Optimal Binary Subspace Codes of Length 6, Constant Dimension 3 and Minimum Subspace Distance 4

Thomas Honold, Michael Kiermaier, and Sascha Kurz

In memoriam Axel Kohnert (1962–2013)

Abstract. It is shown that the maximum size of a binary subspace code of packet length $v = 6$, minimum subspace distance $d = 4$, and constant dimension $k = 3$ is $M = 77$; in Finite Geometry terms, the maximum number of planes in $\mathrm{PG}(5,2)$ mutually intersecting in at most a point is 77. Optimal binary $(v, M, d; k) = (6, 77, 4; 3)$ subspace codes are classified into 5 isomorphism types, and a computer-free construction of one isomorphism type is provided. The construction uses both geometry and finite fields theory and generalizes to any q, yielding a new family of q-ary $(6, q^6 + 2q^2 + 2q + 1, 4; 3)$ subspace codes.

1. Introduction

Let $q > 1$ be a prime power, $v \geq 1$ an integer, and $V \cong \mathbb{F}_q^v$ a v-dimensional vector space over $\mathbb{F}_q$. The set $\mathrm{L}(V)$ of all subspaces of V, or flats of the projective geometry $\mathrm{PG}(V) \cong \mathrm{PG}(v-1, q)$, forms a metric space with respect to the *subspace distance* defined by $\mathrm{d_s}(U, U') = \dim(U + U') - \dim(U \cap U')$. The so-called *Main Problem of Subspace Coding* asks for the determination of the maximum sizes of codes in the spaces $(\mathrm{L}(V), \mathrm{d_s})$ (so-called *subspace codes*) with given minimum distance and the classification of the corresponding optimal codes. Since $V \cong \mathbb{F}_q^v$ induces an isometry $(\mathrm{L}(V), \mathrm{d_s}) \cong (\mathrm{L}(\mathbb{F}_q^v), \mathrm{d_s})$, the particular choice of the ambient vector space V does not matter here.

The metric space $(\mathrm{L}(V), \mathrm{d_s})$ may be viewed as a q-analogue of the Hamming space $(\mathbb{F}_2^v, \mathrm{d_{Ham}})$ used in conventional coding theory via the

2000 *Mathematics Subject Classification.* Primary 94B05, 05B25, 51E20; Secondary 51E14, 51E22, 51E23.

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

The work of the first author was supported by the National Basic Research Program of China (973) under Grant No. 2009CB320903. The work of the two latter authors was supported by the ICT COST Action IC1104.

subset-subspace analogy [**15**].[1] The corresponding main problem of conventional coding theory has been around for several decades and is well-studied by now; cf. the extensive treatise [**19, 20**], for example. Whereas the classical main problem resulted from Shannon's description of point-to-point channel coding, the main problem of subspace coding has emerged only recently in connection with the Kötter-Kschischang model of noncoherent network coding; cf. [**16**] and the survey [**18**]. A recent survey on the main problem of subspace coding can be found in reference [**6**], to which we also refer for more background on this problem. However, it is only fair to say that its surface has only been scratched.

Our contribution to the main problem of subspace coding is the resolution of the smallest hitherto open constant-dimension case—binary subspace codes of packet length $v = 6$ and constant dimension 3. This answers a question posed in [**6**] (Research Problem 11, cf. also the first table following Research Problem 10). It also forms the major step towards the solution of the main problem for the smallest open "mixed-dimension" case $(\mathrm{L}(\mathbb{F}_2^6), \mathrm{d_s})$, which is left for a future publication.

In order to state our results, we make the following fundamental

Definition 1. *A* q-ary (v, M, d) subspace code *(or* subspace code with parameters $(v, M, d)_q$*) is a set* $\mathcal{C}$ *of subspaces of* $V \cong \mathbb{F}_q^v$ *with size* $\#\mathcal{C} = M \geq 2$ *and minimum subspace distance*

$$\mathrm{d_s}(\mathcal{C}) = \min\{\mathrm{d_s}(U, U'); U, U' \in \mathcal{C}, U \neq U'\} = d.$$

If all subspaces in $\mathcal{C}$ *have the same dimension* $k \in \{1, \dots, v-1\}$*, then* $\mathcal{C}$ *is said to be a* q-ary $(v, M, d; k)$ constant-dimension subspace code.[2] *The maximum size of a* q*-ary* (v, M, d) *subspace code (a* q*-ary* $(v, M, d; k)$ *constant-dimension subspace code) is denoted by* $\mathrm{A}_q(v, d)$ *(respectively,* $\mathrm{A}_q(v, d; k)$*).*

