View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by EPub Bayreuth

CONSTRUCTIONS AND BOUNDS FOR MIXED-DIMENSION SUBSPACE CODES

THOMAS HONOLD

Department of Information and Electronic Engineering
Zhejiang University, 38 Zheda Road, 310027 Hangzhou, China

MICHAEL KIERMAIER

Mathematisches Institut, Universität Bayreuth, D-95440 Bayreuth, Germany

SASCHA KURZ

Mathematisches Institut, Universität Bayreuth, D-95440 Bayreuth, Germany

ABSTRACT. Codes in finite projective spaces with the so-called subspace distance as metric have been proposed for error control in random linear network coding. The resulting *Main Problem of Subspace Coding* is to determine the maximum size $\mathrm{A}_q(v,d)$ of a code in $\mathrm{PG}(v-1,\mathbb{F}_q)$ with minimum subspace distance d. Here we completely resolve this problem for $d \geq v-1$. For $d = v-2$ we present some improved bounds and determine $\mathrm{A}_2(7,5) = 34$.

1. INTRODUCTION

For a prime power $q > 1$ let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^v$ the standard vector space of dimension $v \geq 0$ over $\mathbb{F}_q$. The set of all subspaces of $\mathbb{F}_q^v$, ordered by the incidence relation $\subseteq$, is called *$(v-1)$-dimensional (coordinate) projective geometry over* $\mathbb{F}_q$ and denoted by $\mathrm{PG}(v-1,\mathbb{F}_q)$. It forms a finite modular geometric lattice with meet $X \wedge Y = X \cap Y$ and join $X \vee Y = X + Y$.

The study of geometric and combinatorial properties of $\mathrm{PG}(v-1,\mathbb{F}_q)$ and related structures forms the subject of *Galois Geometry* —a mathematical discipline with a long and renowned history of its own but also with links to several other areas of discrete mathematics and important applications in contemporary industry, such as cryptography and error-correcting codes. For a comprehensive introduction to the core subjects of Galois Geometry readers may consult the three-volume treatise [26, 27, 28]. More recent developments are surveyed in [3].

It has long been recognized that classical error-correcting codes, which were designed for point-to-point communication over a period of now more than 60 years, can be studied in the Galois Geometry framework. Recently, through the seminal work of Koetter, Kschischang and Silva [33, 39, 40], it was discovered that essentially the same is true for the network-error-correcting codes developed by Cai, Yeung, Zhang and others [43, 44, 24]. Information in packet networks with underlying packet space $\mathbb{F}_q^v$ can be transmitted using subspaces of $\mathrm{PG}(v-1,\mathbb{F}_q)$ as codewords and secured against errors (both random and

1991 *Mathematics Subject Classification.* Primary 94B05, 05B25, 51E20; Secondary 51E14, 51E22, 51E23.

Key words and phrases. Subspace code, network coding, partial spread.

Th. Honold gratefully acknowledges financial support for a short visit to the University of Bayreuth in March 2015, where part of this research has been done. M. Kiermaier and S. Kurz were supported by EU COST Action IC1104. In addition, S. Kurz's work was also supported through the DFG project "Ganzzahlige Optimierungsmodelle für Subspace Codes und endliche Geometrie" (DFG grant KU 2430/3-1).

adversarial errors) by selecting the codewords subject to a lower bound on their mutual distance in a suitable metric on $\mathrm{PG}(v-1,\mathbb{F}_q)$, resembling the classical block code selection process based on the Hamming distance properties.

Accordingly, we call any set $\mathcal{C}$ of subspaces of $\mathbb{F}_q^v$ a *q-ary subspace code of packet length* v. Two widely used distance measures for subspace codes (motivated by an information-theoretic analysis of the Koetter-Kschischang-Silva model) are the so-called *subspace distance*

$$\begin{aligned}\mathrm{d}_\mathrm{S}(X,Y)&=\dim(X+Y)-\dim(X\cap Y)\\&=\dim(X)+\dim(Y)-2\cdot\dim(X\cap Y)\\&=2\cdot\dim(X+Y)-\dim(X)-\dim(Y)\end{aligned}\tag{1}$$

and *injection distance*

$$\mathrm{d}_\mathrm{I}(X,Y)=\max\left\{\dim(X),\dim(Y)\right\}-\dim(X\cap Y).\tag{2}$$

With this the *minimum distance* in the subspace metric of a subspace code $\mathcal{C}$ containing at least two codewords is defined as

$$\mathrm{d}_\mathrm{S}(\mathcal{C}):=\min\left\{\mathrm{d}_\mathrm{S}(X,Y);X,Y\in\mathcal{C},X\neq Y\right\},\tag{3}$$

and that in the injection metric as

$$\mathrm{d}_\mathrm{I}(\mathcal{C}):=\min\left\{\mathrm{d}_\mathrm{I}(X,Y);X,Y\in\mathcal{C},X\neq Y\right\}.\text{[1]}\tag{4}$$

A subspace code $\mathcal{C}$ is said to be a *constant-dimension code* (or *Grassmannian code*) if all codewords in $\mathcal{C}$ have the same dimension over $\mathbb{F}_q$. Since $\mathrm{d}_\mathrm{S}(X,Y)=2\cdot\mathrm{d}_\mathrm{I}(X,Y)$ whenever X and Y are of the same dimension, we need not care about the specific metric (d_S or d_I) used when dealing with constant-dimension codes. Moreover, $\mathrm{d}_\mathrm{S}(\mathcal{C})=2\cdot\mathrm{d}_\mathrm{I}(\mathcal{C})$ in this case and hence the minimum subspace distance of a constant-dimension code is always an even integer.

As in the classical case of block codes, the transmission rate of a network communication system employing a subspace code $\mathcal{C}$ is proportional to $\log(\#\mathcal{C})$. Hence, given a lower bound on the minimum distance $\mathrm{d}_\mathrm{S}(\mathcal{C})$ or $\mathrm{d}_\mathrm{I}(\mathcal{C})$ (providing, together with other parameters such as the physical characteristics of the network and the decoding algorithm used, a specified data integrity level[2]), we want the code size $M=\#\mathcal{C}$ to be as large as possible. It is clear that constant-dimension codes usually are not maximal in this respect and, as a consequence, we need to look at general mixed-dimension subspace codes for a rigorous solution of this optimization problem.

In the remaining part of this article we will restrict ourselves to the subspace distance d_S, since d_S seems to be more widely used in the network coding literature and consideration of both distance measures was not feasible given the available resources for our research.

From a mathematical point of view, any v-dimensional vector space V over $\mathbb{F}_q$ is just as good as the standard space $\mathbb{F}_q^v$ (since $V\cong\mathbb{F}_q^v$), and it will sometimes be convenient to work with non-standard spaces (for example with the extension field $\mathbb{F}_{q^v}/\mathbb{F}_q$, in order to exploit additional structure). Hence we fix the following terminology:

Definition 1.1. A *q-ary* (v,M,d) *subspace code*, also referred to as a *subspace code with parameters* $(v,M,d)_q$, is a set $\mathcal{C}$ of subspaces of $V\cong\mathbb{F}_q^v$ with $M=\#\mathcal{C}$ and $\mathrm{d}_\mathrm{S}(\mathcal{C})=d$. The space V is called the *ambient space* of $\mathcal{C}$.[3] The *dimension distribution* of $\mathcal{C}$ is

[1] Sometimes it will be convenient to allow $\#\mathcal{C}\leq 1$, in which case we formally set $\mathrm{d}_\mathrm{S}(\mathcal{C})=\mathrm{d}_\mathrm{I}(\mathcal{C})=\infty$.

[2] This integrity level is usually specified by an upper bound on the probability of transmission error allowed.

[3] Strictly speaking, the ambient space is part of the definition of a subspace code and we should write $(V,\mathcal{C})$ in place of $\mathcal{C}$. Since the ambient space is usually clear from the context, we have adopted the more convenient shorthand "$\mathcal{C}$".

the sequence $\delta(\mathcal{C}) = (\delta_0, \delta_1, \ldots, \delta_v)$ defined by $\delta_k = \#\{X \in \mathcal{C}; \dim(X) = k\}$. Two subspace codes $\mathcal{C}_1, \mathcal{C}_2$ are said to be *isomorphic* if there exists an isometry (with respect to the subspace metric) $\phi\colon V_1 \to V_2$ between their ambient spaces satisfying $\phi(\mathcal{C}_1) = \mathcal{C}_2$.

It is easily seen that isomorphic subspace codes $\mathcal{C}_1, \mathcal{C}_2$ must have the same alphabet size q and the same ambient space dimension $v = \dim(V_1) = \dim(V_2)$. The dimension distribution of a subspace code may be seen as a q-analogue of the Hamming weight distribution of an ordinary block code. As in the block code case, the quantities $\delta_k = \delta_k(\mathcal{C})$ are non-negative integers satisfying $\sum_{k=0}^{v} \delta_k = M = \#\mathcal{C}$.

Problem (Main Problem of Subspace Coding). *For a given prime power $q \geq 2$, packet length $v \geq 1$ and minimum distance $d \in \{1, \ldots, v\}$ determine the maximum size $\mathrm{A}_q(v,d) = M$ of a q-ary (v, M, d) subspace code and—as a refinement—classify the corresponding optimal codes up to subspace code isomorphism.*

Although our ultimate focus will be on the main problem for general mixed-dimension subspace codes as indicated, we will often build upon known results for the same problem restricted to constant-dimension codes, or mixed-dimension codes with only a small number of nonzero dimension frequencies δ_k. For this it will be convenient to denote, for subsets $T \subseteq \{0, 1, \ldots, v\}$, the maximum size of a $(v, M, d')_q$ subspace code $\mathcal{C}$ with $d' \geq d$ and $\delta_k(\mathcal{C}) = 0$ for all $k \in \{0, 1, \ldots, v\} \setminus T$ by $\mathrm{A}_q(v, d; T)$, and refer to subspace codes subject to this dimension restriction accordingly as $(v, M, d; T)_q$ codes. In other words, the set T specifies the dimensions of the subspaces which can be chosen as a codeword of a $(v, M, d; T)_q$ code, and determining the numbers $\mathrm{A}_q(v, d; T)$ amounts to extending the main problem to $(v, M, d; T)_q$ codes.[4]

While much research has been done on the determination of the numbers $\mathrm{A}_q(v, d; k) = \mathrm{A}_q(v, d; \{k\})$, the constant-dimension case, only very few results are known for $\#T > 1$.[5]

The purpose of this paper is to advance the knowledge in the mixed-dimension case and determine the numbers $\mathrm{A}_q(v, d)$ for further parameters q, v, d. In this regard we build upon previous work of several authors, as is nicely surveyed by Etzion in [15, Sect. 4]. In the parlance of Etzion's survey, our contribution partially solves Research Problem 20.[6]

The Gaussian binomial coefficients $\begin{bmatrix} v \\ k \end{bmatrix}_q$ give the number of k-dimensional subspaces of $\mathbb{F}_q^v$ (and of any ambient space $V \cong \mathbb{F}_q^v$) and satisfy

$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{v-i} - 1}{q^{k-i} - 1} = q^{k(v-k)} \cdot \bigl(1 + \mathrm{o}(1)\bigr) \quad \text{for } q \to \infty. \tag{5}$$

Since these numbers grow very quickly, especially for $k \approx v/2$, the exact determination of $\mathrm{A}_q(v, d)$ appears to be an intricate task—except for some special cases. Even more challenging is the refined problem of enumerating the isomorphism types of the corresponding optimal subspace codes (i.e. those of size $\mathrm{A}_q(v, d)$). In some cases such an exhaustive enumeration is currently infeasible due to the large number of isomorphism types or due to computational limitations. In this context we regard the determination of certain structural restrictions as a precursor to an exhaustive classification.

[4] In order to make $\mathrm{A}_q(v, d; T)$ well-defined for all $d \in \{1, \ldots, v\}$ and ensure the usual monotonicity property $\mathrm{A}_q(v, d; T) \geq \mathrm{A}_q(v, d'; T)$ for $d \leq d'$, it is necessary to take the maximum in the definition of $\mathrm{A}_q(v, d; T)$ over all codes with $d' \geq d$ (and not only over codes with exact minimum distance d). The definition of $\mathrm{A}_q(v, d)$ didn't require such extra care, since in the unrestricted case we can alter dimensions of codewords freely and hence transform any $(v, M, d')_q$ code with $d' \geq d$ into a $(v, M, d)_q$ code.

[5] Strictly speaking, this remark is true only in the binary case. For $q > 2$ even in the constant-dimension case very few results are known.

[6] For those already familiar with [15] we remark that our numbers $\mathrm{A}_q(v, d)$ translate into Etzion's $\mathcal{A}_q^S(v, d)$.

The remaining part of this paper is structured as follows. In Section 2 we provide further terminology and a few auxiliary concepts and results, which have proved useful for the subsequent subspace code optimization/classification. In Section 3 we determine the numbers $\mathrm{A}_q(v,d)$ for general q, v and some special values of d. Finally, in Section 4 we further discuss the binary case $q=2$ and determine the numbers $\mathrm{A}_2(v,d)$ for $v\leq 7$ and all but a few hard-to-resolve values of d. On the reader's side we will assume at least some rudimentary knowledge of subspace coding, which e.g. can be acquired by reading the survey [17] or its predecessor [15].

2. Preliminaries

2.1. The Automorphism Group of $\bigl(\mathrm{PG}(V),\mathrm{d}_\mathrm{S}\bigr)$.

Let us start with a description of the automorphism group of the metric space $\mathrm{PG}(v-1,\mathbb{F}_q)$ relative to the subspace distance. Since a general v-dimensional ambient space V is isomorphic to $\mathbb{F}_q^v$ as a vector space over $\mathbb{F}_q$ (and hence isometric to $(\mathbb{F}_q^v,\mathrm{d}_\mathrm{S})$), this yields a description of all automorphism groups $\mathrm{Aut}(V,\mathrm{d}_\mathrm{S})$ and also of all isometries between different ambient spaces $(V_1,\mathrm{d}_\mathrm{S})$ and $(V_2,\mathrm{d}_\mathrm{S})$.

It is clear that the linear group $\mathrm{GL}(v,\mathbb{F}_q)$ acts on $\mathrm{PG}(v-1,\mathbb{F}_q)$ as a group of $\mathbb{F}_q$-linear isometries. If q is not prime then there are additional semilinear isometries arising from the Galois group $\mathrm{Aut}(\mathbb{F}_q)=\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ in the obvious way (component-wise action on $\mathbb{F}_q^v$). Moreover, mapping a subspace $X\subseteq\mathbb{F}_q^v$ ("linear code of length v over $\mathbb{F}_q$") to its dual code $X^\perp$ (with respect to the standard inner product) respects the subspace distance and hence yields a further automorphism π of the metric space $\mathrm{PG}(v-1,\mathbb{F}_q)$. The map π also represemts a polarity (correlation of order 2) of the geometry $\mathrm{PG}(v-1,\mathbb{F}_q)$.

Theorem 2.1. *Suppose that $v\geq 3$.*[7] *The automorphism group G of $\mathrm{PG}(v-1,\mathbb{F}_q)$, viewed as a metric space with respect to the subspace distance, is generated by $\mathrm{GL}(v,\mathbb{F}_q)$, $\mathrm{Aut}(\mathbb{F}_q)$ and π. More precisely, G is the semidirect product of the projective general semilinear group $\mathrm{P\Gamma L}(v,\mathbb{F}_q)$ with a group of order 2 acting by matrix transposition on $\mathrm{PGL}(v,\mathbb{F}_q)$ and trivially on $\mathrm{Aut}(\mathbb{F}_q)$.*

Most of this theorem is already contained in [41], but we include a complete proof for convenience.

Proof. Let f be an automorphism of $\mathrm{PG}(v-1,\mathbb{F}_q)$. Then either f interchanges $\{\mathbf{0}\}$ and $\mathbb{F}_q^v$ or leaves both subspaces invariant (using the fact that $\{\mathbf{0}\}$, $\mathbb{F}_q^v$ are the only subspaces with a unique complementary subspace). Moreover, if f fixes $\{\mathbf{0}\}$, $\mathbb{F}_q^v$ then it preserves the dimension of subspaces and hence represents a collineation of the geometry $\mathrm{PG}(v-1,\mathbb{F}_q)$. By the Fundamental Theorem of Projective Geometry (here we use the assumption $v\geq 3$), a collineation is represented by an element of $\mathrm{P\Gamma L}(v,\mathbb{F}_q)$. Since π interchanges $\{\mathbf{0}\}$ and $\mathbb{F}_q^v$, either f or $f\circ\pi$ stabilizes $\{\mathbf{0}\}$, $\mathbb{F}_q^v$ and belongs to $\mathrm{P\Gamma L}(v,\mathbb{F}_q)$. This proves the first assertion and shows that $\mathrm{P\Gamma L}(v,\mathbb{F}_q)$ has index 2 in G.[8] Finally, denoting by ϕ the Frobenius automorphism of $\mathbb{F}_q$ (over its prime field $\mathbb{F}_p$), we have $\phi(x_1y_1+\dots+x_vy_v)=\phi(x_1)\phi(y_1)+\dots+\phi(x_v)\phi(y_v)$ and hence, using a dimension argument, $\phi(X^\perp)=\phi(X)^\perp$, i.e. $\phi\circ\pi=\pi\circ\phi$. Since the adjoint map (with respect to the standard inner product on $\mathbb{F}_q^v$) of $\mathbf{x}\to\mathbf{A}\mathbf{x}$ is $\mathbf{y}\to\mathbf{A}^\mathsf{T}\mathbf{y}$, the second assertion follows and the proof is complete. □

In effect, Theorem 2.1 reduces the isomorphism problem for subspace codes to the determination of the orbits of $\mathrm{GL}(v,\mathbb{F}_q)$, respectively $\Gamma\mathrm{L}(v,\mathbb{F}_q)$, on subsets of $\mathrm{PG}(v-1,\mathbb{F}_q)$.

