i}$ are of type B_1. We denote them by L_2 and L_3. Now we consider the hyperplanes through L_1. Due to Lemma 8.31, Lemma 8.36, and Lemma 8.38 all of them have cardinality at least 33. Since $6 \cdot 33 - 5 \cdot 8 = 158$, we have $\#\mathcal{K} = 158$ and all hyperplanes through L_1 have multiplicity exactly 33. Assume for a moment that such a hyperplane H' through L_1 contains a line L' of multiplicity 13 or 18. Due to Lemma 8.32 we have $\mathcal{K}(L') = 13$, so that Lemma 8.42 and Lemma 8.40 imply that L' is of type C_4. However, the 0-point P is located a line of type B_7, so that it cannot be incident with a 13-line (of type C_4) in H', see Lemma 8.43.

line type	name	two times C_1	one time C_1	one time C_4	no 13-line
$(3,0,0,0,0,0)$	A_1	✓	✓	✓	×
$(2,1,0,0,0,0)$	A_2	✓	✓	✓	
$(1,1,1,0,0,0)$	A_3	×	✓	✓	
$(3,3,2,0,0,0)$	B_1	✓	✓	✓	
$(3,3,1,1,0,0)$	B_2	×	✓	✓	
$(3,2,2,1,0,0)$	B_3	×	✓	✓	
$(3,2,1,1,1,0)$	B_4	×	×	×	
$(3,1,1,1,1,1)$	B_5	×	×	×	
$(2,2,2,2,0,0)$	B_6	✓	×	×	
$(2,2,2,1,1,0)$	B_7	×	×	✓	
$(2,2,1,1,1,1)$	B_8	×	×	×	
$(3,3,3,3,1,0)$	C_1	✓	✓	×	×
$(3,3,3,2,2,0)$	C_2	×	×	×	×
$(3,3,3,2,1,1)$	C_3	×	×	×	×
$(3,3,2,2,2,1)$	C_4	×	×	✓	×
$(3,2,2,2,2,2)$	C_5	×	×	×	×
$(3,3,3,3,3,3)$	D_1	×	×	×	×

Table 8.2: Possible line types in a 33-hyperplane H of a strong $(3 \mod 5)$-arc $\mathcal{K}$ with $\#\mathcal{K} \le 158$.

Thus, all lines through P in $\mathrm{PG}(3,5)$ have multiplicity 3 or 8, so that there are thirteen 8-lines and eighteen 3-lines through P.

Consider a projection of $\mathcal{K}$ through P. The induced arc $\mathcal{K}''$ has thirteen 8-points and eighteen 3-points. Let $\mathcal{K}'$ be the projective $(13, \le 6)$-arc in $\mathrm{PG}(2,5)$ that arises by mapping 8-points to 1-points and 3-points to 0-points. By (a_i') we denote the spectrum of $\mathcal{K}'$. Every 1-point P' in $\mathcal{K}'$ is the image of an 8-line $\tilde{L}$ through P in $\mathcal{K}$. Now let L' be a line incident with P', with respect to $\mathcal{K}'$. The preimage of L' is a plane π. If π contains one of the lines L_1, L_2, or L_3, then π has multiplicity 33, due to the forbidden line types B_1 and B_7 in 18-, 23-, and 28-planes. In that case L' has multiplicity 3 with respect to $\mathcal{K}'$. Otherwise π meets H_i in a 3-line, so that L' cannot have multiplicity six (with respect to $\mathcal{K}'$), i.e., $a_6' = 0$. Moreover, $a_2' = 0$ can be shown, see Exercise 8.4. Using $a_2' = 0$ and $a_6' = 0$ the standard equations for $\mathcal{K}'$ give

$$\begin{aligned}
a_0' &= 5 - a_4' - \frac{8}{3}a_5',\\
a_1' &= 2a_4' + 5a_5',\\
a_3' &= 26 - 2a_4' - \frac{10}{3}a_5'.
\end{aligned}$$

Since $a_0' \in \mathbb{N}_0$, we have that 3 divides a_5' and $a_5' \le \frac{15}{8}$, so that $a_5' = 0$. If $a_4' = 0$, then there would be only 0- and 3-lines. Considering the lines through a 0-point gives that this is impossible, since 13 is not divisible by 3. (Alternatively, we may use the fact that no $(13, \le 3)$-arc in $\mathrm{PG}(2,5)$ exists, see e.g. Example 4.2.) Thus, we have $a_4' > 0$ and consider a 4-line L_4'. Through each 1-point on L_4' there is at least one further 4-line, since the number of lines with even multiplicity has to be even and $a_2' = a_6' = 0$. Thus, we have $a_4' \ge 5$, so that $a_0' \in \mathbb{N}_0$ implies $a_4' = 5$ and $a_0' = 0$. Now consider the image of H_i in $\mathcal{K}'$. It is a 3-line whose 1-points are incident with six 3-lines. Since the three 0-points on this special 3-line have to be incident with an odd number of 4-lines, there exists a 0-point that is incident with at least three 4-lines and at least one 3-line. Since $3 \cdot 4 + 1 \cdot 3 = 15 > 13 = \#\mathcal{K}'$, this is a contradiction. Thus, there is no line of type C_4 in $\mathcal{K}$.

Now assume that L is an 8-line of type B_4 or B_7 in $\mathcal{K}$. Both line types do not occur in 18-, 23-, or 28-planes. Counting points on the hyperplanes through L gives $\#\mathcal{K} \geq 6 \cdot 33 - 5 \cdot 8$ so that $\#\mathcal{K} = 158$ and all six hyperplanes through L have multiplicity 33. Since there can be no line of type C_4 and due to the existence of L, Lemma 8.42 and Lemma 8.40 imply that none of these hyperplanes contains a 13- or an 18-line. From Lemma 8.45 we conclude that non of the six hyperplanes through L contains a 3-line of type A_3. Similar as above, let P be the unique 0-point on L. Again, we consider a projection of $\mathcal{K}$ through P. The induced arc $\mathcal{K}''$ has thirteen 8-points and eighteen 3-points. Let $\mathcal{K}'$ be the projective $(13, \leq 6)$-arc in $\mathrm{PG}(2,5)$ that arises by mapping 8-points to 1-points and 3-points to 0-points. By (a'_i) we denote the spectrum of $\mathcal{K}'$. Since we know from Lemma 8.36 and 8.38 that each 0-point of a 23- or a 28-plane in $\mathcal{K}$ is incident with a line of type A_3 (within that plane), we have $a'_1 = a'_2 = 0$. Counting the points on the lines of a 1-point of $\mathcal{K}'$ gives $\#\mathcal{K}' \geq 6 \cdot 3 - 5 \cdot 1 = 13$, so that all lines which are not 0-lines are 3-lines. Thus, we have $a'_0 = 5$, $a'_3 = 26$, and $a'_j = 0$ otherwise. Since $\#\mathcal{K}' = 13$ is not divisible by 3, this yields a contradiction by considering the multiplicities of the lines through a 0-point. □

LEMMA 8.47

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ of cardinality 33. If L is an 8-line of type B_6, then there is either a 13-line, an 8-line of type B_4, or an 8-line of type B_7.

PROOF. Assume, to the contrary, that there is no 13-line, no 8-line of type B_4, and no 8-line of type B_7. From Lemma 8.45 we know $\lambda_1 = 3\lambda_3 - 3$, $\lambda_2 = 18 - 3\lambda_3$, and $3 \leq \lambda_3 \leq 6$. Since L already contains four 2-points and $\lambda_3 \in \mathbb{N}_0$, we have $\lambda_3 \in \{3, 4\}$ and $\lambda_2 \in \{9, 6\}$. Let P_3 be a 3-point outside of L. Since all lines have multiplicity at most 8, all six lines through P_3 have multiplicity 8. The lines through P_3 that meet L in a 2-point have to be of type B_1 or B_3, so that they contain at most four 1-points. The lines through P_3 that meet L in a 0-point have to be of type B_1, B_2, or B_3, so that they also contain at most four 1-points. From $\lambda_1 \leq 8$ we conclude $\lambda_1 = 6$, $\lambda_2 = 9$, and $\lambda_3 = 3$.

Consider a 2-point P_2 on L. Five of the lines through P_2 have multiplicity 8 and one has multiplicity 3. Since there are no 8-lines of type B_7 none of the five 8-lines through P_2 can contain three 2-points, so that counting 2-points yields that there is a second 8-line L' of type B_6 through P_2. Since $\lambda_2 = 9$, there cannot be a third 8-line of type B_6 through P_2. So, each 2-point is either contained on exactly two 8-lines of type B_6 or on no such line. Now let $P'_2 \neq P_2$ be a 2-point on L' and $L'' \neq L'$ be the second 8-line of type B_6 through P'_2. With this, the lines L, L', and L'' contain at least nine 2-points, so that all 2-points are contained on exactly two 8-lines of type B_6. Counting the number of 8-lines of type B_6 then gives $\lambda_2 \cdot 2/4 = 4.5 \notin \mathbb{N}_0$, which is a contradiction. □

LEMMA 8.48

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$. If $\#\mathcal{K} \leq 158$, then there is neither a line of type B_6 nor a 33-plane with two 13-lines of type C_1.

PROOF. Assume that L is a line of type B_6 and let P be one of its two 0-points. Since no 18-, 23-, or 28-plane contains a line of type B_6 counting the points on the hyperplanes $H_0, \dots, H_5$ through L gives that $\#\mathcal{K} = 158$ and $\mathcal{K}(H_i) = 33$ for all $0 \le i \le 5$. From Lemma 8.46, Lemma 8.47, and Lemma 8.42 we conclude that H_i contains at least one 13-line of type C_1 for all $0 \le i \le 5$. Since L is contained in H_i, Lemma 8.40 yields that the distribution of the lines through P in H_i is given by $A_1^4 B_6 C_1$ in all cases. Thus, we have $\lambda_1 = 6$, $\lambda_2 = 4$, and $\lambda_3 = 48$. Now consider the lines trough a fixed 1-point P_1. Since $\lambda_2 = 4$, at most four of them can be of type A_2. Since $\lambda_1 = 6$, at most two of them can be of type A_3. Thus, at most six of the lines through P_1 can be 3-lines, so that $\#\mathcal{K} \ge 6 \cdot 3 + 25 \cdot 8 - 30 = 188$, which is a contradiction.

If π is a 33-plane containing two 13-lines of type C_1, then Lemma 8.40 yields the existence of an 8-line of type B_6, which we just excluded. □

LEMMA 8.49

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ of cardinality 33. If L is an 8-line of type B_1, then there is either a 13-line, an 8-line of type B_4, an 8-line of type B_6, or an 8-line of type B_7.

The proof is left as an exercise, see Exercise 8.5.

LEMMA 8.50

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$. If $\#\mathcal{K} \le 158$, then there is neither a line of type B_1 nor a line of type C_1.

PROOF. Assume that L is a line of type B_1 and let P be its unique 2-point. Since no 18-, 23-, or 28-plane contains a line of type B_1 counting the points on the hyperplanes $H_0, \dots, H_5$ through L gives that $\#\mathcal{K} = 158$ and $\mathcal{K}(H_i) = 33$ for all $0 \le i \le 5$. From Lemma 8.46 and Lemma we conclude that there are no lines of type B_4, B_6, B_7, C_2, C_3, or C_5, so that Lemma 8.49 and Lemma 8.42 imply that H_i contains at least one 13-line of type C_1 for all $0 \le i \le 5$. With this, Lemma 8.3 and Lemma 8.40 gives that the distribution of the types of the lines through P in H_i, where $0 \le i \le 5$ is arbitrary, is given by $A_2 B_1 B_3^4$. So, the distribution of the types of all lines through P is given by $A_2^6 B_1 B_3^{24}$, i.e., six lines have multiplicity 3 and 25 lines have multiplicity 8. Since 28-planes contain no 2-point, see Lemma 8.38, no hyperplane through P can be a 28-plane. Since lines of type B_1 or B_3 cannot be contained in an 18-plane, $6 \cdot 3 - 5 \cdot 2 = 8 < 18$ implies that no hyperplane through P can be an 18-plane. Since $6 \cdot 8 - 2 \cdot 5 = 38$, all hyperplanes through P have a multiplicity in $\{23, 33, 38\}$. Let x_{23}, x_{33}, and x_{38} denote their corresponding counts. Counting points and hyperplanes gives

$$23x_{23} + 33x_{33} + 38x_{38} = [2]_5 \cdot (\#\mathcal{K} - \mathcal{K}(P)) + [3]_5 \cdot \mathcal{K}(P) = 6 \cdot 156 + 2 \cdot 31 = 998$$

and

$$x_{23} + x_{33} + x_{38} = [3]_5 = 31,$$

so that

$$2x_{33} + 3x_{38} = 57.$$

Since $x_{33}, x_{38} \in \mathbb{N}_0$, this implies that x_{38} is odd and $x_{38} \ge 1$.

Next we conclude the existence of a 38-plane π through P in our situation. Assume that such a plane π exists. First, we note that the lines of type A_2 or B_1 through P cannot be contained in π. Thus, the six lines through P in π all are of type B_3, which implies $(\lambda'_1, \lambda'_2, \lambda'_3) = (6,7,6)$ for the point multiplicities in $\mathcal{K}|_\pi$. With this, the standard equations for $\mathcal{K}|_\pi$ yield $a'_{13} = 3a'_3 - \frac{84}{5}$, $a'_{18} = -a'_3 + \frac{32}{5}$, $a'_8 = -3a'_3 + \frac{207}{5}$ for the spectrum (a'_i) of $\mathcal{K}|_\pi$. So, $a'_{13} \notin \mathbb{N}_0$, which is a contradiction. Thus, $\mathcal{K}$ cannot contain a line of type B_1.

If π is a 33-plane containing a 13-line of type C_1, then Lemma 8.40 yields the existence of an 8-line of type B_1, which we just excluded. □

A strong $(3 \mod 5)$-arc $\mathcal{K}$ in $\mathrm{PG}(3,5)$ of cardinality at most 158 can be obtained by lifting strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ with a cardinality in $\{18,23,28\}$. So, lines of types A_1, A_2, A_3, B_2, B_3, B_5, B_8, C_5, and D_1 can indeed occur in $\mathcal{K}$. For the other types of lines we have proven their non-existence in Lemma 8.46, Lemma 8.3, and Lemma 8.50. So, while our previous argumentation is lengthy and looks a bit ad hoc, it is based on a systematic approach, i.e., try to classify the hyperplanes of small multiplicity (up to the accuracy that is needed later on) and use this information to exclude the existence of lines of certain types. Of course, we can also look at the existence of hyperplanes with a certain multiplicity (or "type"). The lifting construction shows that all strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ with a cardinality in $\{18,23,28\}$ can occur in a hyperplane. Lifting a 3-line gives an 18-plane and lifting an 8-lines gives a 43-plane. So, our next aim is to show that these are all possibilities.

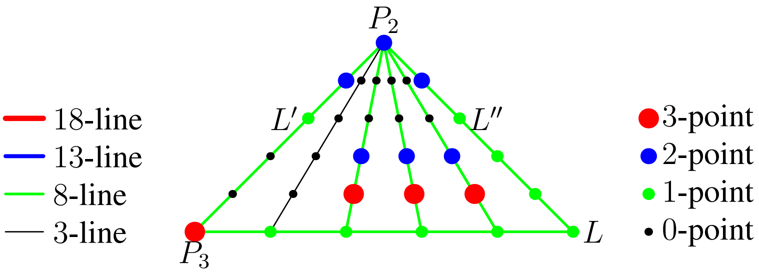
LEMMA 8.51

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ of cardinality 33 that contains a line L of type B_5. If there is no line of one of the types B_1, B_4, B_6, B_7, C_1, or C_4, then we have

A_3	B_2	B_5	λ_1	λ_2	λ_3	a_3	a_8	a_{13}
10	*15*	*6*	*15*	*0*	*6*	*10*	*21*	*0*

Moreover, the pattern of the types of the lines through a 3-point is given by $B_2^5 B_5$.

PROOF. From Lemma 8.42 we conclude that there are no lines of type C_2, C_3, or C_5, so that $a_{13} = 0$. With this, Lemma 8.33 gives $a_3 = 10$,$a_8 = 21$, $\lambda_1 = 3\lambda_3 - 3$, and $\lambda_2 = 18 - 3\lambda_3$. Let P_3 be the unique 3-point on L. Note that all lines through P_3 have multiplicity 8 and attain one of the type B_2, B_3, or B_5. Assume that L' is a line of type B_3 through P_3. Let P_2 denote one of the two 2-points on L'. There are five 8-lines and a unique 3-line through P_2. The four 8-lines that are not equal to L' meet L in a 1-point, so that they are of type B_3 or B_8. In both cases they contain an extra 2-point besides P_2. Thus, we have $\lambda_2 = 6$, $\lambda_3 = 4$, and $\lambda_1 = 9$. Thus, the pattern of the types of the lines through P_2 is given by $A_2 B_3^3 B_5 B_8$. Let L'' denote the unique line of type B_8 through P_2. Not that all nine 1-points are located on the lines L, L', and L''. The same argumentation gives that there is a unique 8-line $\tilde{L}$ of type B_8 through the second 2-point on L'. Since $\tilde{L}$ meets L' in a 2-point and L, L'' in at most two 1-points, we would need two further 1-points that are not located in L, L', or L'' – a contradiction.



Thus, all lines through P_3 are of type B_2 or B_5. Since one of these six lines is of type B_5, we have $\lambda_1 \geq 15$. Using Lemma 8.33 we conclude $\lambda_1 = 15$, $\lambda_2 = 0$, and $\lambda_3 = 6$. Since all lines through a 3-point have multiplicity 8 and there is no 2-point, all ten 3-lines are of type A_3. Since $\lambda_3 = 6$, through each 3-point there are five lines of type B_2 and one line of type B_5. Thus, there are six lines of type B_5 and fifteen lines of type B_2 in total. □

LEMMA 8.52

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ of cardinality 33 consisting only of 3- and 8-lines. If there is no line of one of the types B_1, B_4, B_5, B_6, or B_7, then we have

A_2	A_3	B_2	B_3	B_8	λ_1	λ_2	λ_3	a_3	a_8
6	*4*	*6*	*12*	*3*	*9*	*6*	*4*	*10*	*21*

Moreover, for a point P with $\mathcal{K}(P) \neq 1$ the pattern of the types of the lines through P is unique:

- $\mathcal{K}(P) = 3$: $B_2^3 B_3^3$,
- $\mathcal{K}(P) = 2$: $A_2 B_3^4 B_8$,
- $\mathcal{K}(P) = 0$: $A_2^2 A_3 B_2 B_3^2$,
- $\mathcal{K}(P) = 1$, *P is contained on two lines of type B_8: $A_2^2 B_2^2 B_8^2$ three times,*
- $\mathcal{K}(P) = 1$, *P is contained on one line of type B_8: $A_3^2 B_2 B_3^2 B_8$ six times.*

PROOF. From Lemma 8.33 we conclude $a_3 = 10$,$a_8 = 21$, $\lambda_1 = 3\lambda_3 - 3$, and $\lambda_2 = 18 - 3\lambda_3$, so that $\lambda_3 \geq 1$. The lines through a 3-point P_3 are of type B_2 or B_3. If x is the number of the latter, then we obtain $\lambda_1 = 12 - x$, $\lambda_2 = 2x$, and $\lambda_3 = 7 - x$, so that $x = 3$, $\lambda_1 = 9$, $\lambda_2 = 6$, and $\lambda_3 = 4$. Counting 3-points gives that the lines through a 2-point have the pattern $A_1 B_3^4 B_8$ and the three 8-lines through a 0-point have the pattern $B_2 B_3^2$. Via the 1-points we can complete the latter pattern to $A_2^2 A_3 B_2 B_3^2$. Since there are twelve 0-points and each 0-point is incident with a unique line of type A_3, we have four lines of type A_3 and six lines of type A_2. Since each 2-point is incident with a unique line of type B_8, there are exactly three those lines. Similarly, the number of lines of type B_3 is given by $\lambda_2 \cdot 4/2 = 12$, so that the number of lines of type B_2 is six. Since each 2-point is contained in a unique line of type B_8, two lines of type B_8 intersect in a 1-point. Due to $\lambda_1 = 9 < 10$ not all three lines of type B_8 can intersect in the same 1-point. Thus, there are three 1-points that are contained on exactly two lines of type B_8. Counting 3-points gives that the other two 8-lines are of type B_2, so that counting the 2-points yields that the two 3-lines are of type A_2. For the remaining six cases of 1-points counting 3-points gives that one of the three 8-lines that are not of type B_8 is of type B_2 and two are of type B_3. Counting 2-points then gives that the two 3-lines through the 1-point are of type A_3. □

REMARK 8.53 Strong $(3 \mod 5)$-arcs in $\operatorname{PG}(2,5)$ with cardinality 33 and type distribution $A_2^6 A_3^4 B_2^6 B_3^{12} B_8^3$ or $A_3^{10} B_2^{15} B_5^6$ of the lines, i.e., those characterized in Lemma 8.51 and Lemma 8.52, indeed exist. Generator matrix of the complements of the corresponding blocking sets, see Proposition 8.19, are given by

$$\begin{pmatrix}111111111111111110000000111222333344441111134012134023402341234\end{pmatrix}$$

and

$$\begin{pmatrix}111111111111111110000\\000111222333344441111\\234134034012301241234\end{pmatrix}.$$

The existence of these two arcs contradicts [117, Lemma 4.2] showing that the corresponding proof is flawed.

LEMMA 8.54

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\operatorname{PG}(2,5)$ of cardinality 38. Then, $\mathcal{K}$ contains at least one line of the types B_1, B_4, B_6, B_7, C_1, C_2, C_3, or C_4.

PROOF. Assume, to the contrary, that $\mathcal{K}$ does not contain one of the lines B_1, B_4, B_6, B_7, C_1, C_2, C_3, and C_4. If there is no 0-point at all, then setting $\mathcal{K}'(P) = \mathcal{K}(P) - 1$ for all $P \in \mathcal{P}$ gives a strong $(2 \mod 5)$-arc $\mathcal{K}'$ in $\operatorname{PG}(2,5)$ of cardinality 7, which does not exist. So, let P_0 be an arbitrary 0-point. Counting the points on the lines through P_0 gives that P_0 is contained on exactly two 3-lines. Thus, there cannot be two lines with a type in $\{C_5, D_1\}$, i.e., $a_{13} + a_{18} \le 1$.

First we assume that L is a line of type D_1. There cannot be another 3-point outside of L, since this counting the points on the lines through this point would give $\#\mathcal{K} \le 6 \cdot 8 - 5 \cdot 3 = 33$. Thus, we have $\lambda_3 = 6$. Using $a_{18} = 1$, $\lambda_3 = 6$, and $\lambda_1 + 2\lambda_2 + 3\lambda_3 = 38$, the standard equations yield $a_{13} = a_3 - 6$, $a_8 = -2a_3 + 36$, $\lambda_1 = 60 - 10a_3$, and $\lambda_2 = 5a_3 - 20$. Since $a_{13}, \lambda_1 \ge 0$, we have $a_3 = 6$, $a_{13} = 0$, $a_8 = 20$, $\lambda_1 = 0$, and $\lambda_2 = 10$. However, an 8-line through a 3-point on L must contain at least one point of odd multiplicity outside of L. Thus, we have $a_{18} = 0$.

Next, we assume that L is a 13-line, i.e., L is a line of type C_5, $a_{18} = 0$, and $a_{13} = 1$. The standard equations and $\lambda_1 + 2\lambda_2 + 3\lambda_3 = 38$ imply $a_3 = 5$, $a_8 = 25$, $\lambda_1 = 2 + 3\lambda_3$, and $\lambda_2 = 18 - 3\lambda_3$. Since each 2-point on L is contained in a unique 3-line, the five 3-lines are all of type A_2. Using the fact that each 0-point is contained on exactly two 3-lines, this yields $\lambda_0 = 4a_3/2 = 10$. From $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = [3]_5 = 31$ we then conclude $\lambda_1 = 5$, $\lambda_2 = 15$, and $\lambda_3 = 1$. So, the four 8-lines through a 2-point on L are all of type B_8, which implies $\lambda_1 \ge 16$ – a contradiction.

In the remaining case we have $a_{13} = a_{18} = 0$, so that the standard equations give $a_3 = 4$ and $a_8 = 27$. Since each 0-point is contained on two 3-lines, all four 3-lines have to be of type A_3. With this, counting gives $\lambda_0 = 6$. From the standard equations, $\sum_i \lambda_i = 31$, $\sum_i i\lambda_i = 38$, and $\lambda_0 = 6$ we conclude $\lambda_1 = 12$, $\lambda_2 = 13$, and $\lambda_3 = 0$. However, the possible types of 8-lines that contain a 0-point but no 3-point are all excluded. □

LEMMA 8.55

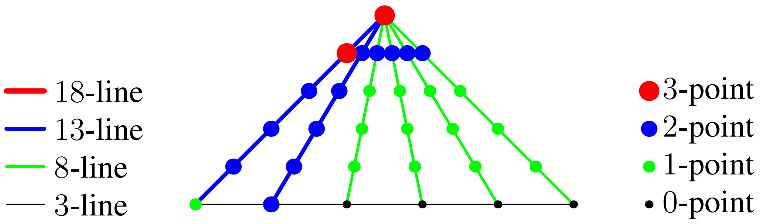
Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc $\mathcal{K}$ in $\mathrm{PG}(2,5)$ of cardinality 43. If every 13-line is of type C_5, then $\mathcal{K}$ is lifted from an 8-line.

PROOF. If there is no 0-point at all, then setting $\mathcal{K}'(P) = \mathcal{K}(P) - 1$ for all $P \in \mathcal{P}$ gives a strong $(2 \mod 5)$-arc $\mathcal{K}'$ in $\mathrm{PG}(2,5)$ of cardinality 12. From Proposition 8.29 we conclude that $\mathcal{K}'$ is the sum of two lines. If those two lines intersect in a unique 2-point P with respect to $\mathcal{K}'$, then P has multiplicity 3 with respect to $\mathcal{K}$ and P is a lifting point in $\mathcal{K}$. The 8-line from which $\mathcal{K}$ is lifted then has type $B_8 = (2,2,1,1,1,1)$. If $\mathcal{K}' = 2 \cdot \chi_L$ for a line L, i.e., a double line, then every point on L is a lifting point for $\mathcal{K}$. The 8-line from which $\mathcal{K}$ is lifted then has type $B_5 = (3,1,1,1,1,1)$.

Now assume that $\mathcal{K}$ contains a 0-point P_0. Counting the points on the lines through P_0 gives that the multiplicities of those lines are given by $3^1 8^5$, since no 0-point is incident with a 13-line and $\#\mathcal{K} = 43$. Let us assume that there exist a 3-line L of type A_1 and let P_3 denote the unique 3-point on L. Since every 0-point is contained in five 8-lines and a unique 3-line, the 25 lines that do not contain P_3 meet L in a 0-point and have multiplicity 8. So, all 3-, 13-, and 18-lines contain P_3. Especially, the unique 3-line through each 0-point contains P_3, so that $a_3 = \frac{\lambda_0}{5}$ and every 8-line trough P_3 is of type B_5. Now let us summarize the possible types of a line L through P_3. For each possibility for $\mathcal{K}(L) \in \{3, 8, 13, 18\}$ there is just one choice, i.e., A_1, B_5, C_5, or D_1. Thus, P_3 is a lifting point and $\#\mathcal{K} = 5 \cdot 8 + 3$ implies that $\mathcal{K}$ is lifted from an 8-line.

It remains to consider the situation where no 3-line of type A_1 but a 0-point P_0 exists. Note that $a_{18} = 0$, since a line of type D_1 would imply a line of type A_1 using the fact that the multiplicities of the lines through a 0-point are given by $8^5 3^1$. From the standard equations we then conclude $a_3 = a_{13} - 2$, so that $a_{13} \ge 2$ and $\lambda_3 \ge 1$. Since the is no line of type A_1 or D_1, the lines through a 3-point P_3 have multiplicities $13^2 8^4$. Let L and L' be the two 13-lines through P_3. The unique 3-line through P_0 cannot meet L and L' in 2-points, so that it contains P_3, which then is a line of type A_1 – contradiction. □

REMARK 8.56 If one only excludes 13-lines of type C_1 or C_2 in Lemma 8.55, then one has to deal with the following configuration:



LEMMA 8.57

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ that contains at least one 0-point P_0 and no lines of one of the types B_1, B_4, B_6, B_7, C_1, C_2, C_3, or C_4. Then, we have $\mathcal{K} \in \{18, 23, 28, 33, 43\}$.

PROOF. Since all lines through P_0 have multiplicity at most 8, we have $\#\mathcal{K} \le 6 \cdot 8 = 48$. Due to Lemma 8.54 it remains to exclude the case $\#\mathcal{K} = 48$, which we assume in the following. Note that each line trough an arbitrary 0-point has multiplicity 8. Thus, we have $a_3 = 0$. From the forbidden line types we then conclude that each 8-line is incident with two 0-points, so that $\lambda_0 = 7$. Consider a point P' that is not a 0-point. Each of the six lines through P' contains an even number of 0-points, which is impossible. □

THEOREM 8.58 (C.f. [136, Theorem 6])

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$ with $\#\mathcal{K} < 163$. Then, $\mathcal{K}$ either contains a full hyperplane, is a lifted arc, or $\#\mathcal{K} = 128$ with spectrum $(a_{18}, a_{23}, a_{28}, a_{33}) = (20, 80, 16, 40)$ and the counts of points per multiplicity and lines per type as well as the distribution of line types through a point and the distribution of the multiplicities of the hyperplanes through a line are given by:

- 0-*point:* $\# = 80$, $A_1^6 A_2^{12} A_3^6 B_2^3 B_3^4$,
- 1-*point:* $\# = 40$, $A_2^6 A_3^{12} B_2^6 B_3^4 B_8^3$,
- 2-*point:* $\# = 20$, $A_2^{12} B_3^{16} B_8^3$,
- 3-*point:* $\# = 16$, $A_1^6 B_2^{15} B_3^{10}$,
- A_1*:* $\# = 96$, $23^5 28^1$,
- A_2*:* $\# = 240$, $18^1 23^4 33^1$,
- A_3*:* $\# = 160$, $18^2 23^2 28^1 33^1$,
- B_2*:* $\# = 120$, $23^2 28^2 33^2$,
- B_3*:* $\# = 160$, $23^3 33^3$,
- B_8*:* $\# = 30$, $18^2 33^4$.

In particular, we have $\#\mathcal{K} \in \{93, 118, 128, 143\}$.

PROOF. In the following we assume that there is no full hyperplane, i.e., each hyperplane contains at least one 0-point, and $\#\mathcal{K} \le 158$. Due to Lemma 8.46, Lemma 8.3, and Lemma 8.46 there is no line of type B_1, B_4, B_6, B_7, C_1, C_2, C_3, or C_4. From Lemma 8.57 we conclude $\mathcal{K}(H) \in \{18, 23, 28, 33, 43\}$ for each hyperplane H.