In what follows, except for the conclusion part, we will restrict ourselves to constant-dimension codes and the numbers $\mathrm{A}_q(v, d; k)$. For $0 \leq k \leq v = \dim(V)$ we write $\begin{bmatrix} V \\ k \end{bmatrix} = \{U \in \mathrm{L}(V); \dim(U) = k\}$ (the set of $(k-1)$-flats of $\mathrm{PG}(V) \cong \mathrm{PG}(v-1, q)$). Since $\mathrm{d_s}(U, U') = 2k - 2\dim(U \cap U') = 2\dim(U + U') - 2k$ for $U, U' \in \begin{bmatrix} V \\ k \end{bmatrix}$, the minimum distance of every constant-dimension code $\mathcal{C} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}$ is an even integer $d = 2\delta$, and δ is characterized by

$$k - \delta = \max\{\dim(U \cap U'); U, U' \in \mathcal{C}, U \neq U'\}.$$

The numbers $\mathrm{A}_q(v, d; k)$ are defined only for $1 \leq k \leq v-1$ and even integers $d = 2\delta$ with $1 \leq \delta \leq \min\{k, v-k\}$. Moreover, since sending a subspace $U \in \begin{bmatrix} V \\ k \end{bmatrix}$ to its orthogonal space $U^\perp$ (relative to

[1] If $\mathbb{F}_2^v$ is identified with the set of subsets of $\{1, \dots, v\}$ in the usual way, then $\mathrm{d_{Ham}}(\mathbf{c}, \mathbf{c}') = \#(\mathbf{c} \cup \mathbf{c}') - \#(\mathbf{c} \cap \mathbf{c}')$ for $\mathbf{c}, \mathbf{c}' \in \mathbb{F}_2^v$.

[2] Here the alternative notation $(v, M, d; k)_q$ also applies.

a fixed non-degenerate symmetric bilinear form on V) induces an isomorphism (isometry) of metric spaces $\left(\begin{bmatrix}V\\k\end{bmatrix},\mathrm{d_s}\right) \to \left(\begin{bmatrix}V\\v-k\end{bmatrix},\mathrm{d_s}\right)$, $\mathcal{C} \mapsto \mathcal{C}^\perp = \{U^\perp; U \in \mathcal{C}\}$, we have $\mathrm{A}_q(v,d;k) = \mathrm{A}_q(v,d;v-k)$. Hence it suffices to determine the numbers $\mathrm{A}_q(v,d;k)$ for $1 \leq k \leq v/2$ and $d \in \{2,4,\dots,2k\}$.

The main result of our present work is

THEOREM 1. $\mathrm{A}_2(6,4;3) = 77$, *and there exist exactly five isomorphism classes of optimal binary* $(6,77,4;3)$ *constant-dimension subspace codes.*

In the language of Finite Geometry, Theorem 1 says that the maximum number of planes in $\mathrm{PG}(5,2)$ intersecting each other in at most a point is 77, with five optimal solutions up to geometric equivalence. Theorem 1 improves on the previously known inequality $77 \leq \mathrm{A}_2(6,4;3) \leq 81$, the lower bound being due to a computer construction of a binary $(6,77,4;3)$ subspace code in [**17**].[3]

The remaining numbers $\mathrm{A}_2(6,d;k)$ are known and easy to find. A complete list is given in Table 1, the new entry being indicated in bold type.[4]

$k\backslash d$	2	4	6
1	63		
2	651	21	
3	1395	**77**	9

TABLE 1. The numbers $\mathrm{A}_2(6,d;k)$

Theorem 1 was originally obtained by an extensive computer search, which is described in Section 3. Subsequently, inspired by an analysis of the data on the five extremal codes provided by the search (cf. Section 3.4) and using further geometric ideas, we were able to produce a computer-free construction of one type of extremal code. This is described in Section 4. It remains valid for all prime powers $q > 2$, proving the existence of q-ary $(6, q^6 + 2q^2 + 2q + 1, 4; 3)$ subspace codes for all q. This improves the hitherto best known construction with the parameters $(6, 4, q^6 + q^2 + 1; 3)$ in [**24**, Ex. 1.4] by $q^2 + 2q$ codewords. As a consequence, we have

THEOREM 2. $\mathrm{A}_q(6,4;3) \geq q^6 + 2q^2 + 2q + 1$ *for all prime powers* $q \geq 3$.