[7] The case $v\leq 2$ is completely trivial—as far as subspace codes are concerned—and can be safely excluded.

[8] The nontrivial coset $\{\pi\circ g; g\in\mathrm{P\Gamma L}(v,\mathbb{F}_q)\}$ consists precisely of all correlations of $\mathrm{PG}(v-1,\mathbb{F}_q)$.

In the most important case $q = 2$ the semilinear part is void, which further simplifies the problem. As a word of caution we remark that, in view of the presence of the polarity π, the dimension distribution of subspace codes is not an isomorphism invariant. Rather we have that $\delta(\mathcal{C}) = (\delta_0, \delta_1, \dots, \delta_v)$ leaves for a code $\mathcal{C}' \cong \mathcal{C}$ the reverse distribution $\delta(\mathcal{C}') = (\delta_v, \delta_{v-1}, \dots, \delta_0)$ as a second possibility.

The formula in (5) for the Gaussian binomial coefficients, which can be put into the form

$$\begin{aligned}\begin{bmatrix} v \\ k \end{bmatrix}_q &= \frac{\prod_{i=0}^{v-1}(q^v - q^i)}{q^{k(v-k)} \cdot \prod_{i=0}^{k-1}(q^k - q^i) \cdot \prod_{i=0}^{v-k-1}(q^{v-k} - q^i)} \\ &= \frac{\#\operatorname{GL}(v, \mathbb{F}_q)}{q^{k(v-k)} \cdot \#\operatorname{GL}(k, \mathbb{F}_q) \cdot \#\operatorname{GL}(v-k, \mathbb{F}_q)},\end{aligned}$$

reflects the group-theoretical fact that $\operatorname{GL}(v, \mathbb{F}_q)$ acts on the set of k-dimensional subspaces of $\mathbb{F}_q^v$ transitively and with a stabilizer isomorphic to

$$\begin{pmatrix} \operatorname{GL}(k, \mathbb{F}_q) & * \\ \mathbf{0} & \operatorname{GL}(v-k, \mathbb{F}_q) \end{pmatrix}.$$

We can go further and ask for a description of the orbits of $\operatorname{GL}(v, \mathbb{F}_q)$ in its induced action on ordered pairs (X, Y) of subspaces. Such a description has significance for modelling the transmission of subspaces in the Koetter-Kschischang-Silva model by a discrete memoryless (stationary) channel, which in essence amounts to specifying time-independent transition probabilities $\mathrm{p}(Y|X)$.

Lemma 2.2. *For any integer triple a, b, c satisfying $0 \leq a, b \leq v$ and $\max\{0, a+b-v\} \leq c \leq \min\{a, b\}$ the group $\operatorname{GL}(v, q)$ acts transitively on ordered pairs of subspaces (X, Y) of $\mathbb{F}_q^v$ with $\dim(X) = a$, $\dim(Y) = b$, and $\dim(X \cap Y) = c$.*[9] *Moreover, each such integer triple gives rise to an orbit of $\operatorname{GL}(v, \mathbb{F}_q)$ on ordered pairs of subspaces of $\mathbb{F}_q^v$ with length*

$$q^{(a-c)(b-c)} \begin{bmatrix} v \\ c \end{bmatrix}_q \begin{bmatrix} v-c \\ a-c \end{bmatrix}_q \begin{bmatrix} v-a \\ b-c \end{bmatrix}_q > 0.$$

Proof. The restrictions on a, b, c are necessary, since $\dim(X \cap Y) \leq \min\{\dim(X), \dim(Y)\}$ and $\dim(X \cap Y) = \dim(X) + \dim(Y) - \dim(X + Y) \geq \dim(X) + \dim(Y) - v$. Conversely, if a, b, c satisfy the restrictions then c, $a - c$, $b - c$ are non-negative with sum $c + (a-c) + (b-c) = a + b - c \leq v$. Hence we can choose $a + b - c$ linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_{a+b-c}$ in $\mathbb{F}_q^v$ and set $X = \langle \mathbf{b}_1, \dots, \mathbf{b}_a \rangle$, $Y = \langle \mathbf{b}_1, \dots, \mathbf{b}_b \rangle$, and consequently $X \cap Y = \langle \mathbf{b}_1, \dots, \mathbf{b}_c \rangle$.

It remains to show that $\operatorname{GL}(v, q)$ acts transitively on those pairs of subspaces and compute the orbit lengths. Transitivity is an immediate consequence of the fact that the corresponding sequences of $a + b - c$ linearly independent vectors, defined as above, can be isomorphically mapped onto each other. The stabilizer of (X, Y) in $\operatorname{GL}(v, \mathbb{F}_q)$ has the form

$$\begin{pmatrix} \operatorname{GL}(c, \mathbb{F}_q) & * & * & * \\ \mathbf{0} & \operatorname{GL}(a-c, \mathbb{F}_q) & \mathbf{0} & * \\ \mathbf{0} & \mathbf{0} & \operatorname{GL}(b-c, \mathbb{F}_q) & * \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \operatorname{GL}(v-a-b+c, \mathbb{F}_q) \end{pmatrix},$$

which leads to the stated formula for the orbit length after a short computation.[10] □

[9] Alternatively, we could prescribe the dimension of the join $X + Y$ in place of $X \cap Y$.

[10] Alternatively, count quadruples (X, Y, Z, W) of subspaces of $\mathbb{F}_q^v$ satisfying $X \cap Y = Z$, $X + Y = W$ and X/Z is complementary to Y/Z in W/Z.

2.2. **Basic Properties of the Numbers** $\mathrm{A}_q(v,d;T)$**.** In this subsection we collect some elementary but useful properties of the numbers $\mathrm{A}_q(v,d;T)$ and consider briefly the growth of $k \mapsto \mathrm{A}_q(v,d;k)$ (the constant-dimension case). Henceforth V will denote a v-dimensional vector space over $\mathbb{F}_q$, if not explicitly stated otherwise, and we will use the abbreviations $\begin{bmatrix}V\\T\end{bmatrix}$ for the set of all subspaces $X \subseteq V$ with $\dim(X) \in T$ ($\begin{bmatrix}V\\k\end{bmatrix}$ in the constant-dimension case $T = \{k\}$) and $\mathcal{C}_T = \mathcal{C} \cap \begin{bmatrix}V\\T\end{bmatrix}$ for subspace codes $\mathcal{C}$ with ambient space V (with the usual convention $\mathcal{C}_k = \mathcal{C}_{\{k\}}$). Further we set $[a,b] = \{a, a+1, \dots, b-1, b\}$ for $0 \leq a \leq b \leq v$.

Note that the following properties apply in particular to $\mathrm{A}_q(v,d) = \mathrm{A}_q(v,d;[0,v])$.

Lemma 2.3. *(i)* $\mathrm{A}_q(v,1;T) = \sum_{t\in T} \begin{bmatrix}v\\t\end{bmatrix}_q$*, and the unique optimal code in this case is* $\begin{bmatrix}V\\T\end{bmatrix} = \biguplus_{t\in T} \begin{bmatrix}V\\t\end{bmatrix}$*;*

(ii) $\mathrm{A}_q(v,d;T) \geq \mathrm{A}_q(v,d';T)$ *for all* $1 \leq d \leq d' \leq v$*;*

(iii) $\mathrm{A}_q(v,d;T) \leq \mathrm{A}_q(v,d;T')$ *for all* $T \subseteq T' \subseteq [0,v]$*;*

(iv) $\mathrm{A}_q(v,d;T \cup T') \leq \mathrm{A}_q(v,d;T) + \mathrm{A}_q(v,d;T')$ *for all* $T, T' \subseteq [0,v]$*; equality holds if* $\min\bigl\{|t-t'|; t \in T, t' \in T'\bigr\}$ *(i.e., the distance between* T *and* T' *in the Euclidean metric) is at least* d*;*

(v) $\mathrm{A}_q(v,d;T) = \mathrm{A}_q(v,d;v-T)$*, where* $v - T = \{v-t; t \in T\}$*.*

(vi) The metric space $\begin{bmatrix}V\\T\end{bmatrix}$*,* $T \neq \emptyset$*, has diameter* $v-d$*, where* $d = \min\bigl\{|s+t-v|; s,t \in T\bigr\}$ *(the distance between* v *and* $T+T \subset \mathbb{R}$ *in the Euclidean metric).*[11]

Proof. Only (iv), (v) and (vi) require a proof.

In (iv) we may assume $T \cap T' = \emptyset$. (Otherwise write $T \cup T' = T \uplus (T' \setminus T)$ and use (iii).) If $\mathcal{C}$ is any $(v,M,d;T\cup T')_q$ code then $\#\mathcal{C}_T \leq \mathrm{A}_q(v,d;T)$, $\#\mathcal{C}_{T'} \leq \mathrm{A}_q(v,d;T')$ and $M = \#\mathcal{C}_T + \#\mathcal{C}_{T'} \leq \mathrm{A}_q(v,d;T) + \mathrm{A}_q(v,d;T')$, as asserted.

For the proof of (v) assume $V = \mathbb{F}_q^v$ and use the fact that the map $\pi\colon X \to X^\perp$ represents an automorphism of the metric space $\mathrm{PG}(v-1,\mathbb{F}_q)$ and maps $\begin{bmatrix}V\\T\end{bmatrix}$ onto $\begin{bmatrix}V\\v-T\end{bmatrix}$.

Finally, (v) implies that the largest possible distance between $X \in \begin{bmatrix}V\\s\end{bmatrix}$, $Y \in \begin{bmatrix}V\\t\end{bmatrix}$ is $\min\{s+t, 2v-s-t\}$. (This is clearly true if $s + t \leq v$, and the case $s + t > v$ can be reduced to the former by setting $s' = v - s$, $t' = v - t$ and using (v).) In particular, the diameter of $\begin{bmatrix}V\\s\end{bmatrix}$ is $2\min\{s, v-s\}$. Assertion (vi) now follows from the observation that $\min\{s+t, 2v-s-t\} = v - |s+t-v|$. □

Next we discuss the growth of the numbers $\mathrm{A}_q(v,d;k)$ as a function of $k \in \{0,1,\dots,\lfloor v/2\rfloor\}$.[12] While not directly applicable to the mixed-dimension case, this analysis provides some useful information also for this case, since mixed-dimension codes are composed of constant-dimension "layers".

Since the minimum distance of a a constant-dimension code is an even integer, we need only consider the case $d = 2\delta \in 2\mathbb{Z}$.

Lemma 2.4. *For* $1 \leq \delta \leq k \leq \lfloor v/2\rfloor$ *the inequality*

$$\frac{\mathrm{A}_q(v,2\delta;k)}{\mathrm{A}_q(v,2\delta;k-1)} > q^{v-2k+\delta} \cdot C(q,\delta)$$

holds with $C(q,1) = 1$ *and* $C(q,\delta) = 1 - 1/q$ *for* $\delta \geq 2$*; in particular,* $\mathrm{A}_q(v,2\delta;k) > q \cdot \mathrm{A}_q(v,2\delta;k-1)$*. As a consequence, the numbers* $\mathrm{A}_q(v,2\delta;k)$*,* $k \in [\delta, v-\delta]$*, form a strictly unimodal sequence.*

[11] In particular, $\begin{bmatrix}V\\T\end{bmatrix}$ has diameter v if there exist $s,t \in T$ with $s+t = v$ and diameter $< v$ otherwise.

[12] By symmetry, the range $k \in \{\lfloor v/2\rfloor + 1, \dots, v\}$ need not be considered; cf. Lemma 2.3(v).

Note that $C(q,\delta)$ is independent of v,k and satisfies $\lim_{q\to\infty} C(q,\delta)=1$. In fact our proof of the lemma will show that for $\delta\geq 2$ the number $C(q,\delta)=1-q^{-1}$ may be replaced by the larger quantity $\prod_{i=\delta}^{\infty}(1-q^{-i})$, which is even closer to 1.

Proof. First we consider the case $\delta=1$, in which the numbers $\mathrm{A}_q(v,2\delta;k)=\mathrm{A}_q(v,2;k)=\begin{bmatrix}v\\k\end{bmatrix}_q$ are already known. Here the assertion follows from

$$\frac{\begin{bmatrix}v\\k\end{bmatrix}_q}{\begin{bmatrix}v\\k-1\end{bmatrix}_q}=\frac{q^{v-k+1}-1}{q^k-1}=q^{v-2k+1}\cdot\frac{1-q^{-(v-k+1)}}{1-q^{-k}}>q^{v-2k+1},$$

using $v-k+1>k$ for the last inequality.

Now assume $\delta\geq 2$. The lifting construction produces $(v,q^{(k-\delta+1)(v-k)},2\delta;k)_q$ constant-dimension codes ("lifted MRD codes") and gives the lower bound $\mathrm{A}_q(v,d;k)\geq q^{(k-\delta+1)(v-k)}$, which is enough for our present purpose. On the other hand, every $(v,M,2\delta;k)_q$ code satisfies $\mathrm{d_S}(X,X')=2k-2\dim(X\cap X')\geq 2\delta$ or, equivalently, $\dim(X\cap X')\leq k-\delta$ for any two distinct codewords $X,X'\in\mathcal{C}$. This says that $(k-\delta+1)$-dimensional subspaces of V are contained in at most one codeword of $\mathcal{C}$ and gives by double-counting the upper bound

$$M\leq\frac{\begin{bmatrix}v\\k-\delta+1\end{bmatrix}_q}{\begin{bmatrix}k\\k-\delta+1\end{bmatrix}_q}=\frac{(q^v-1)(q^{v-1}-1)\cdots(q^{v-(k-\delta)}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q^\delta-1)}\tag{6}$$

for such codes. Simplyfing we get $M<q^{(k-\delta+1)(v-k)}/C(q,\delta,k)$ with $C(q,\delta,k)=\prod_{i=\delta}^{k}(1-q^{-i})$. Replacing k by $k-1$ turns this into an upper bound for $\mathrm{A}_q(v,2\delta,k-1)$ and, together with the previously derived lower bound for $\mathrm{A}_q(v,d;k)$, gives the estimate

$$\begin{aligned}\frac{\mathrm{A}_q(v,2\delta;k)}{\mathrm{A}_q(v,2\delta;k-1)}&>\frac{q^{(k-\delta+1)(v-k)}\cdot C(q,\delta,k)}{q^{(k-\delta)(v-k+1)}}=q^{v-2k+\delta}\cdot C(q,\delta,k)\\&>q^{v-2k+\delta}\cdot\prod_{i=\delta}^{\infty}(1-q^{-i})=q^{v-2k+\delta}\cdot\frac{\prod_{i=1}^{\infty}(1-q^{-i})}{\prod_{i=1}^{\delta-1}(1-q^{-i})}.\end{aligned}\tag{7}$$

From Euler's Pentagonal Number Theorem (see e.g. [42, Th. 15.5]) we have

$$\begin{aligned}\prod_{i=1}^{\infty}(1-q^{-i})&=1+\sum_{m=1}^{\infty}(-1)^m\left(q^{-(3m^2-m)/2}+q^{-(3m^2+m)/2}\right)\\&=1-q^{-1}-q^{-2}+q^{-5}+q^{-7}-q^{-12}-q^{-15}\pm\cdots\\&>1-q^{-1}-q^{-2}.\end{aligned}$$

Hence (and using $\delta\geq 2$), the quotient in (7) is $>\frac{1-q^{-1}-q^{-2}}{1-q^{-1}}=\frac{q^2-q-1}{q^2-q}=1-\frac{1}{q(q-1)}\geq 1-\frac{1}{q}$, as claimed. The remaining assertions of the lemma are clear. □

From the lemma, the numbers $\mathrm{A}_q(v,d;k)$ grow fast as a function of k in the range $0\leq k\leq v/2$. This implies that the following simple estimates yield quite a good appproximation to $\mathrm{A}_q(v,d)$.

Theorem 2.5. *Suppose that for some parameters q,v,d we already know all of the numbers $\mathrm{A}_q(v,d;k)$, $0\leq k\leq v$. Then*

$$\sum_{\substack{k=0\\k\equiv\lfloor v/2\rfloor \bmod d}}^{v}\mathrm{A}_q\bigl(v,2\lceil d/2\rceil;k\bigr)\leq\mathrm{A}_q(v,d)\leq 2+\sum_{k=\lceil d/2\rceil}^{v-\lceil d/2\rceil}\mathrm{A}_q\bigl(v,2\lceil d/2\rceil;k\bigr),$$

and this constitutes the best bound for $\mathrm{A}_q(v,d)$ *that does not depend on information about the cross-distance distribution between different layers* $\begin{bmatrix}V\\k\end{bmatrix}$ *and* $\begin{bmatrix}V\\l\end{bmatrix}$.

Proof. First note that 2δ, where $\delta = \lceil d/2 \rceil$, is the smallest even integer $\geq d$ and hence $\mathrm{A}_q(v,d;k) = \mathrm{A}_q(v,2\delta;k)$. Now the upper bound follows from the observation that the two (isomorphic) metric spaces consisting of all subspaces of V of dimension $< \delta$ (respectively, $> v-\delta$) have diameter $< d$ and thus contain at most one codeword of any $(v,M,d)_q$ code.