Assume that H is a 43-plane. Due to Lemma 8.55 and the non-existence of 8-lines of type B_1 and B_6, there exists an 8-line L of type B_5 in H. Let P_3 be the unique 3-point on L and consider the hyperplanes $H, H_1, \dots, H_5$ through L. From Lemma 8.36 and Lemma 8.38 we conclude $\mathcal{K}(H_i) \notin \{23, 28\}$. Let us further assume $\mathcal{K}(H_1) = 33$. From Lemma 8.51 we conclude that the lines through P_3 in H_1 have the types $B_2^5 B_5$. If $\mathcal{K}(H_i) \in \{18, 43\}$ for some index $2 \le i \le 5$, then P_3 is a lifting point in $\mathcal{K}|_{H_i}$, see Lemma 8.31 and Lemma 8.55. Thus, the types of the lines through P_3 are contained in $\{A_3, B_2, B_5, C_5, D_1\}$. Let L' be a line of type B_2 through P_3 and H' be a hyperplane through L'. Due to Lemma 8.31 we have $\mathcal{K}(H') \neq 18$ and due to Lemma 8.36 we have $\mathcal{K}(H') \neq 23$, since there is no line of type B_3 through P_3. If $\mathcal{K}(H') = 28$, then Lemma 8.36 implies that the lines through P_3 in H' have $A_1 B_2^5$ as type distribution. If $\mathcal{K}(H') = 33$, then Lemma 8.51 implies that the lines through P_3 in H' have $B_2^5 B_5$ as type distribution. If $\mathcal{K}(H') = 43$, then Lemma 8.55 implies that the lines through P_3 in H' have $B_2^5 D_1$ as type distribution. Thus, no line through P_3 can have type C_1, so that H is lifted from an 8-line of type B_5 and the lines through P_3 in H have type distribution $B_5^5 D_1$. With this we can exclude the possibility $\mathcal{K}(H') = 28$, since H does not contain a line through P_3 of type A_1 or B_2. Thus, no line through P_3 can have type A_1, i.e., all lines through P_3 have a type in $\{B_2, B_5, D_1\}$ and $\mathcal{K}(H_i) \in \{33, 43\}$ for all $1 \le i \le 5$. Since $\mathcal{K}(H) = 43$, this gives $\#\mathcal{K} \ge 43 + 5\cdot 33 - 5\cdot 8 = 168 > 158$, which is a contradiction. Thus, our assumption $\mathcal{K}(H_1) = 33$ is wrong. By symmetry we obtain $\mathcal{K}(H), \mathcal{K}(H_i) \in \{18, 43\}$, where $1 \le i \le 5$. Note that P_3 is a lifting point in six hyperplanes through L, so that $\mathcal{K}$ is a lifted arc and $\#\mathcal{K} \in \{5\cdot 18 + 3, 5\cdot 23 + 3, 5\cdot 28 + 3\} = \{93, 118, 143\}$.

In the remaining cases we can assume $\mathcal{K}(H) \in \{18, 23, 28, 33\}$ for each hyperplane H. With this, each line of type D_1 or C_5 can be only contained in 18-planes, so that $\#\mathcal{K} \le 6 \cdot 18 - 5 \cdot 13 = 43 < 93$. Using Lemma 8.27, we conclude that all lines have multiplicity 3 or 8. Let us assume again that L is a line of type B_5 and P_3 be the unique 3-point on L. A hyperplane H through L is either an 18- or a 33-plane and the type distribution of the lines through P_3 in H is either $B_2^5 B_5$ or $A_1^3 B_5^3$. If all hyperplanes through L are 18-planes, then $\#\mathcal{K} = 93$ and Proposition 8.29 yields that $\mathcal{K}$ is a sum of three hyperplanes. Thus, we can assume there exists a 33-plane H_{33} containing L. Let L' be an arbitrary line of type B_2 through P_3. Then, each hyperplane H' through L' is either 28- or 33-plane and the types of the lines through P_3 in H' are either $A_1 B_2^5$ or $B_2^5 B_5$. So, not all hyperplanes through L can be 33-planes and be denote one of the 18-planes by H_{18}. Now consider a plane π through a fix line of type A_1 in H_{18} that is not equal to H_{18}. It meets H_{33} in a line of type B_2 so that π is a 28-plane and all lines through P_3 that are not contained in H_{18} are of type B_2. Thus, the hyperplanes through one of the two 8-lines in H_{18} of type B_5 that are not equal to L are all 33-planes. We have already seen that this is impossible. Thus, there is no line of type B_5.

If the is no 3-point at all, then all hyperplanes are 18-planes and counting the points on the six hyperplanes through an 8-line gives $\#\mathcal{K} \le 68 < 93$, which is impossible. So, let P_3 be a 3-point. Every line through P_3 is contained in a hyperplane with multiplicity in $\{23, 28, 33\}$. The possible patterns of the types of the lines through P_3 in such a hyperplane are given by $A_1^2 B_2^2 B_3^3$, $A_1 B_2^5$, and $B_2^3 B_3^3$, see Lemma 8.52 for the latter. If there would be no line of type A_1 through P_3, then only the pattern $B_2^3 B_3^3$ is possible. Let L_2 be a line of type B_2, which occurs in all three cases. Considering the hyperplanes through a line of type B_2 gives $B_2^{13}B_3^{18}$ and considering the hyperplanes through a line of type B_3 gives $B_2^{18}B_3^{13}$ for the pattern of all lines through P_3. So, let L_1 be a line of type A_1. Similarly, we conclude that there exists a line L_3 of type B_3. By considering the hyperplanes through L_1 we obtain the pattern

$$A_1^{1+x}B_2^{30-3x}B_3^{2x}$$

for some integer $0 \le x \le 6$. Similarly, by considering the hyperplanes through L_3 we obtain the pattern

$$A_1^{2y}B_2^{18-y}B_3^{13-y}$$

for some integer $0 \le y \le 6$. Comparing the exponents for A_1, we conclude $x \in \{1, 3, 5\}$ and $y \in \{1, 2, 3\}$, so that comparing the exponents for B_3 gives $x = 5$ and $y = 3$. So, we have $\#\mathcal{K} = 128$, $\lambda_1 = 40$, $\lambda_2 = 20$, $\lambda_3 = 16$, and $\lambda_0 = 80$. We can also count the number of lines that contain a 3-point. There are $6 \cdot 16 = 96$ lines of type A_1, $16 \cdot 15/2 = 120$ lines of type B_2, and $16 \cdot 10 = 160$ lines of type B_3. Through each 2-point P_2 there are nineteen 8-lines and twelve 3, lines, so that there are 240 lines of type A_2. Counting the 3-points on the lines through P_2 gives that the pattern of the types of the lines through P_2 is given by $A_2^{12}B_3^{16}B_8^3$. Thus, we have 30 lines of type B_8 and $\begin{bmatrix}4\\2\end{bmatrix}_5 - 96 - 240 - 120 - 160 - 30 = 160$ lines of type A_3. The distribution of the multiplicities of the hyperplanes through a line of type A_1 is given by $23^5 28^1$ and for a line of type B_3 we have the pattern $23^3 33^3$. So, for a 1-point, which is contained on a line of type B_3, the distribution of the types of all incident lines is given by $A_2^6 A_3^{12} B_2^6 B_3^4 B_8^3$. Since there are 160 lines of type B_3 and only $\lambda_1 = 40$ 1-points, indeed all 1-points have this pattern. Consider a line of type A_3 and the distribution of the types of the lines through an incident 1-point. In an 18-plane we have $A_2 A_3^4 B_8$, in a 23-plane we have $A_2^2 A_3 2 B_2 B_3$, in a 28-plane we have $A_3^3 B_2^3$, and in a 33-plane we have $A_3^2 B_2 B_3^2 B_8$. Thus, the distribution of the multiplicities of the hyperplanes through L_3 is given by $18^2 23^2 28^1 33^1$. By considering the hyperplanes through L_2 we obtain the pattern

$$A_1^{2z_1+z_2}B_2^{1+z_1+4z_2+2(6-z_1-z_2)}B_3^{2z_1+3(6-z_1-z_2)} = A_1^{2z_1+z_2}B_2^{13-z_1+2z_2}B_3^{18-z_1-3z_2},$$

so that $z_1 = 2$, $z_2 = 2$, and the distribution of the multiplicities of the hyperplanes through a line of type B_2 is given by $23^2 28^2 33^2$. If L' is a line of type B_8, then the hyperplanes through L' have multiplicity 18 or 33, where the first case occurs two and the second case occurs four times. For a line of type A_2 we use the fact that the pattern of types of the lines through a 2-point is $A_2^{12}B_3^{16}B_8^3$ in $\mathcal{K}$, $A_2^4 B_8^2$ in an 18-plane, $A_2^4 B_3^3$ in a 23-plane, and $A_2 B_3^4 B_8$ in a 33-plane. With this, we can compute that the distribution of the multiplicities of the hyperplanes through a line of type A_2 is $18^1 23^4 33^1$. Let P_0 be a 0-point incident with a line $\hat{L}$ of type B_2. The hyperplanes through $\hat{L}$ have multiplicities $23^2 28^2 33^2$. Now consider the distributions of the lines through P_0 in a hyperplane. In a 23-plane we have $A_1 A_2^4 B_2$, in a 28-plane we have $A_1^2 A_3^2 B_2^2$, and in a 33-plane we have $A_2^2 A_3 B_2 B_3^2$. With this, the distribution of all lines through P_0 is given by $A_1^6 A_2^{12} A_3^6 B_2^3 B_3^4$. Double-counting the 0-points incident with lines of type B_2 gives that all $\lambda_0 = 80$ 0-points are of this type. Since each 18-plane and each 33-plane contains exactly three lines of type B_8, we have $a_{18} = 30 \cdot 2/3 = 20$ and $a_{33} = 30 \cdot 4/3 = 40$. Similarly, since each 23-plane contains exactly three and each 28-plane contains exactly fifteen lines of type B_2, we have $a_{23} = 120 \cdot 2/3 = 80$ and $a_{28} = 120 \cdot 2/15 = 16$. Our findings on the properties of the exceptional arc are summarized in the statement of the theorem. □

The exceptional arc of cardinality 128 described in Theorem 8.58 indeed exists and so is a counter example to [117, Theorem 4.1], [136, Theorem 6], and other places where the characterization of strong $(3 \mod 5)$-arcs in $\mathrm{PG}(3, 5)$ of small cardinality was mentioned. A generator matrix is e.g. given by the concatenation of

$$\begin{pmatrix}000000000000000000000000000000000111111111111111111111111111111\\000111111111111111111111111111111000000000000000000001111111111\\111000111111112222222233333333444000111111112223334440001112223\\114013011223331123334401112223224022111234440011331112333330230\end{pmatrix}$$

and

$$\begin{pmatrix}11111111111111111111111111111111111111111111111111111111111111111\\11111111112222222222222223333333333333333333334444444444444444444\\33333334440001112223334440001112223334444444440001111111222333444\\01112334441240120132440330244440443330111224412201113334002111144\end{pmatrix}.$$

The specific example was found by solving an integer linear programming problem. We modeled an arc in $\mathrm{PG}(3,5)$ using binary variables and the restriction of the point multiplicities to 3, require that the line multiplicities are contained in $\{3,8\}$ and that the hyperplane multiplicities are contained in $\{18,23,28,33\}$. Noting that the unique possibility for the contained 33-planes is characterized in Lemma 8.52, we fixed the variables for the points in a specific hyperplane such that they match the corresponding stated generator matrix. Using the ILP solver `CPLEX` a solution was found in less than 10 seconds and less than 20 branch&bound nodes. Of course we might have also prescribed the known number λ_i of i-points and some additional information.

We remark that the restricted structure of 23- and 28-planes in a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$ allows to deduce some structural restriction for the arc arising by projection through a 0-point, which was used to a great degree for non-existence results in the literature.

Lemma 8.59

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$ and P_0 be a 0-point. Consider a projection φ from P_0 onto some plane π not incident with P_0 and set $\mathcal{F} = \frac{1}{5}\left(\mathcal{K}^{\varphi} - 3\right)$. Let X, Y, Z be 1-points in π, such that $\langle X, Y\rangle$ and $\langle X, Z\rangle$ are 2-lines with respect to $\mathcal{F}$. If there exists a 1-point $U \neq X, Y, Z$ in π that is incident with a 2-line, then U does not lie on a 1-line with respect to $\mathcal{F}$.

Proof. First we note that every line through P_0 of multiplicity $3 + 5i$ in $\mathcal{K}$ becomes an i-point in $\mathcal{F}$. Assume that t is a 1-line through U in $\mathcal{F}$. All points on t that are not equal to U are 0-points. Now, let $V := t \cap \langle X, Y\rangle$ and $W := t \cap \langle X, Z\rangle$. Since $U \neq X, Y, Z$ and U is the unique 1-point on t, we have $V \neq X, Y$ and $W \neq X, Z$, i.e., V and W are two different 0-points. Since U, V, W are on 2-lines in $\mathcal{F}$, which are the image of 28-planes in $\mathcal{K}$ that do not contain 2-points, the preimages $\varphi^{-1}(U)$, $\varphi^{-1}(V)$, and $\varphi^{-1}(W)$ are lines without a 2-point in $\mathcal{K}$, see Lemma 8.38. The preimage of t is a 23-plane π' in $\mathcal{K}$ that contains exactly four 2-points, see Lemma 8.36. Moreover, the six lines through P_0 that span π' in $\mathcal{K}$ have either $A_1A_2^4B_2$ or $A_1^2A_2^2A_3B_3$ as type distribution. Since the preimage $\varphi^{-1}(U)$ is an 8-line without a 2-point, the first case occurs. However, since $\varphi^{-1}(V)$ and $\varphi^{-1}(W)$ are 3-lines without a 2-point, there cannot be four lines of type A_2 through P_0. Thus, U does not lie on a 1-line with respect to $\mathcal{F}$. □

So, let us briefly discuss the application of Lemma 8.59 to the newly discovered strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$ of cardinality 128. Consider a projection φ from a 0-point P_0, that is incident with a line $\tilde{L}$ of type B_2, onto some plane π not incident with P_0 and set $\mathcal{F} = \frac{1}{5}\left(\mathcal{K}^{\varphi} - 3\right)$. Every line through P_0 of multiplicity

$3+5i$ becomes an i-point. Since the maximum line multiplicity is 8, the maximum plane multiplicity is 33, and $\#\mathcal{K} = 128 = 24 \cdot 3 + 7 \cdot 8 - 30 \cdot 0$, $\mathcal{F}$ is a projective $(7, \le 3)$-arc in $\mathrm{PG}(2,5)$. Now we set $X := \varphi(\tilde{L})$ and note that X is a 1-point with respect to $\mathcal{F}$. Since the distribution of multiplicities of the hyperplanes through $\tilde{L}$ is $23^2 28^2 33^2$, X is contained on two 2-lines and two 3-lines in $\mathcal{F}$. Let Y and Z be the other 1-point not equal to X on the two two 2-lines through X, respectively. If one of the four other 1-points $P_1, \ldots, P_4$, not equal to X, Y, or Z, is incident with a 2-line, then Lemma 8.59 implies that this point is on six 2-lines, i.e., its preimage is an 8-line that is contained in six 28-plane, which is impossible. Thus, the distribution of the multiplicities of the lines through P_i in $\mathcal{F}$ is given by $3^3 1^3$ for all $1 \le i \le 4$, so that the preimage $\varphi^{-1}(P_i)$ is a line of type B_3. So, the distribution of the multiplicities of the lines through X, Y, and Z in $\mathcal{F}$ is given by $3^2 2^2 1^2$, so that the preimage is a line of type B_2. A corresponding code indeed exists and a generator matrix is given by

$$\begin{pmatrix} 1111100 \\ 0113010 \\ 1013001 \end{pmatrix}.$$

The corresponding arc consists of four 0-lines, 18 tangents, three 2-lines, and six 3-lines.

EXERCISE 8.4 Verify that $a'_2 = 0$ in the proof of Lemma 8.46.

EXERCISE 8.5 Prove Lemma 8.49.

8.4 Computational classification of strong $(3 \mod 5)$-arcs

For strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ we utilize Proposition 8.19 and generate the corresponding blocking sets using the software package `LinCode`, see [98]. In Table 8.3 we list the number of isomorphism types.

In tables 8.4-8.15 we list the counts of the line types and the counts λ_i of the points per multiplicity for strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$, where we give a separate table for each possible cardinality n.

LEMMA 8.60

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$ without a full hyperplane in its support and H be a hyperplane with $\mathcal{K}(H) \ge 33$. Either we have $\#\mathcal{K} \ge 125 + \mathcal{K}(H)$ or $\mathcal{K}|_H$ is one of the following cases:

$\mathcal{K}(H)$	A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#	$\#\mathcal{K} \ge$
33	*0*	*0*	*10*	*0*	*15*	*0*	*0*	*6*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*10*	*15*	*0*	*6*	*1*	*108*
33	*0*	*6*	*4*	*0*	*6*	*12*	*0*	*0*	*0*	*0*	*3*	*0*	*0*	*0*	*0*	*0*	*0*	*12*	*9*	*6*	*4*	*1*	*108*
43	*2*	*0*	*0*	*0*	*0*	*25*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*2*	*1*	*10*	*5*	*10*	*6*	*2*	*118*
43	*2*	*0*	*0*	*0*	*25*	*0*	*0*	*2*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*2*	*10*	*10*	*0*	*11*	*2*	*118*
68	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*25*	*0*	*0*	*0*	*0*	*4*	*5*	*5*	*0*	*21*	*1*	*168*

$\#\mathcal{K}$	m	$\#\mathcal{B}$	line mult.	weights	# isomorphism types
18	3	3	$0, 1, 2, 3$	$0, 1, 2, 3$	4
23	4	9	$1, 2, 3, 4$	$5, 6, 7, 8$	1
28	5	15	$2, 3, 4, 5$	$10, 11, 12, 13$	1
33	6	21	$3, 4, 5, 6$	$15, 16, 17, 18$	10
38	7	27	$4, 5, 6, 7$	$20, 21, 22, 23$	23
43	8	33	$5, 6, 7, 8$	$25, 26, 27, 28$	53
48	9	39	$6, 7, 8, 9$	$30, 31, 32, 33$	49
53	10	45	$7, 8, 9, 10$	$35, 36, 37, 38$	17
58	11	51	$8, 9, 10, 11$	$40, 41, 42, 43$	11
63	12	57	$9, 10, 11, 12$	$45, 46, 47, 48$	9
68	13	63	$10, 11, 12, 13$	$50, 51, 52, 53$	6
73	14	69	$11, 12, 13, 14$	$55, 56, 57, 58$	0
78	15	75	$12, 13, 14, 15$	$60, 61, 62, 63$	0
83	16	81	$13, 14, 15, 16$	$65, 66, 67, 68$	0
88	17	87	$14, 15, 16, 17$	$70, 71, 72, 73$	0
93	18	93	$15, 16, 17, 18$	$75, 76, 77, 78$	1

Table 8.3: Number of isomorphism types of strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2, 5)$ and their corresponding blocking sets.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	12	16	0	0	0	0	0	0	0	3	0	0	0	0	0	0	16	12	3	0	1
3	0	25	0	0	0	0	3	0	0	0	0	0	0	0	0	0	15	15	0	1	1
4	25	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	20	5	5	1	1
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	25	0	0	6	1

Table 8.4: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2, 5)$ of cardinality 18.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
6	12	4	0	3	6	0	0	0	0	0	0	0	0	0	0	0	18	6	4	3	1

Table 8.5: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2, 5)$ of cardinality 23.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
6	0	10	0	15	0	0	0	0	0	0	0	0	0	0	0	0	15	10	0	6	1

Table 8.6: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2, 5)$ of cardinality 28.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	10	0	15	0	0	6	0	0	0	0	0	0	0	0	0	10	15	0	6	1
0	3	7	2	8	2	7	1	0	0	1	0	0	0	0	0	0	11	12	3	5	1
0	6	4	0	6	12	0	0	0	0	3	0	0	0	0	0	0	12	9	6	4	1
0	6	4	2	4	8	4	0	0	2	1	0	0	0	0	0	0	12	9	6	4	2
0	6	4	3	3	6	6	0	0	3	0	0	0	0	0	0	0	12	9	6	4	1
0	9	1	3	0	9	3	0	3	3	0	0	0	0	0	0	0	13	6	9	3	1
2	8	1	8	6	4	0	0	0	1	0	0	0	0	1	0	0	15	5	5	6	1
4	5	2	5	4	10	0	0	0	0	0	1	0	0	0	0	0	15	5	5	6	1
8	4	0	16	0	0	0	0	1	0	0	2	0	0	0	0	0	18	1	4	8	1

Table 8.7: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 33.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	4	0	0	0	0	0	3	18	6	0	0	0	0	0	0	6	12	13	0	1
0	0	5	0	0	6	12	2	0	2	3	1	0	0	0	0	0	7	14	6	4	1
0	1	4	0	0	10	4	1	0	8	2	0	0	1	0	0	0	8	11	9	3	1
0	1	4	0	0	9	6	0	1	6	3	0	0	1	0	0	0	8	11	9	3	1
0	2	3	0	0	6	9	0	1	7	2	0	1	0	0	0	0	8	11	9	3	1
0	2	4	0	12	0	8	3	0	0	0	1	1	0	0	0	0	9	13	2	7	1
0	2	4	4	5	4	8	0	0	2	0	0	0	2	0	0	0	10	10	5	6	2
0	3	2	0	0	8	2	0	4	10	1	0	0	0	1	0	0	9	8	12	2	1
0	3	3	2	6	6	8	0	0	0	1	1	0	0	1	0	0	10	10	5	6	1
0	4	2	4	2	10	3	0	1	3	0	0	0	1	1	0	0	11	7	8	5	1
0	5	0	0	0	5	0	0	10	10	0	0	0	0	0	1	0	10	5	15	1	1
0	5	1	2	4	12	0	1	0	4	0	0	1	0	1	0	0	11	7	8	5	1
0	5	1	3	3	9	4	0	1	3	0	0	1	0	1	0	0	11	7	8	5	1
0	6	0	4	0	12	0	0	6	0	1	0	0	0	2	0	0	12	4	11	4	1
1	1	4	2	4	7	9	0	0	1	0	1	0	1	0	0	0	10	10	5	6	1
1	2	3	3	1	13	2	0	1	3	0	0	0	2	0	0	0	11	7	8	5	1
1	3	2	2	1	13	4	0	1	2	0	1	0	0	1	0	0	11	7	8	5	1
1	4	1	0	4	14	0	1	0	4	0	0	2	0	0	0	0	11	7	8	5	1
1	4	1	1	3	11	4	0	1	3	0	0	2	0	0	0	0	11	7	8	5	1
2	5	0	10	2	7	0	0	2	0	0	0	2	1	0	0	0	14	3	7	7	2
3	0	4	3	15	0	3	0	0	0	0	3	0	0	0	0	0	12	9	1	9	1

Table 8.8: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 38.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	0	0	0	0	0	30	0	0	0	0	0	0	0	0	1	0	25	0	6	1
0	0	0	0	0	0	0	4	0	0	25	0	0	0	0	2	0	0	20	10	1	1
0	0	1	0	0	0	9	3	0	6	9	0	0	0	3	0	0	3	16	9	3	1
0	0	2	0	2	7	8	1	0	4	3	0	0	2	2	0	0	6	12	8	5	2
0	0	2	0	3	1	13	4	0	2	2	0	1	3	0	0	0	5	15	5	6	1
0	0	3	2	8	5	6	1	0	0	1	1	0	4	0	0	0	8	11	4	8	1
0	0	3	4	6	0	12	0	1	0	0	1	0	4	0	0	0	8	11	4	8	1
0	1	0	0	0	0	8	0	0	12	7	0	0	0	1	2	0	4	13	12	2	1
0	1	1	0	2	3	13	0	1	3	3	0	1	1	2	0	0	6	12	8	5	1
0	1	1	0	2	4	11	1	0	5	2	0	1	1	2	0	0	6	12	8	5	2
0	1	1	0	2	8	4	0	2	7	2	0	0	0	4	0	0	7	9	11	4	2
0	1	2	1	9	4	7	1	0	0	1	1	1	3	0	0	0	8	11	4	8	1
0	1	2	6	0	12	0	0	3	2	0	0	0	2	3	0	0	10	5	10	6	1
0	2	0	0	0	12	0	0	4	8	1	0	0	1	0	3	0	8	6	14	3	1
0	2	0	0	1	7	7	0	1	8	1	0	1	0	2	1	0	7	9	11	4	1
0	2	0	0	1	8	5	1	0	10	0	0	1	0	2	1	0	7	9	11	4	1
0	2	1	0	10	3	8	1	0	0	1	1	2	2	0	0	0	8	11	4	8	1
0	2	1	1	8	2	11	1	0	0	0	2	1	1	1	0	0	8	11	4	8	1
0	2	1	2	4	11	5	0	0	0	1	2	0	0	3	0	0	9	8	7	7	1
0	2	1	2	5	10	4	0	0	1	1	1	1	1	2	0	0	9	8	7	7	1
0	2	1	2	6	9	3	0	0	2	1	0	2	2	1	0	0	9	8	7	7	2
0	2	1	3	4	8	6	0	0	2	0	1	1	1	2	0	0	9	8	7	7	1
0	2	1	3	5	7	5	0	0	3	0	0	2	2	1	0	0	9	8	7	7	1
0	3	0	0	7	11	3	0	0	0	2	1	2	0	2	0	0	9	8	7	7	1
0	3	0	2	6	6	6	0	0	3	0	0	3	1	1	0	0	9	8	7	7	1
0	3	0	4	1	12	2	0	2	2	0	0	2	1	1	1	0	10	5	10	6	1
0	3	0	4	2	10	2	0	3	2	0	0	2	0	3	0	0	10	5	10	6	1
0	3	1	12	3	6	0	0	0	0	0	3	0	0	3	0	0	12	4	6	9	1
1	0	0	0	0	0	0	2	0	25	0	0	0	0	0	3	0	5	10	15	1	1
1	0	0	0	0	0	25	3	0	0	0	0	0	0	0	1	1	5	15	5	6	1
1	0	1	0	0	6	8	0	2	9	0	0	1	0	3	0	0	7	9	11	4	1
1	0	2	0	7	5	10	1	0	0	0	2	1	2	0	0	0	8	11	4	8	1
1	0	2	2	4	10	4	0	0	3	0	0	2	3	0	0	0	9	8	7	7	2
1	1	1	1	4	10	6	0	0	2	0	1	2	1	1	0	0	9	8	7	7	2
1	2	0	2	1	14	2	0	2	2	0	0	3	1	0	1	0	10	5	10	6	2
1	2	0	2	2	12	2	0	3	2	0	0	3	0	2	0	0	10	5	10	6	1
1	3	0	9	5	6	0	0	0	1	0	2	3	0	1	0	0	12	4	6	9	1
2	0	0	0	0	0	0	0	25	0	0	0	0	0	0	4	0	10	0	20	1	1
2	0	0	0	0	25	0	1	0	0	0	0	0	0	0	2	1	10	5	10	6	2
2	0	0	0	25	0	0	2	0	0	0	0	0	0	0	0	2	10	10	0	11	2
2	1	1	8	3	10	0	0	0	0	0	3	2	0	1	0	0	12	4	6	9	1
2	2	0	7	5	8	0	0	0	1	0	2	4	0	0	0	0	12	4	6	9	1
3	0	0	25	0	0	0	0	0	0	0	0	0	0	0	1	2	15	0	5	11	1
3	0	0	6	6	12	0	0	0	0	0	0	3	0	0	0	1	12	4	6	9	1

Table 8.9: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 43.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	0	0	12	3	6	3	0	0	0	0	0	6	0	0	1	6	12	3	10	1
0	0	0	0	2	11	0	0	2	6	2	0	0	1	5	2	0	6	7	13	5	1
0	0	0	0	2	4	12	1	0	0	4	0	0	6	1	1	0	4	13	7	7	1
0	0	0	0	2	8	6	0	0	4	3	0	0	3	4	1	0	5	10	10	6	1
0	0	0	0	3	3	10	2	0	2	3	0	0	5	3	0	0	4	13	7	7	1
0	0	0	0	3	6	6	0	1	4	3	0	0	2	6	0	0	5	10	10	6	1
0	0	0	1	0	11	2	0	1	7	1	0	0	2	3	3	0	6	7	13	5	1
0	0	0	1	2	1	12	2	0	3	2	0	0	5	3	0	0	4	13	7	7	1
0	0	0	1	2	4	8	0	1	5	2	0	0	2	6	0	0	5	10	10	6	1
0	0	0	1	2	5	6	1	0	7	1	0	0	2	6	0	0	5	10	10	6	1
0	0	0	1	2	7	2	0	3	7	1	0	0	0	7	1	0	6	7	13	5	1
0	0	0	2	0	4	10	0	0	6	1	0	0	3	4	1	0	5	10	10	6	1
0	0	0	2	0	7	4	0	2	8	0	0	0	1	5	2	0	6	7	13	5	1
0	0	0	2	0	8	0	0	7	6	0	0	0	0	4	4	0	7	4	16	4	1
0	0	0	3	6	6	9	0	0	0	0	0	0	3	3	0	1	7	9	6	9	1
0	0	0	4	2	14	4	0	0	0	0	0	0	1	4	1	1	8	6	9	8	1
0	0	1	0	9	3	6	3	0	0	0	3	0	6	0	0	0	6	12	3	10	1
0	0	1	1	8	7	2	0	0	1	2	0	3	6	0	0	0	7	9	6	9	1
0	0	1	2	5	7	6	0	0	0	1	2	1	4	2	0	0	7	9	6	9	1
0	0	1	3	4	5	8	0	0	1	0	2	1	4	2	0	0	7	9	6	9	1
0	0	1	3	5	4	7	0	0	2	0	1	2	5	1	0	0	7	9	6	9	2
0	0	1	3	6	3	6	0	0	3	0	0	3	6	0	0	0	7	9	6	9	2
0	0	1	4	2	10	2	0	1	2	0	1	2	2	4	0	0	8	6	9	8	2
0	0	1	4	3	9	1	0	1	3	0	0	3	3	3	0	0	8	6	9	8	2
0	0	1	6	0	9	0	0	6	0	0	0	3	0	6	0	0	9	3	12	7	1
0	0	2	6	12	0	0	0	0	0	1	6	0	4	0	0	0	9	8	2	12	1
0	1	0	1	6	6	7	0	0	0	1	2	2	3	2	0	0	7	9	6	9	1
0	1	0	1	7	5	6	0	0	1	1	1	3	4	1	0	0	7	9	6	9	1
0	1	0	2	3	13	0	1	0	2	0	2	2	0	5	0	0	8	6	9	8	1
0	1	0	2	5	4	9	0	0	1	0	2	2	3	2	0	0	7	9	6	9	1
0	1	0	3	1	12	4	0	0	1	0	2	2	1	3	1	0	8	6	9	8	1
0	1	0	3	2	11	3	0	0	2	0	1	3	2	2	1	0	8	6	9	8	1
0	1	0	3	3	10	2	0	0	3	0	0	4	3	1	1	0	8	6	9	8	1
0	1	0	3	3	9	3	0	1	2	0	1	3	1	4	0	0	8	6	9	8	2
0	1	0	3	4	8	2	0	1	3	0	0	4	2	3	0	0	8	6	9	8	2
0	1	0	5	0	10	1	0	5	0	0	0	4	0	4	1	0	9	3	12	7	1
0	2	0	12	0	6	0	0	1	0	0	2	6	1	0	1	0	11	2	8	10	1
1	0	0	0	6	5	8	0	0	2	0	1	4	4	0	0	0	7	9	6	9	1
1	0	0	1	4	10	2	0	1	3	0	0	5	2	2	0	0	8	6	9	8	1
1	0	0	4	14	0	4	0	0	0	0	4	1	2	0	0	1	9	8	2	12	1
1	0	1	4	11	0	4	0	0	0	0	7	1	2	0	0	0	9	8	2	12	1
2	0	0	8	1	8	0	0	2	0	0	2	8	0	0	0	0	11	2	8	10	2