The ideas and methods employed in Section 4 may also prove useful, as we think, for the construction of good constant-dimension subspace

[3]For the (rather elementary) upper bound see Lemma 2.

[4]$\mathrm{A}_2(6,2k;k) = \frac{2^6-1}{2^k-1}$ is equal to the size of a $(k-1)$-spread (partition of the point set into $(k-1)$-flats) of $\mathrm{PG}(5,2)$.

codes with other parameter sets. Since they circumvent the size restriction imposed on constant-dimension codes containing a lifted MRD code, they can be seen as a partial answer to Research Problem 2 in [**6**].

2. Preparations

2.1. The Recursive Upper Bound and Partial Spreads. In the introduction we have seen that a $(v, M, d; k)_q$ constant-dimension subspace code is the same as a set $\mathcal{C}$ of $(k-1)$-flats in $\mathrm{PG}(v-1, q)$ with $\#\mathcal{C} = M$ and the following property: $t = k - d/2 + 1$ is the smallest integer such that every $(t-1)$-flat of $\mathrm{PG}(v-1, q)$ is contained in at most one $(k-1)$-flat of $\mathcal{C}$. This property (and $t \geq 2$) implies that for any $(t-2)$-flat F of $\mathrm{PG}(v-1, q)$ the "derived subspace code" $\mathcal{C}_F = \{U \in \mathcal{C}; U \supseteq F\}$ forms a partial $(k-t)$-spread[5] in the quotient geometry $\mathrm{PG}(v-1, q)/F \cong \mathrm{PG}(v-t, q)$. The maximum size of such a partial spread is $\mathrm{A}_q\bigl(v-t+1, 2(k-t+1); k-t+1\bigr) = \mathrm{A}_q(v-k+d/2, d; d/2)$. Counting the pairs (F, U) with a $(t-2)$-flat F and a $(k-1)$-flat $U \in \mathcal{C}$ containing F in two ways, we obtain the following bound, which can also be easily derived by iterating the Johnson type bound II in [**26**, Th. 3] or [**8**, Th. 4].

LEMMA 1. *The maximum size $M = \mathrm{A}_q(v, d; k)$ of a $(v, M, d; k)_q$ subspace code satisfies the upper bound*

$$\mathrm{A}_q(v, d; k) \leq \frac{\begin{bmatrix} v \\ t-1 \end{bmatrix}_q}{\begin{bmatrix} k \\ t-1 \end{bmatrix}_q} \cdot \mathrm{A}_q\bigl(v - k + d/2, d; d/2\bigr), \tag{1}$$

and the second factor on the right of (1) *is equal to the maximum size of a partial $(d/2-1)$-spread in* $\mathrm{PG}(v-k+d/2-1, q)$.

The numbers $\mathrm{A}_q(v, 2\delta; \delta)$ are unknown in general. The cases $\delta \mid v$ (in which $\mathrm{A}_q(v, 2\delta; \delta) = \frac{q^v-1}{q^\delta-1}$ is realized by any $(\delta-1)$-spread in $\mathrm{PG}(v-1, q)$) and $\delta = 2$ provide exceptions. The numbers $\mathrm{A}_q(v, 4; 2)$ (maximum size of a partial line-spread in $\mathrm{PG}(v-1, q)$ are known for all q and v (cf. Sections 2, 4 of [**1**] or Sections 1.1, 2.2 of [**5**]):

$$\mathrm{A}_q(v, 4; 2) = \begin{cases} q^{v-2} + q^{v-4} + \cdots + q^2 + 1 & \text{if } v \text{ is even}, \\ q^{v-2} + q^{v-4} + \cdots + q^3 + 1 & \text{if } v \text{ is odd}. \end{cases} \tag{2}$$

In particular $\mathrm{A}_q(5, 4; 2) = q^3 + 1$. Substituting this into Lemma 1 gives the best known general upper bound for the size of $(6, M, 4; 3)_q$ subspace codes, the case on which we will focus subsequently:

LEMMA 2. $\mathrm{A}_q(6, 4; 3) \leq (q^3 + 1)^2$.

[5] A partial t-spread is a set of t-flats which are pairwise disjoint when viewed as point sets.