The lower bound follows from the inequality $\mathrm{d_S}(X,Y) \geq |\dim(X) - \dim(Y)|$ and remains valid if we replace $\lceil v/2 \rceil$ by an arbitrary integer r. In order to show that the lower bound is maximized for $r = \lceil d/2 \rceil$, let σ_r denote the sum of all numbers $\mathrm{A}_q(v,2\delta;k)$ with $k \in [0,v]$ and $k \equiv r \bmod d$. Since σ_r is d-periodic and satisfies $\sigma_r = \sigma_{v-r}$ for $0 \leq r \leq v$, it suffices to show $\sigma_r > \sigma_{r-1}$ for $\lceil (v-d)/2 \rceil + 1 \leq r \leq \lfloor v/2 \rfloor$.

For r in the indicated range, $\sigma_r - \sigma_{r-1}$ is a sum of terms of the form

$$\begin{aligned}&\mathrm{A}_q(v,2\delta;r-td) - \mathrm{A}_q(v,2\delta;r-1-td) + \mathrm{A}_q\bigl(v,2\delta;r+(t+1)d\bigr) - \mathrm{A}_q\bigl(v,2\delta;r-1+(t+1)d\bigr)\\ &= \mathrm{A}_q(v,2\delta;r-td) - \mathrm{A}_q(v,2\delta;r-1-td) - \mathrm{A}_q\bigl(v,2\delta;v-r+1-(t+1)d\bigr) + \mathrm{A}_q\bigl(v,2\delta;r+(t+1)d\bigr),\end{aligned}$$

where $0 \leq t \leq \lfloor r/d \rfloor$ and the convention $\mathrm{A}_q(v,2\delta;k) = 0$ for $k \notin [0,v]$ has been used. From Lemma 2.4 we have

$$\mathrm{A}_q(v,2\delta;r-td) \begin{cases} > q \cdot \mathrm{A}_q(v,2\delta;r-1-td), \\ \geq q^{2r-v-1+d} \cdot \mathrm{A}_q\bigl(v,2\delta;v-r+1-(t+1)d\bigr), \end{cases}$$

and $2r - v - 1 + d \geq d - 1 \geq 1$.[13] From this (and $q \geq 2$) we can certainly conclude that $\mathrm{A}_q(v,2\delta;r-td) > \mathrm{A}_q(v,2\delta;r-1-td) + \mathrm{A}_q\bigl(v,2\delta;v-r+1-(t+1)d\bigr)$, so that $\sigma_r - \sigma_{r-1}$ is positive, as claimed. □

2.3. **Shortening and Puncturing Subspace Codes.**

In [33, 15] two different constructions of $(v-1,M',d')_q$ subspace codes from $(v,M,d)_q$ subspace codes were defined and both referred to as "puncturing subspace codes". Whereas the construction in [33] usually has $M' = M$ (as is the case for puncturing block codes), the construction in [15] satisfies $M' < M$ apart from trivial cases and behaves very much like the shortening construction for block codes. For this reason, we propose to change its name to "shortening subspace codes". We will now give a simple, coordinate-free definition of the shortening construction and generalize the puncturing construction of [33] to incorporate simultaneous point-hyperplane puncturing.

Definition 2.6. Let $\mathcal{C}$ be a subspace code with ambient space V, H a hyperplane and P a point of $\mathrm{PG}(V)$. The *shortened codes* of $\mathcal{C}$ in H, P and the pair P, H are defined as

$$\begin{aligned}\mathcal{C}|_H &= \{X \in \mathcal{C}; X \subseteq H\},\\ \mathcal{C}|^P &= \{X/P; X \in \mathcal{C}, P \subseteq X\},\\ \mathcal{C}|_H^P &= \{X \in \mathcal{C}; X \subseteq H\} \cup \{Y \cap H; Y \in \mathcal{C}, P \subseteq Y\}\\ &= \mathcal{C}|_H \cup \{Y \cap H; Y \in \mathcal{C}|_P\}\end{aligned}$$

with ambient spaces H, V/P and H, respectively.

Note that the operations $\mathcal{C} \mapsto \mathcal{C}|^P$ and $\mathcal{C} \mapsto \mathcal{C}|_H$ are dual to each other in the sense that they are switched by the polarity π. Simultaneous point-hyperplane shortening $\mathcal{C} \mapsto \mathcal{C}|_H^P$ glues these parts together by means of the projection map $X \mapsto (X+P) \cap H$. The

[13] Of course this implies that the second inequality above is also strict. The trivial case $d = 1$ has been tacitly excluded.

puncturing construction in [15] is equivalent to $\mathcal{C} \mapsto \mathcal{C}|_H^P$ with the additional assumption that P and H are not incident. This assumption implies $\mathcal{C}|^P \cap \mathcal{C}|_H = \emptyset$ and that $X \mapsto (X+P) \cap H$ maps $\mathcal{C}|^P$ isomorphically onto the subspace code $\{Y \cap H; Y \in \mathcal{C}|^P\}$.[14] Shortening in point-hyperplane pairs (P, H) with $P \subseteq H$ seems of little value and will not be considered further in this paper.

Definition 2.7. Let $\mathcal{C}$ be a subspace code with ambient space V, H a hyperplane and P a point of $\mathrm{PG}(V)$. The *punctured codes* of $\mathcal{C}$ in H, P are defined as

$$\begin{aligned}\mathcal{C}_H &= \{X \cap H; X \in \mathcal{C}\},\\ \mathcal{C}^P &= \big\{(X+P)/P; X \in \mathcal{C}\big\}\end{aligned}$$

with ambient spaces H and V/P, respectively. Moreover, the punctured code of $\mathcal{C}$ in P, H with respect to a splitting $\mathcal{C} = \mathcal{C}_1 \uplus \mathcal{C}_2$ is defined as

$$\mathcal{C}_H^P = (\mathcal{C}_1, \mathcal{C}_2)_H^P = \{X \cap H; X \in \mathcal{C}_1\} \cup \{(Y+P) \cap H; Y \in \mathcal{C}_2\}$$

with ambient space H.

Here mutatis mutandis the same remarks as on the shortening constructions apply. The original puncturing operation in [33] is $\mathcal{C} \to \mathcal{C}_H$, with attention restricted to constant-dimension codes and the following modification: If $\mathcal{C}$ has constant-dimension k then $\mathcal{C}_H$ can be turned into a code of constant-dimension $k-1$ by replacing each subspace $X \in \mathcal{C}$ with $X \cap H = X$ (i.e. $X \subseteq H$) by some $(k-1)$-dimensional subspace contained in X. Simultaneous point-hyperplane puncturing has been defined to round off the construction principles and will not be used in later sections.

The next lemma provides general information about the parameters of shortened and punctured subspace codes. The lemma makes reference to the *degree* of a point P or a hyperplane H with respect to a subspace code $\mathcal{C}$, which are defined as $\deg(P) = \{X \in \mathcal{C}; P \subseteq X\} = \#\left(\mathcal{C}|^P\right)$ and dually as $\deg(H) = \{X \in \mathcal{C}; X \subseteq H\} = \#\left(\mathcal{C}|_H\right)$, respectively.[15]

Lemma 2.8. *Let $\mathcal{C}$ be a $(v, M, d)_q$ subspace code with ambient space V and (P, H) a non-incident point-hyperplane pair in $\mathrm{PG}(V)$.*

(i) If $d \geq 2$ then the shortenend code $\mathcal{C}|_H^P$ has parameters $(v-1, M', d')_q$ with $M' = \deg(P) + \deg(H)$ and $d' \geq d-1$.

(ii) If $d \geq 3$ then the punctured codes $\mathcal{C}_H$, $\mathcal{C}^P$ have parameters $(v-1, M, d')$ with $d' \geq d-2$. The same is true of the punctured code $(\mathcal{C}_1, \mathcal{C}_2)_H^P$ with respect to any splitting $\mathcal{C} = \mathcal{C}_1 \uplus \mathcal{C}_2$ satisfying $\mathrm{d_S}(\mathcal{C}_1, \mathcal{C}_2) \geq d+1$.

The strong bound $d' \geq d-1$ in Part (i) of the lemma accounts for the significance of the shortening construction, as mentioned in [15].

The usefulness of the bounds in Part (ii), which are weaker, is less clear. The first assertion in (ii) was already observed in [33] (for the code $\mathcal{C}_H$). The condition $\mathrm{d_S}(\mathcal{C}_1, \mathcal{C}_2) \geq d+1$ in the second assertion is required, since cross-distances can decrease by 3 during puncturing. Alternatively we could have assumed $d \geq 4$ and replaced $d' \geq d-2$ by $d' \geq d-3$ in the conclusion.

Proof of the lemma. (i) Since $P \nsubseteq H$, the codes $\mathcal{C}|_H$ and $\mathcal{C}|^P$ are disjoint, and since $d \geq 2$, the same is true of $\mathcal{C}|_H$ and $\{Y \cap H; Y \in \mathcal{C}|^P\}$. Hence we have $\#\mathcal{C}|_H^P = \#\left(\mathcal{C}|_H\right) + \#\left(\mathcal{C}|^P\right) = \deg(H) + \deg(P)$.

[14] Moreover, one can show that in this case $\mathcal{C}|_H^P \cong \{X+P; X \in \mathcal{C}|_H\} \cup \mathcal{C}|^P$, the analogous point-hyperplane shortening using $X \mapsto (X \cap H) + P$ instead.

[15] Incidences with the trivial spaces $\{0\}$, V (if they are in $\mathcal{C}$) are thus not counted.

Since $Y \mapsto Y \cap H$ defines an isometry from $\mathrm{PG}(V/P)$ onto $\mathrm{PG}(H)$, we need only check "cross-distances" $\mathrm{d_S}(X, Y \cap H)$ with $X \in \mathcal{C}|_H$, $Y \in \mathcal{C}|^P$. In this case we have

$$\begin{aligned}\mathrm{d_S}(X, Y \cap H) &= \dim(X) + \dim(Y \cap H) - 2\dim(X \cap Y \cap H)\\ &= \dim(X) + \dim(Y) - 1 - 2\dim(X \cap Y)\\ &= \mathrm{d_S}(X, Y) - 1,\end{aligned}$$

and the assertion regarding d' follows.

(ii) As in the proof of (i) one shows

$$\mathrm{d_S}(X+P, Y+P) \in \begin{cases}\{\mathrm{d_S}(X,Y), \mathrm{d_S}(X,Y)-2\} & \text{if } P \nsubseteq X \wedge P \nsubseteq Y\\ \{\mathrm{d_S}(X,Y)+1, \mathrm{d_S}(X,Y)-1\} & \text{if } P \nsubseteq X \wedge P \subseteq Y.\end{cases}$$

This implies the assertion about $\mathcal{C}^P$, and that about $\mathcal{C}_H$ follows by duality. For the last assertion we need only check cross-distances $\mathrm{d_S}\bigl(X \cap H, (Y+P) \cap H\bigr)$ with $X \in \mathcal{C}_1$, $Y \in \mathcal{C}_2$. As shown above, the numbers $\mathrm{d_S}(X,Y)$, $\mathrm{d_S}(X, Y+P)$, $\mathrm{d_S}\bigl(X, (Y+P)\cap H\bigr)$, $\mathrm{d_S}\bigl(X \cap H, (Y+P) \cap H\bigr)$ successively differ by at most one. Hence $\mathrm{d_S}\bigl(X \cap H, (Y+P) \cap H\bigr) \geq \mathrm{d_S}(X,Y) - 3$, and the result follows.[16] □

2.4. **A Property of the Lifted Gabidulin Codes.** A q-ary lifted Gabidulin code $\mathcal{G} = \mathcal{G}_{v,k,\delta}$ has parameters $(v, q^{(k-\delta+1)(v-k)}, 2\delta; k)$, where $1 \leq \delta \leq k \leq v/2$, and can be defined in a coordinate-free manner as follows (see e.g. [30, Sect. 2.5]): The ambient space is taken as $V = W \times \mathbb{F}_{q^n}$, where $n = v - k$ and W denotes a fixed k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$, and $\mathcal{G}$ consists of all subspaces

$$G(a_0, \dots, a_{k-\delta}) = \bigl\{(x, a_0x + a_1x^q + a_2x^{q^2} + \cdots + a_{k-\delta}x^{q^{k-\delta}}); x \in W\bigr\}$$

with $a_i \in \mathbb{F}_{q^n}$. In other words, $\mathcal{G}$ consists of the graphs $\Gamma_f = \bigl\{(x, f(x)); x \in W\bigr\}$ of all $\mathbb{F}_q$-linear maps $f \colon W \to \mathbb{F}_{q^n}$ that are represented by a linearized polynomial of symbolic degree at most $k - \delta$.[17]

The code $\mathcal{G}$ forms a geometrically quite regular object. The most significant property, shared by all lifted MRD codes with the same parameters, is that $\mathcal{G}$ forms an exact 1-cover of the set of all $(k-\delta)$-flats of $\mathrm{PG}(V)$ that are disjoint from the special flat $S = \{0\} \times \mathbb{F}_{q^n}$.[18] A further regularity property, which we will need later, is that every point $P \notin S$ has degree $q^{(k-\delta)(v-k)}$ with respect to $\mathcal{G}$. Indeed, $P = \mathbb{F}_q(a,b) \in \Gamma_f$ if and only if $f(a) = b$ (using $a \neq 0$), which reduces f to a linear map on a $(k-1)$-dimensional subspace of W.[19]

From now on we assume that $n = k$ (or $v = 2k$, the "square" case) and hence $W = \mathbb{F}_{q^k}$. In this case the codes $\mathcal{G} = \mathcal{G}_{2k,k,\delta}$, $1 \leq \delta \leq k$, are invariant under a correlation of $\mathrm{PG}(\mathbb{F}_{q^k} \times \mathbb{F}_{q^k})$ fixing S, as our next theorem shows. In particular, every hyperplane H of $\mathrm{PG}(V)$ with $H \not\supseteq S$ contains, dually so-to-speak, precisely $q^{(k-\delta)(v-k)}$ codewords of $\mathcal{G}$, This property will be needed later in Section 3.3. Before stating the theorem, let us

[16] The distance actually drops by 3 in the case $P \subseteq X + Y \wedge X \cap (P+Y) \subseteq H$, and nontrivial examples of P, H, X, Y that satisfy these conditions are easily found.

[17] Recall that every $\mathbb{F}_q$-linear endomorphism of $\mathbb{F}_{q^n}$ is represented by a unique linearized polynomial of symbolic degree $\leq n-1$. Restriction to W then gives a canonical reprsentation of $\mathbb{F}_q$-linear maps $f \colon W \to \mathbb{F}_{q^n}$ by linearized polynomials of symbolic degree $\leq k-1$.

[18] Since the codewords of $\mathcal{G}$ are disjoint from S (since they are graphs of linear maps), it is clear that only flats disjoint from S are covered. The exact cover property is a consequence of Delsarte's characterization of MRD codes (cf. Footnote 19) and is proved in [30, Lemma 6], for example.

[19] Here the following property of Gabidulin codes (or lifted MRD codes in general) due to Delsarte [10] simplifies the view considerably: Every $\mathbb{F}_q$-linear map $g \colon U \to \mathbb{F}_{q^n}$, defined on an arbitary $(k-\delta+1)$-dimensional subspace U of W, extends uniquely to a linear map $f \in \mathcal{G}$. This property also gives $\#\mathcal{G}$ immediately.

remark that a non-degenerate bilinear form on $V = \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ is given by $\big\langle (a,b),(x,y)\big\rangle = \operatorname{Tr}(ax+by)$, where $\operatorname{Tr}(x) = \operatorname{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(x) = x + x^q + \dots + x^{q^{k-1}}$ is the trace of the field extension $\mathbb{F}_{q^k}/\mathbb{F}_q$. The symbol $\perp$ will denote orthogonality with respect to this bilinear form. Hence hyperplanes of $\operatorname{PG}(V)$ have the form $H_{a,b} = \big\{(x,y) \in V; \operatorname{Tr}(ax+by) = 0\big\} = \mathbb{F}_q(a,b)^\perp$ for a unique point $\mathbb{F}_q(a,b)$ of $\operatorname{PG}(V)$.