Table 8.10: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 48.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	0	0	5	10	0	0	0	0	2	2	4	4	4	0	0	6	7	8	10	1
0	0	0	0	6	4	5	1	0	0	1	3	2	8	1	0	0	5	10	5	11	1
0	0	0	1	3	9	3	0	0	0	1	3	3	3	5	0	0	6	7	8	10	1
0	0	0	1	4	3	8	1	0	0	0	4	1	7	2	0	0	5	10	5	11	1
0	0	0	1	6	0	8	0	1	0	1	2	3	9	0	0	0	5	10	5	11	1
0	0	0	2	2	7	5	0	0	1	0	3	3	3	5	0	0	6	7	8	10	1
0	0	0	2	3	6	4	0	0	2	0	2	4	4	4	0	0	6	7	8	10	2
0	0	0	3	0	11	1	0	1	1	0	1	6	2	3	2	0	7	4	11	9	1
0	0	0	3	2	8	0	0	2	2	0	0	7	2	4	1	0	7	4	11	9	2
0	0	0	9	3	6	0	0	0	0	0	3	6	0	3	0	1	9	3	7	12	1
0	0	1	9	0	6	0	0	0	0	0	6	6	0	3	0	0	9	3	7	12	1
0	1	0	1	12	0	0	2	0	0	0	11	0	4	0	0	0	7	9	1	14	1
0	1	0	8	2	4	0	0	0	1	0	5	8	0	2	0	0	9	3	7	12	1
1	0	0	10	0	0	0	0	5	0	0	0	15	0	0	0	0	10	0	10	11	1
1	0	0	6	2	6	0	0	0	1	0	5	9	0	1	0	0	9	3	7	12	1

Table 8.11: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 53.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	0	0	0	10	0	1	0	0	0	5	5	0	10	0	0	5	5	10	11	1
0	0	0	0	3	3	3	0	0	1	1	3	5	9	3	0	0	4	8	7	12	1
0	0	0	1	1	2	6	0	0	1	0	4	4	8	4	0	0	4	8	7	12	1
0	0	0	1	1	5	2	0	1	1	0	3	7	2	8	0	0	5	5	10	11	1
0	0	0	1	1	6	1	0	0	2	0	2	8	4	5	1	0	5	5	10	11	1
0	0	0	1	2	4	1	0	1	2	0	2	8	3	7	0	0	5	5	10	11	1
0	0	0	1	3	0	4	0	0	3	0	2	6	10	2	0	0	4	8	7	12	1
0	0	0	1	3	3	0	0	1	3	0	1	9	4	6	0	0	5	5	10	11	1
0	0	0	2	1	4	0	0	4	0	0	0	12	0	6	2	0	6	2	13	10	1
0	0	0	3	6	0	3	0	0	0	0	9	3	6	0	0	1	6	7	3	15	1
0	0	1	3	3	0	3	0	0	0	0	12	3	6	0	0	0	6	7	3	15	1

Table 8.12: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 58.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	0	0	0	0	0	0	0	0	5	0	0	15	10	1	0	0	10	10	11	1
0	0	0	0	0	0	0	0	0	3	2	1	2	6	15	2	0	1	7	13	10	1
0	0	0	0	0	0	0	0	1	4	0	0	6	2	12	6	0	2	4	16	9	1
0	0	0	0	0	1	4	1	0	0	0	4	2	14	4	0	1	2	9	6	14	1
0	0	0	0	0	3	3	0	0	0	0	3	6	6	9	0	1	3	6	9	13	1
0	0	0	0	0	6	0	0	0	0	0	0	12	3	6	3	1	4	3	12	12	1
0	0	0	4	1	2	0	0	0	0	0	4	14	0	4	0	2	6	2	8	15	1
0	0	1	0	0	0	0	0	0	3	0	3	9	9	6	0	0	3	6	9	13	1
0	0	1	0	0	0	0	0	3	0	0	3	12	0	12	0	0	4	3	12	12	1

Table 8.13: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 63.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	30	1	0	0	25	6	1
0	0	0	0	0	0	0	1	0	0	0	0	0	0	25	3	2	0	5	15	11	1
0	0	0	0	0	0	0	2	0	0	0	0	0	25	0	1	3	0	10	5	16	1
0	0	0	0	3	0	0	0	0	0	0	6	6	12	0	0	4	3	6	4	18	1
1	0	0	0	0	0	0	0	0	0	0	0	25	0	0	2	3	5	0	10	16	1
1	0	0	0	0	0	0	1	0	0	0	25	0	0	0	0	4	5	5	0	21	1

Table 8.14: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 68.

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	31	0	0	0	31	1

Table 8.15: Strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 93.

PROOF. We use the above tables, where the possible parameters of the strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ are listed. Note we have $\mathcal{K}(H') \geq 33$ for each hyperplane H' that contains a line of type B_1, B_4, B_6, or B_7. So, if $\mathcal{K}|_H$ contains a line of type B_1, B_4, B_6, or B_7, then we have $\#\mathcal{K} \geq \mathcal{K}(H) + 33 \cdot 5 - 5 \cdot 8 = 125 + \mathcal{K}(H)$. Since each hyperplane H' that contains a line of type C_2 or C_3 satisfies $\mathcal{K}(H') \geq 38$, we have $\#\mathcal{K} \geq \mathcal{K}(H) + 38 \cdot 5 - 5 \cdot 13 = 125 + \mathcal{K}(H)$ if H contains a line of type C_2 or C_3. If there are no 0-points in $\mathcal{K}|_H$, then $\mathcal{K}$ contains a full hyperplane in its support. All other cases are summarized in the above table. It remains to explain how a lower bound for $\#\mathcal{K}$ can be obtained. For each line L in H let $m(L)$ denote the minimum cardinality of a strong $(3 \mod 5)$-arc in $\mathrm{PG}(2,5)$ that contains a line with the same type as L, so that $\#\mathcal{K} \geq \mathcal{K}(H) - 5\mathcal{K}(L) + 5m(L)$ gives a lower bound. We take the minimum over all possibilities for the type of L in H. as an example we consider the two cases where $\mathcal{K}(H) = 33$. There is always a line of type B_2 in H with is not contained in an 18-plane, so that $\mathcal{K} \geq 33 + 5 \cdot 23 - 5 \cdot 8 = 108$. □

LEMMA 8.61

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$ without a full hyperplane in its support and cardinality $\#\mathcal{K} = 163$. Then, $\mathcal{K}$ does not contain a line with a type contained in $\{B_6, C_2, C_3, C_4, C_5, D_1\}$.

PROOF. From Lemma 8.60 we conclude that each hyperplane has a multiplicity of at most 43. Moreover, multiplicity 43 can only occur in the two cases explicitly listed in Lemma 8.60.

Assume that L is a line of type D_1. From tables 8.4-8.15 we conclude that the multiplicities of the hyperplanes through L are contained in $\{18, 43\}$. Thus, we have $163 = 18x + (6-x)43 - 5 \cdot 18$, so that $x = \frac{1}{5}$, which is impossible. The non-existence of a line of type D_1 implies that the maximum multiplicity of a hyperplane is at most 38.

Assume that L is a line of type C_5. From tables 8.4-8.15 we conclude that the multiplicities of the hyperplanes through L are contained in $\{18, 38, 43\}$, which leaves the two possible distributions $18^1 38^1 43^4$ and 38^6. In the first case we have $(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = (70, 30, 35, 21)$ and $(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = (60, 30, 65, 1)$ in the second case. Note that in both cases there is a 38-plane with a unique line distribution including a line of type B_6. So, let L' be a line of type B_6 that is contained in a 38-plane. The other five hyperplanes through L have multiplicity 33, so that the data of Table 8.7 gives

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = x \cdot (11, 6, 5, 3) + (5-x) \cdot (16, 1, 0, 8) + (10, 5, 15, 1) = (90-5x, 10+5x, 15+5x, 41-5x)$$

for some integer $0 \leq x \leq 5$. Thus, we are in the first case and $x = 4$. However, each of the possible 43-planes contains a line of type D_1, which have already excluded.

Since the maximum multiplicity of a hyperplane is 38 and $6 \cdot 38 - 5 \cdot 13 = 163$, each 13-line is contained in six 38-planes.

Let H be a 38-plane and let $\widetilde{\lambda}_i$ denote the number of i-points in $\mathcal{K}$ outside of H. Note that a hyperplane H' containing a line of type B_1, B_4, B_6, or B_7 has multiplicity at least 33. So, if H contains such a line L, then the other five hyperplanes through L are 33-planes. Assume that H contains a line L of type B_6, so that

$$\left(\widetilde{\lambda}_0, \widetilde{\lambda}_1, \widetilde{\lambda}_2, \widetilde{\lambda}_3\right) = (55, 30, 25, 15)$$

since there is a unique possibility for a 33-plane that contains a line of type B_6 but no 13-line. If there is a line of type B_1, then we have

$$\left(\widetilde{\lambda}_0, \widetilde{\lambda}_1, \widetilde{\lambda}_2, \widetilde{\lambda}_3\right) = a \cdot (8, 12, 2, 3) + b \cdot (9, 9, 5, 2) + (5 - a - b) \cdot (10, 6, 8, 1)$$

for some integers $a, b \geq 0$ with $a + b \leq 5$, so that $\widetilde{\lambda}_0 \leq 50$, which is a contradiction. If there is a line of type B_7, then we have

$$\left(\widetilde{\lambda}_0, \widetilde{\lambda}_1, \widetilde{\lambda}_2, \widetilde{\lambda}_3\right) = u \cdot (11, 7, 3, 4) + (5 - u) \cdot (12, 4, 6, 3)$$

for some integer $0 \leq u \leq 5$, so that $\widetilde{\lambda}_0 = 55$ implies $u = 5$, which contradicts $\widetilde{\lambda}_1 = 30$. This leaves the following possibilities for 38-planes:

A_1	A_2	A_3	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	C_1	C_2	C_3	C_4	C_5	D_1	λ_0	λ_1	λ_2	λ_3	#
0	0	5	0	0	6	12	2	0	2	3	1	0	0	0	0	0	7	14	6	4	1
0	1	4	0	0	10	4	1	0	8	2	0	0	1	0	0	0	8	11	9	3	1
0	2	4	0	12	0	8	3	0	0	0	1	1	0	0	0	0	9	13	2	7	1
0	2	4	4	5	4	8	0	0	2	0	0	0	2	0	0	0	10	10	5	6	2
0	3	3	2	6	6	8	0	0	0	1	1	0	0	1	0	0	10	10	5	6	1
0	5	1	2	4	12	0	1	0	4	0	0	1	0	1	0	0	11	7	8	5	1
1	1	4	2	4	7	9	0	0	1	0	1	0	1	0	0	0	10	10	5	6	1
1	4	1	0	4	14	0	1	0	4	0	0	2	0	0	0	0	11	7	8	5	1
3	0	4	3	15	0	3	0	0	0	0	3	0	0	0	0	0	12	9	1	9	1

Thus, there is no line of type B_6.

Next we will show that there is no line of type C_4. To this end we assume that L is a line of type C_4. All six hyperplanes through L are 38 planes and there are just two possibilities, so that

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (6-x) \cdot (10, 9, 2, 4) + x \cdot (11, 6, 5, 3) + (0, 1, 3, 2) = (60+x, 55-3x, 15+3x, 26-x)$$

for some integer $0 \leq x \leq 6$. Note that both two types of 38-planes contain a line L' of type B_1 which is contained in five 33-planes. So, for such a 38-plane H we obtain

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = a \cdot (8, 12, 2, 3) + b \cdot (9, 9, 5, 2) + (5-a-b) \cdot (10, 6, 8, 1) + (\lambda_0(H), \lambda_1(H), \lambda_2(H), \lambda_3(H)),$$

for some integers $a, b \geq 0$ with $a+b \leq 5$. If $x = 0$, we have $\lambda_0(H) = 10$, so that $\lambda_0 \geq 60+x \geq 60$ implies $a = b = 0$. If $x \geq 1$, we have $\lambda_0(H) \leq 11$, so that $\lambda_0 \geq 60 + x \geq 61$ also implies $a = b = 0$. Thus, we have $\lambda_0 \in \{60, 61\}$, so that $x = 0$ and $(\lambda_0, \lambda_1 m \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (60, 55, 15, 26)$. However, counting via the line L' of type B_1 gives $(\lambda_0, \lambda_1 m \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (60, 39, 42, 9)$, which is a contradiction. Thus, there is no line of type C_4.

Next we will show that there is no line of type C_3. To this end we assume that L is a line of type C_3. All six hyperplanes through L are 38 planes and there are just two possibility for $(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5)$ restricted to such a hyperplane, so that

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (6-x) \cdot (8, 9, 8, 0) + x \cdot (10, 8, 4, 3) + (0, 2, 1, 3) = (48+2x, 56-x, 49-4x, 3+3x)$$

for some integer $0 \le x \le 6$. Note that all these types of 38-planes contain a line L' of type B_7 which is contained in five 33-planes. So, for such a 38-plane H we obtain

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = u \cdot (11, 7, 3, 4) + (5 - u) \cdot (12, 4, 6, 3) + (\lambda_0(H), \lambda_1(H), \lambda_2(H), \lambda_3(H)),$$

for some integer $0 \le u \le 5$. Thus, we have $\lambda_0 = 4u + (5 - u) \cdot 3 + \lambda_3(H) \le 18$, which implies $x = 6$. With this, we have $\lambda_3(H) = 6$, so that $\lambda_3 > 18$, which is a contradiction. Thus, there is no line of type C_3.

Next we will show that there is no line of type C_2. To this end we assume that L is a line of type C_2. All six hyperplanes through L are 38 planes and there are just two possibilities for $(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5)$ restricted to such a hyperplane, so that

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (6-x)\cdot(8, 13, 0, 4)+x\cdot(10, 7, 6, 2)+(1, 0, 2, 3) = (49+2x, 78-6x, 2+6x, 27-2x)$$

for some integer $0 \le x \le 6$. If $x \ge 1$, then there exists a 38-plane H of the second type that contains a line L' of type B_7. Counting in the hyperplanes through L' gives

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = u \cdot (11, 7, 3, 4) + (5 - u) \cdot (12, 4, 6, 3) + (11, 7, 8, 5)$$

for some integer $0 \le u \le 5$. The equation for λ_0 gives $u = 22 - 2x$, which contradicts the equation for λ_1. Thus, we have $x = 0$ and $(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (49, 78, 2, 27)$. Since each such 38-plane H contains a line L' of type B_4, we have

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = y \cdot (10, 9, 2, 4) + z \cdot (11, 6, 5, 3) + (5 - y - z) \cdot (12, 3, 8, 2) + (9, 13, 2, 7)$$

for some integers $y, z \ge 0$ with $y + z \le 5$. By considering the value for λ_2, we conclude that this is impossible. Thus, there is no line of type C_2.

Next we will show that there is no line of type C_1. To this end we assume that L is a line of type C_1. All six hyperplanes through L are 38 planes and there are just two possibillitites for $(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5)$ restricted to such a hyperplane, so that

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (6-x)\cdot(6, 13, 6, 0)+x\cdot(11, 8, 1, 5)+(1, 1, 0, 4) = (37+5x, 79-5x, 36-5x, 4+5x)$$

for some integer $0 \le x \le 6$. If $x \le 5$ then there exists a 38-plane H with a line L' of type B_7 and counting in the hyperplanes through L' gives

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = u \cdot (11, 7, 3, 4) + (5 - u) \cdot (12, 4, 6, 3) + (7, 14, 6, 4)$$

for some integer $0 \le u \le 5$. Solving the equations for λ_0 and λ_1 gives $u = \frac{15}{2}$ and $x = \frac{9}{2}$, which is a contradiction. □

PROPOSITION 8.62

Let $\mathcal{K}$ be a strong $(3 \mod 5)$*-arc in* $\mathrm{PG}(3, 5)$*. Then, either* $\#\mathcal{K} \neq 163$ *or the support of* $\mathcal{K}$ *contains a full hyperplane*

PROOF. Assume that $\mathcal{K}$ is a strong $(3 \mod 5)$-arc in $\operatorname{PG}(3,5)$ with cardinality $\#\mathcal{K} = 163$ whose support does not contain a full hyperplane. From Lemma 8.61 we conclude that each hyperplane has a multiplicity of at most 33. Since $6 \cdot 33 - 5 \cdot 8 = 158 < 163$, there is no line of multiplicity. However, the only strong $(3 \mod 5)$-arc in $\operatorname{PG}(2,5)$ with cardinality at most 33 without an 8-line is an 18-plane consisting of a unique line of type D_1. Thus, we obtain a contradiction. □

LEMMA 8.63

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\operatorname{PG}(3,5)$ without a full hyperplane in its support and cardinality $\#\mathcal{K} = 168$. If $\mathcal{K}$ is not lifted, then all 43-planes that contain a line of type D_1 are lifted and the multiplicity of an arbitrary hyperplane is at most 43.

PROOF. From Lemma 8.60 we conclude that for each hyperplane $H \in \mathcal{H}$ we have $\mathcal{K}(H) \le 68$. Moreover, either $\mathcal{K}(H) \le 43$ or $\mathcal{K}(H) = 68$ and $\mathcal{K}|_H$ has parameters as specified in the table of Lemma 8.60.

Assume that H is a 43-plane with a 3-point P_3 that is incident with a line L of type C_2 and a line L' of type D_1. Then, the distribution of the types of the lines through P_3 is given by $A_1B_2B_3^2C_2D_1$. Consider the five other hyperplanes through L. All of them have a multiplicity of at least 38, so that all hyperplanes through L, besides H, have a multiplicity of exactly 38. Now we observe that P_3 cannot be incident with a line of type C_1. To this end we note that there is a unique possibility for a 38-plane that both contains a line of type C_1 and a line of type C_2. However, since there is no line of type A_1, these two 13-lines cannot intersect in a 3-point. Consider the five other hyperplanes through L'. Their multiplicities have to be contained in $\{18, 43, 68\}$. If H' is a 68-plane containing L', then the distribution of the types of the lines through P_3 is given by $C_1^5D_1$. Thus, L' is not contained in a 68-plane, so that all hyperplanes through L' have multiplicity 43. Those 43-planes can either by liftings an 8-line with type in $\{B_1, B_2, B_3, B_4\}$ or correspond to the last row in Table 8.9. In the first cases the distribution of the line types through P_3 is given by $B_1^5D_1$, $B_2^5D_1$, $B_3^5D_1$, or $B_4^5D_1$, respectively. In the last case the possible distributions are $A_1B_2B_3^2C_2D_1$ and $B_1^2B_2B_3^2D_1$. So, P_3 is incident with a unique line of type D_1 and the types of the other incident lines are contained in $\{A_1, B_2, B_3, B_4, C_2\}$, where the number of the lines of type C_2 equals the number of the lines of type A_1 and is between 1 and 6. Let L'' be the unique line of type A_1 in H. Since the is no second line of type D_1 and no line of type B_5 or C_5 that is incident with P_3, L'' is not contained in an 18-plane. Since there is no line of type C_1 or C_4 incident with P_3, L'' is not contained in a 33-plane. Now we are ready to show that there are no 43-planes with line pattern $B_1^5D_1$ or $B_4^5D_1$. To this end we note that the line pattern of a 3-point in a 23-plane is $A_1^2B_2^2B_3^2$ and the line pattern of a 3-point in a 28-plane is $A_1B_2^5$. So, if through L'' there is the 43-plane H and five other hyperplanes with multiplicity at least 38, then $\#\mathcal{K} \ge 218$. (Consider the span of a line of type A_1 and a line of type B_1 or B_4 through a 3-point.) No assume that there is a 43-plane with line pattern $B_3^5D_1$ through P_3. Consider the hyperplanes through L''. The other five hyperplanes besides H have either multiplicity 23 or multiplicity at least 38. Since $43 + 5 \cdot 23 - 5 \cdot 3 = 143$ and $43 + 4 \cdot 23 - 5 \cdot 3 + 1 \cdot 48 = 168$ but no 48-plane occurs, L'' can be incident with at most 3 planes of multiplicity 23. However, $1 \cdot 43 + 3 \cdot 23 + 2 \cdot 38 = 173 > \#\mathcal{K}$ is too large. Now assume the there is a line $\tilde{L}$ of type B_1 incident with P_3. All hyperplanes through $\tilde{L}$ have multiplicity at least 33. Since the hyperplane spanned by L and $\tilde{L}$ has multiplicity 38 and the hyperplane spanned by L' and $\tilde{L}$ has multiplicity at least 43, this is impossible. Now assume that there is a second line of type C_2 and consider the hyperplane spanned by this line and L, which has multiplicity. Indeed there are 38-planes containing two lines of type C_2, but none of these contains a 3-point whose incident lines are all contained in $\{A_1, B_2, B_3, C_2\}$. Thus, the five hyperplanes through the D_1-line L' not equal to H all have line pattern $B_2^5D_1$. However, there does not exist an 38-plane through L with line pattern $C_2B_2^5$, since $(\lambda_1,\lambda_2,\lambda_3)=(10,2,8)$ is never attained. We can easily check that all other possibilities for strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ of cardinality 43 that contain a line of type D_1 are lifted, which proves our first claim.

Assume that H is a 68-plane and L line of type C_1 in H. Since each hyperplane H' that contains a line of type C_1 has multiplicity at least 33 and $168=68+5\cdot 33-5\cdot 13$, the other five hyperplanes, besides H, through L all have multiplicity 33. Thus, we have

$$(\lambda_0,\lambda_1,\lambda_2,\lambda_3)=(5-x)\cdot(14,4,5,2)+x\cdot(17,0,4,4)+(5,5,0,21)=(75+3x,25-4x,25-x,31+2x)$$

for some integer $0\le x\le 5$. Now let L' be a line of type D_1 in H and P_3 be the 3-point that is contained on L and L'. In H the point P_3 is incident with a line of type D_1, i.e. L', and five lines of type C_1, one of these is L. Since the distribution of lines through a 3-point on a line of type C_1 is unique for the two possible types of 33-planes, see Lemma 8.40, we can also express the total distribution of the lines through P_3 in terms of x:

$$A_1^5B_1^{5+3x}B_2^{5-x}B_3^{10-2x}C_1^5D_1.$$

So, especially we have the same x for all five lines of type C_1 through P_3. Since the possible multiplicities of the hyperplanes through L' are contained in $\{18,43,68\}$, we have the following possibilities for the distributions of the multiplicities of those hyperplanes: 18^368^3, $18^243^268^2$, and $18^143^468^1$. In the first case we have $\lambda_2=0$, so that $x=25$, which is a contradiction. For the second case we consider λ_3. The two 18-planes and the two 68-planes contribute $6+2\cdot 0+2\cdot 15=36$ and the additional contribution of a 43-plane (containing a line of type D_1) is contained in $\{0,3,5\}$, so that $\lambda_3\in\{36,39,41,42,44,46\}$. From $\lambda_3=31+2x$ we deduce $x\in\{4,5\}$, so that $(\lambda_0,\lambda_1,\lambda_2,\lambda_3)=(87,9,21,39)$ or $(\lambda_0,\lambda_1,\lambda_2,\lambda_3)=(90,5,20,41)$. Now we consider λ_2. Both the two 18-planes and the two 68-planes do not contain 2-points while the contribution of a 43-plane is contained in $\{0,5,6,10\}$. Thus, we have $x=5$ and $(\lambda_0,\lambda_1,\lambda_2,\lambda_3)=(90,5,20,41)$. However, if the 43-planes contain ten 2-points each, then they do not contain further 3-points besides those on L', which is a contradiction. It remains to consider the distribution $18^143^468^1$. Now let us consider $(\lambda_0,\lambda_1,\lambda_2,\lambda_3)=(75+3x,25-4x,25-x,31+2x)$. The 18-plane and the 68-plane contribute $(30,5,0,21)$ and for the 43-planes we only need to consider those that contain a line of type D_1 and at least one 0-point, so that

$$\begin{aligned}(75+3x,25-4x,25-x,31+2x) &= (30,5,0,21)+a\cdot(5,15,5,0)+b\cdot(10,5,10,0)+c\cdot(10,10,0,5)\\ &\quad +d\cdot(15,0,5,5)+(4-a-b-c-d)\cdot(12,4,6,3)\end{aligned}$$

for some integers $a,b,c,d\ge 0$ with $a+b+c+d\le 4$. The parametric solution of the corresponding equation system is given by

$$\begin{aligned} b &= a+2c,\\ d &= -1+x+3a+2c.\end{aligned}$$

The lines of types A_1 and C_1 as well as the line of type D_1 are used by the 18- and the 68-plane. So, the four 43-planes consist of a line of type D_1 and five lines with a type in $\{B_1,B_2,B_3\}$. Thus, we have $a=0$. Now, we observe that the last last type can occur, i.e., $4-a-b-c-d>0$, cannot occur since we have excluded this special hyperplane in the previous paragraph. Thus, we have $a+b+c+d=4$. For the fourth type we have $B_1^5D_1$, i.e., the restricted arc is a lifting of a line of type B_1. For the second type we have $B_3^5D_1$, i.e., the restricted arc is a lifting of a line of type B_3. For the third type we have $B_2^5D_1$, i.e., the restricted arc is a lifting of a line of type B_2. Since $4\ge b+c=3c$, we have $c\in\{0,1\}$. If $c=1$, then $(a,b,c,d;x)=(0,2,1,1;0)$. If $c=0$, then $(a,b,c,d;x)=(0,0,0,-1+x;x)$, where $1\le x\le 5$. Since

$a+b+c+d=4$, we have $d=4$ and $x=5$.

Now let us summarize our findings and have a closer look at the 68-plane. First we observe that it is a lifting of a line of type C_1 with a unique lifting point Q. Q is incident in H with a A_1-line L_0, a B_5-line L_1, and four D_1-lines $L_2,\dots,L_6$. Let L_6 be the line L' in the above consideration and P_3 be the chosen 3-point on L'. The five other hyperplanes through L_6 are lifted 43-planes and we have two possibilities encoded by $(a,b,c,d;x)=(0,2,1,1;0)$ and $(a,b,c,d;x)=(0,0,0,4;5)$. Note that P_3 is incident with five lines of type C_1 which are contained five isomorphic 33-planes. Again the type is encode by $(a,b,c,d;x)=(0,2,1,1;0)$ and $(a,b,c,d;x)=(0,0,0,4;5)$. The same is true if we choose a different point $P_3'\neq Q$ on L_6. Since the type is already specified by the 43-planes through L_6, we have 125 isomorphic 33-planes, i.e., exactly those that do not contain Q. We already know that H is a lifted 68-plane with unique lifting point Q. Now let $\tilde{H}$ be one of the five 43-planes through L_6. Since $\tilde{H}$ is lifted it contains a line of type B_5 or C_5 with a unique 3-point Q', which is the unique lifting point of that 43-plane. Clearly Q' is located on L_6. Since the 125 hyperplanes not containing Q do not contain a line of type B_5 or B_6, we have $Q'=Q$ and $\mathcal{K}$ is lifted. Thus, there is no 68-plane, which proves our second claim. □

LEMMA 8.64

Let $\mathcal{K}$ be a strong $(3 \mod 5)$*-arc in* $\operatorname{PG}(3,5)$ *without a full hyperplane in its support and cardinality* $\#\mathcal{K}=168$. *Then, either $\mathcal{K}$ is lifted from a 33-plane, $\mathcal{K}$ does not contain a line of type D_1, or $\mathcal{K}$ has spectrum* $(a_{28},a_{33},a_{43})=(60,60,36)$ *and we have the following data on counts and distributions:*

- 0-*point;* $\#=60$*;* $A_1^6A_3^{10}B_2^{15}$, $28^{15}33^{10}43^6$*;*
- 1-*point:* $\#=60$, $A_3^{10}B_2^{15}B_5^6$, $28^{10}33^{15}43^6$*;*
- 3-*point:* $\#=36$*;* $A_1^2B_2^{25}B_5^2D_1^2$*;*
- A_1*:* $\#=72$, $28^5 43^1$*;*
- A_3*:* $\#=200$, $28^3 33^3$*;*
- B_2*:* $\#=450$, $28^2 33^2 43^2$*;*
- B_5*:* $\#=72$, $33^5 43^1$*;*
- D_1*:* $\#=12$*;* 43^6.

PROOF. Assume that L is a line of type D_1. Applying Lemma 8.63 we conclude that all hyperplanes through L are 43-planes which are liftings of an 8-line. Let L' be an arbitrary 13-line. If L' meets L, then the hyperplane spanned by L and L' is a 43-plane that is lifted, so that L' is of type C_5 that is incident with an 18-line. If L and L' are disjoint, then consider an arbitrary hyperplane H' containing L' and let $P=H\cap L$ denote the intersection point of H with L. Especially P is not incident with L'. Let P' denote an arbitrary 3-point on L' and consider the line $\tilde{L}=\langle P,P'\rangle$. If $\tilde{L}$ is an 18-line, then L' is incident with an

18-line and thus of type C_5. Otherwise, the hyperplane spanned by $\tilde{L}$ and L is 43-plane that is lifted from an 8-line with lifting point $\tilde{P} \neq P$. Thus, the line $\langle \tilde{P}, P' \rangle$ is an 18-line. Again, we conclude that L' intersects an 18-line and thus is of type C_5. To sum up, all 13-lines are of type C_5 and intersect at least one 18-line of type D_1.