For a subspace code $\mathcal{C}$ of size close to this upper bound there must exist many points P in $\mathrm{PG}(5,q)$ such that the derived code $\mathcal{C}_P$ forms a partial spread of maximum size q^3+1 in $\mathrm{PG}(5,q)/P \cong \mathrm{PG}(4,q)$. Available information on such partial spreads may then be used in the search for (and classification of) optimal $(6,M,4;3)_q$ subspace codes.

The hyperplane section $\{E \cap H; E \in \mathcal{T}\}$ of a plane spread $\mathcal{T}$ in $\mathrm{PG}(5,q)$ with respect to any hyperplane H yields an example of a partial spread of maximum size q^3+1 in $\mathrm{PG}(4,q)$, provided one replaces the unique plane $E \in \mathcal{T}$ contained in the hyperplane by a line $L \subset E$. For the smallest case $q=2$, a complete classification of partial spreads of size $2^3+1=9$ in $\mathrm{PG}(4,2)$ is known; see [**22, 13**]. We will describe this result in detail, since it forms the basis for the computational work in Section 3.

First let us recall that a set $\mathcal{R}$ of $q+1$ pairwise skew lines in $\mathrm{PG}(3,q)$ is called a *regulus* if every line in $\mathrm{PG}(3,q)$ meeting three lines of $\mathcal{R}$ forms a transversal of $\mathcal{R}$. Any three pairwise skew lines L_1, L_2, L_3 of $\mathrm{PG}(3,q)$ are contained in a unique regulus $\mathcal{R}=\mathcal{R}(L_1,L_2,L_3)$. The transversals of the lines in $\mathcal{R}$ form another regulus $\mathcal{R}^\circ$, the so-called *opposite regulus*, which covers the same set of $(q+1)^2$ points as $\mathcal{R}$. In a similar vein, we call a set of $q+1$ pairwise skew lines in $\mathrm{PG}(4,q)$ a regulus if they span a $\mathrm{PG}(3,q)$ and form a regulus in their span. For $q=2$ things simplify: A regulus in $\mathrm{PG}(3,2)$ is just a set of three pairwise skew lines, and a regulus in $\mathrm{PG}(4,2)$ is a set of three pairwise skew lines spanning a solid (3-flat).

Now suppose that $\mathcal{S}$ forms a partial line spread of size 9 in $\mathrm{PG}(4,2)$. Let Q be the set of 4 *holes* (points not covered by the lines in $\mathcal{S}$). An easy counting argument gives that each solid H, being a hyperplane of $\mathrm{PG}(4,2)$, contains $\alpha \in \{1,2,3\}$ lines of $\mathcal{S}$ and $\beta \in \{0,2,4\}$ holes, where $2\alpha+\beta=6$. This implies that $Q=E \setminus L$ for some plane E and some line $L \subset E$. Since a solid H contains no hole iff $H \cap E = L$, there are 4 such solids ($\beta=0$, $\alpha=3$) and hence 4 reguli contained in $\mathcal{S}$. Moreover, a line M of $\mathcal{S}$ is contained in 4 reguli if $M=L$, two reguli if $M \cap L$ is a point, or one regulus if $M \cap L = \emptyset$. This information suffices to determine the "regulus pattern" of $\mathcal{S}$, which must be either (i) four reguli sharing the line L and being otherwise disjoint (referred to as Type X in [**22, 13**]), or (ii) one regulus containing 3 lines through the points of L and three reguli containing one such line (Type E), or (iii) three reguli containing 2 lines through the points of L and one regulus consisting entirely of lines disjoint from E (Type IΔ).[6]

The partial spread obtained from a plane spread in $\mathrm{PG}(5,2)$ as described above has Type X. Replacing one of its reguli by the opposite regulus gives a partial spread of Type E. A partial spread of Type IΔ can be constructed as follows: Start with 3 lines L_1, L_2, L_3 in $\mathrm{PG}(4,2)$

[6]Note that the letters used for the types look like the corresponding regulus patterns.