Theorem 2.9. *The q-ary Gabidulin codes $\mathcal{G} = \mathcal{G}_{2k,k,\delta}$ are linearly isomorphic to their duals $\mathcal{G}^\perp = \{X^\perp; X \in \mathcal{G}\}$ and hence invariant under a correlation of* $\operatorname{PG}(v-1,\mathbb{F}_q)$. *Any correlation κ fixing $\mathcal{G}$ fixes also S.*

Proof. The condition $\mathbb{F}_q(a,b) \in G(a_0,\dots,a_{k-\delta})^\perp$, or

$$\begin{aligned}\operatorname{Tr}\big(ax + bf(x)\big) &= \operatorname{Tr}\big((a+ba_0)x + ba_1x^q + \dots + ba_{k-\delta}x^{q^{k-\delta}}\big)\\ &= \operatorname{Tr}\big((a+ba_0)^{q^{k-\delta}}x^{q^{k-\delta}} + (ba_1)^{q^{k-\delta-1}}x^{q^{k-\delta}} + \dots + ba_{k-\delta}x^{q^{k-\delta}}\big)\\ &= 0\end{aligned}$$

for all $x \in \mathbb{F}_{q^k}$, is equivalent to

$$a^{q^{k-\delta}} = \sum_{i=0}^{k-\delta}(-a_{k-\delta-i}^{q^i})b^{q^i},$$

since the trace bilinear form on $\mathbb{F}_{q^k}$ is non-degenerate. This shows

$$\mathbb{F}_q(a,b) \in G(a_0,\dots,a_{k-\delta})^\perp \iff \mathbb{F}_q(b,a^{q^{k-\delta}}) \in G(-a_{k-\delta},-a_{k-\delta-1}^q,\dots,-a_0^{q^{k-\delta}})$$

In other words, the $\mathbb{F}_q$-linear map $\phi\colon V \to V$, $(a,b) \mapsto (b,a^{q^{k-\delta}})$, which represents a collineation of $\operatorname{PG}(V)$, maps $G(a_0,\dots,a_{k-\delta})^\perp$ to $G(-a_{k-\delta},-a_{k-\delta-1}^q,\dots,-a_0^{q^{k-\delta}})$ and $\mathcal{G}^\perp = \big\{G(a_0,\dots,a_{k-\delta})^\perp; a_i \in \mathbb{F}_{q^k}\big\}$ to $\mathcal{G}$. The correlation $\kappa\colon \mathbb{F}_q(a,b) \mapsto H_{b,a^{q^{k-\delta}}} = \mathbb{F}_q\phi(a,b)^\perp$ then satisfies $\kappa(\mathcal{G}) = \mathcal{G}$, since $\operatorname{Tr}(ax+by) = \operatorname{Tr}(by + a^{q^{k-\delta}}x^{q^{k-\delta}})$ implies $\phi(H_{a,b}) = H_{b,a^{q^{k-\delta}}}$, i.e. ϕ and $\perp$ commute.[20]

The last assertion follows from the fact that S is the unique $(k-1)$-flat complementary to all codewords of $\mathcal{G}$. □

Remark 1. The automorphism group $\operatorname{Aut}(\mathcal{G})$ of $\mathcal{G} = \mathcal{G}_{2k,k,\delta}$ obviously contains all collineations of $\operatorname{PG}(V)$, $V = \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$, induced by linear maps of the form $(x,y) \mapsto \big(ax, by + f(x)\big)$ with $a,b \in \mathbb{F}_{q^k}^\times$ and $f(x)$ as above. These collineations form a subgroup of $\operatorname{Aut}(\mathcal{G})$, which has two orbits on the point set $\mathcal{P}$ of $\operatorname{PG}(V)$, viz. S and $\mathcal{P} \setminus S$.[21] From this and Theorem 2.9 we have that for any point $P \notin S$ and any hyperplane $H \not\supseteq S$ there exists a correlation $\kappa \in \operatorname{Aut}(\mathcal{G})$ satisfying $\kappa(P) = H$.

3. Classification Results for General Parameter Sets

In this section we present old and new results on optimal subspace codes in the mixed-dimension case for general q, v, and d. We start with the largest possible minimum distances (i.e. $d \approx v$) and later switch to small d. Whenever possible, we determine the numbers $\mathrm{A}_q(v,d)$, the dimension distributions realized by the corresponding optimal codes, and a classification of the different isomorphism types. In order to avoid trivialties, we assume from now on $v \geq 3$ and $2 \leq d \leq v$.

[20] This also shows that the square of κ is the collineation induced by $\phi^2\colon \mathbb{F}_q(a,b) \mapsto \mathbb{F}_q(a^q,b^q)$.

[21] Clearly this subgroup is also transitive on $\mathcal{G}$, but this fact won't be used in the sequel.

3.1. **Subspace Distance** v**.** Apart from the trivial case $d = 1$ covered by Lemma 2.3(i), the case $d = v$ is the easiest to settle. For the statement of Part (ii) of the classification result recall that the largest size of a $(2k, M, 2k; k)_q$ constant-dimension code is $M = \mathrm{A}_q(2k, 2k; k) = q^k + 1$ and that optimal $(2k, q^k + 1, 2k; k)_q$ codes are the same as $(k-1)$-spreads in $\mathrm{PG}(2k-1, \mathbb{F}_q)$, i.e. sets of mutually disjoint $(k-1)$-flats (or k-dimensional subspaces of $\mathbb{F}_q^{2k}$) partitioning the point set of $\mathrm{PG}(2k-1, \mathbb{F}_q)$. The number of isomorphism classes of such spreads or, equivalently, the number of equivalence classes of translation planes of order q^k with kernel containing $\mathbb{F}_q$ under the equivalence relation generated by isomorphism and transposition [11, 31], is generally unknown (and astronomically large even for modest parameter sizes).

Theorem 3.1. *(i) If v is odd then $\mathrm{A}_q(v, v) = 2$. There are $(v+1)/2$ isomorphism classes of optimal $(v, 2, v)_q$ subspace codes. These have the form $\{X, X'\}$ with $\dim(X) = i \in [0, (v-1)/2]$, $\dim(X') = v - i$ and $X \cap X' = \{0\}$.*

(ii) If $v = 2k$ is even then $\mathrm{A}_q(v, v) = \mathrm{A}_q(v, v, k) = q^k + 1$. Every optimal $(v, q^k + 1, v)_q$ subspace code has constant dimension k. The exact number of isomorphism classes of such codes is known in the following cases:

q	v	*# isomorphism classes*
2	4	1
2	6	1
2	8	7
3	4	2
3	6	7
4	4	3
5	4	20
7	4	973

The numbers $\mathrm{A}_q(v, v)$ have also been determined in [22, Sect. 5].

Proof of the theorem. (i) Subspaces X, X' of V are at distance $\mathrm{d_S}(X, X') = v$ iff they are complementary ($X \cap X' = \{0\}$, $X + X' = V$). Since v is odd, subspaces of the same dimension cannot be complementary, excluding the existence of three mutually complementary subspaces. This implies $\mathrm{A}_q(v, v) = 2$. The classification of optimal $(v, 2, v)_q$ codes is then immediate.

(ii) Suppose that $\mathcal{C}$ is an arbitrary $(2k, M, 2k)_q$ code. If $\mathcal{C}$ contains a codeword of dimension $i \neq k$ then all other codewords must have dimension $2k - i \neq i$ and hence $\#\mathcal{C} \leq 2$. Certainly $\mathcal{C}$ cannot be optimal in this case. Hence $\mathcal{C}$ has constant dimension k and size $M = q^k + 1$.

Determining the isomorphism classes of the optimal $(2k, q^k + 1, 2k; k)_q$ codes in the table amounts to classifying the translation planes of order ≤ 49 up to isomorphism and polarity. This has been done in a series of papers [9, 12, 13, 25, 35], from which we have collected the relevant information; cf. also [37, Sect. 5]. [22] □

[22] Uniqueness of the projective planes of orders 4 and 8 gives the uniqueness of the $(4, 5, 4; 2)_2$ and $(6, 9, 6; 3)_2$ codes. The 8 translation planes of order 16 include 1 polar pair (the Lorimer-Rahilly and Johnson-Walker planes), accounting for 7 isomorphism classes of $(8, 17, 8; 4)_2$ codes. The 2 translation planes of order 9 ($\mathrm{PG}(2, \mathbb{F}_3)$ and the Hall plane) are both self-polar, accounting for 2 isomorphism classes of $(4, 10, 4; 2)_3$ codes. The 7 translation planes of order 27 are all self-polar, accounting for 7 isomorphism classes of $(6, 28, 6; 3)_3$ codes. Among the translation planes of order 16, three planes ($\mathrm{PG}(2, \mathbb{F}_{16})$, the Hall plane and one of the two semifield planes) have a kernel of order 4. All three planes are self-polar, accounting for 3 isomorphism classes of $(4, 17, 4; 2)_4$ codes. Finally, there are 21 translation planes of order 25 including 1 polar pair (the two Foulser

We remark that it is easy to obtain the numbers $\mathrm{A}_q(v,v;T)$ for arbitrary subsets $T\subseteq[0,v]$ from Theorem 3.1.

3.2. **Subspace Distance $v-1$.** The case $d=v-1$ is considerably more involved. Here we can no longer expect that optimal subspace codes have constant dimension, since for example in a $(2k,q^k+1,2k;k)_q$ constant-dimension code replacing any codeword by an incident $(k-1)$- or $(k+1)$-dimensional subspace produces a subspace code with $d=v-1$. However, it turns out that the largest constant-dimension codes satisfying $d\geq v-1$ are still optimal among all $(v,M,v-1)_q$ codes and that there are only few possibilities for the dimension distribution of an optimal $(v,M,v-1)_q$ code.

Before stating the classification result for $d=v-1$, let us recall that in the case of odd length $v=2k+1$ the optimal constant-dimension codes in the two largest layers $\left[\begin{smallmatrix}V\\k\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}V\\k+1\end{smallmatrix}\right]$ (which are isomorphic as metric spaces) correspond to maximal partial $(k-1)$-spreads in $\mathrm{PG}(2k,\mathbb{F}_q)$ and their duals.[23] The maximum size of a partial $(k-1)$-spread in $\mathrm{PG}(2k,\mathbb{F}_q)$ is $q^{k+1}+1$, as determined by Beutelspacher [4, Th. 4.1]; cf. also [14, Th. 2.7]. This gives $\mathrm{A}_q(2k+1,2k;k)_q=\mathrm{A}_q(2k+1,2k;k+1)_q=q^{k+1}+1$. Moreover, there are partial spreads $\mathcal{S}$ of the following type: The q^k holes (uncovered points) of $\mathcal{S}$ form the complement of a k-dimensional subspace X_0 in a $(k+1)$-dimensional subspace Y_0, and $X_0\in\mathcal{S}$. We may call X_0 the “moving subspace” of $\mathcal{S}$, since it can replaced by any other k-dimensional subspace of Y_0 without destroying the spread property of $\mathcal{S}$.

Theorem 3.2. *(i) If $v=2k$ is even then $\mathrm{A}_q(v,v-1)=\mathrm{A}_q(v,v;k)=q^k+1$. All optimal subspace codes contain, apart from codewords of dimension k, at most one codeword of each of the dimensions $k-1$ and $k+1$. The dimension distributions realized by optimal subspace codes are $(\delta_{k-1},\delta_k,\delta_{k+1})=(0,q^k+1,0)$, $(1,q^k,0)$, $(0,q^k,1)$, $(1,q^k-1,1)$ (and $\delta_t=0$ for all other t).*

(ii) If $v=2k+1\geq 5$ is odd then $\mathrm{A}_q(v,v-1)=\mathrm{A}_q(v,v-1;k)=q^{k+1}+1$. The dimension distributions realized by optimal subspace codes are $(\delta_{k-1},\delta_k,\delta_{k+1},\delta_{k+2})=(0,q^{k+1}+1,0,0)$, $(0,0,q^{k+1}+1,0)$, $(0,q^{k+1},1,0)$, $(0,1,q^{k+1},0)$, $(0,q^{k+1},0,1)$, and $(1,0,q^{k+1},0)$.

In (ii) it is necessary to exclude the case $v=3$, since $\mathrm{A}_q(3,2)=q^2+q+2$; cf. Section 3.4. Some results on the numbers $\mathrm{A}_q(v,v-1)$ can also be found in [22, Sect. 5]

Proof. (i) Let $\mathcal{C}$ be an optimal $(2k,M,2k-1)_q$ code. Since $\left[\begin{smallmatrix}V\\<k\end{smallmatrix}\right]$ has diameter $2k-2$, at most one codeword of dimension $<k$ can occur in $\mathcal{C}$, and similarly for dimension $>k$. This and Theorem 3.1(ii) give $q^k+1\leq M\leq q^k+3$. Clearly there must be codewords of dimension k, and hence none of dimensions $<k-1$ or $>k+1$.

If there exists $X_0\in\mathcal{C}$ with $\dim(X_0)=k-1$ then $X_0\cap Z=\emptyset$ for all other codewords $Z\in\mathcal{C}_k$. Similarly, if there exists $Y_0\in\mathcal{C}$ with $\dim(Y_0)=k+1$ then $Y_0\cap Z=P$ is a point for all $Z\in\mathcal{C}_k$, and if both X_0 and Y_0 exist then they must be complementary subspaces of V.

If $\delta_k=q^k+1$ then $\mathcal{C}_k$ is a spread and covers all points. Hence X_0 cannot exist, i.e. $\delta_{k-1}=0$. By duality we then have also $\delta_{k+1}=0$ and hence $M=q^k+1$. Next suppose $\delta_k=q^k$. Then $\mathcal{C}_k$ is a partial spread with exactly $1+q+\dots+q^{k-1}$ holes (uncovered points). If X_0 exists, it contains $1+q+\dots+q^{k-2}$ of these holes. If Y_0 exists, it contains $\#Y_0-q^k=1+q+\dots+q^{k-1}$ of these holes (i.e. all holes). Since these two properties

planes) and 1347 translation planes of order 49 including 374 polar-pairs, accounting for the remaining two table entries.

[23] A partial spread is a set of mutually disjoint subspaces of the same dimension which does not necessarily cover the whole point set of the geometry.

conflict with each other, we must have $\delta_{k-1}\delta_{k+1} = 0$ and hence $M = q^k + 1$. The only remaining possibility is $\delta_k = q^k - 1$, $\delta_{k-1} = \delta_{k+1} = 1$; here $M = q^k + 1$ as well.

Until now we have shown that $\mathrm{A}_q(v, v-1; k) = q^k + 1$ and the dimension distributions realized by optimal codes are among those listed. Conversely, the distribution $(\delta_{k-1}, \delta_k, \delta_{k+1}) = (0, q^k + 1, 0)$ is realized by a $(k-1)$-spread, $(1, q^k, 0)$ by a $(k-1)$-spread with one subspace X replaced by a $(k-1)$-dimensional subspace $X_0 \subset X$, $(0, q^k, 1)$ by the dual thereof, and $(1, q^k - 1, 1)$ by removing from a $(k-1)$-spread a pair of subspaces X, Y and adding X_0, Y_0 with $\dim(X_0) = k-1$, $\dim(Y_0) = k+1$, $X_0 \subset X$, $Y_0 \supset Y$ and $X_0 \cap Y_0 = \emptyset$.[24]

(ii) Let $\mathcal{C}$ be an optimal $(2k+1, M, 2k)_q$ code. From the remarks preceding Theorem 3.2 we know that $M \geq q^{k+1} + 1$. For reasons of diameter (cf. the proof of (i)[25]), $\mathcal{C}$ can contain only codewords of dimensions $k-1$, k, $k+1$ and $k+2$; moreover, $\delta_{k-1}, \delta_{k+2} \leq 1$ and $\delta_{k-1}\delta_k = \delta_{k+1}\delta_{k+2} = 0$.

If $\delta_{k-1} = \delta_{k+2} = 1$ then $M = 2$, which is absurd.[26] If exactly one of $\delta_{k-1}, \delta_{k+2}$ is nonzero, we can assume by duality that $\delta_{k+2} = 1$. The δ_k codewords in $\mathcal{C}_k$ form a partial spread and meet the single codeword $Y_0 \in \mathcal{C}_{k+2}$ in distinct points. Hence Y_0 contains $1 + q + \cdots + q^{k+1} - \delta_k$ holes of $\mathcal{C}_k$ and $1 + q + \cdots + q^{k+1} - \delta_k \leq 1 + q + \cdots + q^{2k} - \delta_k(1 + q + \cdots + q^{k-1})$, the total number of holes of $\mathcal{C}_k$. This implies $\delta_k \leq q^{k+1}$ and hence $M = q^{k+1} + 1$, $(\delta_{k-1}, \delta_k, \delta_{k+1}, \delta_{k+2}) = (0, q^{k+1}, 0, 1)$. A subspace code realizing this dimension distribution can be obtained from a maximal partial $(k-1)$-spread $\mathcal{S}$ of the type discussed before Theorem 3.2, if we replace the moving subspace X_0 by any $(k+2)$-dimensional subspace $Y \supset Y_0$.[27]

In the remaining case $\delta_{k-1} = \delta_{k+2} = 0$ we may assume $\delta_{k+1} \leq \delta_k$, again by duality. Assuming further $\delta_{k+1} \in \{0, 1\}$ or, by symmetry, $\delta_k \in \{q^{k+1} + 1, q^{k+1}\}$ easily leads to $M = q^{k+1} + 1$ and one of the dimension distributions $(0, q^{k+1} + 1, 0, 0)$, $(0, q^{k+1}, 1, 0)$. The first distribution is realized by any maximal partial $(k-1)$-spread and the second distribution by a subspace code obtained from a maximal partial $(k-1)$-spread $\mathcal{S}$ of the type discussed before Theorem 3.2, if we replace the moving subspace X_0 by Y_0.