Assume for a moment that L' is a line of type C_5 and L be a line of type D_1 intersecting L' in a 3-point P_3. Note that the hyperplane H spanned by L and L' is a 43-plane with P_3 as lifting point, i.e., all lines through P_3 in H are of a type in $\{A_1, B_5, C_5, D_1\}$. Now consider the hyperplanes through L'. The distribution of their multiplicities is either $18^1 43^5$ or $38^5 43^1$. In the first case the pattern of the lines through P_3 in the unique 18-plane is $A_1^4 B_5 C_5$. The hyperplanes spanned by L and one of these four lines of type A_1 are 43-planes lifted from an 8-line with lifting point P_3, i.e., the lines through P_3 in these hyperplanes all have a type contained in $\{A_1, B_5, C_5, D_1\}$. Now consider the hyperplane spanned by L and the unique line of type B_5 in the 18-plane containing L'. Either P_3 is a lifting point or the hyperplane is lifted from the line of type B_5. In both cases the lines through P_3 in that hyperplane have a type contained in $\{A_1, B_5, C_5, D_1\}$. Thus, $\mathcal{K}$ is lifted from a 33-plane with lifting point P_3. (We may also observe that the line of type B_5 through P_3 generates a full hyperplane in the support of $\mathcal{K}$ via the line L.) In the second case we observe that there is a unique type of a 38-plane containing a line of type C_5. There P_3 is the unique 3-point and we have ten 0-points, five 1-points, and fifteen 2-points. The distribution of the line types through P_3 in such a 38-plane is given by $B_3^5 C_5$. So, if $\tilde{L}$ is a line in H through P_3 that is not equal to L or L', then the hyperplanes through $\tilde{L}$ not equal to H contain five lines of type B_3 and $\tilde{L}$. We already know that $\tilde{L}$ has a type in $\{A_1, B_5, C_5, D_1\}$. Since their is neither a 228- nor a 33-plane with a unique 3-point, the cases B_1 and B_5 cannot occur. However, this contradicts the assumption that H is a 43-plane.

So, now we are in the situation where we assume that L is a line of type D_1 and there are no 13-lines at all. Thus, any line intersecting L (in a 3-point) has a type contained in $\{A_1, B_2, B_5, D_1\}$. From the classification of strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2, 5)$ we conclude that there are no 23- and no 38-planes. Moreover, any 43-planes is lifted from a line of type B_2. (A lifting from a line of type B_5 ensures a full hyperplane in the support of $\mathcal{K}$.) So, since each hyperplane through L is such a 43-plane, we have $(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = (60, 60, 0, 36)$. Each 33-plane consists of ten 0-points, fifteen 1-points, six 3-points, ten lines of type A_1, fifteen lines of type B_2, and six lines of type B_5. Looking at 18- and 28-planes we conclude that all line types are contained in $\{A_1, A_3, B_2, B_5, D_1\}$ and $\lambda_2 = 0$. Counting gives that through each 1-point there are ten 3-lines, i.e., lines of type A_3, and twenty-one 8-lines. Counting 3-points then gives that fifteen lines are of type B_2 and six lines are of type B_5, i.e., we have the pattern $A_3^{10} B_2^{15} B_5^6$. Now consider the line patterns through a 1-point in a hyperplane. For an 18-plane we have $A_3^5 B_5$, for a 28-plane we have $A_3^3 B_2^3$, for a 33-plane we have $A_3^2 B_2^2 B_5^2$, and for a 43-plane we have $B_2^5 B_5$. From this information we can compute that each 1-point is contained in ten 28-planes, fifteen 33-planes, and six 43-planes. With this, we have $a_{28} = 60$, $a_{33} = 60$, and $a_{43} = 36$ and the stated data can be computed easily from the classification of the strong $(3 \mod 5)$-arcs in $\mathrm{PG}(2, 5)$. □

The exceptional, non-lifted arc of cardinality 168 described in Lemma 8.64 indeed exists. A generator matrix is e.g. given by the concatenation of

$$\begin{pmatrix}
0000000000000000000000000000111111111111111111111111111111111111111111111111111111111 \\
0000000011111111111111111111000000000000000000000011111111111111111111111111111111111 \\
0001111100000222223333344444000001111122222444440000011111222223333344444444444444444 \\
1110002312444022224000140111201112000140222241244411134011120111211134000111222333444
\end{pmatrix}$$

and

$$\begin{pmatrix}
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111\\
2222222222222222222222222333333333333333333333333344444444444444444444444444444444444\\
0000011111222223333344444000001111122222333334444400000111112222222222222223333344444\\
0123411134000142333402224000230123412444233340111200014000230001112223334440002300014
\end{pmatrix}.$$

9. The non-existence of $(104, 22)$-arcs in $\mathrm{PG}(3, 5)$

The aim of this chapter is to prove the non-existence of $(104, 22)$-arcs in $\mathrm{PG}(3, 5)$. It is based on [116]. As an implication we have $n_5(4, 82) = 105$, which leaves only three open cases for the determination of $n_5(4, d)$. The insights of Chapter 8, especially the classification result of strong $(3 \mod 5)$-arcs in $\mathrm{PG}(3, 5)$ of small cardinality, see Theorem 8.58, will be essential for our argumentation.

First we observe some straightforward properties of a hypothetical $(104, 22)$-arc in $\mathrm{PG}(3, 5)$, reminding the reader that γ_i denotes the maximal multiplicity of an i-dimensional subspace for a given arc.

LEMMA 9.1

The spectrum (a_i) of a $(22, 5)$-arc $\mathcal{K}$ in $PG(2, 5)$ satisfies $a_1 = 0$, $a_3 = 13 - 10a_0 - 3a_2$, $a_4 = -3 + 15a_0 + 3a_2$, and $a_5 = 21 - 6a_0 - a_2$, where $a_0 \leq 1$ and $a_2 \leq \lfloor (13 - 10a_0)/3 \rfloor$.

PROOF. From Lemma 2.1 and $m \leq 5$ we conclude that $\mathcal{K}$ is projective, i.e., $\mathcal{K}(P) \in \{0, 1\}$ for all $P \in \mathcal{P}$. Applying Lemma 2.1 with $m = 1$ givens a maximum point multiplicity of 0 on this line, which is absurd, so that we assume $a_1 = 0$ in the following. With this, the standard equations from Lemma 1.5 are given by $a_0 + a_2 + a_3 + a_4 + a_5 = 31$, $2a_2 + 3a_3 + 4a_4 + 5a_5 = 132$, and $a_2 + 3a_3 + 6a_4 + 10a_5 = 231$, so that $a_3 = 13 - 10a_0 - 3a_2$, $a_4 = -3 + 15a_0 + 3a_2$, and $a_5 = 21 - 6a_0 - a_2$. Since $a_3 \geq 0$ and $a_0, a_2 \in \mathbb{N}$, we have $a_0 \leq 1$ and $a_2 \leq \lfloor (13 - 10a_0)/3 \rfloor$. □

LEMMA 9.2

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$ with spectrum (a_i). Then:

(a) The maximal multiplicity of a line in an m-plane is $\lfloor (6 + m)/5 \rfloor$.

(b) $\gamma_1 = 1$, $\gamma_2 = 5$, $\gamma_3 = 22$.

(c) There do not exist planes with 2, 3, 7, 8, 12, 13, 17, or 18 points.

(d) No 22-plane contains a 1-line.

(e) $a_1 = 0$.

PROOF.

(a) Apply Lemma 2.1.

(b) $\gamma_3 = 22$ follows from the definition of the arcs. (a) implies $\gamma_2 \le 5$. If $\gamma_2 \le 4$, then considering the 31 lines through a point of multiplicity at least 1 would yield $\#\mathcal{K} \le 1 + 31 \cdot 3 < 104$. Obviously $\gamma_1 \ge 1$. Considering the 31 lines through a point of multiplicity at least 2 would yield $\#\mathcal{K} \le 5 + 31 \cdot 3 < 104$. (Of course, we can also directly apply Proposition 2.16, since $\mathcal{K}$ would be a Griesmer arc.)

(c) Using (a), this follows from the non-existence of $(2, 1)$-, $(7, 2)$-, $(12, 3)-$, and $(17, 4)$-arcs in $\operatorname{PG}(2, 5)$, see Lemma 9.10.

(d) Let H be a 22-plane. Since no $(22, 4)$-arc exists in $\operatorname{PG}(2, 5)$, see Lemma 9.10, $\mathcal{K}|_H$ is a $(22, 5)$-arc, so that we can apply Lemma 9.1.

(e) Assume that H_0 is a 1-plane and consider a 1-line L in H_0. By $H_1, \dots, H_5$ we denote the other 5 planes through L. From (d) we conclude $\mathcal{K}(H_i) \le 21$ for all $1 \le i \le 5$, so that $\#\mathcal{K} = \sum_{i=0}^{5} \mathcal{K}(H_i) - 5 \cdot \mathcal{K}(L) \le 101 < 104$, which is a contradiction.

□

So, each $(104, 22)$-arc $\mathcal{K}$ in $\operatorname{PG}(3, 5)$ is 3-quasidivisible (modulo 5) and we apply Definition 8.5 to obtain a dual arc $\widetilde{\mathcal{K}}$. More precisely, $\widetilde{\mathcal{K}}$ is the σ-dual arc, where σ is given by Equation (8.1) for $t = 3$ and $n = 104$. In other words, hyperplanes of multiplicity congruent to $104 + a \pmod 5$ become $(3 - a)$-points in the dual geometry. In particular, 22-hyperplanes become 0-points with respect to $\widetilde{K}$. Note that $\widetilde{\mathcal{K}}$ is a strong $(3 \mod 5)$-arc in $\operatorname{PG}(3, 5)$. From Theorem 8.6 we conclude that $\mathcal{K}$ is extendible if $\widetilde{\mathcal{K}}$ contains a hyperplane in its support. However, no $(105, 22)$-arc in $\operatorname{PG}(3, 5)$ exists. To that end observe that a similar argumentation as in Lemma 9.2.(c) show that such an arc is 2-quasidivisible (modulo 5 and we can apply Corollary 8.25 to conclude the existence of a $(106, 22)$-arc in $\operatorname{PG}(3, 5)$. The later arc does not exist, see e.g. Exercise 8.2. This reasoning can also be found in [115, Theorem 4.8] and a more direct proof, without using the results from Chapter 8, can be found in [114].

As observed earlier for the general case, the cardinality of $\widetilde{\mathcal{K}}$ cannot be obtained from the parameters of $\mathcal{K}$. However, we can deploy the knowledge obtained in Section 8.3, especially the classification of strong $(3 \mod 5)$-ars in $\operatorname{PG}(3, 5)$ of small cardinality, see Theorem 8.58. So, first we exclude some special cases in our situation and then conclude $\#\widetilde{\mathcal{K}} \ge 163$.

LEMMA 9.3

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\operatorname{PG}(3, 5)$ and $\widetilde{\mathcal{K}}$ be the corresponding dual strong $(3 \mod 5)$-arc. Then, there exists no plane $\widetilde{\pi}$ in the dual space such that $\widetilde{\mathcal{K}}|_{\widetilde{\pi}}$ is $3\chi_{\widetilde{L}}$ for some line $\widetilde{L}$ in the dual space.

PROOF. Let P be the point corresponding to $\widetilde{\pi}$ and L be the line corresponding to $\widetilde{L}$. Summing up the multiplicities of all all planes through P gives

$$\sum_{H \in \mathcal{H} \,:\, P \le H} \mathcal{K}(H) = 6\#\mathcal{K} + 25\mathcal{K}(P)$$

and summing up the multiplicities of all all planes through L gives

$$\sum_{H\in\mathcal{H}\,:\,L\le H} \mathcal{K}(H) = \#\mathcal{K} + 5\mathcal{K}(L).$$

Since $\widetilde{L}$ is incident with $\widetilde{\pi}$, P is incident with L. Those hyperplanes H through P that do not contain L, correspond to points $\widetilde{H}$ in the dual space that are not contained on $\widetilde{L}$, so that $\widetilde{\mathcal{K}}(\widetilde{H}) = 0$ and H is a maximal plane, i.e., $\mathcal{K}(H) = 22$. Thus, all $[3]_5 - [2]_5 = 25$ hyperplanes through P that do not contain L are 22-planes and we have

$$\mathcal{K}(H) = 6\#\mathcal{K} + 25\mathcal{K}(P) = 25 \cdot 22 + \mathcal{K}(H) = \#\mathcal{K} + 5\mathcal{K}(L),$$

which is equivalent to

$$25\mathcal{K}(P) = 30 + 5\mathcal{K}(L).$$

Since $\mathcal{K}(P) \in \{0, 1\}$ and $\mathcal{K}(L) \ge 0$, this is a contradiction. □

LEMMA 9.4

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$ and $\widetilde{\mathcal{K}}$ be the corresponding dual strong $(3 \mod 5)$-arc, then $\#\widetilde{\mathcal{K}} \ge 163$.

PROOF. We apply Theorem 8.58. As argued above, the non-existence of a $(105, 22)$-arc in $\mathrm{PG}(3, 5)$ implies that $\widetilde{\mathcal{K}}$ cannot contain a full hyperplane in its support. If $\widetilde{\mathcal{K}}$ is lifted and $\#\widetilde{\mathcal{K}} < 168$, then $\widetilde{\mathcal{K}}$ is lifted from a strong $(3 \mod 5)$-arc $\mathcal{F}$ in $\mathrm{PG}(2, 5)$ with $\#\mathcal{F} \in \{18, 23, 28\}$. In the first case $\#\mathcal{F} = 18$ there is a full line, see Lemma 8.31, so that the lifted arc $\mathcal{K}$ would contain a full hyperplane in its support. In the two other cases the characterizations of $\mathcal{F}$ in Lemma 8.36 and Lemma 8.38 imply that $\mathcal{F}$ contains a line of type A_1, so that Lemma 9.3 gives a contradiction for $\widetilde{\mathcal{K}}$. □

Given the lower bound $\#\widetilde{\mathcal{K}} \ge 163$, we refine Definition 4.4 and Lemma 4.5. In general, for a given (n, s)-arc $\mathcal{K}$ in $\mathrm{PG}(k-1, q)$, where $k \ge 3$ and H_0 is a fixed hyperplane, and its dual $\widetilde{\mathcal{K}}$, we denote by $H_1(S), \dots, H_q(S)$ the q hyperplanes through S and set

$$\eta_{i,j}(H_0) = \max_{S\,:\,\mathcal{K}(S)=i, \tilde{\mathcal{K}}(\tilde{S})=j, S\le H_0, \dim(S)=k-2} \sum_{h=1}^{q} \binom{w - \mathcal{K}(H_h(S))}{2}. \tag{9.1}$$

If here exists no hyperline S with $\mathcal{K}(S) = i$ or $\tilde{\mathcal{K}}(\tilde{S}) = j$, then we set $\eta_{i,j} = 0$. We abbreviate $\eta_{i,j}(H_0)$ as $\eta_{i,j}$ whenever H_0 is clear from the context. Of course we have

$$\eta_i(H_0) = \max_j \eta_{i,j}(H_0),$$

so that Equation (9.1) gives a bit finer information than Equation (4.12).

LEMMA 9.5

Let $\mathcal{K}$ be an (n, s)-arc in $\mathrm{PG}(k-1, q)$, where $k \ge 3$, H_0 be a hyperplane, $\tilde{K}$ be the σ-dual arc with respect *to Equation (8.1), $b_{i,j}$ be the number of hyperlines S in H_0 with $\mathcal{K}(S) = i$ and $\tilde{\mathcal{K}}(\tilde{S}) = j$ of the restriction $\mathcal{K}|_{H_0}$, and $\widehat{\eta}_{i,j}$ some numbers satisfying $\eta_{i,j} \le \widehat{\eta}_{i,j}$ for all $i, j \in \mathbb{N}_0$. Then, we have*

$$\begin{aligned}\sum_{i,j} b_{i,j}\widehat{\eta}_i + \binom{s-\mathcal{K}(H_0)}{2} &\ge \binom{s}{2} \cdot [k]_q - n(s-1) \cdot [k-1]_q + \binom{n}{2} \cdot [k-2]_q + q^{k-2} \cdot \sum_{i\ge 2} \binom{i}{2}\lambda_i \\ &\ge \binom{s}{2} \cdot [k]_q - n(s-1) \cdot [k-1]_q + \binom{n}{2} \cdot [k-2]_q, \qquad (9.2)\end{aligned}$$

where $\lambda_h = \#\{P \in \mathcal{P} \,:\, \mathcal{K}(P) = h\}$.

Plugging in the data $k = 4$, $n = 104$, $s = 22$, $q = 5$, $[4]_5 = 156$, $[3]_5 = 31$, $[2]_5 = 6$, $\binom{s}{2} = 231$, $n(s-1) = 2184$, and $\binom{n}{2} = 5356$ from our situation into Inequality (9.2) gives

$$\sum_{i,j} b_{i,j}\widehat{\eta}_{i,j} + \binom{22-\mathcal{K}(H_0)}{2} \ge 468. \qquad (9.3)$$

Summing up the multiplicities of the lines $\tilde{L}$ through $\tilde{H}_0$ gives

$$\#\tilde{\mathcal{K}} = \tilde{\mathcal{K}}(H_0) + \sum_{i,j} b_{i,j}\left(j - \tilde{\mathcal{K}}(H_0)\right) \ge 163, \qquad (9.4)$$

taking Lemma 9.4 into account. The strategy of the remaining argumentation is the following. We pick a not excluded possibility for the multiplicity $\mathcal{K}(H_0)$ of a hyperplane H_0 and determine some information on the spectrum (b_i) of $\mathcal{K}|_{H_0}$ and compute values $\widehat{\eta}_{i,j}$ based on the current knowledge of the possible hyperplane multiplicities with respect to $\mathcal{K}$. Surely, the unknown values $b_{i,j} \in \mathbb{N}_0$ are linked to the b_i via

$$\sum_j b_{i,j} = b_i$$

for all $i \in \mathbb{N}_0$. Then we will show that Inequality (9.3) and Inequality (9.4) cannot be satisfied simultaneously, i.e., we apply a variant of the ILP method, see Chapter 4.

Before we start to exclude possible hyperplane multiplicities $\mathcal{K}(H_0)$, we determine some information on the spectrum (b_i) of $\mathcal{K}|_{H_0}$ for some special cases.

LEMMA 9.6

The spectrum (a_i) of a $(6, 2)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, 5)$-arc satisfies $a_0 = 10$, $a_1 = 6$, and $a_2 = 15$.

PROOF. From Lemma 2.1 and $m \le 2$ we conclude that $\mathcal{K}$ is projective, i.e., $\mathcal{K}(P) \in \{0, 1\}$ for all $P \in \mathcal{P}$. With this, the standard equations from Lemma 1.5 are given by $a_0 + a_1 + a_2 = 31$, $a_1 + 2a_2 = 36$, and $a_2 + 3a_2 = 15$, yielding the stated unique solution. □

LEMMA 9.7

The spectrum (a_i) of a $(9, 3)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, 5)$ satisfies $a_0 = 13 - a_3$, $a_1 = -18 + 3a_3$, and $a_2 = 36 - 3a_3$, where $6 \le a_3 \le 12$.

PROOF. From Lemma 2.1 and $m \le 3$ we conclude that $\mathcal{K}$ is projective, i.e., $\mathcal{K}(P) \in \{0,1\}$ for all $P \in \mathcal{P}$. With this, the standard equations from Lemma 1.5 are given by $a_0+a_1+a_2+a_3 = 31$, $a_1+2a_2+3a_3 = 54$, and $a_2 + 3a_3 = 36$, so that $a_0 = 13 - a_3$, $a_1 = -18 + 3a_3$, and $a_2 = 36 - 3a_3$. Since $a_1 \ge 0$ and $a_2 \ge 0$, we have $6 \le a_3 \le 12$. □

Note that the cases $a_3 \in \{6, 11, 12\}$ in Lemma 9.7 cannot occur, see Exercise 9.1.

LEMMA 9.8

The spectrum (a_i) of a $(10, 3)$-arc $\mathcal{K}$ in $\operatorname{PG}(2, 5)$ satisfies $a_0 = 16-a_3$, $a_1 = -30+3a_3$, and $a_2 = 45-3a_3$, where $10 \le a_3 \le 13$.

PROOF. From Lemma 2.1 and $m \le 3$ we conclude that $\mathcal{K}$ is projective, i.e., $\mathcal{K}(P) \in \{0,1\}$ for all $P \in \mathcal{P}$. With this, the standard equations from Lemma 1.5 are given by $a_0+a_1+a_2+a_3 = 31$, $a_1+2a_2+3a_3 = 60$, and $a_2 + 3a_3 = 45$, so that $a_0 = 16 - a_3$, $a_1 = -30 + 3a_3$, and $a_2 = 45 - 3a_3$. Since $a_1 \ge 0$ and $a_2 \ge 0$, we have $10 \le a_3 \le 15$.

It remains to exclude the cases $a_3 \in \{14, 15\}$. First we note $a_0 \ge 1$, so that we can consider a 0-line L_0. Let P be an arbitrary point on P, which then is a 0-point, and $L_0, L_1, \dots, L_5$ be the six lines through P. Since $\#\mathcal{K} = 10$ and the number of lines through P are even, the set $\{0 \le i \le 5 : \mathcal{K}(L_i) \equiv 0 \pmod 2\}$ must have even cardinality. In other words, at least one of the lines $L_1, \dots, L_5$ must have an even multiplicity. However, for $a_3 = 15$ we have $a_0 = 1$, $a_1 = 15$, and $a_2 = 0$, so that this is impossible. For $a_3 = 14$ we have $a_0 = 2$, $a_1 = 12$, and $a_2 = 3$, i.e., there are four lines with even multiplicity besides L_0. Since there are six 0-points on L this is again impossible. □

LEMMA 9.9

The spectrum (a_i) of an $(11, 3)$-arc $\mathcal{K}$ in $\operatorname{PG}(2, 5)$ satisfies $a_0 = 20 - a_3$, $a_1 = -44 + 3a_3$, and $a_2 = 55 - 3a_3$, where $15 \le a_3 \le 18$.

PROOF. From Lemma 2.1 and $m \le 3$ we conclude that $\mathcal{K}$ is projective, i.e., $\mathcal{K}(P) \in \{0,1\}$ for all $P \in \mathcal{P}$. With this, the standard equations from Lemma 1.5 are given by $a_0+a_1+a_2+a_3 = 31$, $a_1+2a_2+3a_3 = 66$, and $a_2 + 3a_3 = 55$, so that $a_0 = 20 - a_3$, $a_1 = -44 + 3a_3$, and $a_2 = 55 - 3a_3$. Since $a_1 \ge 0$ and $a_2 \ge 0$, we have $15 \le a_3 \le 18$. □

In Exercise 4.1 we had obtained:

LEMMA 9.10

No $(5s - 3, s)$-arc exists in $\operatorname{PG}(2, 5)$ for $1 \le s \le 4$.

In the following lemmas we always start with a hyperplane H_0 of a $(104, 22)$-arc $\mathcal{K}$ in $\mathrm{PG}(3, 5)$. For an arbitrary fixed line L in H_0 we denote by $H_1(L), \ldots, H_5(L)$ the other 5 planes through L. For brevity, we write H_i instead of $H_i(L)$, where $1 \le i \le 5$.

LEMMA 9.11

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$. Then $a_0 = 0$.

PROOF. Let H_0 be a 0-plane, so that $\mathcal{K}(L) = 0$ for each line L in H_0. Looping over all possibilities, while taking into account $\mathcal{K}(H_i) \in \{0, 4, 5, 6, 9, 10, 11, 14, 15, 16, 19, 20, 21, 22\}$, we compute the values of $\sum_{i=1}^{5} \binom{22-\mathcal{K}(H_i)}{2}$ as follows:

$\mathcal{K}(L)$	$\tilde{\mathcal{K}}(\tilde{L})$	$(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5))$	$\sum_{i=1}^{5} \binom{22-\mathcal{K}(H_i)}{2}$	type of $\tilde{L}$
0	3	$(0, 22, 22, 22, 22, 16)$	15	A_2
0	8	$(0, 21, 21, 21, 21, 20)$	1	B_8
		$(0, 22, 21, 21, 20, 20)$	2	B_7
		$(0, 22, 21, 21, 21, 19)$	3	B_4
		$(0, 22, 22, 20, 20, 20)$	3	B_6
		$(0, 22, 22, 21, 20, 19)$	4	B_3
		$(0, 22, 22, 22, 19, 19)$	6	B_1

We can condense this information to the following non-zero upper bounds for $\widehat{\eta}_{i,j}$:

$i = \mathcal{K}(L)$	$j = \tilde{\mathcal{K}}(\tilde{L})$	$\widehat{\eta}_{i,j}$	$(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5))$
0	3	15	$(0, 22, 22, 22, 22, 16)$
0	8	6	$(0, 22, 22, 22, 19, 19)$

Denote by x the number of lines L in H_0 such that $\tilde{\mathcal{K}}(\tilde{L}) = 3$. With this, we have $b_{0,3} = x$ and $b_{0,8} = 31 - x$. With this, Inequality (9.3) gives

$$x \cdot 15 + (31 - x) \cdot 6 + \binom{22}{2} \ \ge \ 468,$$

so that $x \ge \lceil \frac{51}{9} \rceil = 6$. Using $\widetilde{\mathcal{K}}(\widetilde{H}_0) = 2$ Inequality (9.4) yields

$$\#\widetilde{K} = 2 + x \cdot 1 + (31 - x) \cdot 6 = 188 - 5x \le 158 < 163,$$

which is a contradiction. □

In the following lemmas we will not list the values $\sum_{i=1}^{5} \binom{22-\mathcal{K}(H_i)}{2}$ for all possibilities but just the resulting non-zero upper bounds for $\widehat{\eta}_{i,j}$. See Exercise 9.2 for the case $\mathcal{K}(H_0) = 6$.

As an alternative proof of Lemma 9.11 one may also embed $\mathcal{K}$ in $\mathrm{AG}(3,5)$, due to the existence of a 0-plane, and consider the 1-complementary arc. However, it can be concluded from e.g. [12, Corollary 2.3] that there is no $(125-104, 25-22) = (21,3)$-blocking set in $\mathrm{AG}(3,5)$. We remark that the proof of the cited result is based on the so-called polynomial method, associating polynomials over $\mathbb{F}_q$ to sets of points in $\mathrm{AG}(k-1,q)$ or $\mathrm{PG}(k-1,q)$, which is a very effective technique, e.g.,for blocking sets.

Lemma 9.12

Let $\mathcal{K}$ be a $(104,22)$-arc in $\mathrm{PG}(3,5)$. Then $a_4 = 0$.

Proof. Let H_0 be a 4-plane. From Lemma 2.1 we conclude $\mathcal{K}(L) \le 2$ for each line L in H_0. Looping over all possibilities, while taking into account $\mathcal{K}(H_i) \in \{4,5,6,9,10,11,14,15,16,19,20,21,22\}$ and that a 22-plane cannot contain a 1-line, we compute the following non-zero upper bounds for $\widehat{\eta}_{i,j}$:

$i=\mathcal{K}(L)$	$j=\widetilde{\mathcal{K}}(\tilde{L})$	$\widehat{\eta}_{i,j}$	$(\mathcal{K}(H_0),\ldots,\mathcal{K}(H_5))$
2	3	0	$(4,22,22,22,22,22)$
1	8	0	$(4,21,21,21,21,21)$
0	8	29	$(4,22,22,22,20,14)$
0	13	9	$(4,22,21,19,19,19)$

Denote by x the number of lines L in H_0 such that $\mathcal{K}(L) = 0$ and $\tilde{\mathcal{K}}(\tilde{L}) = 8$. Note that $\mathcal{K}|_{H_0}$ is a $(4,2)$-arc in $\mathrm{PG}(2,5)$ with spectrum $b_0 = 13$, $b_1 = 12$, $b_2 = 6$, so that $b_{2,3} = 6$, $b_{1,8} = 12$, $b_{0,8} = x$, and $b_{0,13} = 13 - x$. With this, Inequality (9.3) reads

$$6 \cdot 0 + 12 \cdot 0 x \cdot 29 + (13-x) \cdot 9 + \binom{18}{2} \ \ge \ 468,$$

so that $x \ge \left\lceil \frac{99}{10} \right\rceil = 10$. Using $\widetilde{\mathcal{K}}(\widetilde{H}_0) = 3$ this contradicts Inequality (9.4) since

$$\#\widetilde{K} = 3 + 6 \cdot 0 + 12 \cdot 5 + x \cdot 5 + (13-x) \cdot 10 = 193 - 5x \le 143 < 163.$$

□

Lemma 9.13

Let $\mathcal{K}$ be a $(104,22)$-arc in $\mathrm{PG}(3,5)$. Then $a_5 = 0$.

Proof. Let H_0 be a 5-plane. From Lemma 2.1 we conclude $\mathcal{K}(L) \le 2$ for each line L in H_0. Looping over all possibilities, while taking into account $\mathcal{K}(H_i) \in \{5,6,9,10,11,14,15,16,19,20,21,22\}$ and that a 22-plane cannot contain a 1-line, we compute the following non-zero upper bounds for $\widehat{\eta}_{i,j}$:

$i = \mathcal{K}(L)$	$j = \tilde{\mathcal{K}}(\tilde{L})$	$\widehat{\eta}_{i,j}$	$(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5))$
2	3	0	$(5, 22, 22, 22, 22, 21)$
1	8	1	$(5, 21, 21, 21, 21, 20)$
0	3	55	$(5, 22, 22, 22, 22, 11)$
0	8	31	$(5, 22, 22, 22, 19, 14)$
0	13	10	$(5, 22, 20, 19, 19, 19)$

Denote by x the number of lines L in H_0 such that $\mathcal{K}(L) = 0$ and $\tilde{\mathcal{K}}(\tilde{L}) = 3$ and by y the number of lines L in H_0 such that $\mathcal{K}(L) = 0$ and $\tilde{\mathcal{K}}(\tilde{L}) = 8$. Note that $\mathcal{K}|_{H_0}$ is a $(5, 2)$-arc in $\mathrm{PG}(2, 5)$ with spectrum $a_0 = 11$, $a_1 = 10$, $a_2 = 10$, so that $b_{2,3} = 10$, $b_{1,8} = 10$, $b_{0,3} = x$, $b_{0,8} = y$, and $b_{0,11} = 13 - x - y$. With this, Inequality (9.3) reads

$$10 \cdot 0 + 10 \cdot 1 + x \cdot 55 + y \cdot 31 + (11 - x - y) \cdot 10 + \binom{17}{2} \;\geq\; 468,$$

so that $45x + 7y \geq 212$, which implies $90x + 45y \geq 90x + 42y \geq 424$. Thus, we have $2x + y \geq 10$. Combining this with $\widetilde{\mathcal{K}}(\widetilde{H}_0) = 2$, Inequality (9.4) yields the contradiction

$$\#\widetilde{K} = 2 + 10 \cdot 1 + 10 \cdot 6 + x \cdot 1 + y \cdot 6 + (11 - x - y) \cdot 11 = 193 - 10x - 5y \leq 143 < 163.$$

□

LEMMA 9.14

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$. Then $a_6 = 0$.

PROOF. Let H_0 be a 6-plane. From Lemma 2.1 we conclude $\mathcal{K}(L) \leq 2$ for each line L in H_0. Looping over all possibilities, while taking into account $\mathcal{K}(H_i) \in \{6, 9, 10, 11, 14, 15, 16, 19, 20, 21, 22\}$ and that a 22-plane cannot contain a 1-line, we compute the following non-zero upper bounds for $\widehat{\eta}_{i,j}$:

$i = \mathcal{K}(L)$	$j = \tilde{\mathcal{K}}(\tilde{L})$	$\widehat{\eta}_{i,j}$	$(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5))$
2	3	1	$(6, 22, 22, 22, 22, 20)$
1	8	3	$(6, 21, 21, 21, 21, 19)$
0	3	66	$(6, 22, 22, 22, 22, 10)$
0	8	31	$(6, 22, 22, 21, 19, 14)$
0	13	12	$(6, 22, 19, 19, 19, 19)$

Denote by x the number of lines L in H_0 such that $\mathcal{K}(L) = 0$ and $\tilde{\mathcal{K}}(\tilde{L}) = 3$ and by y the number of lines L in H_0 such that $\mathcal{K}(L) = 0$ and $\tilde{\mathcal{K}}(\tilde{L}) = 8$.