not forming a regulus (i.e. not contained in a solid). The lines L_i have a unique transversal line L (the intersection of the three solids $H_1 = \langle L_2, L_3\rangle$, $H_2 = \langle L_1, L_3\rangle$, $H_3 = \langle L_1, L_2\rangle$).[7] In $\mathrm{PG}(4,2)/L \cong \mathrm{PG}(2,2)$ the solids H_1, H_2, H_3 form the sides of a triangle. Hence there exist a unique plane E and a unique solid H_4 in $\mathrm{PG}(4,2)$ such that $H_i \cap E = L$ for $1 \leq i \leq 4$. Let $E_i = \langle L, L_i\rangle$ for $1 \leq i \leq 3$ (the planes in which the solids H_1, H_2, H_3 intersect). Choose 3 further lines $L_i' \subset H_i$, $1 \leq i \leq 3$, such that L_1, L_2, L_3, L_1', L_2', L_3' are pairwise skew.[8] Let $y_i = L_i' \cap H_4$ for $1 \leq i \leq 3$. Then $L' = \{y_1, y_2, y_3\} \subset H_4$ must be a line, since it is the only candidate for the transversal to L_1', L_2', L_3' (which span the whole geometry).[9] Hence $H_4 \cong \mathrm{PG}(3,2)$ contains the disjoint lines L, L' and 9 points not covered by the 6 lines chosen so far. A partial spread of Type IΔ can now be obtained by completing L, L' to a spread of H_4.

With a little more effort, one can show that there are exactly 4 isomorphism types of partial spreads of size 9 in $\mathrm{PG}(4,2)$, one of Type X, one of Type E, and two of Type IΔ, represented by the two possible ways to complete L, L' to spread of H_4; see [**22, 13**] for details.

2.2. A property of the reduced row echelon form. Subspaces U of $\mathbb{F}_q^v$ with $\dim(U) = k$ are conveniently represented by matrices $\mathbf{U} \in \mathbb{F}_q^{k\times v}$ with row space U; notation $U = \langle \mathbf{U}\rangle$. It is well-known that every k-dimensional subspace of $\mathbb{F}_q^v$ has a unique representative $\mathbf{U}$ in *reduced row echelon form*, which is defined as follows: $\mathbf{U} = (u_{ij}) = (\mathbf{u}_1|\mathbf{u}_2|\dots|\mathbf{u}_v)$ contains the $k \times k$ identity matrix $\mathbf{I}_k$ as a submatrix, i.e. there exist column indices $1 \leq j_1 < j_2 < \cdots < j_k \leq v$ ("pivot columns") such that $\mathbf{u}_{j_i} = \mathbf{e}_i$ (the i-th standard unit vector in $\mathbb{F}_q^k$) for $1 \leq i \leq k$, and every entry to the left of $u_{i,j_i} = 1$ ("pivot element") is zero.[10] The reduced row echelon form of $\{\mathbf{0}\}$ is defined as the "empty matrix" $\emptyset$.

We will call $\mathbf{U}$ the *canonical matrix* of U and write $\mathbf{U} = \mathrm{cm}(U)$. Denoting the set of all canonical matrices (matrices in reduced row echelon form without all-zero rows) over $\mathbb{F}_q$ with v columns (including the empty matrix) by $\mathcal{K} = \mathcal{K}(v,q)$ and writing $\mathcal{L} = \mathrm{L}(v,q) = \mathrm{L}(\mathbb{F}_q^v)$, we have that $\mathcal{L} \to \mathcal{K}$, $U \mapsto \mathrm{cm}(U)$ and $\mathcal{K} \to \mathcal{L}$, $\mathbf{U} \mapsto \langle \mathbf{U}\rangle$ are mutually inverse bijections.

---

[7] This property remains true for any q. Thus three pairwise skew lines in $\mathrm{PG}(4,q)$ have $q+1$ transversals if they are contained in a solid, and a unique transversal otherwise.

[8] This can be done in 8 possible ways, "wiring" the 6 points in $(E_1 \cup E_2 \cup E_3) \setminus (L_1 \cup L_2 \cup L_3)$. All these choices lead to isomorphic partial spreads of size 6, as can be seen using the fact that $(L_1 \cup L_2 \cup L_3) \setminus L$ forms a projective basis of $\mathrm{PG}(4,2)$.

[9] The image of the transversal in $\mathrm{PG}(4,2)/L$ must be a line, leaving only one choice for the transversal.

[10] Although $\mathbf{I}_k$ may occur multiple times as a submatrix of $\mathbf{U}$, both properties together determine the set $\{j_1, \dots, j_k\}$ of pivot columns uniquely.