The only remaining case is $2 \leq \delta_{k+1} \leq \delta_k \leq q^{k+1} - 1$ (and $\delta_{k-1} = \delta_{k+2} = 0$). Here our goal is to show that this forces $\delta_k + \delta_{k+1} < q^{k+1} + 1$, a contradiction. Since $M = \#\mathcal{C} > q^{k+1} + 1$ implies the existence of a $(2k+1, q^{k+1} + 1, 2k)_q$ code, we can assume $\delta_k = q^{k+1} + 1 - \delta_{k+1}$ and hence $2 \leq \delta_{k+1} \leq \lfloor (q^{k+1} + 1)/2 \rfloor$.[28]

Let A, B be the sets of points covered by $\mathcal{C}_k$ and $\mathcal{C}_{k+1}$, respectively. Since codewords in $\mathcal{C}_k$ are mutually disjoint and disjoint from those in $\mathcal{C}_{k+1}$, we have $A \cap B = \emptyset$, $\#A = \delta_k(1 + q + \cdots + q^{k-1}) = (q^{k+1} + 1 - \delta_{k+1})(1 + q + \cdots + q^{k-1}) = 1 + q + \cdots + q^{k-1} + q^{k+1} + \cdots + q^{2k} - \delta_{k+1}(1 + q + \cdots + q^{k-1})$, and hence $\#B \leq q^k + \delta_{k+1}(1 + q + \cdots + q^{k-1})$. Further we know that codewords in $\mathcal{C}_{k+1}$ intersect each other in at most a point. Hence the desired contradiction will follow if we can show that the minimum number $c(\delta)$ of points covered by δ subspaces of V of dimension $k+1$ mutually intersecting in at most a point is strictly larger than than the linear function $g(\delta) = q^k + \delta(1 + q + \cdots + q^{k-1})$ for all $\delta \in \{2, 3, \ldots, q^{k+1} - 1\}$.

[24] This can be done, since the (final) choice of Y_0 amounts to selecting a complement to $(X_0 + Y)/Y$ in V/Y, i.e. a point outside a hyperplane in the quotient geometry $\mathrm{PG}(V/Y)$.

[25] The argument is almost the same: There must be codewords of dimension k or $k+1$ (otherwise $\#\mathcal{C} \leq 2$), and hence none of dimension $< k-1$ or $> k+2$

[26] We know already that $M \geq q^{k+1} + 1$.

[27] The remaining blocks $X \in \mathcal{S}$ satisfy $X \cap Y_0 = \emptyset$ and hence $\dim(X \cap Y) \leq 1$.

[28] Using the smaller upper bound for δ_{k+1}, however, does not simplify the subsequent proof, and we may just consider the full range $2 \leq \delta_{k+1} \leq q^{k+1} - 1$.

For bounding $c(\delta)$ we use the *degree distribution* $(b_0, b_1, b_2, \dots)$ of such a set $\mathcal{D}$ of subspaces, which is defined by $b_i = \#\{P; \deg(P) = i\}$ and satisfies the "standard equations"

$$\begin{aligned}\sum_{i\geq 0} b_i &= 1 + q + \cdots + q^{2k},\\ \sum_{i\geq 1} ib_i &= \delta(1 + q + \cdots + q^k),\\ \sum_{i\geq 2}\binom{i}{2} b_i &= \binom{\delta}{2};\end{aligned}$$

moreover, $c(\delta) = \sum_{i\geq 1} b_i = 1 + q + \cdots + q^{2k} - b_0$. Using the standard equations, we can evaluate $\sum_i p(i)b_i$ for every quadratic polynomial $p(X)$. If $p(0) > 0$ and $p(i) \geq 0$ for $i = 1, 2, \dots$, this will give an upper bound for b_0 and hence a lower bound for $c(\delta)$ as desired.[29]

The polynomials

$$p(X) = \binom{X - i_0}{2} = \frac{1}{2}(X-i_0)(X-i_0-1) = \binom{X}{2} - i_0\binom{X}{1} + \frac{i_0(i_0+1)}{2}, \quad i_0 \in \mathbb{Z}^+,$$

have this property, since they are convex and vanish at two successive integers. We obtain

$$\begin{aligned}\frac{i_0(i_0+1)}{2} b_0 = p(0)b_0 &\leq \sum_i p(i)b_i\\ &= \frac{i_0(i_0+1)}{2}(1 + q + \cdots + q^{2k}) - i_0\delta(1 + q + \cdots + q^k) + \binom{\delta}{2}\end{aligned}$$

and

$$\begin{aligned}c(\delta) = 1 + q + \cdots + q^{2k} - b_0 &\geq \frac{2\delta(1 + q + \cdots + q^k)}{i_0 + 1} - \frac{\delta(\delta - 1)}{i_0(i_0 + 1)}\\ &= \frac{\delta\bigl(1 + 2i_0(1 + q + \cdots + q^k) - \delta\bigr)}{i_0(i_0 + 1)} = f_{i_0}(\delta),\end{aligned}$$

say, a convex quadratic function with zeros 0 and $1 + 2i_0(1 + q + \cdots + q^k)$. The maximum value of f_{i_0} restricted to integral arguments is

$$\begin{aligned}f_{i_0}\bigl(i_0(1 + q + \cdots + q^k)\bigr) &= f_{i_0}\bigl(1 + i_0(1 + q + \cdots + q^k)\bigr)\\ &= \frac{\bigl(1 + i_0(1 + q + \cdots + q^k)\bigr)i_0(1 + q + \cdots + q^k)}{i_0(i_0 + 1)}\\ &= \frac{\bigl(1 + i_0(1 + q + \cdots + q^k)\bigr)(i_0 + 2)(1 + q + \cdots + q^k)}{(i_0 + 1)(i_0 + 2)}\\ &= f_{i_0+1}\bigl(1 + i_0(1 + q + \cdots + q^k)\bigr).\end{aligned}$$

Since f_{i_0+1} is still increasing at $\delta = 1 + i_0(1 + q + \cdots + q^k)$, we see that the best lower bound obtained from all functions f_{i_0} simultaneously is

$$c(\delta) \geq f_{i_0}(\delta) \quad \text{for} \quad \delta \in \bigl[(i_0 - 1)(1 + q + \cdots + q^k) + 1, i_0(1 + q + \cdots + q^k)\bigr], \tag{8}$$

and that this lower bound has a continuous extension $f\colon [1, q^{k+1}] \to \mathbb{R}$, which is strictly convex in the intervals displayed in (8) and constant on the "holes" of length 1 in between.

[29] Exhibiting a polynomial $p(X)$ suitable for a particular problem in Combinatorics is sometimes referred to as the "variance trick"; cf. [7, p. 6].

From this it is clear that we need only check the inequality $f_{i_0}(\delta) > g(\delta)$ at the points $\delta = (i_0 - 1)(1 + q + \cdots + q^k) + 1$, $1 \leq i_0 \leq q$ (left endpoints of the intervals in (8)). Moreover, at the first endpoint $\delta = 1$ ($i_0 = 1$) and the last endpoint $\delta = q^{k+1}$ ($i_0 = q$) equality is sufficient.[30]

In the boundary cases we have indeed equality, $f_1(1) = q^k + 1 \cdot (1 + q + \cdots + q^{k-1}) = g(1)$ and $f_q(q^{k+1}) = q^k + q^{k+1}(1 + q + \cdots + q^{k-1}) = g(q^{k+1})$, as is easily verified from the definition of $f_{i_0}(\delta)$.[31] Finally, for $2 \leq i_0 \leq q - 1$ we have

$$\begin{aligned} f_{i_0}\bigl(1 + (i_0 - 1)(1 + q + \cdots + q^k)\bigr) &= \frac{1}{i_0}(1 + q + \cdots + q^k)\bigl(1 + (i_0 - 1)(1 + q + \cdots + q^k)\bigr) \\ &= (1 + q + \cdots + q^k)\left(1 + \tfrac{i_0-1}{i_0} \cdot (q + \cdots + q^k)\right) \\ &> (1 + q + \cdots + q^k)\bigl(1 + (i_0 - 1)(1 + \cdots + q^{k-1})\bigr) \\ &= 1 + \cdots + q^k + (i_0 - 1)(1 + \cdots + q^k)(1 + \cdots + q^{k-1}) \\ &= q^k + \bigl(1 + (i_0 - 1)(1 + \cdots + q^k\bigr)(1 + \cdots + q^{k-1}) \\ &= g\bigl(1 + (i_0 - 1)(1 + q + \cdots + q^k)\bigr), \end{aligned}$$

where we have used $\frac{i_0-1}{i_0} \cdot q > i_0 - 1$. This completes the proof of the theorem.[32] □

Remark 2. It is known that any partial $(k - 1)$-spread in $\mathrm{PG}(2k - 1, \mathbb{F}_q)$ of cardinality $q^k - 1$ can be completed to a spread; see for example [14, Th. 4.5]. This implies that all optimal $(2k, q^k + 1, 2k - 1)_q$ subspace codes arise from a $(k-1)$-spread by the constructions described at the end of the proof of Part (i) of Theorem 3.2.

3.3. **Subspace Distance $v - 2$.** The case $d = v - 2$ is yet more involved and we are still far from being able to determine the numbers $\mathrm{A}_q(v, v - 2)$ in general. For even $v = 2k$ the problem almost certainly includes the determination of the numbers $\mathrm{A}_q(2k, 2k - 2; k)$, which are known so far only in a single nontrivial case, viz. $\mathrm{A}_2(6, 4; 3) = 77$ [30]. On the other hand, we will present rather complete information on the odd case $v = 2k + 1$, for which the corresponding numbers $\mathrm{A}_q(2k + 1, 2k - 1; k) = \mathrm{A}_q(2k + 1, 2k; k) = q^{k+1} + 1$, equal to the size of a maximal partial $(k - 1)$-spread in $\mathrm{PG}(2k, \mathbb{F}_q)$, are known; cf. the references in Section 3.2. Our results are collected in Theorem 3.3 below. For the proof of the theorem we will need the fact that a maximal partial $(k - 1)$-spread $\mathcal{S}$ in $\mathrm{PG}(2k, \mathbb{F}_q)$ covers each hyperplane at least once. This (well-known) fact may be seen as follows: If a hyperplane H of $\mathrm{PG}(2k, \mathbb{F}_q)$ contains t members of $\mathcal{S}$, it intersects the remaining $q^{k+1} + 1 - t$ members in a $(k - 1)$-dimensional space and hence

$$t(1+q+\cdots+q^{k-1}) + (q^{k+1}+1-t)(1+q+\cdots+q^{k-2}) \leq \#H = 1+q+\cdots+q^{2k-1},$$

or $tq^{k-1} \leq q^{k-1} + q^k$. The difference $q^{k-1} + q^k - tq^{k-1} = q^{k-1}(q + 1 - t)$ gives the number of holes of $\mathcal{S}$ in H, which must be $\leq q^k$ (the total number of holes of $\mathcal{S}$). This implies $1 \leq t \leq q + 1$, as asserted.

We also see that the number of holes of $\mathcal{S}$ in every hyperplane of $\mathrm{PG}(2k, \mathbb{F}_q)$ is of the form sq^{k-1} with $s \in \{0, 1, \ldots, q\}$. Further, since the average number of members of $\mathcal{S}$ in

[30] The last point $\delta = q^{k+1}$ is best viewed as the right endpoint of the hole $[q^{k+1} - 1, q^{k+1}]$, since the function f_q not really matters. Alternatively, one could check the strict inequality at $\delta = 2$ and $\delta = q^{k+1} - 1$, respectively.

[31] This comes not unexpected, since in these cases the optimal codes have size $q^{k+1} + 1$ and the sets A, B partition the point set of $\mathrm{PG}(2k, \mathbb{F}_q)$.

[32] The last computation could be replaced by another convexity argument involving the function $i_0 \mapsto f_{i_0}\bigl(1+(i_0 - 1)(1 + q + \cdots + q^k)\bigr)$.

a hyperplane is

$$\frac{(q^{k+1}+1)(1+q+\cdots+q^k)}{1+q+\cdots+q^{2k}}=\frac{1+q+\cdots+q^{2k+1}}{1+q+\cdots+q^{2k}}>q,$$

there exists at least one hyperplane containing $q+1$ members, and hence no holes of $\mathcal{S}$. The latter says that the set of holes of $\mathcal{S}$ does not form a blocking set with respect to hyperplanes and implies in particular that no line consists entirely of holes of $\mathcal{S}$. This fact will be needed later in Remark 4.

Theorem 3.3. *(i) If $v=2k\geq 8$ is even then $\mathrm{A}_q(v,v-2)=\mathrm{A}_q(v,v-2;k)$, and the known bound $q^{2k}+1\leq\mathrm{A}_q(v,v-2;k)\leq(q^k+1)^2$ applies. Moreover, $\mathrm{A}_q(4,2)=q^4+q^3+2q^2+q+3$ for all q, $\mathrm{A}_2(6,4)=77$ and $q^6+2q^2+2q+1\leq\mathrm{A}_q(6,4)\leq(q^3+1)^2$ for all $q\geq 3$.*

(ii) If $v=2k+1$ is odd then $\mathrm{A}_q(v,v-2)\in\{2q^{k+1}+1,2q^{k+1}+2\}$. Moreover, $\mathrm{A}_q(5,3)=2q^3+2$ for all q and $\mathrm{A}_2(7,5)=2\cdot 2^4+2=34.$[33]

Proof. (i) The evaluation of $\mathrm{A}_q(4,2)$ is a special case of Theorem 3.4 (but could also be easily accomplished adhoc). From now on we assume $k\geq 3$.

In the constant-dimension case the bounds $q^{2k}+1\leq\mathrm{A}_q(v,v-2;k)\leq(q^k+1)^2$ are well-known; see e.g. [30]. In order to show that the upper bound holds in the mixed-dimension case as well, let $\mathcal{C}$ be an optimal $(2k,M,2k-2)_q$ code and suppose $\mathcal{C}$ contains a codeword X_0 with $t=\dim(X_0)\neq k$. By duality we may assume $t\leq k-1$, and we certainly have $t\geq k-2$, since otherwise $\mathcal{C}_{k-1}=\mathcal{C}_k=\emptyset$ and $\#\mathcal{C}\leq 1+\mathrm{A}_q\bigl(2k,2k-2;[k+1,2k]\bigr)=1+\mathrm{A}_q\bigl(2k,2k-2;[0,k-1]\bigr)=1+\mathrm{A}_q(2k,2k-2;k-1)\leq 1+\frac{q^{2k}-1}{q^{k-1}-1}\leq q^{2k}$, contradicting the optimality of $\mathcal{C}$. The codewords in $\mathcal{C}_{k-2}\cup\mathcal{C}_{k-1}\neq\emptyset$ must be mutually disjoint and also disjoint from every codeword in $\mathcal{C}_k$. Moreover, $\delta_{k-2}\delta_{k-1}=0$ and $\delta_{k-2}\leq 1$.

Our strategy now is to bound the size of the "middle layer" $\#\mathcal{C}_k$ in terms of $t=\dim(X_0)$. If this leads to a sharp upper bound for $\mathcal{C}$, which conflicts with the best known lower bound for $\mathrm{A}_q(2k,2k-2;k)$, we can conclude $\mathcal{C}=\mathcal{C}_k$, and hence $\mathrm{A}_q(2k,2k-2)=\mathrm{A}_q(2k,2k-2;k)$.

Since any two codewords in $\mathcal{C}_k$ span at least a $(2k-1)$-dimensional space, we have that any $(2k-2)$-dimensional subspace of V contains at most one codeword of $\mathcal{C}_k$. Conversely, every codeword of $\mathcal{C}_k$, being disjoint from X_0, is contained in a $(2k-2)$-dimensional subspace intersecting X_0 in a subspace of the smallest possible dimension, viz. $\max\{t-2,0\}$.[34] Denoting by $\mathcal{S}$ the set of all such $(2k-2)$-dimensional subspaces and by r the (constant) degree of $\#\mathcal{C}_k$ with respect to $\mathcal{S}$, we get the bound $\#\mathcal{C}_k\leq\#\mathcal{S}/r$. It is easily seen that

$$\#\mathcal{S}=\begin{bmatrix}t\\t-2\end{bmatrix}_q q^{2(2k-t)}=\begin{bmatrix}t\\2\end{bmatrix}_q q^{4k-2t},$$

$$r=\begin{bmatrix}t\\t-2\end{bmatrix}_q q^{2(k-t)}=\begin{bmatrix}t\\2\end{bmatrix}_q q^{2k-2t}$$

for $t\geq 2$ and hence $\#\mathcal{C}_k\leq q^{2k}$ in this case.

For $t=1$ (the case $t=0$ does not occur on account of our assumption $k\geq 3$) we are in the case $k=3$ and have instead $\#\mathcal{S}=(1+q+q^2+q^3+q^4)q^4$, $r=q^2+q$, yielding only the weaker bound $\#\mathcal{C}_3\leq\lfloor q^3(1+q+q^2+q^3+q^4)/(1+q)\rfloor=q^6+q^4+q^2-q$.

[33] The bounds for $\mathrm{A}_2(v,v-2)$ were already established in [15, Th. 5] and $\mathrm{A}_2(5,3)=18$ in [18, Th. 14].

[34] The condition $\dim(S\cap X_0)=t-2$ is of course equivalent to $S+X_0=V$, but we need the former for the counting argument.

However, this bound can be sharpened by using for $\mathcal{S}$ the set of hyperplanes H not incident with the point X_0 and the bound $\#(\mathcal{C} \cap H) \leq q^3 + 1$. The improved bound is $\#\mathcal{C}_3 \leq (q^3 + 1)\#\mathcal{S}/r = (q^3 + 1)q^5/q^2 = q^6 + q^3$.

These bounds are sufficient to conclude the proof in the case where at most one codeword of dimension $\neq k$ exists. But for the case $\delta_{k-1} \geq 2$ and its dual, and for several cases having $\delta_{k-2} + \delta_{k-1} = \delta_{k+1} + \delta_{k+2} = 1$ we need better bounds.