From Lemma 2.1 and the non-existence of $(6, 1)$-arcs in $\mathrm{PG}(2, 5)$ we conclude that the restricted arc $\mathcal{K}|_{H_0}$ is a $(6, 2)$-arc in $\mathrm{PG}(2, 5)$. Let (b_i) be the spectrum of $\mathcal{K}|_{H_0}$. Given the above enumeration of the possible combinations of $i = \mathcal{K}(L)$ and $j = \tilde{\mathcal{K}}(\tilde{L})$ we obtain $b_{2,3} = b_2$, $b_{1,8} = b_1$, $b_{0,3} = x$, $b_{0,8} = y$, and $b_{0,13} = b_0 - x - y$, so that Inequality (9.3) reads

$$b_2 \cdot 1 + b_1 \cdot 3 + x \cdot 66 + y \cdot 31 + (b_0 - x - y) \cdot 12 + \binom{16}{2} \geq 468 \tag{9.5}$$

and combining $\widetilde{\mathcal{K}}(\widetilde{H}_0) = 1$ with Inequality (9.4) gives

$$\#\widetilde{K} = 1 + b_2 \cdot 2 + b_1 \cdot 7 + x \cdot 2 + y \cdot 7 + (b_0 - x - y) \cdot 12 \geq 163. \tag{9.6}$$

Plugging in $b_0 = 10$, $b_1 = 6$, and $b_2 = 15$, see Lemma 9.6, into Inequality (9.5) and Inequality (9.6) gives

$$54x + 19y \geq 195 \tag{9.7}$$

and

$$\#\widetilde{\mathcal{K}} = 193 - 10x - 5y \geq 163,$$

respectively. The latter constraint yields $2x + y \leq 6$, so that

$$54x + 19y \leq 27(2x + y) \leq 162,$$

which contradicts Inequality (9.7). □

Note that our application of Inequality (9.6) differs from the one in the proof of [116, Lemma 4.4] due to a typo; the approach is essentially the same.

LEMMA 9.15

Let $\mathcal{K}$ *be a* $(104, 22)$*-arc in* $\mathrm{PG}(3, 5)$. *Then* $a_9 = 0$.

PROOF. Let H_0 be a 9-plane. From Lemma 2.1 we conclude $\mathcal{K}(L) \leq 3$ for each line L in H_0. Taking into account $\mathcal{K}(H_i) \in \{9, 10, 11, 14, 15, 16, 19, 20, 21, 22\}$ and that a 22-plane cannot contain a 1-line, we compute the following non-zero upper bounds for $\widehat{\eta}_{i,j}$:

$i = \mathcal{K}(L)$	$j = \tilde{\mathcal{K}}(\tilde{L})$	$\widehat{\eta}_{i,j}$	$(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5))$
3	3	0	$(9, 22, 22, 22, 22, 22)$
2	8	4	$(9, 22, 22, 22, 20, 19)$
1	8	15	$(9, 21, 21, 21, 21, 16)$
1	13	7	$(9, 21, 21, 20, 19, 19)$
0	8	79	$(9, 22, 22, 22, 20, 9)$
0	13	34	$(9, 22, 21, 19, 19, 14)$
0	18	15	$(9, 19, 19, 19, 19, 19)$

Denote by x the number of lines L in H_0 such that $\mathcal{K}(L) = 1$ and $\tilde{\mathcal{K}}(\tilde{L}) = 8$. Similarly, denote by u, resp. v, the number of lines L in H_0 with $\mathcal{K}(L) = 0$, $\tilde{\mathcal{K}}(\tilde{L}) = 8$, resp. $\mathcal{K}(L) = 0$, $\tilde{\mathcal{K}}(\tilde{L}) = 13$.

From Lemma 2.1 and the non-existence of $(9, 2)$-arcs in $\operatorname{PG}(2, 5)$ we conclude that the restricted arc $\mathcal{K}|_{H_0}$ is a $(9, 3)$-arc in $\operatorname{PG}(2, 5)$. Let (b_i) be the spectrum of $\mathcal{K}|_{H_0}$. Given the above enumeration of the possible combinations of $i = \mathcal{K}(L)$ and $j = \widetilde{\mathcal{K}}(\tilde{L})$ we obtain $b_{3,3} = b_3,$, $b_{2,8} = b_2$, $b_{1,8} = x$, $b_{1,13} = b_1 - x$, $b_{0,8} = u$, $b_{0,13} = v$, and $b_{0,18} = b_0 - u - v$, so that Inequality (9.3) reads

$$b_3 \cdot 0 + b_2 \cdot 4 + x \cdot 15 + (b_1 - x) \cdot 7 + u \cdot 79 + v \cdot 34 + (b_0 - u - v) \cdot 15 + \binom{13}{2} \geq 468. \qquad (9.8)$$

Using $\widetilde{\mathcal{K}}(\widetilde{H}_0) = 3$ Inequality (9.4) gives

$$\#\widetilde{K} = 3 + b_3 \cdot 0 + b_2 \cdot 5 + x \cdot 5 + (b_1 - x) \cdot 10 + u \cdot 5 + v \cdot 10 + (b_0 - u - v) \cdot 15 \geq 163. \qquad (9.9)$$

Plugging in the parameterization from Lemma 9.7 into Inequality (9.8) and Inequality (9.9) gives

$$8x + 64u + 19v \geq 177 + 6b_3 \geq 213 \qquad (9.10)$$

and

$$\#\widetilde{\mathcal{K}} = 198 - 5x - 10u - 5v \geq 163,$$

respectively. The latter constraint yields $x + 2u + v \leq 7$, so that $u \leq 3$. Using $x + y \leq 7 - 2u$ we conclude

$$8x + 64u + 19v \leq 19 \cdot (7 - 2u) + 64u = 133 + 26 \leq 211$$

from $u \leq 3$, which contradicts Inequality (9.10). □

REMARK 9.16 Only some of the used restrictions for $\mathcal{K}(H)$, e.g., $\mathcal{K}(H_i) \notin \{2, 3, 7, 8, 12, 13, 17, 18\}$, are necessary to conclude the stated $\widehat{\eta}_{i,j}$. However, allowing $\mathcal{K}(H_i) = 17$ would yield the new case $\mathcal{K}(L) = 2$ and $\widetilde{\mathcal{K}}(\tilde{L}) = 3$ via $(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5)) = (9, 22, 22, 22, 22, 17)$. Similarly, allowing $\mathcal{K}(H_i) = 18$ would increase $\widehat{\eta}_{2,8}$ from 4 to 6 via $(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5)) = (9, 22, 22, 22, 21, 18)$. Moreover, the insight that no 22-plane can contain a 1-line is essential. Otherwise we would have $\widehat{\eta}_{1,8} = 29$ via $(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5)) = (9, 22, 22, 22, 20, 14)$ and $\widehat{\eta}_{1,13} = 9$ via $(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5)) = (9, 22, 21, 19, 19, 19)$.

LEMMA 9.17

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\operatorname{PG}(3, 5)$. Then $a_{10} = 0$.

PROOF. Let H_0 be a 10-plane. From Lemma 2.1 we conclude $\mathcal{K}(L) \leq 3$ for each line L in H_0. Looping over all possibilities, while taking into account $\mathcal{K}(H_i) \in \{10, 11, 14, 15, 16, 19, 20, 21, 22\}$ and that a 22-plane cannot contain a 1-line, we compute the following non-zero upper bounds for $\widehat{\eta}_{i,j}$:

$i = \mathcal{K}(L)$	$j = \widetilde{\mathcal{K}}(\tilde{L})$	$\widehat{\eta}_{i,j}$	$(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5))$
3	3	0	$(10, 22, 22, 22, 22, 21)$
2	3	15	$(10, 22, 22, 22, 22, 16)$
2	8	6	$(10, 22, 22, 22, 19, 19)$
1	8	21	$(10, 21, 21, 21, 21, 15)$
1	13	9	$(10, 21, 21, 19, 19, 19)$
0	8	69	$(10, 22, 22, 21, 19, 10)$
0	13	35	$(10, 22, 20, 19, 19, 14)$

Denote by x the number of lines L in H_0 such that $\mathcal{K}(L) = 2$ and $\tilde{\mathcal{K}}(\tilde{L}) = 3$, by y the number of lines L in H_0 such that $\mathcal{K}(L) = 1$ and $\tilde{\mathcal{K}}(\tilde{L}) = 8$, and by z the number of lines L in H_0 such that $\mathcal{K}(L) = 0$ and $\tilde{\mathcal{K}}(\tilde{L}) = 8$.

From Lemma 2.1 and the non-existence of $(10, 2)$-arcs in $\mathrm{PG}(2, 5)$ we conclude that the restricted arc $\mathcal{K}|_{H_0}$ is a $(10, 3)$-arc in $\mathrm{PG}(2, 5)$. Let (b_i) be the spectrum of $\mathcal{K}|_{H_0}$. Given the above enumeration of the possible combinations of $i = \mathcal{K}(L)$ and $j = \tilde{\mathcal{K}}(\tilde{L})$ we obtain $b_{3,3} = b_3$, $b_{2,3} = x$, $b_{2,8} = b_2 - x$, $b_{1,8} = y$, $b_{1,13} = b_1 - y$, $b_{0,8} = z$, and $b_{0,13} = b_0 - z$, so that Inequality (9.3) reads

$$b_3 \cdot 0 + x \cdot 15 + (b_2 - x) \cdot 6 + y \cdot 21 + (b_1 - y) \cdot 9 + z \cdot 69 + (b_0 - z) \cdot 35 + \binom{12}{2} \geq 468. \quad (9.11)$$

Using $\widetilde{\mathcal{K}}(\widetilde{H}_0) = 2$ Inequality (9.4) gives

$$\#\widetilde{K} = 2 + b_3 \cdot 1 + x \cdot 1 + (b_2 - x) \cdot 6 + y \cdot 6 + (b_1 - y) \cdot 11 + z \cdot 6 + (b_0 - z) \cdot 11 \geq 163. \quad (9.12)$$

Plugging in the parameterization from Lemma 9.8 into Inequality (9.11) and Inequality (9.12) gives

$$9x + 12y + 34z \geq 26b_3 - 158 \quad (9.13)$$

and

$$\#\widetilde{\mathcal{K}} = 118 - 5x - 5y - 5z + 5b_3 \geq 163,$$

respectively. The latter constraint yields $x + y + z \leq b_3 - 9$, so that

$$9x + 12y + 34z \leq 34 \cdot (b_3 - 9) = 34b_3 - 306.$$

Thus, we can conclude $34b_3 - 306 \geq 26b_3 - 158$ from Inequality (9.13), which is equivalent to $b_3 \geq 18.5$. Since we have $b_3 \leq 13 \geq$ due to Lemma 9.8, we obtain a contradiction. □

Note that in the proof of Lemma 9.17 we actually do not need the tight version of Lemma 9.8 showing $b_3 \leq 13$. The more easily obtainable assertion $b_3 \leq 15$ is sufficient for our conclusion.

LEMMA 9.18

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$. Then $a_{11} = 0$.

PROOF. Let H_0 be a 11-plane. From Lemma 2.1 we conclude $\mathcal{K}(L) \leq 3$ for each line L in H_0. Looping over all possibilities, while taking into account $\mathcal{K}(H_i) \in \{11, 14, 15, 16, 19, 20, 21, 22\}$ and that a 22-plane cannot contain a 1-line, we compute the following non-zero upper bounds for $\widehat{\eta}_{i,j}$:

$i = \mathcal{K}(L)$	$j = \tilde{\mathcal{K}}(\tilde{L})$	$\widehat{\eta}_{i,j}$	$(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5))$
3	3	1	$(11, 22, 22, 22, 22, 20)$
2	3	21	$(11, 22, 22, 22, 22, 15)$
2	8	6	$(11, 22, 22, 21, 19, 19)$
1	8	28	$(11, 21, 21, 21, 21, 14)$
1	13	10	$(11, 21, 20, 19, 19, 19)$
0	3	70	$(11, 22, 22, 22, 16, 11)$
0	8	61	$(11, 22, 22, 19, 19, 11)$
0	13	37	$(11, 22, 19, 19, 19, 14)$

Denote by x the number of lines L in H_0 such that $\mathcal{K}(L) = 2$ and $\tilde{\mathcal{K}}(\tilde{L}) = 3$, by y the number of lines L in H_0 such that $\mathcal{K}(L) = 1$ and $\tilde{\mathcal{K}}(\tilde{L}) = 8$, by u the number of lines L in H_0 such that $\mathcal{K}(L) = 0$ and $\tilde{\mathcal{K}}(\tilde{L}) = 3$, and by v the number of lines L in H_0 such that $\mathcal{K}(L) = 0$ and $\tilde{\mathcal{K}}(\tilde{L}) = 8$.

From Lemma 2.1 and the non-existence of $(11, 2)$-arcs in $\mathrm{PG}(2, 5)$ we conclude that the restricted arc $\mathcal{K}|_{H_0}$ is a $(11, 3)$-arc in $\mathrm{PG}(2, 5)$. Let (b_i) be the spectrum of $\mathcal{K}|_{H_0}$. Given the above enumeration of the possible combinations of $i = \mathcal{K}(L)$ and $j = \tilde{\mathcal{K}}(\tilde{L})$ we obtain $b_{3,3} = b_3$, $b_{2,3} = x$, $b_{2,8} = b_2 - x$, $b_{1,8} = y$, $b_{1,13} = b_1 - y$, $b_{0,3} = u$, $b_{0,8} = v$, and $b_{0,13} = b_0 - u - v$, so that Inequality (9.3) reads

$$b_3 \cdot 1 + x \cdot 21 + (b_2 - x) \cdot 6 + y \cdot 28 + (b_1 - y) \cdot 10 + u \cdot 70 + v \cdot 61 + (b_0 - u - v) \cdot 37 + \binom{11}{2} \geq 468. \quad (9.14)$$

Using $\widetilde{\mathcal{K}}(\widetilde{H}_0) = 1$ Inequality (9.4) gives

$$\#\widetilde{K} = 1 + b_3 \cdot 2 + x \cdot 2 + (b_2 - x) \cdot 7 + y \cdot 7 + (b_1 - y) \cdot 12 + u \cdot 2 + v \cdot 7 + (b_0 - u - v) \cdot 12 \geq 163. \quad (9.15)$$

Plugging in the parameterization from Lemma 9.9 into Inequality (9.14) and Inequality (9.15) gives

$$15x + 18y + 33u + 24v \geq 24b_3 - 217 \quad (9.16)$$

and

$$\#\widetilde{\mathcal{K}} = 98 - 5x - 5y - 10u - 5v + 5b_3 \geq 163,$$

respectively. The latter constraint yields $x + y + 2u + v \leq b_3 - 13$, so that $x + y + v \leq b_3 - 13 - 2u$ and

$$15x + 18y + 33u + 24v \leq 33u + 24\,(b_3 - 13 - 2u) = 24b_3 - 15u - 312.$$

Thus, we can conclude $24b_3 - 15u - 312 \geq 24b_3 - 217$ from Inequality (9.16), which is equivalent to $u \leq -\frac{19}{3}$ contradicting $u \geq 0$. □

LEMMA 9.19

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$. Then $a_{22} = 0$.

PROOF. Let H_0 be a 22-plane. Looping over all possibilities, while taking into account

$$\mathcal{K}(H_i) \in \{14, 15, 16, 19, 20, 21, 22\}$$

and that a 22-plane cannot contain a 1-line, we compute the following non-zero upper bounds for $\widehat{\eta}_{i,j}$:

$b_{i,j}$	$i = \mathcal{K}(L)$	$j = \tilde{\mathcal{K}}(\tilde{L})$	$\widehat{\eta}_{i,j}$	$(\mathcal{K}(H_0), \ldots, \mathcal{K}(H_5))$
b_5	5	3	3	$(22, 22, 22, 22, 22, 19)$
x	4	3	28	$(22, 22, 22, 22, 22, 14)$
$b_4 - x$	4	8	7	$(22, 22, 22, 20, 19, 19)$
u	3	3	36	$(22, 22, 22, 22, 16, 15)$
v	3	8	32	$(22, 22, 22, 20, 19, 14)$
$b_3 - u - v$	3	13	12	$(22, 21, 19, 19, 19, 19)$
y	2	3	45	$(22, 22, 22, 16, 16, 16)$
z	2	8	57	$(22, 22, 22, 20, 14, 14)$
$b_2 - y - z$	2	13	37	$(22, 21, 19, 19, 19, 14)$
$b_0 - s$	0	8	86	$(22, 22, 16, 16, 14, 14)$
s	0	13	87	$(22, 21, 19, 14, 14, 14)$

From the non-existence of a $(22,4)$-arc in $\mathrm{PG}(2,5)$ we conclude that $\mathcal{K}|_{H_0}$ is a $(22,5)$-arc in $PG(2,5)$. Let (b_i) be the spectrum of $\mathcal{K}|_{H_0}$. Using the non-negative integer variables x, y, z, u, v, and s, we express the counts $b_{i,j}$ of the number of lines L in H_0 such that $\mathcal{K}(L)=i$ and $\widetilde{\mathcal{K}}(\tilde{L})=j$, see the above table. With this, Inequality (9.3) reads

$$\begin{aligned} b_5\cdot 3+x\cdot 28+(b_4-x)\cdot 7+u\cdot 36+v\cdot 32+(b_3-u-v)\cdot 12 & \\ +y\cdot 45+z\cdot 57+(b_2-y-z)\cdot 37+s\cdot 87+(b_0-s)\cdot 86+\binom{0}{2} &\geq 468. \end{aligned} \tag{9.17}$$

Using $\widetilde{\mathcal{K}}(\widetilde{H}_0)=0$ Inequality (9.4) gives

$$\#\widetilde{K}=3\,(b_5+x+u+y)+8\,(b_4-x+v+z+b_0-s)+13\,(b_3-u-v+b_2-y-z+s)\geq 163. \tag{9.18}$$

Plugging in the parameterization from Lemma 9.1 into Inequality (9.17) and Inequality (9.18) gives

$$21x+24u+20v+8y+20z+s\geq 270-53b_0-19b_2 \tag{9.19}$$

and

$$\#\widetilde{\mathcal{K}}=208-20b_0-5b_2-5x-10u-10y-5v-5z+5s\geq 163,$$

respectively. The latter constraint yields $x+v+z+2u+2y-s\leq 9-4b_0-b_2$, so that $x+v+z\leq 9-4b_0-b_2-2(u+y)+s$ and

$$\begin{aligned} 21x+24u+20v+8y+20z+s &\leq 21(9-4b_0-b_2-2(u+y)+s)+24(u+y)+s \\ &= 189-84b_0-21b_2-18(u+y)+22s. \end{aligned}$$

Thus, we can conclude

$$189-84b_0-21b_2-18(u+y)+22s\ \geq\ 270-53b_0-19b_2$$

from Inequality (9.19), which is equivalent to

$$189+22s\ \geq\ 270+31b_0+2b_2+18(u+y).$$

This contradicts $s\leq b_0\leq 1$. □

A direct implication of Lemma 9.19 is the non-existence of $(104,22)$-arcs in $\mathrm{PG}(3,5)$:

THEOREM 9.20 ([116, Theorem 4.6])
There is no $(104,22)$*-arc in* $\mathrm{PG}(3,5)$.

COROLLARY 9.21
A linear code with parameters $[104,4,82]_5$ *does not exist. In particular,* $n_5(4,82)=105$.

We remark that there are more direct proof variants of Lemma 9.12 and Lemma 9.13 not relying on the partial classification of strong $(3 \mod 5)$-arcs in $\mathrm{PG}(3,5)$, see Theorem 8.58.

LEMMA 9.22

Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$. Then $a_4 = 0$.

PROOF. Let H_0 be a 4-plane so that $\mathcal{K}|_{H_0}$ is a $(4, 2)$-arc. Since the number of 0-points in $\mathcal{K}|_{H_0}$ is 27 and each of the six 2-lines contains four 0-points there are at least three 0-points that are not contained in any 2-line in H_0. Let X be one of these. Denote the six lines through X in H_0 by $L_0, \ldots, L_5$, where $\mathcal{K}(L_i) \leq 1$. W.l.o.g. we assume $\mathcal{K}(L_0) = 1$ and denote the five hyperplanes through L_0 not equal to H_0 by $H_1, \ldots, H_5$. Since no 22-plane can contain the 1-line L_0, we have $\mathcal{K}(H_i) = 21$ for all $1 \leq i \leq 5$. Assume that there exists an index $1 \leq i \leq 5$ and a line $X \leq L' \leq H_i$ with $\mathcal{K}(L') = 5$ (note that the maximum line multiplicity is 5). Set $H'_0 = H_i$ and denote by $H'_1, \ldots, H'_5$ the other hyperplanes through L'. Counting gives that we have $\mathcal{K}(H'_j) = 22$ for at least three indices $1 \leq j \leq 5$. Since each of the six hyperplanes H'_h contains exactly one of the lines L_l, where four are 1-lines, at least one of the hyperplanes with $\mathcal{K}(H'_j) = 22$ contains a 1-line, which is a contradiction. Thus, the multiplicity of the 31 lines through X is contained in $\{0, 1, 4\}$. Since each hyperplane H' through X contains one of the lines $L_0, \ldots, L_5$, we have $\mathcal{K}(H') \leq 1 + 5 \cdot 4 = 21 < 22$. With this we can define a $(105, 22)$-arc by $\mathcal{K}'(X) = \mathcal{K}(X) + 1$ and $\mathcal{K}'(P) = \mathcal{K}(P)$ for all $P \in \mathcal{P} \backslash \{X\}$, which does not exist. Thus, we have obtained a contradiction and $a_4 = 0$. □

REMARK 9.23 Actually we can formulate the proof of Lemma 9.22 in terms of the $(104, 22)$-arc in $\mathrm{PG}(2, 5)$ arising by a projection through X. A similar approach can also be applied to show $a_5 = 0$, see Exercise 9.3.

EXERCISE 9.1 Show that a $(9, 3)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, 5)$ cannot have 6, 11, or 12 three-lines; cf. Lemma 9.7.

EXERCISE 9.2 For $\mathcal{K}(H_0) = 6$ and the assumption $\mathcal{K}(H_i) \notin \{2, 3, 7, 8, 12, 13, 17, 18\}$, compute all possibilities $\sum_{i=1}^{5} \binom{22-\mathcal{K}(H_i)}{2}$, cf. the proof of Lemma 9.14.

EXERCISE 9.3 Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$. Use the approach of the proof of Lemma 9.22 to show $a_5 = 0$.

Bibliography

[1] Erik Agrell. Voronoi regions for binary linear block codes. *IEEE Transactions on Information Theory*, 42(1):310–316, 1996.

[2] Erik Agrell. On the Voronoi neighbor ratio for binary linear block codes. *IEEE Transactions on Information Theory*, 44(7):3064–3072, 1998.

[3] Erik Agrell, Alexander Vardy, and Kenneth Zeger. Upper bounds for constant-weight codes. *IEEE Transactions on Information Theory*, 46(7):2373–2395, 2000.

[4] Rudolf Ahlswede and Haratyun Aydinian. On error control codes for random network coding. In *Network Coding, Theory, and Applications, 2009. NetCod'09. Workshop on*, pages 68–73. IEEE, 2009.

[5] Adel Alahmadi, Robert EL Aldred, Romar de la Cruz, Patrick Solé, and Carsten Thomassen. The maximum number of minimal codewords in an $[n, k]$-code. *Discrete Mathematics*, 313(15):1569–1574, 2013.

[6] Clementa Alonso-González, Miguel Ángel Navarro-Pérez, and Xaro Soler-Escrivà. Flag codes from planar spreads in network coding. *arXiv preprint 2004.14867*, 2020.

[7] Alexei Ashikhmin and Alexander Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 1998.

[8] Christine Bachoc. Semidefinite programming, harmonic analysis and coding theory. *arXiv preprint 0909.4767*, 2009.

[9] Christine Bachoc, Dion C Gijswijt, Alexander Schrijver, and Frank Vallentin. Invariant semidefinite programs. In *Handbook on semidefinite, conic and polynomial optimization*, pages 219–269. Springer, 2012.

[10] Christine Bachoc, Alberto Passuello, and Frank Vallentin. Bounds for projective codes from semidefinite programming. *Advances in Mathematics of Communications*, 7(2):127, 2013.

[11] Christine Bachoc, Alberto Passuello, and Frank Vallentin. Bounds for projective codes from semidefinite programming. *Advances in Mathematics of Communications*, 7(2):127–145, 2013.

[12] Simeon Ball. On intersection sets in Desarguesian affine spaces. *European Journal of Combinatorics*, 21(4):441–446, 2000.

[13] Simeon Ball. On the graph of a function in many variables over a finite field. *Designs, Codes and Cryptography*, 47(1-3):159–164, 2008.

[14] Simeon Ball, Ray Hill, Ivan Landjev, and Harold Ward. On $\left(q^2+q+2, q+2\right)$-arcs in the projective plane $\mathrm{PG}(2,q)$. *Designs, Codes and Cryptography*, 24(2):205–224, 2001.

[15] Wolf Barth. Two projective surfaces with many nodes, admitting the symmetries of the icosahedron. *Journal of Algebraic Geometry*, 5(1):173–186, 1996.

[16] A. B. Basset. The maximum number of double points on a surface. *Nature*, 73:246, 1906.

[17] L.D. Baumert and R.J. McEliece. A note on the Griesmer bound (corresp.). *IEEE Transactions on Information Theory*, 19(1):134–135, 1973.

[18] Albrecht Beutelspacher. Partial spreads in finite projective spaces and partial designs. *Mathematische Zeitschrift*, 145(3):211–229, 1975.

[19] Aart Blokhuis. On the size of a blocking set in $\mathrm{PG}(2,p)$. *Combinatorica*, 14(1):111–114, 1994.

[20] Aart Blokhuis, Andries E Brouwer, and Henny A Wilbrink. Blocking sets in $\mathrm{PG}(2,p)$ for small p, and partial spreads in $\mathrm{PG}(3,7)$. *Advances in Geometry*, pages 245–253, 2003.

[21] Aart Blokhuis, A Seress, and HA Wilbrink. On sets of points in $\mathrm{PG}(2,q)$ without tangents. *Mitteilungen aus dem Mathematischem Seminar Giessen*, 201:39–44, 1991.

[22] Aart Blokhuis, Tamás Szőnyi, and Zsuzsa Weiner. On sets without tangents in galois planes of even order. *Designs, Codes and Cryptography*, 29(1-3):91–98, 2003.

[23] Raj C Bose and Katherine A Bush. Orthogonal arrays of strength two and three. *The Annals of Mathematical Statistics*, pages 508–524, 1952.

[24] Iliya Bouyukliev, Stefka Bouyuklieva, and Sascha Kurz. Computer classification of linear codes. *arXiv preprint 2002.07826*, 2020.

[25] Iliya Bouyukliev and David B Jaffe. Optimal binary linear codes of dimension at most seven. *Discrete Mathematics*, 226(1-3):51–70, 2001.

[26] Iliya Bouyukliev, David B Jaffe, and Vesselin Vavrek. The smallest length of eight-dimensional binary linear codes with prescribed minimum distance. *IEEE Transactions on Information Theory*, 46(4):1539–1544, 2000.

[27] Alfred Brauer. On a problem of partitions. *American Journal of Mathematics*, 64(1):299–312, 1942.

[28] Michael Braun, Tuvi Etzion, Patric R. J. Östergård, Alexander Vardy, and Alfred Wassermann. Existence of q-analogs of Steiner systems. *Forum of Mathematics, Pi*, 4, 2016.

[29] Andries E. Brouwer and Marijn van Eupen. The correspondence between projective codes and 2-weight codes. *Designs, Codes and Cryptography*, 11(3):261–266, 1997.

[30] Marco Buratti, Michael Kiermaier, Sascha Kurz, Anamari Nakić, and Alfred Wassermann. q-analogs of group divisible designs. In *Combinatorics and Finite Fields : Difference Sets, Polynomials, Pseudorandomness and Applications*, volume 23 of *Radon Series on Computational and Applied Mathematics*. De Gruyter, Berlin, 2019.

[31] Robert Calderbank and William M Kantor. The geometry of two-weight codes. *Bulletin of the London Mathematical Society*, 18(2):97–122, 1986.

[32] Fabrizio Catanese and Fabio Tonoli. Even sets of nodes on sextic surfaces. *Journal of the European Mathematical Society (JEMS)*, 9(4):705–737, 2007.

[33] Hervé Chabanne, Gérard Cohen, and Alain Patey. Towards secure two-party computation from the wire-tap channel. In *International Conference on Information Security and Cryptology*, pages 34–46. Springer, 2013.

[34] Hao Chen, Xianmang He, Jian Weng, and Liqing Xu. New constructions of subspace codes using subsets of MRD codes in several blocks. *arXiv preprint 1908.03804*, 2019.

[35] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pages 41–50. IEEE, 1995.

[36] Antonio Cossidente, Sascha Kurz, Giuseppe Marino, and Francesco Pavese. Combining subspace codes. *arXiv preprint 1911.03387*, 2019.

[37] Rumen N Daskalov and T Aaron Gulliver. Bounds on minimum distance for linear codes over $\mathrm{GF}(5)$. *Applicable Algebra in Engineering, Communication and Computing*, 9(6):547–558, 1999.

[38] Jan De Beule, Jeroen Demeyer, Sam Mattheus, and Péter Sziklai. On the cylinder conjecture. *Designs, Codes and Cryptography*, 87(4):879–893, 2019.

[39] Romar de la Cruz, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. On the minimum number of minimal codewords. *arXiv preprint 1912.09804*, 2019.

[40] Philippe Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.

[41] Philippe Delsarte and Vladimir I. Levenshtein. Association schemes and coding theory. *IEEE Transactions on Information Theory*, 44(6):2477–2504, 1998.

[42] Luis Armando Dissett. *Combinatorial and computational aspects of finite geometries*. PhD thesis, National Library of Canada= Bibliothèque nationale du Canada, 2000.

[43] Stefan Dodunekov and Juriaan Simonis. Codes and projective multisets. *The electronic Journal of Combinatorics*, 5(1):23. pp, 1998. research paper 37.

[44] György Dósa, István Szalkai, Claude Laflamme, et al. The maximum and minimum number of circuits and bases of matroids. *Pure Mathematics and Applications*, 15(4):383–392, 2004.

[45] D.A. Drake and J.W. Freeman. Partial t-spreads and group constructible (s, r, μ)-nets. *Journal of Geometry*, 13(2):210–216, 1979.

[46] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence. The maximum size of a partial 3-spread in a finite vector space over $GF(2)$. *Designs, Codes and Cryptography*, 54(2):101–107, 2010.