In addition we consider $\mathcal{K}(\infty,q)=\bigcup_{v=1}^{\infty}\mathcal{K}(v,q)$, the set of all matrices over $\mathbb{F}_q$ in canonical form. The following property of $\mathcal{K}(\infty,q)$ seems not to be well-known, but forms the basis for determining the canonical matrices of all subspaces of U from $\mathrm{cm}(U)$; see Part (ii).

LEMMA 3. *(i) $\mathcal{K}(\infty,q)$ is closed with respect to multiplication whenever it is defined; i.e., if $\mathbf{Z},\mathbf{U}\in\mathcal{K}(\infty,q)$ and the number of columns of $\mathbf{Z}$ equals the number of rows of $\mathbf{U}$, then $\mathbf{ZU}\in\mathcal{K}(\infty,q)$ as well.*

(ii) Let U and V be subspaces of $\mathbb{F}_q^v$ with $V\subseteq U$. Then $\mathrm{cm}(V)=\mathbf{Z}\cdot\mathrm{cm}(U)$ for a unique matrix $\mathbf{Z}$ in reduced row echelon form. More precisely, if $\dim(U)=k$ then $\mathbf{Z}\mapsto\mathbf{Z}\cdot\mathrm{cm}(U)$ defines a bijection from $\mathcal{K}(k,q)$ to the set of all matrices in $\mathcal{K}(v,q)$ that represent subspaces of U, and $\langle\mathbf{Z}\rangle\mapsto\langle\mathbf{Z}\cdot\mathrm{cm}(U)\rangle$ defines a bijection from the set of subspaces of $\mathbb{F}_q^k$ to the set of subspaces of U.

PROOF. (ii) follows easily from (i). For the proof of (i) assume $\mathbf{Z}=(z_{ri})\in\mathbb{F}_q^{l\times k}$, $\mathbf{U}=(u_{ij})\in\mathbb{F}_q^{k\times v}$, and $\mathbf{U}$ has pivot columns $j_1<\dots<j_k$. Then $\mathbf{Z}$ appears as a submatrix of $\mathbf{ZU}$ in columns $j_1,\dots,j_k$, and hence $\mathbf{I}_l$ appears as a submatrix of $\mathbf{ZU}$ as well, viz. in columns $j_{i(1)},j_{i(2)},\dots,j_{i(l)}$, where $i(1)<i(2)<\dots<i(l)$ are the pivot columns of $\mathbf{Z}$. Now suppose $j<j_{i(r)}$, so that the entry $(\mathbf{ZU})_{rj}=\sum_{i=1}^{k}z_{ri}u_{ij}$ lies to the left of the r-th pivot element of $\mathbf{ZU}$. Since $z_{ri}=0$ for $i<i(r)$, we have $(\mathbf{ZU})_{rj}=\sum_{i=i(r)}^{k}z_{ri}u_{ij}$. But $i\geq i(r)$ implies $j_i\geq j_{i(r)}>j$ and hence $u_{ij}=0$. Thus $(\mathbf{ZU})_{rj}=0$, proving that $\mathbf{ZU}$ is indeed canonical. $\square$

It is worth noting that for a given subspace U of $\mathbb{F}_q^v$ represented by its canonical matrix, Lemma 3(ii) provides an efficient way to enumerate all subspaces of U (or all subspaces of U of a fixed dimension).

2.3. Geometry of Rectangular Matrices. Left multiplication with matrices in $\mathrm{M}(m,q)$ (the ring of $m\times m$ matrices over $\mathbb{F}_q$) endows the $\mathbb{F}_q$-space $\mathbb{F}_q^{m\times n}$ of $m\times n$ matrices over $\mathbb{F}_q$ with the structure of a (left) $\mathrm{M}(m,q)$-module. Following [**27**], we call the corresponding coset geometry *left affine geometry of $m\times n$ matrices over $\mathbb{F}_q$* and denote it by $\mathrm{AG}_\ell(m,n,q)$.[11] For $0\leq k\leq n$, the k-flats of $\mathrm{AG}_\ell(m,n,q)$ are the cosets $\mathbf{A}+\mathcal{U}$, where $\mathbf{A}\in\mathbb{F}_q^{m\times n}$ and the submodule $\mathcal{U}$ consists of all matrices $\mathbf{U}\in\mathbb{F}_q^{m\times n}$ whose row space $\langle\mathbf{U}\rangle$ is contained in a fixed k-dimensional subspace of $\mathbb{F}_q^n$. The size of a k-flat is $\#(\mathbf{A}+\mathcal{U})=\#\mathcal{U}=q^{mk}$, and

[11]This viewpoint is different from that in the classical Geometry of Matrices [**25**, Ch. 3], which studies the structure of $\mathbb{F}_q^{m\times n}$ as an $\mathrm{M}(m,q)$-$\mathrm{M}(n,q)$ bimodule.

the number of k-flats in $\mathrm{AG}_\ell(m,n,q)$ is $q^{m(n-k)}\genfrac{[}{]}{0pt}{}{n}{k}_q$.[12] Point residues $\mathrm{AG}_\ell(m,n,q)/\mathbf{A}$ are isomorphic to $\mathrm{PG}(n-1,q)$.