First we do the case $\delta_{k-1} \geq 2$. Let X_1, X_2 be two distinct codewords in $\mathcal{C}_{k-1}$. Then X_1, X_2 are disjoint, and every $X \in \mathcal{C}_k$ is simultaneously disjoint from both X_1 and X_2. In this case we can bound $\#\mathcal{C}_k$ in the same way as above, using for $\mathcal{S}$ the set of $(2k-2)$-dimensional subspaces S of V satisfying $\dim(S \cap X_1) = \dim(S \cap X_2) = k - 3$. Since the number of simultaneous complements of two disjoint lines in $\mathrm{PG}(n-1, \mathbb{F}_q)$ is $q^{2n-7}(q^2 - 1)(q - 1)$,[35] we obtain

$$\#\mathcal{S} = \begin{bmatrix} k-1 \\ k-3 \end{bmatrix}_q^2 q^{2\cdot 6-7}(q^2-1)(q-1) = \begin{bmatrix} k-1 \\ 2 \end{bmatrix}_q^2 q^5(q^2-1)(q-1).$$

The degree r of $X \in \mathcal{C}_k$ with respect to $\mathcal{S}$ is equal to the number of $(k-2)$-dimensional subspaces of the k-dimensional space V/X meeting the (not necessarily distinct) hyperplanes $H_1 = (X_1 + X)/X$ and $H_2 = (X_2 + X)/X$ in a $(k-3)$-dimensional space. By duality, r is also equal to the number of lines in $\mathrm{PG}(k-1, \mathbb{F}_q)$ off two points P_1, P_2 (which may coincide or not), and hence

$$\begin{aligned} r &\geq \begin{bmatrix} k \\ 2 \end{bmatrix}_q - 2\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q + 1 = \begin{bmatrix} k-1 \\ 2 \end{bmatrix}_q q^2 - \left(\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q - 1\right) \\ &= \frac{(q^k - q)(q^{k-1} - q)}{(q^2-1)(q-1)} - \frac{q^{k-1} - q}{q-1} = \frac{(q^{k-1} - q)(q^k - q^2 - q + 1)}{(q^2-1)(q-1)}, \\ \#\mathcal{C}_k &\leq \frac{q^4(q^{k-1}-1)^2(q^{k-2}-1)}{q^k - q^2 - q + 1} = \frac{q^{3k} - q^{2k+2} - 2q^{2k+1} + 2q^{k+3} + q^{k+2} - q^4}{q^k - q^2 - q + 1} \\ &\leq q^{2k} - q^{k+1}, \end{aligned}$$

where the last inequality follows from a straightforward computation.[36] This new bound is sufficient for the range $2 \leq \delta_{k-1} \leq \frac{1}{2}q^{k+1}$ (since we may obviously assume $\delta_{k+1} \leq \delta_{k-1}$), but there remains a gap to the known upper bound $\delta_{k-1} \leq q^{k+1} + q^2$ for $k \geq 4$, respectively, $\delta_2 \leq q^4 + q^2 + 1$ for $k = 3$. However, for $\delta_{k-1} > \frac{1}{2}q^{k+1}$ the standard method to bound $\#\mathcal{C}_k$ in terms of the point degrees can be used: Since the $\delta_{k-1}(1 + q + \cdots + q^{k-2})$ points covered by the codewords in $\mathcal{C}_{k-1}$ must have degree 0 in $\mathcal{C}_k$, we obtain

$$\begin{aligned} \#\mathcal{C}_k &\leq \frac{q^k+1}{q^k-1}\left(q^{2k} - 1 - \delta_{k-1}(q^{k-1}-1)\right) = (q^k+1)^2 - \delta_{k-1} \cdot \frac{(q^k+1)(q^{k-1}-1)}{q^k-1} \\ &< q^{2k} + 1 - \delta_{k-1}\left(\frac{(q^k+1)(q^{k-1}-1)}{q^k-1} - \frac{4}{q}\right). \end{aligned}$$

[35] This is probably well-known and perhaps most easily established by counting triples (L_1, L_2, U) of mutually skew subspaces of $\mathbb{F}_q^n$ with $\dim(L_1) = \dim(L_2) = 2$, $\dim(U) = n-2$ in two ways: Using canonical matrices, the number $\#\{(L_1, L_2, S)\} = \#\{(S, L_1, L_2)\}$ of such triples is easily found to be $\left[{n \atop n-2}\right]_q q^{2(n-2)}(q^{n-2}-1)(q^{n-2}-q)$. Dividing this number by $\#\{(L_1, L_2)\} = \left[{n \atop 2}\right]_q \left[{n-2 \atop 2}\right]_q q^4$ gives $q^{2n-7}(q^2-1)(q-1)$, as asserted.

[36] The inequality is sharp precisely in the case $k = 3$, all q.

The factor of δ_{k-1} is ≥ 2 in all cases except $q = 2$, $k = 3$, leading to the desired contradiction $\#\mathcal{C} \leq \#\mathcal{C}_k + 2\delta_{k-1} \leq q^{2k}$. in the exceptional case we have $\#\mathcal{C} \leq 64 + 1 + \frac{1}{7}\delta_{k-1} \leq 68$, which also does the job.

It remains to consider the cases with $\delta_{k-2} + \delta_{k-1} = \delta_{k+1} + \delta_{k+2} = 1$. We may assume $k \geq 4$ and need only improve the previously established bound $\#\mathcal{C}_k \leq q^{2k}$ by one. We denote the unique codewords of dimensions $t < k$ and $u > k$ by X_0 and Y_0, respectively. From the proof we have $\#\mathcal{C}_k = q^{2k}$ if and only if every $(2k-2)$-dimensional subspace of V meeting X_0 in a $t-2$-dimensional space contains a codeword of $\mathcal{C}_k$. Since $\dim(X_0 \cap Y_0) = \frac{1}{2}\bigl(t + u - \mathrm{d_S}(X_0, Y_0)\bigr) \leq \bigl\lfloor \frac{1}{2}\bigl(k - 1 + k + 2 - (2k-2)\bigr)\bigr\rfloor = \bigl\lfloor \frac{3}{2} \bigr\rfloor = 1$, there exists a $(2k-2)$-dimensional subspace $S \subset V$ such that $\dim(S \cap X_0) = t - 2$ and $\dim(S \cap Y_0) \geq u - 1$. Then $\dim(S + Y_0) \leq 2k - 1$ and hence $S + Y_0$, and a fortiori S, cannot contain a codeword of $\mathcal{C}_k$.[37] This gives $\#\mathcal{C}_k \leq q^{2k} - 1$ and $\#\mathcal{C} \leq q^{2k} + 1$, as desired.

Finally, the equality $\mathrm{A}_2(6,4) = \mathrm{A}_2(6,4;3) = 77$ follows from $\mathrm{A}_2(6,4;3) > 2^6 + 2^3$, which implies $\delta_i = 0$ for $i \in \{1,2,4,5\}$. The lower bound for $\mathrm{A}_q(6,4)$, $q \geq 3$ follows from the corresponding bound for $\mathrm{A}_q(6,4;3)$, established in [30, Th. 2].

(ii) First we show $\mathrm{A}_q(2k+1, 2k-1) \geq 2q^{k+1} + 1$. For this we take the q-ary lifted $(2k+2, q^{2(k+1)}, 2k; k+1)$ Gabidulin code $\mathcal{G} = \mathcal{G}_{2k+2,k+1,k}$, which contains q^{k+1} codewords passing through any point P outside the special subspace $S = \{0\} \times \mathbb{F}_{q^{k+1}}$ and similarly q^{k+1} codewords in any hyperplane $H \nsubseteq S$; cf. Theorem 2.9. Among these points and hyperplanes we choose a non-incident pair (P, H) and shorten the code $\mathcal{G}$ in (P, H); cf. Section 2.3. The code $\mathcal{C} = \mathcal{G}|_H^P \cup \{H \cap S\}$ then has the required parameters $(2k+1, 2k-1, 2q^{k+1}+1)$.[38] Let us remark here that $\mathcal{C}$ admits only extensions (without decreasing the minimum distance) by $(k+1)$-dimensional subspaces of $\mathrm{PG}(H)$ containing $S \cap H$ (which is k-dimensional) and by k-dimensional subspaces contained in the $(k+1)$-dimensional subspace $(S + P) \cap H$. Hence, if $k \geq 3$ then it is impossible to extend $\mathcal{C}$ by more than one subspace and improve the construction.[39]

Next we establish the upper bound $\mathrm{A}_q(2k+1, 2k-1) \leq 2q^{k+1} + 2$. Let $\mathcal{C}$ be an optimal $(2k+1, M, 2k-1)_q$ code. If $\mathcal{C}$ contains only codewords of dimensions k and $k+1$, the bound follows from $\mathrm{A}_q(2k+1, 2k; k) = \mathrm{A}_q(2k+1, 2k; k+1) = q^{k+1} + 1$. Otherwise we must have $\delta_t = 0$ for $t \notin \{k-1, k, k+1, k+2\}$, since a codeword of dimension $t \leq k-2$ forces $\mathcal{C}_k = \emptyset$, contradicting $M \geq 2q^{k+1} + 1$ (and likewise, using duality, for $t \geq k+3$). The remaining cases to consider are $(\delta_{k-1}, \delta_{k+2}) = (1,0)$, $(0,1)$ or $(1,1)$. In these cases the bound is established using the remarks preceding the theorem. For example, if $X \in \mathcal{C}_{k-1}$ exists then all $Y \in \mathcal{C}_{k+1}$ must be disjoint from X. Since the dual of a maximal partial $(k-1)$-spread in $\mathrm{PG}(2k, \mathbb{F}_q)$ necessarily covers every point, this excludes the possibility $\delta_{k+1} = q^{k+1} + 1$.

It remains to construct codes meeting the upper bound for $k = 2$, all q and for $k = 3$, $q = 2$.

First we consider the case $k = 2$. Using the shortening construction from Section 2.3, it suffices to exhibit a $(6, 2q^3 + 2, 6; 3)_q$ constant-dimension code consisting of $q^3 + 1$ planes through a point P and $q^3 + 1$ planes in a hyperplane H of $\mathrm{PG}(5, \mathbb{F}_q)$ with $P \notin H$. This can be accomplished by adding to the $(6, q^6, 4; 3)_q$ Gabidulin code two planes E, E' with $\mathrm{d_S}(E, E') = 4$ meeting the special plane $S = \{0\} \times \mathbb{F}_{q^3}$ in distinct lines $L \neq L'$,

[37] Note that $X + Y_0 = V$ for every $X \in \mathcal{C}_k$, the dual of $X \cap X_0 = \{0\}$.

[38] The dimension distribution of $\mathcal{C}$ is $\delta_k = q^{k+1} + 1$, $\delta_{k+1} = q^{k+1}$, and $\delta_t = 0$ otherwise. It is also possible to add a $(k+1$-dimensional space, either through P or in H, to $\mathcal{G}$ before shortening.

[39] For $k = 2$ we can extend by a line in H meeting S in a point and a plane in H above S; cf. a subsequent part of the proof.

respectively, and choose for shortening a point $P \in E \setminus S$ and a hyperplane $H \supset E'$ with $H \cap S = L'$. Clearly P, H can be taken as non-incident, and then shortening the $(6, q^6 + 2, 4; 3)_q$ code $\mathcal{G} \cup \{E, E'\}$ in (P, H) yields the desired $(5, 2q^3 + 2, 3)_q$ code.[40]

In the case $k = 3$, $q = 2$ we have performed a computer search for $(7, 34, 5)_2$ codes and found several examples of such codes. Details can be found in Section 4.

The proof of Theorem 3.3 is now complete. □

Remark 3. It seems likely that $\mathrm{A}(v, v-2) = \mathrm{A}_q(v, v-2; k)$, $k = v/2$, holds for $v = 6$ as well.[41] From the proof of Part (i) it is clear that an optimal $(6, M, 4)_q$ code has $\delta_1 \leq 1$, $\delta_5 \leq 1$, $\delta_2 = \delta_4 = 0$, and hence $\mathrm{A}_q(6, 4) \leq \mathrm{A}_q(6, 4; 3) + 2$. The proof also shows that $\mathrm{A}_q(6, 4) > \mathrm{A}_q(6, 4; 3)$ requires $\mathrm{A}_q(6, 4; 3) \leq q^6 + q^3$, and hence $\mathrm{A}_q(6, 4) = \mathrm{A}_q(6, 4; 3)$ would follow from an improved lower bound on $\mathrm{A}_q(6, 4; 3)$.

In those cases where $\mathrm{A}(v, v-2) = \mathrm{A}_q(v, v-2; k)$ one may ask whether all optimal codes must have constant dimension. The parameter set $(v, d; k)_q = (8, 6; 4)_2$ illustrates the difficulties in answering this question: Presently it is only known that $257 \leq \mathrm{A}_2(8, 6) = \mathrm{A}_2(8, 6; 4) \leq 289$, with the corresponding Gabidulin code $\mathcal{G} = \mathcal{G}_{8,4,3}$ of size 256 accounting for the lower bound. If the true value turns out to be 257 then there are both constant-dimension and mixed-dimension codes attaining the bound, since $\mathcal{G}$ can be extended by any at least 2-dimensional subspace of its special solid S; cf. Section 2.4.[42]

Remark 4. The dimension distributions realized by $(2k + 1, 2q^{k+1} + 2, 2k - 1)_q$ codes, provided that codes with these parameters actually exist, can be completely determined.

In the case $k = 2$ these are all four distributions that have "survived" the proof of Theorem 3.3(ii), viz. $(0, 0, q^3 + 1, q^3 + 1, 0, 0)$, $(0, 1, q^3 + 1, q^3, 0, 0)$, $(0, 0, q^3, q^3 + 1, 1, 0)$ and $(0, 1, q^3, q^3, 1, 0)$.[43] This can be seen as follows:

The shortening construction used in the proof yields a code $\mathcal{C}$ in $\mathrm{PG}(H)$ with $\delta_2 = \delta_3 = q^3 + 1$ and such that the layers $\mathcal{C}_2$ and $\mathcal{C}_3$ are (dual) partial spreads of the type discussed before Theorem 3.2. Let E_1, L_1 be the special plane (containing the holes) and the moving line of $\mathcal{C}_2$, and L_2, E_2 the special line (meet of the dual holes) and moving plane of $\mathcal{C}_3$. Then, using the notation in the proof of Theorem 3.3, $E_1 = (S + P) \cap H$, $L_1 = E \cap H$, $L_2 = L'$, $E_2 = E'$. In other words, L_1, L_2 meet in a point (the point $L \cap L' \in S$), $E_1 = L_1 + L_2$, and E_2 is some other plane through L_2. Replacing the plane $E_2 \in \mathcal{C}$ by any point $Q \in L_2 \setminus L_1$ minimum distance 3, since $Q \in E_1 \setminus L_1$ is a hole of $\mathcal{C}_2$ and E_2 is the only plane in $\mathcal{C}_3$ containing Q,[44] and hence gives a $(5, 2q^3 + 2, 3)_q$ code with dimension distribution $(0, 1, q^3 + 1, q^3, 0, 0)$. Similarly, replacing L_1 by any solid T containing E_1 but not E_2 produces a $(5, 2q^3 + 2, 3)_q$ code with dimension distribution $(0, 0, q^3, q^3 + 1, 1, 0)$. Finally, since $\mathrm{d_S}(Q, T) = 3$, the code $\{Q\} \cup (\mathcal{C}_2 \setminus \{L_1\}) \cup (\mathcal{C}_3 \setminus \{E_2\}) \cup \{T\}$ has parameters $(5, 2q^3 + 2, 3)_q$ as well and dimension distribution $(0, 1, q^3, q^3, 1, 0)$.

For $k \geq 3$ the only possible dimension distribution is $\delta_k = \delta_{k+1} = q^{k+1} + 1$. In order to see this, we may suppose by duality that $(\delta_{k-1}, \delta_k, \delta_{k+1}, \delta_{k+2}) = (1, q^{k+1} + 1, q^{k+1}, 0)$ or $(1, q^{k+1}, q^{k+1}, 1)$ and must reduce this ad absurdum. In the first case, the codeword of dimension $k - 1$ must be disjoint from the codewords in $\mathcal{C}_k$, which form a maximal partial

[40] Another construction for $(5, 2q^3 + 2, 3)_q$ codes was recently found by Cossidente, Pavese and Storme [8].

[41] For $q = 2$ this is known, as we stated in the theorem.

[42] Apart from such extensions, it is also possible to extend $\mathcal{G}$ by any 5- or 6-dimensional space containing S and by a solid meeting S in a plane. Extensions by more than one codeword are not possible (i.e. the minimum distance would necessarily be < 6).

[43] Recall from the proof that $\delta_1 = 1$ forces $\delta_3 \leq q^3$, and similarly for $\delta_4 = 1$.

[44] For the latter note that the points of degree 1 with respect to $\mathcal{C}_3$ are those on L_2, since they are contained in q^2 dual holes of $\mathcal{C}_3$.

spread in $\mathrm{PG}(2k,\mathbb{F}_q)$. This is impossible, since $k-1\geq 2$ but the set of holes of $\mathcal{C}_k$ cannot contain a line. In the second case, let $X\in\mathcal{C}_{k-1}$, $Y\in\mathcal{C}_{k+2}$ be the unique codewords of their respective dimensions, and note that the codewords in $\mathcal{C}_{k-1}\cup\mathcal{C}_k$ are mutually disjoint and meet Y in at most a point. Since $\delta_k=q^{k+1}$ is one less than the size of a maximal partial spread, $\mathcal{C}_k$ has $1+q+\cdots+q^k$ holes. The set of holes contains X and at least $\#Y-(q^{k+1}+1)=q+q^2+\cdots+q^k$ further points from Y. This gives the inequality

$$1+2(q^1+q^2+\cdots+q^{k-2})+q^{k-1}+q^k\leq 1+q+\cdots+q^k,$$

which is impossible for $k\geq 3$.