[47] Tuvi Etzion. Covering of subspaces by subspaces. *Designs, Codes and Cryptography*, 72(2):405–421, 2014.

[48] Tuvi Etzion, Sascha Kurz, Kamil Otal, and Ferruh Özbudak. Subspace packings. In *The Eleventh International Workshop on Coding and Cryptography 2019 : WCC Proceedings*. Saint-Jacut-de-la-Mer, 2019.

[49] Tuvi Etzion, Sascha Kurz, Kamil Otal, and Ferruh Özbudak. Subspace packings: constructions and bounds. *Designs, Codes and Cryptography*, 88:1781–1810, 2020.

[50] Tuvi Etzion and Natalia Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Transactions on Information Theory*, 55(7):2909–2919, 2009.

[51] Tuvi Etzion and Natalia Silberstein. Codes and designs related to lifted MRD codes. *IEEE Transactions on Information Theory*, 59(2):1004–1017, 2012.

[52] Tuvi Etzion and Alexander Vardy. Error-correcting codes in projective space. *IEEE Transactions on Information Theory*, 57(2):1165–1173, 2011.

[53] Arman Fazeli, Alexander Vardy, and Eitan Yaakobi. PIR with low storage overhead: coding instead of replication. *arXiv preprint 1505.06241*, 2015.

[54] Tao Feng, Sascha Kurz, and Shuangqing Liu. Bounds for the multilevel construction. *arXiv preprint 2011.06937*, 2020.

[55] Thomas Feulner. Classification and nonexistence results for linear codes with prescribed minimum distances. *Designs, Codes and Cryptography*, 70(1-2):127–138, 2014.

[56] Heide Gluesing-Luerssen and Carolyn Troha. Construction of subspace codes through linkage. *Advances in Mathematics of Communications*, 10(3):525–540, 2016.

[57] James H. Griesmer. A bound for error-correcting codes. *IBM Journal of Research and Development*, 4(5):532–542, 1960.

[58] Xianmang He. Construction of constant dimension code from two parallel versions of linkage construction. *arXiv preprint 1910.04472*, 2019.

[59] Xianmang He and Yindong Chen. Construction of constant dimension codes from several parallel lifted MRD code. *arXiv preprint 1911.00154*, 2019.

[60] Xianmang He, Yindong Chen, Kunxiao Zhou, and Jianguang Deng. A hierarchical-based greedy algorithm for echelon-Ferrers construction. *arXiv preprint 1911.00508*, 2019.

[61] Olof Heden. On the length of the tail of a vector space partition. *Discrete Mathematics*, 309(21):6169–6180, 2009.

[62] Olof Heden. A survey of the different types of vector space partitions. *Discrete Mathematics, Algorithms and Applications*, 4(01):1250001, 2012.

[63] Daniel Heinlein. New LMRD code bounds for constant dimension codes and improved constructions. *IEEE Transactions on Information Theory*, 65(8):4822–4830, 2019.

[64] Daniel Heinlein, Thomas Honold, Michael Kiermaier, and Sascha Kurz. Generalized vector space partitions. *Australasian Journal of Combinatorics*, 73(1):162–178, 2019.

[65] Daniel Heinlein, Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. Projective divisible binary codes. In *The Tenth International Workshop on Coding and Cryptography*, pages 1–10, 2017. arXiv preprint 1703.08291.

[66] Daniel Heinlein, Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. Classifying optimal binary subspace codes of length 8, constant dimension 4 and minimum distance 6. *Designs, Codes and Cryptography*, 87(2-3):375–391, 2019.

[67] Daniel Heinlein, Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. On projective q^r-divisible codes. *arXiv preprint 1912.10147*, 2019.

[68] Daniel Heinlein, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. Tables of subspace codes. *arXiv preprint 1601.02864*, 2016.

[69] Daniel Heinlein, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. A subspace code of size 333 in the setting of a binary q-analog of the Fano plane. *Advances in Mathematics of Communications*, 13(3), 2019.

[70] Daniel Heinlein and Sascha Kurz. Asymptotic bounds for the sizes of constant dimension codes and an improved lower bound. In *International Castle Meeting on Coding Theory and Applications*, pages 163–191. Springer, 2017.

[71] Daniel Heinlein and Sascha Kurz. Coset construction for subspace codes. *IEEE Transactions on Information Theory*, 63(12):7651–7660, 2017.

[72] Daniel Heinlein and Sascha Kurz. Binary subspace codes in small ambient spaces. *Advances in Mathematics of Communications*, 12(4):817, 2018.

[73] Marcel Herzog and Jochanan Schönheim. Group partition, factorization and the vector covering problem. *Canadian Mathematical Bulletin*, 15(2):207–214, 1972.

[74] R. Hill and D.E. Newton. Some optimal ternary linear codes. *Ars Combinatoria*, 25:61–72, 1988.

[75] James Hirschfeld. *Projective geometries over finite fields*. Oxford University Press, 1998.

[76] Tracey Ho, Muriel Médard, Ralf Koetter, David R Karger, Michelle Effros, Jun Shi, and Ben Leong. A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, 52(10):4413–4430, 2006.

[77] Thomas Honold, Michael Kiermaier, and Sascha Kurz. Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4. *Topics in finite fields*, 632:157–176, 2015.

[78] Thomas Honold, Michael Kiermaier, and Sascha Kurz. Constructions and bounds for mixed-dimension subspace codes. *Advances in Mathematics of Communications*, 10(3):649, 2016.

[79] Thomas Honold, Michael Kiermaier, and Sascha Kurz. Partial spreads and vector space partitions. In *Network Coding and Subspace Designs*, pages 131–170. Springer, 2018.

[80] Thomas Honold, Michael Kiermaier, and Sascha Kurz. Classification of large partial plane spreads in $\operatorname{PG}(6,2)$ and related combinatorial objects. *Journal of Geometry*, 110(1):1–31, 2019.

[81] Thomas Honold, Michael Kiermaier, and Sascha Kurz. Johnson type bounds for mixed dimension subspace codes. *The Electronic Journal of Combinatorics*, pages P3–39, 2019.

[82] Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. The lengths of projective triply-even binary codes. *IEEE Transactions on Information Theory*, 66(5):2713–2716, 2019.

[83] Anna-Lena Horlemann-Trautmann and Joachim Rosenthal. Constructions of constant dimension codes. In *Network Coding and Subspace Designs*, pages 25–42. Springer, 2018.

[84] Tai-Yang Hwang. Decoding linear block codes for minimizing word error rate (corresp.). *IEEE Transactions on Information Theory*, 25(6):733–737, 1979.

[85] David B Jaffe. A brief tour of split linear programming. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 164–173. Springer, 1997.

[86] David B. Jaffe and Daniel Ruberman. A sextic surface cannot have 66 nodes. *Journal of Algebraic Geometry*, 6(1):151–168, 1997.

[87] Selmer Johnson. A new upper bound for error-correcting codes. *IRE Transactions on Information Theory*, 8(3):203–207, 1962.

[88] Fatemeh Kazemi, Sascha Kurz, and Emina Soljanin. A geometric view of the service rates of codes problem and its application to the service rate of the first order Reed-Muller codes. *arXiv preprint 2001.09121*, 2020.

[89] A. Khaleghi, D. Silva, and F.R. Kschischang. Subspace codes. In *IMA International Conference on Cryptography and Coding*, pages 1–21. Springer, 2009.

[90] Michael Kiermaier and Sascha Kurz. On the lengths of divisible codes. *IEEE Transactions on Information Theory*, 66(7):4051–4060, 2020.

[91] Michael Kiermaier, Sascha Kurz, Patrick Solé, Michael Stoll, and Alfred Wassermann. On strongly walk regular graphs, triple sum sets and their codes. *arXiv preprint 2012.06160*, 2020.

[92] Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. The order of the automorphism group of a binary q-analog of the Fano plane is at most two. *Designs, Codes and Cryptography*, 86(2):239–250, 2018.

[93] Ralf Koetter and Frank R Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information theory*, 54(8):3579–3591, 2008.

[94] Axel Kohnert and Sascha Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In *Mathematical methods in computer science*, pages 31–42. Springer, 2008.

[95] S. Kurz. Packing vector spaces into vector spaces. *The Australasian Journal of Combinatorics*, 68(1):122–130, 2017.

[96] Sascha Kurz. Improved upper bounds for partial spreads. *Designs, Codes and Cryptography*, 85(1):97–106, 2017.

[97] Sascha Kurz. Hedens bound on the tail of a vector space partition. *Discrete Mathematics*, 341(12):3447–3452, 2018.

[98] Sascha Kurz. Lincode – computer classification of linear codes. *arXiv preprint 1912.09357*, 2019.

[99] Sascha Kurz. A note on the linkage construction for constant dimension codes. *arXiv preprint 1906.09780*, 2019.

[100] Sascha Kurz. Bounds for flag codes. *arXiv preprint 2005.04768*, 2020.

[101] Sascha Kurz. Classification of 8-divisible binary linear codes with minimum distance 24. *arXiv preprint 2012.06163*, 2020.

[102] Sascha Kurz. Classification of indecomposable 2^r-divisible codes spanned by by codewords of weight 2^r. *arXiv preprint 2011.05872*, 2020.

[103] Sascha Kurz. Designing codes for storage allocation, Dezember 2020.

[104] Sascha Kurz. Generalized LMRD code bounds for constant dimension codes. *IEEE Communications Letters*, 24(10):2100–2103, 2020.

[105] Sascha Kurz. Lifted codes and the multilevel construction for constant dimension codes. *arXiv preprint 2004.14241*, 2020.

[106] Sascha Kurz. No projective 16-divisible binary linear code of length 131 exists. *arXiv preprint 2006.10382*, 2020.

[107] Sascha Kurz. A note on the growth of the dimension in complete simple games. *arXiv preprint 2006.05193*, 2020.

[108] Sascha Kurz. On the number of minimal codewords in codes generated by the adjacency matrix of a graph. *arXiv preprint arXiv:2006.02975*, 2020.

[109] Sascha Kurz. The $[46, 9, 20]_2$ code is unique. *Advances in Mathematics of Communications*, to appear. doi:10.3934/amc.2020074.

[110] Sascha Kurz, Xavier Molinero, Martin Olsen, and Maria Serna. Dimension and codimension of simple games. *Electronic Notes in Discrete Mathematics*, 55:147–150, 2016.

[111] Sascha Kurz and Stefan Napel. Dimension of the Lisbon voting rules in the EU council: a challenge and new world record. *Optimization Letters*, 10(6):1245–1256, 2016.

[112] Sascha Kurz and Eitan Yaakobi. PIR codes with short block length. *arXiv preprint 2001.03433*, 2020.

[113] Ivan Landgev. The geometry of $(n, 3)$-arcs in the projective plane of order 5. In *Fifth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 1996), June 1-7, 1996, Sozopol, Bulgaria*, pages 170–175, 1996.

[114] Ivan Landgev and Assia Rousseva. Optimal linear codes over $\mathbb{F}_5$. In *Seventh International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2000) , June 18-24, 2000, Bansko, Bulgaria*, pages 207–212, 2000.

[115] I Landjev, Assya Rousseva, Tatsuya Maruta, and Ray Hill. On optimal codes over the field with five elements. *Designs, Codes and Cryptography*, 29(1-3):165–175, 2003.

[116] Ivan Landjev and Assia Rousseva. The non-existence of $(104, 22; 3, 5)$-arcs. *Advances in Mathematics of Communications*, 10(3):601, 2016.

[117] Ivan Landjev and Assia Rousseva. On the characterization of $(3 \mod 5)$ arcs. *Electronic Notes in Discrete Mathematics*, 57:187–192, 2017.

[118] Ivan Landjev and Assia Rousseva. Divisible arcs, divisible codes, and the extension problem for arcs and codes. *Problems of Information Transmission*, 55(3):226–240, 2019.

[119] Ivan Landjev, Assia Rousseva, and Leo Storme. On the extendability of quasidivisible griesmer arcs. *Designs, Codes and Cryptography*, 79(3):535–547, 2016.

[120] Huimin Lao, Hao Chen, Jian Weng, and Xiaoqing Tan. Parameter-controlled inserting constructions of constant dimension subspace codes. *arXiv preprint 2008.09944*, 2020.

[121] Michel Lavrauw and Geertrui Van de Voorde. Field reduction and linear sets in finite geometry. In *Topics in finite fields*, volume 632 of *Contemp. Math.*, pages 271–293. Amer. Math. Soc., Providence, RI, 2015.

[122] Dirk Liebhold, Gabriele Nebe, and Ángeles Vazquez-Castro. Network coding with flags. *Designs, Codes and Cryptography*, 86(2):269–284, 2018.

[123] Dirk Liebhold, Gabriele Nebe, and María Ángeles Vázquez-Castro. Generalizing subspace codes to flag codes using group actions. In *Network Coding and Subspace Designs*, pages 67–89. Springer, 2018.

[124] VN Logacev. An improvement of the griesmer bound in the case of small code distances. In *Optimization Methods and Their Applications*, pages 107–111. 182 Sibirsk. Energet. Inst., Sibirsk. Otdel. Akad. Nauk SSSR, 1974.

[125] L Lovász and A Schrijver. Remarks on a theorem of Rédei. *Studia Scient. Math. Hungar*, 16(449-454):15–32, 1981.

[126] Florence Jessie MacWilliams. A theorem on the distribution of weights in a systematic code. *Bell System Technical Journal*, 42(1):79–94, 1963.

[127] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.

[128] Tatsuya Maruta. A new extension theorem for linear codes. *Finite Fields and Their Applications*, 10(4):674–685, 2004.

[129] James L Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279. Citeseer, 1993.

[130] Esmeralda Năstase and Papa Sissokho. The maximum size of a partial spread in a finite projective space. *Journal of Combinatorial Theory. Series A*, 152:353–362, 2017.

[131] Liam O'Dwyer and Arkadii Slinko. Growth of dimension in complete simple games. *Mathematical Social Sciences*, 90:2–8, 2017.

[132] Martin Olsen, Sascha Kurz, and Xavier Molinero Albareda. On the construction of high dimensional simple games. In *ECAI 2016: 22nd European Conference on Artificial Intelligence: 29 August–2 September 2016, The Hague, The Netherlands: proceedings*, pages 880–885. IOS Press, 2016.

[133] Kjell Fredrik Pettersen. *On nodal determinantal quartic hypersurfaces in* $\mathbb{P}^4$. PhD thesis, University of Oslo, 1998.

[134] Vera Pless. Power moment identities on weight distributions in error correcting codes. *Information and Control*, 6(2):147–152, 1963.

[135] László Rédei. *Lückenhafte Polynome über endlichen Körpern*, volume 42 of *Lehrbücher und Monographien auf dem Gebiet der exakten Wissenschaften.* Birkhäuser Verlag, 1970.

[136] Assia Rousseva. On the structure of $(t \mod q)$-arcs in finite projective geometries. *Annuaire de l'Univ. de Sofia*, 102, 2015.

[137] Beniamino Segre. Teoria di galois, fibrazioni proiettive e geometrie non desarguesiane. *Annali di Matematica Pura ed Applicata*, 64(1):1–76, 1964.

[138] John Sheekey. MRD codes: Constructions and connections. In *Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications*, volume 23, pages 255–286. de Gruyter, 2019.

[139] Natalia Silberstein and Anna-Lena Trautmann. Subspace codes based on graph matchings, Ferrers diagrams, and pending blocks. *IEEE Transactins on Information Theory*, 61(7):3937–3953, 2015.

[140] Danilo Silva and Frank R Kschischang. On metrics for error correction in network coding. *IEEE Transactions on Information Theory*, 55(12):5479–5490, 2009.

[141] Danilo Silva, Frank R. Kschischang, and Ralf Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, 2008.

[142] Juriaan Simonis. MacWilliams identities and coordinate partitions. *Linear Algebra and its Applications*, 216:81–91, 1995.

[143] D. Slepian. Some further theory of group codes. *Bell System Technical Journal*, 39(5):1219–1252, 1960.

[144] Gustave Solomon and Jack J. Stiffler. Algebraically punctured cyclic codes. *Information and Control*, 8(2):170–179, 1965.

[145] Vladimir D. Tonchev. Codes and designs. *Handbook of Coding Theory*, 2:1229–1267, 1998.

[146] Geertrui Van de Voorde. On sets without tangents and exterior sets of a conic. *arXiv preprint 1201.0484*, 2012.

[147] Henk Van Tilborg. On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound. *Information and control*, 44(1):16–35, 1980.

[148] Henk CA van Tilborg. A proof of the nonexistence of a binary $(55, 7, 26)$ code. TH-Report 79-WSK-09, Technische Hogeschool Eindhoven, 1979.

[149] CA van Tilborg Henk. The smallest length of binary 7–dimensional linear codes with prescribed minimum distance. *Discrete Mathematics*, 33(2):197–207, 1981.

[150] Huaxiong Wang, Chaoping Xing, and Reihaneh Safavi-Naini. Linear authentication codes: bounds and constructions. *IEEE Transactions on Information Theory*, 49(4):866–872, 2003.

[151] Harold Ward. Divisible codes – a survey. *Serdica Mathematical Journal*, 27(4):263p–278p, 2001.

[152] Harold N. Ward. Divisible codes. *Archiv der Mathematik*, 36(1):485–494, 1981.

[153] Harold N. Ward. A bound for divisible codes. *IEEE Transactions on Information Theory*, 38(1):191–194, 1992.

[154] Harold N. Ward. Divisibility of codes meeting the Griesmer bound. *Journal of Combinatorial Theory Series A*, 83(1):79–93, 1998.

[155] Shu-Tao Xia and Fang-Wei Fu. Johnson type bounds on constant dimension codes. *Designs, Codes and Cryptography*, 50(2):163–172, 2009.

[156] Liqing Xu and Hao Chen. New constant–dimension subspace codes from maximum rank distance codes. *IEEE Transactions on Information Theory*, 64(9):6315–6319, 2018.

10. Lengths of projective divisible codes

This chapter is based on [79, 65, 67]. Here we want to follow up Chapter 5 and ask for the possible length of projective q^r-divisible codes or q^r-divisible sets. Mostly we will assume that r is an integer.

LEMMA 10.1

If there are projective q^r-divisible arcs of cardinalities n_1 and n_2 over $\mathbb{F}_q$, then there is a projective q^r-divisible arc of cardinality $n_1 + n_2$ over $\mathbb{F}_q$.

PROOF. Let $\mathcal{K}_1$ be a projective q^r-divisible arc in $\operatorname{PG}(v_1 - 1, q)$ and $\mathcal{K}_2$ be a projective q^r-divisible arc in $\operatorname{PG}(v_2 - 1, q)$. Now let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the corresponding codes with generator matrices G_1 and G_2. With this, we construct a code $\mathcal{C}$ with generator matrix

$$\begin{pmatrix} G_1 & \mathbf{0} \\ \mathbf{0} & G_2 \end{pmatrix}.$$

Clearly $\mathcal{C}$ is q^r-divisible, projective, and has effective length $n_1 + n_2$. So, the corresponding arc $\mathcal{K}$ in $\operatorname{PG}(v_1 + v_2 - 1, q)$ is projective, q^r-divisible, and has cardinality $n_1 + n_2$. □

Lemma 6.5 excludes quite some values. We start by analyzing the right side of the corresponding interval. First we note that examples of q^r-divisible sets of cardinality $m \cdot \left[{r+1 \atop 1}\right]_q$ can be obtained from $(r+1)$-spaces, if $r \in \mathbb{N}_0$, for all $m \in \mathbb{N}_{>0}$. If m is not too large, then cardinalities one less are impossible.

LEMMA 10.2

For $1 \le m \le \left\lfloor \sqrt{(q-1)q\Delta} - q + \frac{3}{2} \right\rfloor$, we have

$$(q-1)(n - m\Delta) - (m - q/2)\Delta + \frac{1}{2} \le \frac{1}{2} \cdot \sqrt{q^2\Delta^2 - 4qm\Delta + 2q\Delta + 1},$$

where $n = m \cdot \left[{r+1 \atop 1}\right]_q - 1$ and $\Delta = q^r$.

PROOF. Plugging in and simplifying yields

$$q\Delta + 3 - 2m - 2q \le \sqrt{q^2\Delta^2 - (4m-2)q\Delta + 1},$$

so that squaring and simplifying gives $m \le \sqrt{(q-1)q\Delta} - q + \frac{3}{2}$. □

THEOREM 10.3 [79, Theorem 11]
Let $\mathcal{K}$ be a projective q^1-divisible arc in $\operatorname{PG}(v-1,q)$ *with cardinality n. If $2 \le n = |\mathcal{C}| \le q^2$, then either $n = q^2$ or $q+1$ divides n. Additionally, the non-excluded cases can be realized.*

PROOF. First we show $n \notin [(m-1)(q+1)+2, m(q+1)-1]$ for $1 \le m \le q-1$. To this end, we apply Lemma 6.5 to deduce $\tau_q(u,q,m) \le 0$ for $m+1-q \le u \le m-1$, so that the statement follows from Corollary 6.4. For $u \ge m+1-q$ we have

$$\begin{aligned}(q-1)u-(m-q/2)\Delta+\frac{1}{2} &\ge -\frac{1}{2}\cdot\left(q^2-4q+1+2m\right)\\ &\ge -\frac{1}{2}\cdot\left(q^2-2m-3\right)\\ &\ge -\frac{1}{2}\cdot\sqrt{q^4-4mq^2+2q^2+1}\\ &= -\frac{1}{2}\cdot\sqrt{q^2\Delta^2-4qm\Delta+2q\Delta+1}\end{aligned}$$

and for $u \le m-1$ we have

$$\begin{aligned}(q-1)u-(m-q/2)\Delta+\frac{1}{2} &\le \frac{1}{2}\cdot\left(q^2-2m-2q+3\right)\\ &\overset{\star}{\le} \frac{1}{2}\cdot\sqrt{q^4-4mq^2+2q^2+1}\\ &= \frac{1}{2}\cdot\sqrt{q^2\Delta^2-4qm\Delta+2q\Delta+1}.\end{aligned}$$

With respect to the estimation $\star$, we remark that

$$-4q^3+8q^2-12q+8+4m(m+2q-3) \overset{m\le q-1}{\le} -4(q-1)(q^2-4q+6) \overset{q\ge 2}{\le} 0.$$

Applying Corollary 6.2 with $u = m+1$ and $\Delta = q$ yields $n \ne m(q+1)+1$ for all $1 \le m \le q-2$. A line is a q-divisible set $\mathcal{K}$ of cardinality $q+1$ and due to Lemma 10.1 all multiples of $q+1$ can be realized. An affine plane yields a q-divisible set of cardinality q^2 in $\operatorname{PG}(2,q)$. □

We remark that there exists a q^1-divisible set of cardinality q^2+1 for all $q \ge 2$ (given by ovoids for $q \ge 3$ and a projective base for $q = 2$).

THEOREM 10.4 [79, Theorem 12]
For the cardinality n of a projective q^r-divisible arc $\mathcal{K}$ in $\operatorname{PG}(v-1,q)$*, where $r \in \mathbb{N}$, we have*

$$n \notin \left[(a(q-1)+b)\begin{bmatrix}r+1\\1\end{bmatrix}_q + a+1, (a(q-1)+b+1)\begin{bmatrix}r+1\\1\end{bmatrix}_q - 1\right],$$

where $a, b \in \mathbb{N}_0$ with $b \le q-2$ and $a \le r-1$. If $n \le rq^{r+1}$, then all other cases can be realized.

PROOF. Combinations of $(r+1)$-spaces and affine $(r+2)$-spaces give a construction of a q^r-divisible set with cardinality n iff there exists an integer $m \in \mathbb{N}_{>0}$ with $(m-1)\cdot\left[{r+1 \atop 1}\right]_q \le n \le (m-1)\cdot\left[{r+1 \atop 1}\right]_q + \left\lfloor \frac{m-1}{q-1} \right\rfloor$. It remains to exclude the stated cases. We prove by induction on r, set $\Delta = q^r$, and write $n = (m-1)\left[{r+1 \atop 1}\right]_q + x$, where $a+1 \le x \le \left[{r+1 \atop 1}\right]_q - 1$ and $m-1 = a(q-1)+b$ for integers $0 \le b \le q-2$, $0 \le a \le r-1$.

The induction start $r = 1$ is given by Theorem 10.3.

Now, assume $r \ge 2$. From the induction hypothesis we conclude that for $0 \le b' \le q-2$, $0 \le a' \le r-2$ we have

$$n' \notin \left[(a'(q-1)+b')\begin{bmatrix} r \\ 1\end{bmatrix}_q + a' + 1, (a'(q-1)+b'+1)\begin{bmatrix} r \\ 1\end{bmatrix}_q - 1\right]$$

for the cardinality n' of a q^{r-1}-divisible set. If $a \le r-2$ and $x \le \left[{r \atop 1}\right]_q - 1$, then $b' = b$, $a' = a$ yields $\mathcal{T}(\mathcal{C}) \subseteq \{u, u+\Delta, \dots, u+(m-2)\Delta\}$ for $u = \Delta + (m-1)\left[{r \atop 1}\right]_q + x$. We compute

$$(q-1)u = q^{r+1} - q^r + (m-1)q^r - (m-1) + (q-1)x \overset{x \ge a+1}{\ge} (m-2)q^r + q^{r+1} > (m-2)\Delta,$$

so that we can apply Corollary 6.2. If $a = r-1$ and $a+1 \le x \le \left[{r \atop 1}\right]_q - 1$, then $b' = b$, $a' = a-1$ yields $\mathcal{T}(\mathcal{C}) \subseteq \{u, u+\Delta, \dots, u+(m-1)\Delta\}$ for $u = (m-1)\left[{r \atop 1}\right]_q + x$. We compute $(q-1)u = (m-1)q^r - (m-1) + x(q-1) > (m-1)\Delta$ using $x \ge a+1$, so that we can apply Corollary 6.2. Thus, we can assume $\left[{r \atop 1}\right]_q \le x \le \left[{r+1 \atop 1}\right]_q - 1$ in the remaining part. Additionally we have $m \le r(q-1)$.

We aim to apply Lemma 6.5. Due to Lemma 10.2 for the upper bound of the interval it suffices to show

$$r(q-1) \le \left\lfloor \sqrt{(q-1)q\Delta} - q + \frac{3}{2} \right\rfloor.$$

For $q = 2$ the inequality is equivalent to $r \le \left\lfloor \sqrt{2^{r+1}} - \frac{1}{2} \right\rfloor$, which is valid for $r \ge 2$. Since the right hand side is larger then $(q-1)(\sqrt{\Delta}-1)$, it suffices to show $q^{r/2} - 1 \ge r$, which is valid for $q \ge 3$ and $r \ge 2$. For the left hand side of the interval if suffices to show

$$(q-1)(n-m\Delta) - (m-q/2)\Delta + \frac{1}{2} \ge -\frac{1}{2}\cdot\sqrt{(\Delta q)^2 - (4m-2)\Delta q + 1},$$

which can be simplified to

$$\Delta q + 2m - 3 - 2(q-1)x \le \sqrt{(\Delta q)^2 - (4m-2)\Delta q + 1}$$

using $n = (m-1)\left[{r+1 \atop 1}\right]_q + x$. Since $(q-1)x \ge q^r - 1$ and $m \le r(q-1)$ it suffices to show

$$-\Delta^2 + 2rq\Delta - 2r\Delta - \Delta - r + r^2q - r^2 \le 0. \tag{10.1}$$

For $q = 2$ this inequality is equivalent to $-2^{2r} + r2^{r+1} + r^2 - 2 - 2^r \le 0$, which is valid for $r \ge 2$. For $r = 2$ Inequality (10.1) is equivalent to $-q^4 + 4q^3 - 4q^2 - q^2 + 4q - 6$, which is valid for $q \in \{2,3\}$ and $q \ge 4$. For $q \ge 3$ and $r \ge 3$ we have $\Delta \ge 3rq$, so that Inequality (10.1) is satisfied. □

In other words Theorem 10.4 says that the cardinality n of a q^r-divisible set can be written as $a\left[{r+1 \atop 1}\right]_q+bq^{r+1}$ for some $a, b \in \mathbb{N}_0$ if $n \le rq^{r+1}$.

For $r = 1$ the required example of cardinality $n = rq^{r+1}$ is given by an ovoid for $q \ge 3$ and by a projective base for $q = 2$. For $r = 2$ our current knowledge is rather sparse. For $q = 2$ we know three isomorphism types of 2^2-divisible sets of cardinality $n = 17$. For $q = 3$ we know an example of cardinality $n = 55$ given by a shortening the Hill cap. For $q = 4$ we do not know a 4^2-divisible set of cardinality $n = 129$ so far.

LEMMA 10.5

Let $\mathcal{K}$ be a projective 2^1-divisible arc in $\mathrm{PG}(v-1, 2)$. If $\#\mathcal{K} = n$, then $n \ge 3$ and all cases can be realized.

PROOF. The values $n \in \{1, 2\}$ are excluded by Theorem 10.3. For examples with $n \in \{3, 4, 5\}$ we refer to [79], so that Lemma 10.1 provides examples for the mentioned cases. □

LEMMA 10.6

Let $\mathcal{K}$ be a projective 2^2-divisible arc in $\mathrm{PG}(v-1, 2)$. If $\#\mathcal{K} = n$, then $n \in \{7, 8\}$ or $n \ge 14$ and all mentioned cases can be realized.

PROOF. The cases $1 \le n \le 6$ and $9 \le n \le 13$ are excluded by Theorem 10.4. For examples with $n \in \{7, 8, 15, \ldots, 20\}$ we refer to [79], so that Lemma 10.1 provides examples for the mentioned cases. □

LEMMA 10.7

Let $\mathcal{K}$ be a projective 2^3-divisible arc in $\mathrm{PG}(v-1, 2)$. If $\#\mathcal{K} = n$, then

$$n \in \{15, 16, 30, 31, 32, 45, 46, 47, 48, 49, 50, 51\}$$

or $n \ge 60$ and all cases can be realized.

PROOF. The cases $1 \le n \le 14$, $17 \le n \le 29$, and $33 \le n \le 44$ are excluded by Theorem 10.4. The case $n = 52$ is excluded by Corollary 6.9 with $t = 3$, see also Lemma 6.7. The cases $53 \le n \le 58$ are excluded by Lemma 6.3 using $m = 4$. The special case $n = 59$ is treated in [82].

For examples with $n \in \{15, 16, 49, 50, 51, 63, \ldots, 74\}$ we refer to [79], so that Lemma 10.1 provides examples for the mentioned cases. □

LEMMA 10.8

Let $\mathcal{K}$ be a projective 3^1-divisible arc in $\mathrm{PG}(v-1, 3)$. If $\#\mathcal{K} = n$, then $n = 4$ or $n \ge 8$ and all cases can be realized.

PROOF. The values $1 \le n \le 3$ and $5 \le n \le 7$ are excluded by Theorem 10.3. For examples with $n \in \{4, 9, 10, 11\}$ we refer to [79], so that Lemma 10.1 provides examples for the mentioned cases. □

LEMMA 10.9

Let $\mathcal{K}$ be a projective 4^1-divisible arc in $\operatorname{PG}(v-1,4)$. *If $\#\mathcal{K} = n$, then*

$$n \in \{5, 10, 15, 16, 17\}$$

or $n \ge 20$ and all cases can be realized.