Conjecture 1. $\mathrm{A}_q(7,5)=2q^4+2$ *(all q) and* $\mathrm{A}_q(v,v-2)=2q^{k+1}+1$ *for odd* $v=2k+1\geq 9$ *(all q). Thus a "doubling construction" of a* $(2k+1,2q^{k+1}+2,2k-1)_q$ *code from a maximal partial $(k-1)$-spread and the dual of another maximal partial $(k-1)$-spread in* $\mathrm{PG}(2k,\mathbb{F}_q)$ *is possible precisely for* $k\in\{2,3\}$*, independently of q.*

3.4. **Subspace distance** 2. The projective geometry $\mathrm{PG}(v-1,\mathbb{F}_q)$ or, in the vector space view, the set of $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^v$ under set inclusion, forms a finite modular geometric lattice. In particular $\mathrm{PG}(v-1,\mathbb{F}_q)$ is a ranked poset with rank function $X\mapsto\dim(X)$. The theory of finite posets can be used to determine the numbers $\mathrm{A}_q(v,2)$ and the corresponding optimal codes, as outlined in [1]. The proof uses a result of Kleitman [32] on finite posets with the so-called LYM property, of which the geometries $\mathrm{PG}(v-1,\mathbb{F}_q)$ are particular examples. Partial results on the numbers $\mathrm{A}_q(v,2)$ can also be found in [22, Sect. 4].

The classification of optimal $(v,M,2)_q$ subspace codes is stated as Theorem 3.4 below. We will provide a self-contained proof of the theorem. The underlying idea is to use information on the intersection patterns of a $(v,M,2)_q$ code with the various maximal chains of subspaces of $\mathbb{F}_q^v$ for a bound on the code size M. Recall that a maximal chain in a poset is a totally ordered subset which is maximal with respect to set inclusion among all such subsets. The maximal chains in $\mathrm{PG}(v-1,\mathbb{F}_q)$ have the form $\mathcal{K}=\{X_0,X_1,\dots,X_v\}$ with $\dim(X_i)=i$ and $X_i\subset X_{i+1}$.

If we assign to a subspace X as weight $w(X)$ the reciprocal of the number of maximal chains containing X, we can express the code size as

$$\#\mathcal{C}=\sum_{X\in\mathcal{C}}1=\sum_{X\in\mathcal{C}}w(X)\cdot\#\{\mathcal{K};X\in\mathcal{K}\}=\sum_{\mathcal{K}}\left(\sum_{X\in\mathcal{C}\cap\mathcal{K}}w(X)\right).$$

Since $w(X)=n_i$ depends only on $i=\dim(X)$, the inner sums are all alike, and it turns out that they attain a simultaneous maximum at some subspace code, which then of course must be optimal. For other parameters the same method could in principle be applied using suitably chosen families of subsets of the lattice $\mathrm{PG}(v-1,\mathbb{F}_q)$, but it seems difficult to find families producing tight bounds.[45]

Theorem 3.4. *(i) If $v=2k$ is even then*

$$\mathrm{A}_q(v,2)=\sum_{\substack{0\leq i\leq v\\ i\equiv k \bmod 2}}\begin{bmatrix}v\\i\end{bmatrix}_q.$$

The unique (as a set of subspaces) optimal code in $\mathrm{PG}(v-1,\mathbb{F}_q)$ *consists of all subspaces X of $\mathbb{F}_q^v$ with* $\dim(X)\equiv k \bmod 2$*, and thus of all even-dimensional subspaces for* $v\equiv 0 \bmod 4$ *and of all odd-dimensional subspaces for* $v\equiv 2 \bmod 4$.

[45] Usually much is lost through the fact that no subspace code can maximize all inner sums simultaneously.

(ii) $v = 2k + 1$ *is odd then*

$$\mathrm{A}_q(v, 2) = \sum_{\substack{0 \le i \le v \\ i \equiv 0 \bmod 2}} \begin{bmatrix} v \\ i \end{bmatrix}_q = \sum_{\substack{0 \le i \le v \\ i \equiv 1 \bmod 2}} \begin{bmatrix} v \\ i \end{bmatrix}_q, \tag{9}$$

and there are precisely two distinct optimal codes in $\mathrm{PG}(v-1, \mathbb{F}_q)$*, containing all even-dimensional and all odd-dimensional subspaces of* $\mathbb{F}_q^v$*, respectively. Moreover these two codes are isomorphic.*

Proof. Since the collineation group of $\mathrm{PG}(v-1, \mathbb{F}_q)$ is transitive on subspaces of fixed dimension, the number n_i of maximal chains through a subspace X of dimension i does not depend on the choice of X. Further, since each maximal chain passes through a unique subspace of dimension i, we must have $n_i = n / \left[\begin{smallmatrix} v \\ i \end{smallmatrix}\right]_q$, where n denotes the total number of maximal chains. Hence (9) can be rewritten as

$$\#\mathcal{C} = \frac{1}{n} \sum_{\mathcal{K} = \{X_0, \dots, X_v\}} \left(\sum_{\substack{i \in \{0, \dots, v\} \\ X_i \in \mathcal{C}}} \begin{bmatrix} v \\ i \end{bmatrix}_q \right) \tag{10}$$

In order to maximize one of the inner sums in (10), the best we can do (remember the constraint $d \ge 2$) is to choose $\mathcal{C}$ such that either $\mathcal{C} \cap \mathcal{K} = \{X_0, X_2, X_4, \dots\}$ or $\mathcal{C} \cap \mathcal{K} = \{X_1, X_3, X_5, \dots\}$, depending on which of the sums $\sum_{i \text{ even}} \left[\begin{smallmatrix} v \\ i \end{smallmatrix}\right]_q$, $\sum_{i \text{ odd}} \left[\begin{smallmatrix} v \\ i \end{smallmatrix}\right]_q$ is larger.

For odd v both sums are equal, since $\left[\begin{smallmatrix} v \\ i \end{smallmatrix}\right]_q = \left[\begin{smallmatrix} v \\ v-i \end{smallmatrix}\right]_q$. Hence the inner sums are maximized by either choice, and for simultaneous maximization of all inner sums it is necessary and sufficient that the code $\mathcal{C}$ consists either of all even-dimensional subspaces or of all odd-dimensional subspaces of $\mathbb{F}_q^v$.[46]

For even $v = 2k$ we use that the Gaussian binomial coefficients satisfy $\left[\begin{smallmatrix} v \\ i \end{smallmatrix}\right]_q > q\left[\begin{smallmatrix} v \\ i-1 \end{smallmatrix}\right]_q$ for $1 \le i \le k$; cf. the proof of Lemma 2.4. Together with symmetry this implies $\left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q > \left[\begin{smallmatrix} v \\ k-1 \end{smallmatrix}\right]_q + \left[\begin{smallmatrix} v \\ k+1 \end{smallmatrix}\right]_q$ and $\left[\begin{smallmatrix} v \\ k-2t \end{smallmatrix}\right]_q + \left[\begin{smallmatrix} v \\ k+2t \end{smallmatrix}\right]_q > \left[\begin{smallmatrix} v \\ k-2t-1 \end{smallmatrix}\right]_q + \left[\begin{smallmatrix} v \\ k+2t+1 \end{smallmatrix}\right]_q$ for $1 \le t \le (k-1)/2$. It follows that $\sum_{i \equiv k \bmod 2} \left[\begin{smallmatrix} v \\ i \end{smallmatrix}\right]_q > \sum_{i \equiv k+1 \bmod 2} \left[\begin{smallmatrix} v \\ i \end{smallmatrix}\right]_q$ and that the unique subspace code $\mathcal{C}$ simultaneously maximizing all inner sums in (10) consists of all subspaces X of $\mathbb{F}_q^v$ with $\dim(X) \equiv k \bmod 2$. □

4. Bounds and Classification Results for Small Parameters

In this section we present the best currently known bounds for the numbers $\mathrm{A}_2(v, d)$, $v \le 7$, and the classification of the optimal subspace codes in those cases, where the numbers $\mathrm{A}_2(v, d)$ are known. In particular we show that $\mathrm{A}_2(7, 5) = 34$, providing the yet missing part of the proof of Theorem 3.3.

Before turning attention to the binary case $q = 2$, let us remark that the results of Section 3 determine the numbers $\mathrm{A}_q(v, d)$ for all q and $v \le 5$; see Table 1. Regarding the corresponding classification, we remark that for $(v, d) = (3, 2)$, $(4, 2)$, $(5, 2)$ the optimal codes are unique up to subspace code isomorphism (cf. Theorem 3.4); those for $(v, d) = (3, 3)$, $(5, 5)$ are classified by Theorem 3.1(i);[47] those for $(v, d) = (4, 3)$ (and essentially

[46] Since $\{0\}$ and $\mathbb{F}_q^v$ belong to all maximal chains, the choice of $\mathcal{C} \cap \mathcal{K}$ for one chain determines all others.

[47] The different isomorphism types are represented by $\{\{0\}, \mathbb{F}_q^3\}$ and a non-incident point-line pair in $\mathrm{PG}(2, \mathbb{F}_q)$, respectively, by $\{\{0\}, \mathbb{F}_q^5\}$, a non-incident point-solid pair and a complementary line-plane pair in $\mathrm{PG}(4, \mathbb{F}_q)$.

$v\backslash d$	2	3	4	5
3	q^2+q+2	2		
4	$q^4+q^3+2q^2+q+3$	q^2+1	q^2+1	
5	$q^6+q^5+3q^4+3q^3+3q^2+2q+3$	$2q^3+2$	q^3+1	2

TABLE 1. The numbers $\mathrm{A}_q(v,d)$ for $v \leq 5$

for $(v,d)=(4,4)$ as well) have been classified for $q \leq 7$ as part of the classification of translation planes of small order (cf. Theorems 3.1(ii) and 3.2(i)).

The remainder of this section is devoted exclusively to the case $q=2$. With a few notable exceptions, the numbers $\mathrm{A}_2(v,d)$ are known for $v \leq 7$; see Table 2.

$v\backslash d$	2	3	4	5	6	7
3	$8(1)$	$2(2)$				
4	$37(1)$	$5(3)$	$5(1)$			
5	$187(1)$	$18(24298)$	$9(7)$	$2(3)$		
6	$1521(1)$	104–118	$77(4)$	$9(4)$	$9(1)$	
7	$14606(1)$	593–776	330–463	$34(20)$	$17(>715+37)$	$2(4)$

TABLE 2. $\mathrm{A}_2(v,d)$ and isomorphism types of optimal codes for $v \leq 7$

The exact values in the table come from Section 3 except for $\mathrm{A}_2(7,5)=34$. The number of isomorphism types of optimal $\big(v,\mathrm{A}_2(v,d),d\big)_2$ codes is given in parentheses.

Lemma 4.1. *We have* $329 \leq \mathrm{A}_2(7,4;\{3,4\}) \leq 381$.

Proof. Let $\mathcal{C} \subseteq \begin{bmatrix}V\\3,4\end{bmatrix}$ be an optimal $(7,M,4;\{3,4\})_2$ code. By duality we may assume $\delta_4 \leq \delta_3$. The codewords in $\mathcal{C}_3$ cover each line of $\mathrm{PG}(6,\mathbb{F}_2)$ at most once. Codewords in $\mathcal{C}_4$ may cover a line multiple times (up to 9 times, the size of a maximal partial spread in $\mathrm{PG}(4,\mathbb{F}_2)$), but at least they cannot cover the same line as a codeword in $\mathcal{C}_3$. Denoting by $c(\delta)$ the minimum number of lines covered by δ solids $S_1,\dots,S_\delta$ in $\mathrm{PG}(6,\mathbb{F}_2)$) at mutual distance ≥ 4, we have the bound $7\delta_3+c(\delta_4) \leq 7\cdot 381 = 2667$, the total number of lines in $\mathrm{PG}(6,\mathbb{F}_2)$. Our goal now is to show $c(\delta) \geq 7\delta$ for $\delta \in [0,381]$, which obviously implies $\#\mathcal{C}=\delta_3+\delta_4 \leq 381$, as needed in this case.

For lower-bounding $c(\delta)$ we use a similar method as in the proof of Theorem 3.2(ii). If b_i is the number of lines contained in exactly i solids then

$$\sum_{i\geq 0} b_i = 2667,$$
$$\sum_{i\geq 1} i b_i = 35\delta,$$
$$\sum_{i\geq 2} \binom{i}{2} b_i = e \leq \binom{\delta}{2},$$

where e denotes the number of edges of the distance-4 graph of $\{S_1,\dots,S_\delta\}$, and $c(\delta)=\sum_{i\geq 1} b_i = 2667-b_0$. Since the degree of S_i in the distance-4 graph is at most $7\cdot(21-1)=$

140,[48] a reasonable bound for e is

$$e \leq \begin{cases} \delta(\delta-1)/2 & \text{if } \delta \leq 141, \\ 70\delta & \text{if } \delta > 141. \end{cases}$$

Using again the polynomials $\binom{X-i_0}{2}$, $i_0 \in \mathbb{Z}^+$, to bound $c(\delta)$, we obtain

$$c(\delta) \geq \begin{cases} \frac{\delta(1+70i_0-\delta)}{i_0(i_0+1)} & \text{if } \delta \leq 141, \\ \frac{\delta(70i_0-140)}{i_0(i_0+1)} & \text{if } \delta > 141. \end{cases}$$

The best of these bounds, as a function of δ, is

$$c(\delta) \geq \begin{cases} \frac{\delta(1+70i_0-\delta)}{i_0(i_0+1)} & \text{if } 35(i_0-1)+1 \leq \delta \leq 35i_0,\ 1 \leq i_0 \leq 4, \\ 7\delta & \text{if } \delta \geq 141. \end{cases}$$

It implies $c(\delta) \geq 7\delta$ for all δ, as is easily verified, completing this part of the proof.[49] □

Corollary 1. *We have* $330 \leq \mathrm{A}_2(7,4) \leq 463$.

Proof. The lower bound is realized by adding the whole space $V = \mathbb{F}_2^7$ to the best currently known $(7,329,4;3)_2$ constant-dimension code [5, 34, 29]. If a 2-analogue of the Fano plane exists, the same construction yields a $(7,382,4)_2$ code. For the upper bound we observe $\mathrm{A}_2(7,4;\{5,6,7\}) = \mathrm{A}_2(7,4;\{0,1,2\}) \leq \mathrm{A}_2(7,4;2) = 41$. □

Let us remark that the previously best known upper bound $\mathrm{A}_2(7,4) \leq 776$ [2].

Regarding the corresponding classification of the optimal codes, we have that the codes for $d = 2$ are unique (Theorem 3.4) and those for $d = v \in \{3,5,7\}$ are classified into 2, 3 and 4 isomorphism types, respectively (Theorem 3.1(i)). The codes for $(v,d) = (4,4)$, $(6,6)$ are unique, since they correspond to the unique line spread in $\mathrm{PG}(3,\mathbb{F}_2)$, respectively, the unique plane spread in $\mathrm{PG}(5,\mathbb{F}_2)$; cf. Theorem 3.1(ii). For $(v,d) = (4,3)$ there are 3 different isomorphism types, represented by (i) a line spread $\mathcal{S} = \{L_1,L_2,L_3,L_4,L_5\}$, (ii) the lines L_1,L_2,L_3,L_4 and a point on L_5 and (iii) the lines L_1,L_2,L_3, a point $P \in L_4$ and a plane $E \supset L_5$ with $P \notin E$. For the proof of this assertion we use that by Theorem 3.2(i) the dimension distribution of an optimal $(4,5,3)_2$ code up to duality must be one of $(\delta_1,\delta_2,\delta_3) = (0,5,0)$, $(1,4,0)$, $(1,3,1)$ and that the corresponding codes form a single $\mathrm{GL}(4,\mathbb{F}_2)$-orbit. The latter has already been noted for the line spread and can be seen for the other two configurations as follows: The (element-wise) stabilizer in $\mathrm{GL}(4,\mathbb{F}_2)$ of 3 pairwise skew lines L_1,L_2,L_3, which may be taken as the row spaces of $\left(\begin{smallmatrix}1&0&0&0\\0&1&0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0&1&0\\0&0&0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1&0&1&0\\0&1&0&1\end{smallmatrix}\right)$, is conjugate to the subgroup formed by all block-diagonal matrices of the form $\left(\begin{smallmatrix}\mathbf{A}&\\&\mathbf{A}\end{smallmatrix}\right)$ with $\mathbf{A} \in \mathrm{GL}(2,\mathbb{F}_2)$. This subgroup acts regularly on the 6 points in $L_4 \cup L_5$, as is easily verified,[50] and leaves $\{L_4,L_5\}$ invariant.[51] Hence the stabilizer of L_1,L_2,L_3,L_4 (and L_5) acts transitively on L_5, showing uniqueness of the code with dimension distribution $(1,4,0)$. Moreover, the subgroup of $\mathrm{GL}(4,\mathbb{F}_2)$ fixing $\{L_1,L_2,L_3\}$

[48] The bound is the same as for the distance-4 graph of a set of planes at mutual distance ≥ 4.

[49] Also, since the first bound is stronger than the second (in the range where it applies), the equality $\#\mathcal{C} = 381$ can hold only for $141 \leq \delta_4 \leq 190$ ($141 \leq \delta_3, \delta_4 \leq 240$ without the assumption $\delta_4 \leq \delta_3$).

[50] The 6 points have the form $\mathbb{F}_2(\mathbf{x},\mathbf{y})$ with $\mathbf{x},\mathbf{y} \in \mathbb{F}_2^2$ nonzero and distinct, so that regularity follows from the doubly-transitive action of $\mathrm{GL}(2,\mathbb{F}_2)$ on $\mathbb{F}_2^2 \setminus \{\mathbf{0}\}$.

[51] This follows from the fact that $L_4 \cup L_5$ is uniquely a union of two lines; in other words, the spread containing L_1, L_2, L_3 is uniquely determined.

set-wise and the point P is isomorphic to S_3, and hence there exists $\mathbf{M} \in \mathrm{GL}(4, \mathbb{F}_2)$ interchanging L_1, L_2 and fixing L_3, P.[52] The matrix $\mathbf{M}$ cannot fix all three points on L_3 (otherwise it would fix all points in the plane $L_3 + P$ and hence also L_1, L_2). Since the three planes containing L_5 are transversal to L_3 and one of them (the plane containing P) is fixed by $\mathbf{M}$, the other two planes must be switched by $\mathbf{M}$. This shows that the code with dimension distribution $(1, 3, 1)$ is unique as well.

For $(v, d) = (6, 5)$ a similar argument shows that there are 4 isomorphism types of optimal codes, unique codes with dimension distribution $(\delta_2, \delta_3, \delta_4) = (0, 9, 0)$, $(1, 8, 0)$ and two non-isomorphic codes with distribution $(1, 7, 1)$. Taking the ambient space as $\mathbb{F}_8 \times \mathbb{F}_8$, $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ with $\alpha^3 + \alpha + 1 = 0$, the latter two codes can be obtained from the partial plane spread $\{\mathbb{F}_8(1, y); y \in \mathbb{F}_8^\times\}$ by adding the line $\{0, \alpha, \alpha^2, \alpha^4\} \times \{0\}$ and either the solid $\mathbb{F}_2 \times \mathbb{F}_8$ or $\mathbb{F}_2\alpha^3 \times \mathbb{F}_8$.

In the remaining cases, which are more complex, we will often rely on computer calculations. For isomorphism checks and the computation of automorphism groups, we use nauty [36] and the algorithm described in [20] (based on [19], see also [21]). To find subspace codes of maximum possible size, we use different approaches.

4.1. **The Case** $(v, d) = (5, 4)$.

For $v = 5$, $d = 4$, by Theorem 3.2 we have to consider the dimension distributions $(0, 0, 9, 0, 0, 0)$, $(0, 0, 8, 1, 0, 0)$ and $(0, 0, 8, 0, 1, 0)$, up to duality. The codes with dimension distribution $(0, 0, 9, 0, 0, 0)$ are exactly the $(5, 9, 4; 2)_2$ constant dimension codes or in other words, the partial line spreads of $\mathrm{PG}(4, \mathbb{F}_2)$ of size 9. Up to equivalence, there are 4 such partial spreads [23]; see also [30].

The codes realizing the remaining two dimension distributions contain a partial line spread $\mathcal{S}_8$ of size 8 as a subcode. Up to equivalence, there are 9 types of $\mathcal{S}_8$, all contained in some maximal partial line spread $\mathcal{S}_9$ of size 9 [23, Sect. 5.2]. For the dimension distribution $(0, 0, 8, 1, 0, 0)$, the plane Y_0 represented by the unique codeword of dimension 3 must be disjoint from each of the 8 lines in $\mathcal{S}_8$. Thus, these codes $\mathcal{C}$ are exactly the partitions of V into 8 lines and a single plane. Extending $\mathcal{S}_8$ by a line $X_0 \subset Y_0$, we get an $\mathcal{S}_9$ having a moving line X_0 in the sense of Section 3.2 or, using the terminology of [23], an $\mathcal{S}_9$ of regulus type X with the 4 reguli sharing the line X_0. Thus the $\mathcal{S}_8$ contained in $\mathcal{C}$ is the unique regulus-free partial spread (regulus type O in [23]). If follows that up to equivalence there is a unique code with dimension distribution $(0, 0, 8, 1, 0, 0)$. It is given by the lifted Gabidulin code $\mathcal{G}_{5,2,2}$ together with its special plane.

Now let $\mathcal{C}$ be a subspace code with dimension distribution $(0, 0, 8, 0, 1, 0)$. It has the form $\mathcal{C} = \mathcal{S}_8 \cup \{H\}$ with a hyperplane (solid) H. The code $\mathcal{C}$ has minimum distance 4 if and only if for each line $L \in \mathcal{S}$, $\dim(L \cap H) = 1$. Consider a maximal partial spread $\mathcal{S}_9$ containing $\mathcal{S}_8$. Since H contains at most one line of $\mathcal{S}_9$, it must be one of the 3 solids containing the special plane Y_0 of $\mathcal{S}_9$ and contain exactly one line L of $\mathcal{S}_9$. If L is contained in Y_0, $\mathcal{S}_8$ has regulus type O and $\mathcal{C} = \mathcal{S}_8 \cup \{H\}$ has the type mentioned in the proof of Theorem 3.2(ii) with $H = Y$. Moreover, it is readily checked that the 3 possible choices for Y yield equivalent codes. If L is not contained in Y_0, then $H = L + Y_0$ and L is contained in 2 reguli of $\mathcal{S}_9$. This implies that $\mathcal{S}_8$ has regulus type II and is again uniquely determined [23]. Since H is determined by $\mathcal{S}_8$ (for example, as the span of the 7 holes of $\mathcal{S}_8$), $\mathcal{C}$ is uniquely determined as well.

In all we have seen that up to equivalence there are 2 subspace codes realizing the dimension distribution $(0, 0, 8, 0, 1, 0)$.

Alltogether, there are $4 + 1 + 2 = 7$ types of $(5, 9, 4)_2$ subspace codes.

[52] Using coordinates as above and writing $P = \mathbb{F}_2(\mathbf{x}|\mathbf{y})$, we have $\mathbf{M} = \begin{pmatrix} & \mathbf{A} \\ \mathbf{A} & \end{pmatrix}$, where $\mathbf{A} \in \mathrm{GL}(2, \mathbb{F}_2)$ is the "transposition" satisfying $\mathbf{xA} = \mathbf{y}$, $\mathbf{yA} = \mathbf{x}$.

4.2. **The Case** $(v,d)=(5,3)$**.** For $v=5$, $d=3$, by Remark 4 we have to consider the dimension distributions $(0,0,9,9,0,0)$, $(0,1,8,8,1,0)$ and $(0,0,8,9,1,0)$, up to duality. So in each case, there is a subcode of dimension distribution $(0,0,9,0,0,0)$ or $(0,0,8,0,1,0)$ and subspace distance 4 (all dimensions of the codewords in the subcode have the same parity, so distance 3 implies distance 4). We have already seen that up to equivalence, the number of possibilities for this subcode is 4 or 2, respectively. For these 6 starting configurations, we enumerated all extensions to a code of size 18 by a clique search [38]. The resulting codes have been filtered for equivalence using nauty. In the end, we got the following numbers of equivalence classes: For $\delta=(0,0,9,9,0,0)$, there are 17708 codes, among them 306 self-dual ones. For $\delta=(0,1,8,8,1,0)$, there are 2164 codes, among them 73 self-dual ones. For $\delta=(0,0,8,9,1,0)$, there are 4426 codes, of course none of them self-dual. In total, there are $17708+2164+4426=24298$ types of $(5,9,3)_2$ subspace codes.

4.3. **The Cases** $(v,d)=(6,3)$ **and** $(v,d)=(7,3)$**.** Etzion and Vardy obtained the lower bound $\mathrm{A}_2(6,3)\geq 85$ in [18], and in [15] Etzion conjectured that this lower bound could be raised by extending optimal $(6,M,4;3)_2$ constant-dimension codes. Since $\mathrm{A}_2(6,4;3)=77$ and the optimal codes fall into 5 isomorphism types [30], we can easily compute the corresponding cardinality-maximal extensions:

- Type A, Type B: $|C|\leq 91$; an attained dimension distribution is $\delta=(0,0,7,77,7,0,0)$;
- Type C: $|C|\leq 93$; an attained dimension distribution is $\delta=(0,0,8,77,8,0,0)$;
- Type D: $|C|\leq 95$; an attained dimension distribution is $\delta=(0,0,8,77,10,0,0)$;
- Type E: $|C|\leq 95$; an attained dimension distribution is $\delta=(0,0,11,77,7,0,0)$.

Restricting the allowed dimensions to $\{0,1,2,3\}$ we obtain the following maximal extensions:

- Type A, Type B: $|C|\leq 84$; an attained dimension distribution is $\delta=(0,0,7,77,0,0,0)$;
- Type C: $|C|\leq 86$; an attained dimension distribution is $\delta=(0,0,9,77,0,0,0)$;
- Type D, Type E: $|C|\leq 88$; an attained dimension distribution is $\delta=(0,0,11,77,0,0,0)$.

Since $\mathrm{A}_2(6,3;\{0,1,2\})=\mathrm{A}_2(6,3;\{4,5,6\})=21$, we have $\mathrm{A}_2(6,3)\leq 118$. Using an integer linear programming approach, combined with some heuristics, we found a $(6,104,3)_2$ code.

For the case $(v,d)=(7,3)$ we have $\mathrm{A}_2(7,3)\leq 776$ [2]. The previously best known lower bound was $\mathrm{A}_2(7,3)\geq 584$ [16]. Using an integer linear programming approach one of the $(7,329,4;3)_2$ constant-dimension codes from [29] is extendable by at least 262 four-dimensional codewords. Adding the null space and $\mathbb{F}_2^7$ yields the improved lower bound $\mathrm{A}_2(7,3)\geq 329+262+1+1=593$.

Acknowledgments

The authors are grateful to Tuvi Etzion for comments regarding the upper bound in Corollary 1.

References

1. R. Ahlswede and H. Aydinian, *On error control codes for random network coding*, Network Coding, Theory, and Applications, 2009. NetCod'09. Workshop on, IEEE, 2009, pp. 68–73.
2. C. Bachoc, A. Passuello, and F. Vallentin, *Bounds for projective codes from semidefinite programming*, Advances in mathematics of communications **7** (2013), no. 2, 127–145.
3. J. De Beule and L. Storme (eds.), *Current research topics in Galois geometry*, Nova Science Publishers, 2011.
4. A. Beutelspacher, *Partial spreads in finite projective spaces and partial designs*, Mathematische Zeitschrift **145** (1975), 211–230, Corrigendum, ibid. 147:303, 1976.

5. M. Braun and J. Reichelt, *q-analogs of packing designs*, Journal of Combinatorial Designs **22** (2014), no. 7, 306–321.
6. P.J. Cameron and J.H. van Lint, *Graphs, codes and designs*, London Mathematical Society Lecture Note Series, no. 43, Cambridge University Press, 1980, A revised edition of these notes is [7].
7. ———, *Designs, graphs, codes and their links*, London Mathematical Society Student Texts, no. 22, Cambridge University Press, 1991, Revised edition of [6].
8. A. Cossidente, F. Pavese, and L. Storme, *Optimal subspace codes in* $PG(4, q)$, in preparation (2015).
9. T. Czerwinski and D. Oakden, *The translation planes of order twenty-five*, Journal of Combinatorial Theory, Series A **59** (1992), no. 2, 193–217.
10. P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, Journal of Combinatorial Theory, Series A **25** (1978), 226–241.
11. P. Dembowski, *Finite geometries*, Springer-Verlag, 1968, Classics in Mathematics Series, 1997.
12. U. Dempwolff, *Translation planes of order 27*, Designs, Codes and Cryptography **4** (1994), no. 2, 105–121, Erratum ibid. 5(1):81, 1995.
13. U. Dempwolff and A. Reifart, *The classification of the translation planes of order 16, I*, Geometriae Dedicata **15** (1983), no. 2, 137–153.
14. J. Eisfeld and L. Storme, *(partial)* t*-spreads and minimal* t*-covers in finite projective spaces*, Lecture notes, Ghent University, 2000.
15. T. Etzion, *Problems on q-analogs in coding theory*, Preprint arXiv: 1305.6126, 37 pages, 2013.
16. T. Etzion and N. Silberstein, *Codes and designs related to lifted MRD codes, IEEE Transactions on Information Theory **59** (2013), no. 2, 1004–1017.*
17. T. Etzion and L. Storme, *Galois geometries and coding theory*, Designs, Codes and Cryptography (2015), 1–40.
18. T. Etzion and A. Vardy, *Error-correcting codes in projective space*, IEEE Transactions on Information Theory **57** (2011), no. 2, 1165–1173.
19. T. Feulner, *The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes*, Advances in Mathematics of Communications **3** (2009), no. 4, 363–383.
20. T. Feulner, *Canonical Forms and Automorphisms in the Projective Space*, Preprint arXiv:1305.1193, 37 pages, 2013.
21. T. Feulner, *Eine kanonische Form zur Darstellung äquivalenter Codes – Computergestützte Berechnung und ihre Anwendung in der Codierungstheorie, Kryptographie und Geometrie*, PhD thesis, Universität Bayreuth, 2014.
22. E.M. Gabidulin and M. Bossert, *Algebraic codes for network coding*, Problems of Information Transmission **45** (2009), no. 4, 343–356.
23. N.A. Gordon, R. Shaw, and L.H. Soicher, *Classification of partial spreads in* $\mathrm{PG}(4, 2)$, available online as `http://www.maths.qmul.ac.uk/~leonard/partialspreads/PG42new.pdf`, 2004.
24. X. Guang and Z. Zhang, *Linear network error correction coding*, SpringerBriefs in Computer Science, Springer-Verlag, 2014.
25. M. Hall, Jr., J.D. Swift, and R.J. Walker, *Uniqueness of the projective plane of order eight*, Mathematics of Computation **10** (1956), no. 56, 186–194.
26. J.W.P. Hirschfeld, *Finite projective spaces of three diemsnions*, Oxford University Press, 1985.
27. ———, *Projective geometries over finite fields*, 2nd ed., Oxford University Press, 1998.
28. J.W.P. Hirschfeld and Joseph A. Thas, *General Galois geometries*, Oxford University Press, 1991.
29. T. Honold and M. Kiermaier, *On putative q-analogues of the Fano plane and related combinatorial structures*, Preprint arXiv:1504.06688, 37 pages, 2015.
30. T. Honold, M. Kiermaier, and S. Kurz, *Optimal binary subspace codes of length* 6*, constant dimension* 3 *and minimum subspace distance* 4, Topics in Finite Fields. 11th International Conference on Finite Fields and their Applications, July 22–26, 2013, Magdeburg, Germany (Gohar Kyureghyan, Gary L. Mullen, and Alexander Pott, eds.), Contemporary Mathematics, vol. 632, American Mathematical Society, 2015, pp. 157–176.
31. N.L. Johnson, V. Jha, and M. Biliotti, *Handbook of finite translation planes*, CRC Press, 2007.
32. D.J. Kleitman, *On an extremal property of antichains in partial orders. the lym property and some of its implications and applications*, Combinatorics, Springer, 1975, pp. 277–290.
33. R. Koetter and F. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory **54** (2008), no. 8, 3579–3591.
34. H. Liu and T. Honold, *Poster: A new approach to the main problem of subspace coding*, 9th International Conference on Communications and Networking in China (ChinaCom 2014, Maoming, China, Aug. 14–16), 2014, Full paper available as arXiv:1408.1181, pp. 676–677.
35. R. Mathon and G.F. Royle, *The translation planes of order 49*, Designs, Codes and Cryptography **5** (1995), no. 1, 57–72.

36. B. D. McKay and A. Piperno, *Practical graph isomorphism II*, Journal of Symbolic Computation **60** (2014), 94–112.

37. G.E. Moorhouse, *Two-graphs and skew two-graphs in finite geometries*, Linear Algebra and its Applications **226–228** (1995), 529–551.

38. S. Niskanen and P.R.J. Östergård, *Cliquer User's Guide, Version 1.0*, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, Tech. Rep. T48, 2003.

39. D. Silva, F. Kschischang, and R. Koetter, *A rank-metric approach to error control in random network coding*, IEEE Transactions on Information Theory **54** (2008), no. 9, 3951–3967.

40. ———, *Communication over finite-field matrix channels*, IEEE Transactions on Information Theory **56** (2010), no. 3, 1296–1306.

41. A.-L. Trautmann, *Isometry and automorphisms of constant dimension codes*, Advances in Mathematics of Communications **7** (2013), no. 2, 147–160.

42. J.H. van Lint and R.M. Wilson, *A course in combinatorics*, Cambridge University Press, 1992.

43. R.W. Yeung and N. Cai, *Network error correction, part I: Basic concepts and upper bounds*, Communications in Information and Systems **6** (2006), no. 1, 19–35.

44. ———, *Network error correction, part II: Lower bounds*, Communications in Information and Systems **6** (2006), no. 1, 37–54.

E-mail address: honold@zju.edu.cn
E-mail address: michael.kiermaier@uni-bayreuth.de
E-mail address: sascha.kurz@uni-bayreuth.de