PROOF. The values $1 \le n \le 4$, $6 \le n \le 9$, and $11 \le n \le 14$ are excluded by Theorem 10.3. The cases $n \in \{18, 19\}$ are excluded by Lemma 6.3 using $m = 4$.

For examples with $n \in \{5, 16, 17, 21, \ldots, 24\}$ we refer to [79], so that Lemma 10.1 provides examples for the mentioned cases. □

LEMMA 10.10

Let $\mathcal{K}$ be a projective 4^1-divisible arc in $\operatorname{PG}(v-1,4)$. *If $\#\mathcal{K} = n$, then*

$$n \in \{6, 12, 18, 24, 25, 26, 30, 31, 32, 36, \ldots, 40\}$$

or $n \ge 41$ and all cases, possibly except $n = \mathbf{40}$, can be realized.

PROOF. The values $1 \le n \le 5$, $7 \le n \le 11$, $13 \le n \le 17$, and $19 \le n \le 23$ are excluded by Theorem 10.3. The cases $27 \le n \le 29$ and $34 \le n \le 35$ are excluded by Lemma 6.3 using $m = 5$ and $m = 6$, respectively. The case $n = 33$ is excluded by Corollary 6.9 with $t = 5$.

For examples with $n \in \{6, 25, 26, 39, 41, 46\}$ we refer to [79], so that Lemma 10.1 provides examples for the mentioned cases, i.e., excluding $n = 40$. □

We remark that the first four MacWilliams identities for a hypothetical projective 5-divisible $[40, 5, 30]_5$-code have the unique solution given by $A_{30} = 1872$, $A_{35} = 1248$, $A_{40} = 4$, and $B_3 = 0$. While the Griesmer bound give $g_5(5, 30) = 40$, $n_5(5, 30) = 41$ is known, see e.g. `http://mars39.lomo.jp/opu/bound5_5.htm`. For $k \ge 6$ the Griesmer bound gives the non-existence of $[40, k, 30]_5$-codes. For $k \le 3$ a $[40, k]_5$-code cannot be projective. For $k = 4$ solving the first four MacWilliams identities of a hypothetical projective 5-divisible $[40, 4]_5$-code for $\{A_{25}, A_{30}, A_{35}, B_3\}$ gives

$$\begin{aligned}
A_{25} &= -16 - 15A_5 - 10A_{10} - 6A_{15} - 3A_{20} - A_{40} \\
A_{30} &= 400 + 24A_5 + 15A_{10} + 8A_{15} + 3A_{20} + 3A_{40} \\
A_{35} &= 240 - 10A_5 - 6A_{10} - 3A_{15} - A_{20} - 3A_{40} \\
B_3 &= 720 + 500A_5 + 250A_{10} + 100A_{15} + 25A_{20} - 25A_{40},
\end{aligned}$$

so that A_{25} would be strictly negative. Thus, we can assume that $k \ge 5$ and a weight in $\{5, 10, 15, 20, 25\}$ is attained. If $k = 5$, then solving the first four MacWilliams identities of a hypothetical projective 5-divisible $[40, 5]_5$-code for $\{A_{25}, A30, A_{35}, B_3\}$ gives

$$\begin{array}{rcl}A_{25} &=& 4 - 15A_5 - 10A_{10} - 6A_{15} - 3A_{20} - A_{40}\\ A_{30} &=& 1860 + 24A_5 + 15A_{10} + 8A_{15} + 3A_{20} + 3A_{40}\\ A_{35} &=& 1260 - 10A_5 - 6A_{10} - 3A_{15} - A_{20} - 3A_{40}\\ B_3 &=& 20 + 100A_5 + 50A_{10} + 20A_{15} + 5A_{20} - 5A_{40},\end{array}$$

so that $A_{25} \ge 0$ and $A_5, A_{10}, A_{15}, A_{20} \in \mathbb{N}_0$ implies $A_5 = A_{10} = A_{15}, A_{20} = 0$. Since $A_{25} \in 4\mathbb{N}_0$ and there exists a weight in $\{5, 10, 15, 20, 25\}$, we have $A_{25} = 4$ and $A_{40} = 0$, i.e., $A_{25} = 4$, $A_{30} = 1860$, $A_{35} = 1260$, and $B_3 = 20$. Thus, there exists a $[39, 4, \{30, 35\}]_5$-code that is possibly non-projective. Solving the first four MacWilliams identities gives $A_{30} = 468$, $A_{35} = 156$, $B_2 = 0$, and $B_3 = 676$. Such projective two-weight codes indeed exist. Using `LinCode` we could classify all 8 such codes in roughly 4 hours of computation time. Six of these have already been found in [42]. We remark that there are 1628 $[15, 4, 10]_5$-codes, which are the candidates for residual codes of a codeword of weight 25. Given this classification, we verified that no $[16, 5, 10]_5$-code exists, c.f. [55].

11. The number of minimum codewords in 2^r-divisible binary codes

This chapter is based on [102]. For an application see e.g. [91].

12. Restrictions on the weight distribution of binary linear codes imposed by the structure of Reed-Muller codes

18012. Restrictions on the weight distribution of binary linear codes imposed by the structure of Reed-Muller codes

13. Exhaustive generation of linear codes

REMARK 13.1 The classification of the unique projective $[64, 11, \{16, 32, 48\}]_2$-code is computationally infeasible by an direct application of `QextNewEdition` (see e.g. [24]). After 8 days of computation more than 130 GB of intermediate data where produced, so that we stopped the program.

REMARK 13.2 The classification of the $[65, 12, \{24, 32, 40, 56\}]_2$-codes using `QextNewEdition` needed almost 2 months. Three 12-dimensional codes and no 13-dimensional code have been found.

REMARK 13.3 We have verified the non-existence of some small Griesmer codes using `QextNewEdition`. The running times are as follows:

code parameters	running time
$[12, 5, 5]_2$	0.00s
$[28, 6, 13]_2$	0.10s
$[40, 6, 19]_2$	12.55s
even $[41, 6, 20]_2$	2.73s
projective $[41, 6, \{20, 24, 26, 40\}]_2$	0.93s

14. Random linear network coding

“Classical” coding theory considers the situation where information should be transmitted from a unique sender to a unique receiver along a chanel of a certain type. (Indeed, different types of chanels are considered and modeled in the literature.) Now we want to consider a more recent application of coding theoretic technics and models. As an introduction we consider the network depicted in Figure 14.1. Assume that vertices s_1 and s_2 are senders, t_1, t_2 are receivers, and the remaining nodes u, v are intermediate nodes. We further assume that the senders s_1 and s_2 send *different* information, which we denote by A and B, respectively. The receivers t_1 and t_2 are interested in both kinds of messages. For the directed arcs we assume unit capacities, i.e., they can transmit one information unit per time unit. Let us first consider a classical situation from operations research. Assume that s_1 and s_2 are delivering some liquids, like oil or water, or some other kind of solid material, which then is routed along the network towards the receivers. This problem is known under the name maximum flow problem, which occurs in different variants.

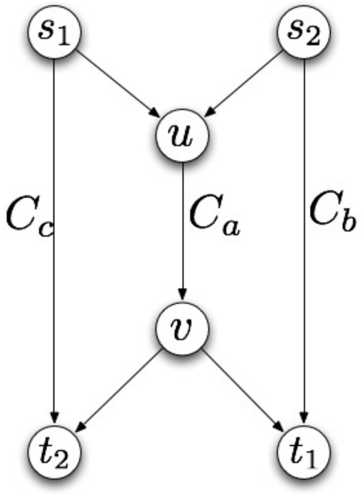


Figure 14.1: The “Butterfly network”.

Now let us consider the arcs C_a, C_b, and C_c. They form a so called cut, every path from one of the senders to one of the receivers contains at least one arc in this subset of arcs. Adding the capacities of the three cut arcs we conclude, that in one time step the receivers can receive at most 3 units in total. So, especially it is not possible that both receivers t_1 and t_2 both receive one item of A and one item of B in a single time step. The maximum-flow-minimum-cut theorem states that the value of the maximum flow equals the value of the minimum cut, i.e., we can always get constructive tight upper bounds for the maximum flow. In our situation the bottleneck is clearly the arc C_a, which can either route A or B, so that the same applies to the subsequent arcs from v to the senders t_1 and t_2 in the next time step.

The situation changes if A and B are digital information, see Figure 14.2 for an improved routing scheme. Along the arc C_a the message $A + B$ is transmitted, which can be computed in the intermediate node u, since this node receives A and B. Receiver t_1 can obtain A and B from the received information A and $A + B$ by suitable linear combinations.

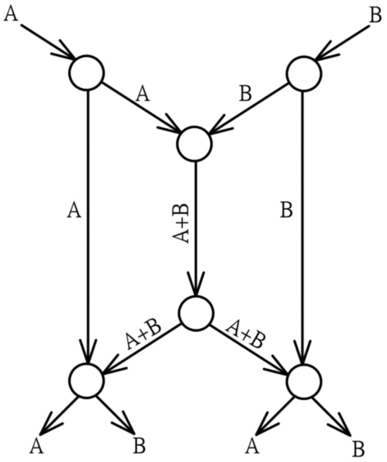


Figure 14.2: A solution for the butterfly network.

So, in our model the nodes are allowed to compute arbitrary linear combinations of the incoming information. Moreover, also the number of outgoing arcs is unbounded and for each of them a different linear combination of the inputs can be computed. For a given network the computation of an optimal transmission scheme, i.e., the determination of suitable linear combinations of the inputs for each outgoing arc in order to achieve the maximum possible throughput is still a complicated unsolved open problem. An asymptotically optimal solution was found in [76]: At each outgoing arc just compute a random linear combination of the ingoing arcs. With a probability that exponentially tends to 1, in terms of the field size q, the achieved throughput equals the maximum possible throughput. This statement remains true even if we allow arbitrary combinations of the inputs for the maximum possible throughput. Moreover this approach, besides being conceptionally easy, is very robust with respects to changes or local failures of the network.

So far we have not considered the problems of error detection and error correction in this setting. A general model was introduced in [93] and we just sketch the underlying idea very briefly. Instead of caring about sets of transmitted base vectors we just consider the span, i.e., the set of all possible linear combinations – this are just subspaces of $\mathbb{F}_q^v$ for a suitable dimension v. So if we fix the field size q and the dimension of the ambient space v, a subspace code $\mathcal{C}$ is just a set of subspaces of $\mathbb{F}_q^v$. If all subspaces have the same dimension we speak of a constant-dimension code. A metric space is obtained by using the subspace distance

$$d_S(U,W) := dim(U+W) - \dim(U\cap W) = \dim(U) + \dim(W) - 2\dim(U\cap W) \tag{14.1}$$

for two subspaces U and W, see e.g. [93] for the corresponding channel model. Another possibility is the injection distance

$$d_I(U,W) = \max\{\dim(U),\dim(W)\} - \dim(U\cap W), \tag{14.2}$$

see [140]. If $\dim(U) = \dim(W) = k$, then we have

$$d_S(U,W) = 2k - 2\dim(U \cap W) = 2d_I(U,W),$$

so that it makes no difference if we use the subspace distance or the injection distance for constant-dimension codes. In the following we will just use the subspace distance and write d instead of d_S. The minimum distance $d(\mathcal{C})$ of a subspace code $\mathcal{C}$ is the minimum of $d(U,W)$ over all pairs of different codewords $U, W \in \mathcal{C}$. If $\#\mathcal{C} \le 1$, then we set $d(\mathcal{C})\infty$. By $A_q(v,d)$ we denote the maximum possible cardinality $\mathcal{C}$ of a subspace code $\mathcal{C}$ in $\mathbb{F}_q^v$ with minimum subspace distance (at least) d. For constant-dimension codes with codewords of dimension k we denote the corresponding quantity by $A_q(v,d;k)$. Note that $d(\mathcal{C})$ is an even integer for every constant-dimension code $\mathcal{C}$. By $\mathcal{C}\ \perp = \left\{U^\perp : U \in \mathcal{C}\right\}$ we denote the orthogonal code of $\mathcal{C}$, where $U^\perp$ denote the orthogonal subspace with respect to some non-degenerated billinear form. Since $d(U,W) = d(U^\perp, W^\perp)$, we have $A_q(v,d;k) = A_q(v,d;v-k)$. An online table with known lower and upper bounds for $A_q(v,d)$ and $A_q(v,d;k)$ can be found at `http:\www.subspacecodes.uni-bayreuth.de`, see [68] for the corresponding technical manual. In Chapter 15 we survey upper bounds and in Chapter 16 we consider some constructive lower bounds for $A_q(v,d;k)$. For lower and upper bounds for $A_q(v,d)$ we refer to e.g. [78, 72, 80].

Finally, we mention a generalization of subspace codes where instead of subspaces flags of subspaces, i.e., increasing chains of subspaces, are used as codewords, see [122, 123]. A few further constructions can be found in [6] and upper bounds in [100].

15. Bounds for constant-dimension codes

In this chapter we consider upper bounds for the maximum possible cardinality $A_q(v,d;k)$ of constant-dimension codes in $\mathbb{F}_q^v$ with minimum subspace distance d and codewords of dimension k. Most oft our considerations are based on [70]. Another survey with quite some overlap is [89]. Due to $A_q(v,d;k) = A_q(v,d;v-k)$ we assume $2k \le v$. For $d \le 2$ or $k \le 1$ we have $A_q(v,d;k) = \begin{bmatrix} v \\ k \end{bmatrix}_q$, so that we also assume $d \ge 4$ and $k \ge 2$.

The fact that the Grassmann graph, i.e., the graph consisting of the k-dimensional subspaces of $\mathbb{F}_q v$ that are joined by an edge iff the are at subspace distance at least d, is distance-regular implies:

THEOREM 15.1 (Sphere-packing bound) [93, Theorem 6]

$$A_q(v,d;k) \le \frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\sum\limits_{i=0}^{\lfloor (d/2-1)/2 \rfloor} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} v-k \\ i \end{bmatrix}_q}$$

By defining a puncturing operation one can decrease the dimension of the ambient space and the codewords. Since the minimum distance decreases by at most two, we can iteratively puncture $d/2-1$ times, so that $A_q(v,d;k) \le \begin{bmatrix} v-d/2+1 \\ k-d/2+1 \end{bmatrix}_q = \begin{bmatrix} v-d/2+1 \\ v-k \end{bmatrix}_q$ since $A_q(v',2;k') = \begin{bmatrix} v' \\ k' \end{bmatrix}_q$. Considering either the code or its orthogonal code gives:

THEOREM 15.2 (Singleton bound) [93, Theorem 9]

$$A_q(v,d;k) \le \begin{bmatrix} v-d/2+1 \\ \max\{k, v-k\} \end{bmatrix}_q$$

Referring to [93] the authors of [89] state that even a relaxation of the Singleton bound is always stronger than the sphere packing bound for non-trivial codes. However, for $q=2$, $v=8$, $d=6$, and $k=4$, the sphere-packing bound gives an upper bound of $200787/451 \approx 445.20399$ while the Singleton bound gives an upper bound of $\begin{bmatrix} 6 \\ 4 \end{bmatrix}_2 = 651$. For $q=2$, $v=8$, $d=4$, and $k=4$ it is just the other way round, i.e., the Singleton bound gives $\begin{bmatrix} 7 \\ 3 \end{bmatrix}_2 = 11811$ and the sphere-packing bound gives $\begin{bmatrix} 8 \\ 4 \end{bmatrix}_2 = 200787$. Examples for the latter case are easy to find. For $d=2$ both bounds coincide and for $d=4$ the Singleton bound is always stronger than the sphere-packing bound since $\begin{bmatrix} v-1 \\ k \end{bmatrix}_q < \begin{bmatrix} v \\ k \end{bmatrix}_q$. The asymptotic bounds [93, Corollaries 7 and

10], using normalized parameters, and [93, Figure 1] suggest that there is only a small range of parameters where the sphere-packing bound can be superior to the Singleton bound.[1]

THEOREM 15.3 (Anticode bound) [150, Theorem 5.2]

$$A_q(v,d;k) \le \frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\begin{bmatrix} \max\{k,v-k\}+d/2-1 \\ d/2-1 \end{bmatrix}_q}$$

Codes that can achieve the (unrounded) value $\begin{bmatrix} v \\ k \end{bmatrix}_q / \begin{bmatrix} \max\{k,v-k\}+d/2-1 \\ d/2-1 \end{bmatrix}_q$ are called Steiner structures. It is a well-known and seemingly very hard problem to decide whether a Steiner structure for $v=7$, $d=4$, and $k=3$ exists. For $q=2$ the best known bounds are $333 \le A_2(7,4;3) \le 381$, see [69] for the constructive lower bound. Additionally it is known that a code attaining the upper bound can have automorphisms of at most order 2, see [92]. So far, the only known (non-trivial) Steiner structure corresponds to $A_2(13,4;3) = 1597245$ [28].

Since the sphere underlying the proof of Theorem 15.1 is also an anticode, Theorem 15.1 is implied by Theorem 15.3. For $d=2$ both bounds coincide. In [155, Section 4] Xia and Fu verified that the Anticode bound is always stronger than the Singleton bound for the ranges of parameters considered by us.

Mimicking a classical bound of Johnson on binary error-correcting codes with respect to the Hamming distance, see [87, Theorem 3] and also [145], Xia and Fu proved:

THEOREM 15.4 (Johnson type bound I) [155, Theorem 2]

If $\left(q^k-1\right)^2 > \left(q^v-1\right)\left(q^{k-d/2}-1\right)$, *then*

$$A_q(v,d;k) \le \frac{\left(q^k-q^{k-d/2}\right)\left(q^v-1\right)}{\left(q^k-1\right)^2-\left(q^v-1\right)\left(q^{k-d/2}-1\right)}.$$

However, the required condition of Theorem 15.4 is rather restrictive and can be simplified considerably.

PROPOSITION 15.5

For $0 \le k < v$, *the bound in Theorem 15.4 is applicable iff* $d = 2\min\{k, v-k\}$ *and* $k \ge 1$. *Then, it is equivalent to*

$$A_q(v,d;k) \le \frac{q^v-1}{q^{\min\{k,v-k\}}-1}.$$

[1] By a tedious computation one can check that the sphere-packing bound is strictly tighter than the Singleton bound iff $q=2$, $v=2k$ and $d=6$.

PROOF. If $k=0$ we have $\left(q^k-1\right)^2=0$, so that we assume $k\ge 1$ in the following. If $k\le v-k$ and $d\le 2k-2$, then

$$(q^v-1)\left(q^{k-d/2}-1\right)\ge\left(q^{2k}-1\right)(q-1)\ge q^{2k}-1\overset{q\ge2,k\ge1}{>}q^{2k}-2q^k+1=\left(q^k-1\right)^2.$$

If $k\ge v-k+1$ and $d\le 2v-2k-2$, then

$$(q^v-1)\left(q^{k-d/2}-1\right)\ge(q^v-1)\left(q^2-1\right)\overset{q\ge2,v\ge1}{>}\left(q^{(v+1)/2}-1\right)^2\ge\left(q^k-1\right)^2.$$

If $d=2\min\{k,v-k\}$, $q\ge 2$, and $k\ge 1$, then it can be easily checked that the condition of Theorem 15.4 is satisfied and we obtain the proposed formula after simplification.

□

For $k=v$ Theorem 15.4 gives $A_q(v,d;v)\le 1$ which is trivially satisfied with equality. In Subsection **??** we will provide tighter upper bounds for the special case where $d=2k$, i.e., partial spreads. Indeed, the bound stated in Proposition 15.5 corresponds to the most trivial upper bounds for partial spreads that is tight iff k divides v, as we will see later on. So, due to orthogonality, Theorem 15.4 is dominated by the partial spread bounds discussed later on.

While the previously mentioned generalization of a classical bound of Johnson on binary error-correcting codes yields the rather weak Theorem 15.4, generalizing [87, Inequality (5)], see [155] yields a very strong upper bound:

THEOREM 15.6 (Johnson type bound II) [155, Theorem 3], [52, Theorem 4,5]

$$A_q(v,d;k) \le \frac{q^v-1}{q^k-1}A_q(v-1,d;k-1) \qquad (15.1)$$

$$A_q(v,d;k) \le \frac{q^v-1}{q^{v-k}-1}A_q(v-1,d;k) \qquad (15.2)$$

Note that for $d=2k$ Inequality (15.1) gives $A_q(v,2k;k)\le\left\lfloor\frac{q^v-1}{q^k-1}\right\rfloor$ since we have $A_q(v-1,2k;k-1)=1$ by definition. Similarly, for $d=2(v-k)$, Inequality (15.2) gives $A_q(v,2v-2k;k)\le\left\lfloor\frac{q^v-1}{q^{v-k}-1}\right\rfloor$.

Of course we can round down the right-hand side of Inequality (15.1). Applying Lemma 5.22.(i) yields a sharpened rounding:

COROLLARY 15.7

$$A_q(v,d;k)\le\llbracket A_q(v-1,d;k-1)\cdot[v]_q/[k]_q\rrbracket_{q^{k-1}}. \qquad (15.3)$$

As an example we consider upper bounds for $A_2(9,6;4)$. Due to $A_2(8,6;3) = 34$, Theorem 15.6 yields $A_2(9,6;4) \le 1158$ and Corollary 15.7 yields $A_2(9,6;4) \le 1156$.

Some sources like [155, Theorem 3] list just Inequality 15.1 and omit Inequality 15.2. This goes in line with the treatment of the classical Johnson type bound II for binary error-correcting codes, see e.g. [127, Theorem 4 on page 527], where the other bound is formulated as Problem (2) on page 528 with the hint that ones should be replaced by zeros. Analogously, we can consider orthogonal codes:

PROPOSITION 15.8

Inequality (15.1) and Inequality (15.2) are equivalent using orthogonality, cf. [52, Section III, esp. Lemma 13].

PROOF. We have

$$\begin{aligned} A_q(v,d;k) &= A_q(v,d;v-k) \overset{(15.1)}{\le} \frac{q^v-1}{q^{v-k}-1} A_q(v-1,d;v-k-1) \\ &= \frac{q^v-1}{q^{v-k}-1} A_q(v-1,d;k), \end{aligned}$$

which is Inequality (15.2), and

$$\begin{aligned} A_q(v,d;k) &= A_q(v,d;v-k) \overset{(15.2)}{\le} \frac{q^v-1}{q^k-1} A_q(v-1,d;v-k) \\ &= \frac{q^v-1}{q^k-1} A_q(v-1,d;k-1), \end{aligned}$$

which is Inequality (15.1).

□

Of course, the bounds in Theorem 15.6 can be applied iteratively. In the classical Johnson space the optimal order of the corresponding inequalities is unclear, see e.g. [127, Research Problem 17.1]. Denoting the maximum size of a binary constant-weight block code of length n, Hamming distance d and weight k by $A(n,d,w)$, the two corresponding variants of the inequalities in Theorem 15.6 are $A(n,d,w) \le \lfloor n/w \cdot A(n-1,d,w-1)\rfloor$ and $A(n,d,w) \le \lfloor n/(n-w) \cdot A(n-1,d,w)\rfloor$. Applying the first bound yields

$$A(28,8,13) \le \lfloor 28/13 \cdot A(27,8,12)\rfloor \le \lfloor 28/13 \cdot 10547\rfloor = 22716$$

while applying the second bound yields

$$A(28,8,13) \le \lfloor 28/15 \cdot A(27,8,13)\rfloor \le \lfloor 28/15 \cdot 11981\rfloor = 22364$$

using the numerical bounds from

`http://webfiles.portal.chalmers.se/s2/research/kit/bounds/cw.html`, cf. [3].

The authors of [52, 89] state that the optimal choice of Inequality (15.1) or Inequality (15.2) is unclear, too. However, this question is much easier to answer for constant dimension codes.

PROPOSITION 15.9

For $k \le v/2$ we have

$$\left\lfloor \frac{q^v-1}{q^k-1} A_q(v-1,d;k-1) \right\rfloor \le \left\lfloor \frac{q^v-1}{q^{v-k}-1} A_q(v-1,d;k) \right\rfloor,$$

where equality holds iff $v = 2k$.

PROOF. By considering orthogonal codes we obtain equality for $v = 2k$. Now we assume $k < v/2$ and show

$$\frac{q^v-1}{q^k-1} A_q(v-1,d;k-1) + 1 \le \frac{q^v-1}{q^{v-k}-1} A_q(v-1,d;k), \tag{15.4}$$

which implies the proposed statement. Considering the size of the LMRD code we can lower bound the right hand side of Inequality (15.4) to

$$\frac{q^v-1}{q^{v-k}-1} A_q(v-1,d;k) \ge \frac{q^v-1}{q^{v-k}} \cdot q^{(v-k-1)(k-d/2+1)}.$$

Since

$$\frac{\begin{bmatrix} v-1 \\ k-1 \end{bmatrix}_q}{\begin{bmatrix} v-k+d/2-1 \\ d/2-1 \end{bmatrix}_q} = \frac{\prod_{i=1}^{k-1} \frac{q^{v-k+i}-1}{q^i-1}}{\prod_{i=1}^{d/2-1} \frac{q^{v-k+i}-1}{q^i-1}} \le \prod_{i=d/2}^{k-1} \frac{q^{v-k+i}}{q^i-1} = q^{(v-k)(k-d/2)} \prod_{i=d/2}^{k-1} \frac{1}{1-q^{-i}}$$

we can use the Anticode bound to upper bound the left hand side of Inequality (15.4) to

$$\frac{q^v-1}{q^k-1} A_q(v-1,d;k-1) + 1 \le \frac{q^v-1}{q^k-1} \cdot q^{(v-k)(k-d/2)} \cdot \mu(k-1,d/2,q) + 1,$$

where $\mu(a,b,q) := \prod_{i=b}^{a} \left(1-q^{-i}\right)^{-1}$. Thus, it suffices to verify

$$\frac{q^{k-d/2+1}}{q^k-1} \cdot \mu(k-1,d/2,q) + \frac{1}{f} \le 1, \tag{15.5}$$

where we have divided by

$$f := \frac{q^v-1}{q^{v-k}} \cdot q^{(v-k-1)(k-d/2+1)} = \frac{q^v-1}{q} \cdot q^{(v-k-1)(k-d/2)}.$$

Since $d \ge 4$, we have $\mu(k-1,d/2,q) \le \prod_{i=2}^{\infty} \left(1-q^{-i}\right)^{-1} \le \prod_{i=2}^{\infty} \left(1-2^{-i}\right)^{-1} < 1.74$. Since $v \ge 4$ and $q \ge 2$, we have $\frac{1}{f} \le \frac{2}{15}$. Since $k \ge 2$, we have $\frac{q^{k-d/2+1}}{q^k-1} \le \frac{q}{q^2-1}$, which is at most $\frac{3}{8}$ for $q \ge 3$. Thus, Inequality (15.5) is valid for all $q \ge 3$.

If $d \geq 6$ and $q = 2$, then $\mu(k-1, d/2, q) \leq \prod\limits_{i=3}^{\infty} \left(1 - 2^{-i}\right)^{-1} < 1.31$ and $\frac{q^{k-d/2+1}}{q^k-1} \leq \frac{1}{3}$, so that Inequality (15.5) is satisfied.

In the remaining part of the proof we assume $d = 4$ and $q = 2$. If $k = 2$, then $\mu(k-1, d/2, q) = 1$ and $\frac{q^{k-d/2+1}}{q^k-1} = \frac{2}{3}$. If $k = 3$, then $\mu(k-1, d/2, q) = \frac{4}{3}$ and $\frac{q^{k-d/2+1}}{q^k-1} = \frac{4}{7}$. If $k \geq 4$, then $\frac{q^{k-d/2+1}}{q^k-1} \leq \frac{8}{15}$, $\mu(k-1, d/2, q) \leq 1.74$, and $\frac{1}{f} \leq \frac{2}{255}$ due to $v \geq 2k \geq 8$. Thus, Inequality (15.5) is valid in all cases. □

Knowing the optimal choice between Inequality (15.1) and Inequality (15.2), we can iteratively apply Theorem 15.6 in an ideal way initially assuming $k \leq v/2$:

Corollary 15.10

$$A_q(v,d;k) \leq \left\lfloor \frac{q^v-1}{q^k-1} \left\lfloor \frac{q^{v-1}-1}{q^{k-1}-1} \left\lfloor \dots \left\lfloor \frac{q^{v-k+d/2+1}-1}{q^{d/2+1}-1} A_q(v-k+d/2, d; d/2) \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor$$

We remark that this upper bound is commonly stated in an explicit version, where $A_q(v-k+d/2, d; d/2) \leq \left\lfloor \frac{q^{v-k+d/2}-1}{q^{d/2}-1} \right\rfloor$ is inserted, see e.g. [52, Theorem 6], [89, Theorem 7], and [155, Corollary 3]. However, currently much better bounds for partial spreads are available.

It is shown in [155] that the Johnson bound of Theorem 15.6 improves on the Anticode bound in Theorem 15.3, see also [11]. To be more precise, removing the floors in the upper bound of Corollary 15.10 and replacing $A_q(v-k+d/2, d; d/2)$ by $\frac{q^{v-k+d/2}-1}{q^{d/2}-1}$ gives

$$\prod_{i=0}^{k-d/2} \frac{q^{v-i}-1}{q^{k-i}-1} = \frac{\prod_{i=0}^{k-1} \frac{q^{v-i}-1}{q^{k-i}-1}}{\prod_{i=k-d/2+1}^{k-1} \frac{q^{v-i}-1}{q^{k-i}-1}} = \frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\begin{bmatrix} v-k+d/2-1 \\ d/2-1 \end{bmatrix}_q},$$

which is the right hand side of the Anticode bound for $k \leq v-k$. So, all upper bounds mentioned so far are (weakly) dominated by Corollary 15.10, if we additionally assume $k \leq v-k$. As a possible improvement [4, Theorem 3] was mentioned as [89, Theorem 8]. In both cases there is a typo in the statement, see [70, Theorem 8] for a correct version. This additional bound is parametric and contains Theorem 15.6 as a special case. However, no strict improvement over Theorem 15.6 is known up to now.

To sum up, the sharpest known parametric upper bound for $A_q(v,d;k)$ is given by Corollary 15.7 refering back to the situation of partial spreads where $d = 2k$ (assuming $v \geq 2k$). For partial spreads all currently known upper bounds can be obtained from non-existence results for projective q^{k-1}-divisible codes, see the subsequent Section 15.1. Besides that the only known improvements with respect to upper bounds are $A_2(6,4;3) = 77 < 81$ [77] and $A_2(8,6;4) = 257 < 289$ [66], which are both based on integer linear programming computations.

For the special case where the constant-dimension code contains a so-called lifted MRD code tighter bounds are known [51, 63]. In both cases only a subset of the possible parameters is covered. A general and unifying version can be found in [104].

Finally, we remark that the very effective idea of the Johnson bound in Theorem 15.6 was generalized to general subspace codes and upper bounds for $A_q(v,d)$ in [81]. However, the computations are far more involved and there is no easy explicit formula any more.

15.1 Upper bounds for partial spreads

The case of constant dimension codes with maximum possible subspace distance $d = 2k$ is known under the name partial spreads. Counting points, i.e., 1-dimensional subspaces, in $\mathbb{F}_q^v$ and $\mathbb{F}_q^k$ gives the obvious upper bound $A_q(v,2k;k) \le \begin{bmatrix} v \\ 1 \end{bmatrix}_q / \begin{bmatrix} k \\ 1 \end{bmatrix}_q = (q^v - 1) \,/\, \left(q^k - 1\right)$. In the case of equality one speaks of spreads, for which a handy existence criterion is known from the work of Segre in 1964.

THEOREM 15.11 [137, §VI]
$\mathbb{F}_q^v$ *contains a spread if and only if* k *is a divisor of* v.

If k is not a divisor of v, far better bounds are known including some recent improvements, which we will briefly summarize. For a more detailed treatment we refer to e.g. [79]. The best known parametric construction was given by Beutelspacher in 1975:

THEOREM 15.12 [18]
For positive integers v,k *satisfying* $v = tk + r$, $t \ge 2$ *and* $1 \le r \le k-1$ *we have* $A_q(v,2k;k) \ge 1 + \sum_{i=1}^{t-1} q^{ik+r} = \frac{q^v - q^{k+r} + q^k - 1}{q^k - 1}$ *with equality for* $r = 1$.

The determination of $A_2(v,6;3)$ for $v \equiv 2 \pmod 3$ was achieved more than 30 years later in [46] and continued to $A_2(v,2k;k)$ for $v \equiv 2 \pmod k$ and arbitrary k in [96]. Besides the parameters of $A_2(8+3l,6;3)$, for $l \ge 0$, see [46] for an example showing $A_2(8,6;3) \ge 34$, no partial spreads exceeding the lower bound from Theorem 15.12 are known.

For a long time the best known upper bound on $A_q(v,2k;k)$ was the one obtained by Drake and Freeman in 1979:

THEOREM 15.13 [45, Corollary 8]
If $v = kt + r$ *with* $0 < r < k$, *then*

$$A_q(v,2k;k) \le \sum_{i=0}^{t-1} q^{ik+r} - \lfloor \theta \rfloor - 1 = q^r \cdot \frac{q^{kt} - 1}{q^k - 1} - \lfloor \theta \rfloor - 1,$$

where $2\theta = \sqrt{1 + 4q^k(q^k - q^r)} - (2q^k - 2q^r + 1)$.

Quite recently this bound has been generalized to:

THEOREM 15.14 [95, Theorem 2.10]
For integers $r \geq 1$, $t \geq 2$, $y \geq \max\{r,2\}$, $z \geq 0$ *with* $\lambda = q^y$, $y \leq k$, $k = \begin{bmatrix} r \\ 1 \end{bmatrix}_q + 1 - z > r$, $v = kt + r$, *and* $l = \frac{q^{v-k}-q^r}{q^k-1}$, *we have* $A_q(v, 2k; k) \leq lq^k + \left\lceil \lambda - \frac{1}{2} - \frac{1}{2}\sqrt{1 + 4\lambda\left(\lambda - (z+y-1)(q-1) - 1\right)} \right\rceil$.

The construction of Theorem 15.12 is asymptotically optimal for $k \gg r = v \bmod k$, as recently shown by Năstase and Sissokho:

THEOREM 15.15 [130, Theorem 5]
Suppose $v = tk + r$ *with* $t \geq 1$ *and* $0 < r < k$. *If* $k > \begin{bmatrix} r \\ 1 \end{bmatrix}_q$ *then* $A_q(v, 2k; k) = 1 + \sum_{i=1}^{t-1} q^{ik+r} = \frac{q^v - q^{k+r} + q^k - 1}{q^k - 1}$.

Applying similar techniques, the result was generalized to $k \leq \begin{bmatrix} r \\ 1 \end{bmatrix}_q$:

THEOREM 15.16 [95, Theorem 2.9]
For integers $r \geq 1$, $t \geq 2$, $u \geq 0$, *and* $0 \leq z \leq \begin{bmatrix} r \\ 1 \end{bmatrix}_q/2$ *with* $k = \begin{bmatrix} r \\ 1 \end{bmatrix}_q + 1 - z + u > r$ *we have* $A_q(v, 2k; k) \leq lq^k + 1 + z(q-1)$, *where* $l = \frac{q^{v-k}-q^r}{q^k-1}$ *and* $v = kt + r$.

Using Theorem 15.14 the restriction $z \leq \begin{bmatrix} r \\ 1 \end{bmatrix}_q/2$ can be removed from Theorem 15.16, see [79].

We remark that all currently known upper bounds for partial spreads, i.e., bounds for $A_q(v, 2k, k)$, where $v \geq 2k$, can be deduced from non-existence results for projective q^{k-1}-divisible linear codes, see Chapter 10 or [79], via Lemma 5.25. Currently, Theorem 15.11, Theorem 15.14, and Theorem 15.16 constitute the tightest parametric bounds for $A_q(v, 2k; k)$. Known improvements, by exactly one in every case, are given by the 21 specific bounds stated in [95], which are based on the linear programming method applied to projective q^{k-1}-divisible linear error-correcting codes over $\mathbb{F}_q$ with respect to the Hamming distance, see [79]. The non-existence of projective a 16-divisible binary linear code of length 131, which implies $A_2(13, 10; 5) \leq 259$, was shown in [106]. It is very likely that more sophisticated methods from classical coding theory can improve further values, which then imply improved upper bounds for constant dimension codes via the Johnson bound of Theorem 15.6 or its improvement in Corollary 15.7.

16. Constructions for constant-dimension codes

In this chapter we want to briefly discuss constructions for constant-dimension codes. We will directly dive into more recent developments, in order to state some open problems, and refer to the survey [83] for a more extensive overview.

Let us start with a few preliminaries, see [36]. The row space $R(M)$ of any full-rank matrix $M \in \mathbb{F}_q^{k\times n}$ gives rise to such a k-subspace U. Here M is called a generator matrix of U. For the other direction we denote by $\tau(U)$ the unique full-rank matrix in $\mathbb{F}_q^{k\times n}$ that is in reduced row echelon form (rre). By $p(U) \in \mathbb{F}_2^n$ we denote the binary vector whose 1-entries coincide with the pivot columns of $\tau(U)$. Its Hamming weight $w_{\mathrm{h}}(p(U))$, i.e., the number of non-zero entries, equals the dimension k of U. Slightly abusing notation, we also write $\tau(M) = \tau(R(M))$ and $p(M) = p(R(M))$ for a matrix $M \in \mathbb{F}_q^{k\times n}$. For $M = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{2\times 4}$ we have $\tau(M) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ and $p(M) = (1,1,0,0)$. The subspace distance $d(U,U')$ between two subspaces U and U' of $\mathbb{F}_q^n$ can be expressed via the rank of their generator matrices:

$$\begin{aligned} d(U,U') &= \dim(U+U') - \dim(U\cap U') = 2\dim(U+U') - \dim(U) - dim(U') \\ &= 2\,\mathrm{rk}\begin{pmatrix} \tau(U) \\ \tau(U') \end{pmatrix} - \mathrm{rk}(\tau(U)) - \mathrm{rk}(\tau(U')). \end{aligned} \tag{16.1}$$

If $p(U) = p(U')$, then Equation (16.1) simplifies to $d(U,U') = 2\,\mathrm{rk}(\tau(U) - \tau(U'))$. More generally, for two matrices $M, M' \in \mathbb{F}_q^{m\times n}$ we define the rank distance via $d_{\mathrm{r}}(M,M') = \mathrm{rk}(M - M')$, so that $\left(\mathbb{F}_q^{m\times n}, d_{\mathrm{r}}\right)$ is a metric space. A subset $\mathcal{M} \subseteq \mathbb{F}_q^{m\times n}$ is called a rank metric code. More precisely, we speak of an $(m \times n, d_r)_q$-rank metric code, where d_r is the minimum rank distance $d_{\mathrm{r}}(\mathcal{M}) = \min\{d_{\mathrm{r}}(M,M') : M, M' \in \mathcal{M}, M \neq M'\}$. A rank metric code is called linear if it is a subspace of $\mathbb{F}_q^{m\times n}$ over $\mathbb{F}_q$ and additive if it is closed under addition. The maximum size of an $(m \times n, d_r)_q$-rank metric code is given by $m(q,m,n,d_{\mathrm{r}}) := q^{\max\{m,n\}\cdot(\min\{m,n\}-d_{\mathrm{r}}+1)}$. A rank metric code $\mathcal{M} \subseteq \mathbb{F}_q^{m\times n}$ attaining this bound is said to be a *maximum rank distance (MRD) code* with parameters $(m \times n, d_{\mathrm{r}})_q$ or $(m \times n, d_r)_q$*–MRD code*, see e.g. the recent survey [138]. Linear MRD codes exist for all parameters. Moreover, for $d_{\mathrm{r}} < d'_{\mathrm{r}}$ we can assume the existence of a linear $(m \times n, d_{\mathrm{r}})_q$–MRD code that contains an $(m \times n, d'_{\mathrm{r}})_q$–MRD code as a subcode. The rank distribution of an additive $(m \times n, d_{\mathrm{r}})_q$–MRD code is completely determined by its parameters, i.e., the number of codewords of rank r is given by

$$a(q,m,n,d_{\mathrm{r}},r) = \begin{bmatrix} \min\{n,m\} \\ r \end{bmatrix}_q \sum_{s=0}^{r-d_r} (-1)^s q^{\binom{s}{2}} \cdot \begin{bmatrix} r \\ s \end{bmatrix}_q \cdot \left(q^{\max\{n,m\}\cdot(r-d_r-s+1)} - 1\right) \tag{16.2}$$

for all $d_r \le r \le \min\{n,m\}$, see e.g. [40, Theorem 5.6] or [138, Theorem 5]. Clearly, there is a unique codeword of rank strictly smaller than d_{r} – the zero matrix.

The Hamming distance $d_{\mathrm{h}}(u,u')=\#\{i \mid u_i \neq u'_i\}$, for two vectors $u,u' \in \mathbb{F}_2^n$, can be used to lower bound the subspace distance between two subspaces U and U' (not necessarily of the same dimension) of $\mathbb{F}_q^n$:

LEMMA 16.1 [50, Lemma 2]
For $U,U' \le \mathbb{F}_q^n$, we have $d(U,U') \ge d_h(p(U),p(U'))$.

Based on Lemma 16.1, in [50] the Echelon-Ferrers construction was introduced, see e.g. [139] for refinements. Here different subcodes with diverse pivot vectors are combined according to Lemma 16.1. The search for suitable skeleton codes, i.e., sets of non-contradicting pivot vectors, is still an active line of research, see e.g, [60]. A recent overview with lower and upper bounds for the achievable code sizes can be found in [54]. Considering only the pivot vector $(1,\dots,1,0,\dots 0)$ this contains the so-called lifted MRD (LMRD) codes from [141]. Here, the codewords are of the form $R(I_k|M)$, where I_k denotes the $k\times k$ unit matrix and M is a matrix from an MRD code. This construction yields $A_q(n,d;k) \ge m(q,k,n-k,\frac{d}{2})$. A bit more general, we can consider codewords of the form $R(\tau(U)|M)$, where M is an element of an $(k\times(n-m),\frac{d}{2})_q$-MRD code and U is an element of an $(m,d;k)_q$-CDC. Since this lifting step created an $(n-m)$-subspace that is disjoint to all codewords, more codewords can be added. This approach is called the linkage construction [56], see also [139], and yields $A_q(n,d;k) \ge A_q(m,d;k)\cdot m(q,k,n-m,\frac{d}{2})+A_q(n-m,d;k)$. Lifting of codes can also be combined with the Echelon-Ferrers construction, see e.g. [105].

LEMMA 16.2 [36, Lemma 4.1]
For a subspace distance d, let $\bar{n}=(n_1,\dots,n_l)\in\mathbb{N}^l$, where $l\ge 2$, be such that $\sum_{i=1}^l n_i = n$ and $n_i \ge k$ for all $1\le i\le l$. Let $\mathcal{C}_i$ be an $(n_i,\star,d;k)_q$-CDC and $\mathcal{M}_i$ be a $(k\times n_i,\frac{d}{2})_q$-rank metric code for $1\le i\le l$. Then $\mathcal{C}=\bigcup_{i=1}^l \mathcal{C}^i$, where

$$\mathcal{C}^i=\Big\{R(M_1|\dots|M_{i-1}|\tau(U_i)|M_{i+1}|\dots|M_l) \quad:\quad U_i\in\mathcal{C}_i, M_j\in\mathcal{M}_j,\ \forall 1\le j\le l, i\neq j,$$
$$\textit{and } \operatorname{rk}(M_j)\le k-\tfrac{d}{2},\ \forall 1\le j<i\Big\},$$

is an $(n,\star,d;k)_q$-CDC of cardinality

$$\#\mathcal{C}=\sum_{i=1}^{l}\left(\prod_{j=1}^{i-1}\#\left\{M\in\mathcal{M}_j\ :\ \operatorname{rk}(M)\le k-\tfrac{d}{2}\right\}\right)\cdot\#\mathcal{C}_i\cdot\left(\prod_{j=i+1}^{l}\#\mathcal{M}_j\right).$$

PROOF. Since $\operatorname{rk}(\tau(U_i))=k$ for all $U_i\in\mathcal{C}_i$ the elements of $\mathcal{C}^i$ are k-subspaces of $\mathbb{F}_q^n$ for all $1\le i\le l$; so they are in $\mathcal{C}$.

For the distance analysis let $U\in\mathcal{C}^i$, $U'\in\mathcal{C}^{i'}$ for some indices $1\le i\le i'\le l$. By construction there exist $U_i\in\mathcal{C}_i$ and $M_j\in\mathcal{M}_j$ for $1\le j\le l$, $j\neq i$, with

$$U=R(M_1|\dots|M_{i-1}|\tau(U_i)|M_{i+1}|\dots|M_l)$$

and $\mathrm{rk}(M_j) \le k - \frac{d}{2}$ for all $1 \le j < i$. Similarly, there exist $U'_{i'} \in \mathcal{C}_{i'}$ and $M'_j \in \mathcal{M}_j$ for $1 \le j \le l$, $j \ne i'$, with $U' = R(M'_1|\dots|M'_{i'-1}|\tau(U'_{i'})|M'_{i'+1}|\dots|M'_l)$ and $\mathrm{rk}(M'_j) \le k - \frac{d}{2}$ for all $1 \le j < i'$.

If $i < i'$ we set $\overline{U} = R(\tau(U_i)|M_{i'})$ and $\overline{U}' = R(M'_i|\tau(U'_{i'}))$, which are both k-subspaces of $V \simeq \mathbb{F}_q^{n_i+n_{i'}}$ and satisfy $d(U,U') \ge d(\overline{U},\overline{U}') \ge d$. The later inequality follows from Lemma 16.1 and $d_\mathrm{h}(p(\overline{U}),p(\overline{U}')) \ge d$, which is true since $p(\overline{U})$ has its k ones in the first n_i components while $p(\overline{U}')$ has at least $\frac{d}{2}$ of its k ones in the last $n_{i'}$ components.

If $i = i'$ and $U_i \ne U'_i$ we have $d(U,U') \ge d(U_i,U'_i) \ge d$ since $U_i, U'_i \in \mathcal{C}_i$ and $d(\mathcal{C}_i) \ge d$. Now let $i = i'$, $U_i = U'_i$, and $1 \le j \le l$ be an index with $M_j \ne M'_j$ and $j \ne i$. For $\overline{U} = R(\tau(U_i)|M_j), \overline{U}' = R(\tau(U_i), M'_j)$, we have $d(U,U') \ge d(\overline{U},\overline{U}')$ and $d(\overline{U},\overline{U}') \ge d$, since $M_j \ne M'_j \in \mathcal{M}_j$ and $d_\mathrm{r}(\mathcal{M}_j) \ge \frac{d}{2}$. □

We remark that Lemma 16.2 generalizes results from several papers e.g. [34, 58, 59, 99, 156].

COROLLARY 16.3 [36, Corollary 4.2]

For a subspace distance d, $\bar{n} = (n_1,\dots,n_l) \in \mathbb{N}^l$, $l \ge 2$, be such that $\sum_{i=1}^{l} n_i = n$ and $n_i \ge k$ for all $1 \le i \le l$. Then, we have

$$A_q(n,d;k) \ge \sum_{i=1}^{l} \left(\prod_{j=1}^{i-1} \left(1 + \sum_{r=\frac{d}{2}}^{k-\frac{d}{2}} a(q,k,n_j,\tfrac{d}{2},r) \right) \right) \cdot A_q(n_i,d;k) \cdot \left(\prod_{j=i+1}^{l} m(q,k,n_j,\tfrac{d}{2}) \right).$$

A crucial observation is that the codes constructed by Lemma 16.2 have a special structure that allows the addition of further codewords.

LEMMA 16.4 [36, Lemma 4.3]

With the same notation used in Lemma 16.2, set $\sigma_i = \sum_{j=1}^{i} n_j$, $1 \le i \le l$ and $\sigma_0 = 0$. Let E_i denote the $(n-n_i)$-subspace of $\mathbb{F}_q^n$ consisting of all vectors in $\mathbb{F}_q^n$ that have zeroes for the coordinates between $\sigma_{i-1}+1$ and σ_i for all $1 \le i \le l$. Then, the elements of $\mathcal{C}^i$ are disjoint from E_i for all $1 \le i \le l$.

PROOF. Let $U \in \mathcal{C}^i$ be arbitrary. By construction there exist $U_i \in \mathcal{C}_i$ and $M_j \in \mathcal{M}_j$ for $1 \le j \le l$, $j \ne i$ with $U = R(M)$, where $M = (M_1|\dots|M_{i-1}|\tau(U_i)|M_{i+1}|\dots|M_l)$, and $\mathrm{rk}(M_j) \le k - \frac{d}{2}$ for all $1 \le j < i$. Note that $E_i = R(N)$ and $\tau(E_i) = N$, where $N \in \mathbb{F}_q^{(n-n_i)\times n}$ is obtained from the unit matrix I_n by deleting the rows in position between $\sigma_{i-1}+1$ and σ_i. Consider a non-trivial linear combination of the k rows of M. The entries in the coordinates between $\sigma_{i-1}+1$ and σ_i are obtained by the same non-trivial linear combination applied to $\tau(U_i)$. Since $\mathrm{rk}(\tau(U_i)) = k$ the statement follows. □

In [36, Lemma 4.4] and [36, Corollary 4.5] this observation was used to give a parametric construction for suitable additional codewords. The approach was improved in [120] and leaves a lot of room for further refinements. A building block might be generator matrices of the form

$$\begin{pmatrix} I_{k_1} & M_1 & 0 & M_3 \\ 0 & M_4 & I_{k_2} & M_2 \end{pmatrix},$$

where M_1, M_2, M_3, M_4 are taken from suitable rank distance codes. We leave the details for the interested reader and remark that instead of the unit I_{k_1} we may also use $\tau(U)$, where U is a k_1-dimensional codeword from a suitable constant-dimension code. Instead of the the zero matrix below I_{k_1} we only need zeros in the pivot columns and can use a rank-metric code for the other columns, see e.g. [71] where similar techniques were applied. Of course on may also adopt the ILP formulation for constant-dimension codes, see e.g. [94], to the situation where we only have the information from Lemma 16.4 to add further codewords. It is also possible to conclude upper bounds for the maximum number of additional codewords along the lines of the techniques used in [104].

17. Further topics

In this chapter we briefly intorduce a few further topics and point to open problems.

17.1 Minimal codewords

Let C be a linear code. A minimal codeword in C is a non-zero codeword whose support is not properly contained in the support of another non-zero codeword. They are equivalent to circuits in matroids and cycles in graphs. In coding theory, minimal codewords were first used in decoding algorithms, see e.g. [1, 2, 7, 84]. They have also found applications in cryptography: in secret sharing schemes [129] and in secure two-party computation [33].

Note that a codeword and its non-zero scalar multiples have the same support. We say that two codewords are equivalent if one is a scalar multiple of the other. We use the notation $M(C)$ for the number of non-equivalent minimal codewords of C. Let $M_q(n,k)$ be the maximum of $M(C)$ for all $[n,k]_q$ codes C. Since C has q^k-1 nonzero codewords, we have

$$M_q(n,k) \le \frac{q^k-1}{q-1}.$$

In the setting of matroids, it was shown in [44], that

$$M_q(n,k) \le \binom{n}{k-1}. \tag{17.1}$$

This is bound is also called the matroid upper bound. Inequality (17.1) is satisfied with equality for MDS codes. In [5], it was shown that $M_2(k+1,k) = \binom{k+1}{2}$ for $k \ge 2$. Looking more generally at $M_2(k+t,k)$ for a fixed value of t, the formula

$$M_2(k+2,k) = k + k(k-1)/2 + \lfloor (k-1)/3 \rfloor \cdot \lfloor k/3 \rfloor \cdot \lfloor (k+1)/3 \rfloor \tag{17.2}$$

was shown in [] and a formula for $M_2(k+3,k)$ was conjectured. For general values of t the authors conjecture

$$M_2(k+t,k) = \left(\frac{k}{t+1}\right)^{t+1} + \mathcal{O}\left(k^t\right). \tag{17.3}$$

The exact determination of $M_q(k,n)$ is an open problem even for small parameters. In the binary case all values of $M_2(k,n)$ with $k,n \le 15$ are determined in [].

Taking the $k \times k$ unit matrix as a generator matrix of a linear code C over $\mathbb{F}_q$ yields $M(C) = k$. So, when asking for the minimum value $m_q(n,k)$ of $M(C)$ for all $[n,k]_q$-codes C it makes sense to assume that C is projective. For the exact values of $m_2(k,n)$ with $n, k \leq 15$ we refer to [39].

We remark that $M(C)$ is known for rather few families of codes only. An interesting problem arise if we choose a binary code via a generator matrix $(I_k|A)$, where A is the adjacency matrix of a graph. The problem of determining $M(C)$ was fully solved for complete multipartite graphs, paths, and cycles in [108], while there are many other interesting graph classes remaining as open problems.

17.2 Private information retrieval codes

A private information retrieval (PIR) protocol is a protocol that allows a user to retrieve an item from a server in possession of a database without revealing which item is retrieved. Formulated more sloppy, how can we google without letting Google know what we are interested about? The problem was introduced in [35] and protocols based on the generator matrix of a linear code proposed in [53]. Given a generator matrix G of an $[n,k]_q$-code, we say that a subset $S \subseteq \{1,\dots,n\}$ we say that S is a recovery set for unit vector $\mathbf{e}_i$ if the columns of G with indices in S contain $\mathbf{e}_i$ in their span. We say that G has the s-PIR property if for each index $1 \leq i \leq k$ there exist s pairwise disjoint recovery sets for $\mathbf{e}_i$. By $P(k,s)$ we denote the maximum possible length n of an $[n,k]_2$-code with a generator matrix satisfying the s-PIR property. An example showing $P(4,4) \leq 9$ is given by the generator matrix

$$G = \begin{pmatrix} 100011111 \\ 010001011 \\ 001011001 \\ 000100111 \end{pmatrix}.$$

For e_4 we can use the recovery sets

$$\{4\}, \{1,7\}, \{6,9\}, \{2,3,5,8\}.$$

Note that there is also a different list of recovery sets:

$$\{4\}, \{6,9\}, \{3,5,7\}, \{1,2,8\}.$$

The later might have the advantage that it only uses recovery sets of cardinality at most 3.

A lower bound for $P(k,s)$ is given by the minimum length of an $[n,k,s]_2$-code, i.e.,

$$P(k,s) \geq n_2(k,s). \tag{17.4}$$

Thus, we indeed have $P(4,4) = 9$. Formulas for $P(k,s)$ for all $k \leq 5$ have been determined in [112] while there are open cases for larger values of k. We remark that $P(k,s) > n_2(k,s)$ is possible. E.g. we have $P(5,8) = 18 > 16 = n_2(5,8)$. However, for fixed k and sufficiently large values of s we have $P(k,s) = n_2(k,s)$, so that the determination of $P(k,s)$ is, as $n_2(k,s)$, a finite problem for each value of k. Of course it would be interesting if further values can be determined exactly.

For distributed storage systems an interesting variant arises. Here the generator matrix of a linear code can be seen as a storage scheme and the columns of the generator matrix encode which linear combination of the files information are stored at the corresponding storage node. A recovery set S for $\mathbf{e}_i$ is said to recover file i. In this application it makes sense that a recovery set S is used with a certain rate λ_S such that for each node j the node's usage $\sum_{S:j\in S}\lambda_S$ is not above its capacity (which may be assume to equal 1 for simplicity). If λ_i is the sum over all λ_S where S recovers file i, then $\lambda=(\lambda_1,\dots,\lambda_k)$ is the vector of rates for the reception of the files. The set of all possible values of λ is the service rate region of the code (generator matrix). For more details we refer e.g. to [88], where the service rate regions of the first order Reed-Muller codes are determined. For $k=2$ files the service rate regions of all possible $[n,2]_2$-codes can be completely described. Partial results for $k=3$ files can be found in [103].

17.3 Vector space partitions

A vector space partition $\mathcal{P}$ in $\mathbb{F}_q^v\cong\operatorname{PG}(v-1,q)$ is a collection of subspaces with the property that every non-zero vector is contained in a unique member of $\mathcal{P}$. Let m_d be integers such that $\mathcal{P}$ contains m_d subspaces of dimension d. With this, $k^{m_k}\dots1^{m_1}$ is called the type of $\mathcal{P}$, where we may leave out some of the cases with $m_d=0$. An example of a vector space partition is given by a k-spread in $\mathbb{F}_q^v$, where $m_k:=\begin{bmatrix}v\\1\end{bmatrix}_q/\begin{bmatrix}k\\1\end{bmatrix}_q$ k-subspaces partition the set of points of $\mathbb{F}_q^v$, i.e., the corresponding type is given by k^{m_k}. If d_1 is the smallest dimension with $m_{d_1}\neq0$, we call m_{d_1} the length of the tail and call the set of the corresponding d_1-subspace the tail. Vector space partitions with a tail of small length are of special interest. In [61] the following result was obtained:

THEOREM 17.1 (Theorem 1 in [61])
Let $\mathcal{P}$ be a vector space partition of type $d_l{}^{u_l}\dots d_2{}^{u_2}d_1{}^{u_1}$ in $\mathbb{F}_q^v$, where $u_1,u_2>0$ and $d_l>\dots>d_2>d_1\geq1$.

(i) If $q^{d_2-d_1}$ does not divide u_1 and if $d_2<2d_1$, then $u_1\geq q^{d_1}+1$;

(ii) if $q^{d_2-d_1}$ does not divide u_1 and if $d_2\geq2d_1$, then either d_1 divides d_2 and $u_1=\begin{bmatrix}d_2\\1\end{bmatrix}_q/\begin{bmatrix}d_1\\1\end{bmatrix}_q$ or $u_1>2q^{d_2-d_1}$;

(iii) if $q^{d_2-d_1}$ divides u_1 and $d_2<2d_1$, then $u_1\geq q^{d_2}-q^{d_1}+q^{d_2-d_1}$;

(iv) if $q^{d_2-d_1}$ divides u_1 and $d_2\geq2d_1$, then $u_1\geq q^{d_2}$.

Moreover, in Theorem 2 and Theorem 3 of [61] Heden classified the possible sets of d_1-subspaces for $u_1=q^{d_1}+1$ and $u_1=\begin{bmatrix}d_2\\1\end{bmatrix}_q/\begin{bmatrix}d_1\\1\end{bmatrix}_q$, respectively. The results were obtained using the theory of mixed perfect 1-codes, see e.g. [73]. A refinement of Theorem 17.1 was proven in [97] using restrictions on the lengths of projective q^r-divisible codes. While the minimum possible value of u_1 is now known, one can ask for further excluded values for u_1.

The possible types of vector space partitions in $\mathbb{F}_2^v$ have been completely charaterized, see e.g. the survey [62]. For $v > 9$ or $q > 2$ the problem is widely open. The non-existence of a projective 2^3-divisible code of length $n = 59$ show in [82], e.g. excludes the existence of the types $5^4 4^{56} 1^{59}$ and $5^{19} 4^{25} 1^{59}$. Finally, we remark that there is a generalization of a vector space partition that has implications for lower bounds of constant-dimension subspace codes, see [64]. The existence problem for these generalized vector space partitions is also widely open.

17.4 Dimension of simple games and coding theory

A simple game is a mapping $v\colon 2^N \to \{0,1\}$ from the subsets of $N = \{1,\dots,n\}$ to $\{0,1\}$ satisfying $v(\emptyset) = 0$, $v(N) = 1$, and $v(S) \le T$ for all $S \subseteq T$. In other words, v is a surjective monotone Boolean function. In the context of voting a simple game is the formalization of a voting rule for binary decisions. I.e., all voters in N are asked whether they are in favor of a given proposal and S is the set of voters that are in favor. The proposal is accepted if $v(S) = 1$ and rejected otherwise. If there exists a quota $q \in \mathbb{R}_{>0}$ and weights $w_1,\dots,w_n \in \mathbb{R}_{\ge 0}$ such that $v(S) = 1$ iff $w(S) := \sum_{i \in S} w_i \ge q$, then v is called weighted game and denoted as $[q; w_1,\dots,w_n]$. The intersection $v \wedge v'$ of two simple games is defined by $(v \wedge v')(S) = \min\{v(S), v'(S)\}$. It is well known that each simple game can be written as the intersection of a finite number of weighted games. The smallest possible such number is called the dimension of the simple game. As an example we consider the simple game v with $t = 2$ equivalence classes of voters $N_1 = \{1,2\}$ and $N_2 = \{3,4,5,6\}$ such that a coalition S is winning, i.e., $v(S) = 1$, if $\#\left(S \cap N_1\right) \ge 2$ or $\#S \ge 4$. Since $v(\{1,2\}) = v(\{3,4,5,6\}) = 1$, $v(\{1,3,4\}) = v(\{2,5,6\}) = 0$, and the coalitions $\{1,2\}$, $\{3,4,5,6\}$ form the same multiset of voters as the coalitions $\{1,3,4\}$, $\{1,5,6\}$, the simple game v is not weighted, i.e., its dimension is at least 2. Due to the representation

$$[8; 5, 3, 2, 2, 2, 2] \wedge [8; 3, 5, 2, 2, 2, 2]$$

the dimension of v is exactly 2. For a more extensive introduction we refer e.g. to [110], where a lower bound for the dimension of the voting system of the EU Council according to the Lisbon voting rules was determined. The worst case bahaviour of the dimension of a simple game for n voters was determined in [132] using coding theory. For related complexity questions we refer e.g. to [111]. For complete simple games, a subclass of simple games, first results on the dimension where obtained in [131] and refined in [107], again using coding theory. For the details we refer to the mentioned papers and remark that with respect to the worst case behaviour of the dimension of a simple or complete simple game only the asymptotic order is determined and the determination of exact numbers is a widely open problem.