Our interest in these geometries comes from the following

LEMMA 4. $\mathbf{A}\mapsto\langle(\mathbf{I}_m|\mathbf{A})\rangle$ *maps* $\mathrm{AG}_\ell(m,n,q)$ *isomorphically onto the subgeometry* $\mathscr{H}$ *of* $\mathrm{PG}(m+n-1,q)$ *whose* k*-flats,* $0\leq k\leq n$*, are the* $(m+k)$*-dimensional subspaces of* $\mathbb{F}_q^{m+n}$ *meeting* $S=\langle\mathbf{e}_{m+1},\dots,\mathbf{e}_{m+n}\rangle$ *in a subspace of dimension* k*. A parallel class* $\{\mathbf{A}+\mathcal{U};\mathbf{A}\in\mathbb{F}_q^{m\times n}\}$ *of* k*-flats is mapped to the set of* $(m+k)$*-dimensional subspaces of* $\mathbb{F}_q^{m+n}$ *meeting* S *in* $U=\sum_{\mathbf{U}\in\mathcal{U}}\langle\mathbf{U}\rangle$ *(with coordinates rearranged in the obvious way), so that* U *represents the common* k*-dimensional "space at infinity" of the flats in* $\mathbf{A}+\mathcal{U}$*.*[13]

In particular the points of $\mathrm{AG}_\ell(m,n,q)$ correspond to the $(m-1)$-flats of $\mathrm{PG}(m+n-1,q)$ disjoint from the special $(n-1)$-flat S, and the lines of $\mathrm{AG}_\ell(m,n,q)$ correspond to the m-flats of $\mathrm{PG}(m+n-1,q)$ meeting S in a point. The lemma seems to be well-known (cf. [**2**, Ex. 1.5], [**3**, 2.2.7]), but we include a proof for completeness.

PROOF. For an $(m+k)$-dimensional subspace F of $\mathbb{F}_q^{m+n}$ the condition $\dim(F\cap S)=k$ is equivalent to $\mathrm{cm}(F)=\begin{pmatrix}\mathbf{I}_m & \mathbf{A}\\ \mathbf{0} & \mathbf{Z}\end{pmatrix}$ for some $\mathbf{A}\in\mathbb{F}_q^{m\times n}$ and some canonical $\mathbf{Z}\in\mathbb{F}_q^{k\times n}$. The m-dimensional subspaces $E\subseteq F$ with $E\cap S=\{\mathbf{0}\}$ are precisely those with $\mathrm{cm}(E)=(\mathbf{I}_m|\mathbf{A}+\mathbf{VZ})$ for some $\mathbf{V}\in\mathbb{F}_q^{m\times k}$. Clearly $\{\mathbf{VZ};\mathbf{V}\in\mathbb{F}_q^{m\times k}\}=\{\mathbf{U}\in\mathbb{F}_q^{m\times n};\langle\mathbf{U}\rangle\subseteq\langle\mathbf{Z}\rangle\}=\mathcal{U}$, say, is a k-flat in $\mathrm{AG}_\ell(m,n,q)$ (containing $\mathbf{0}\in\mathbb{F}_q^{m\times n}$). This shows that F contains precisely those E which correspond to points on the k-flat $\mathbf{A}+\mathcal{U}$. The induced map on k-flats is clearly bijective, and maps the parallel class of $\mathbf{A}+\mathcal{U}$ to the subspaces F intersecting S in $\langle\mathbf{Z}\rangle=\sum_{\mathbf{U}\in\mathcal{U}}\langle\mathbf{U}\rangle$. The result follows.[14] $\square$

2.4. Maximum Rank Distance Codes. The set $\mathbb{F}_q^{m\times n}$ of $m\times n$ matrices over $\mathbb{F}_q$ forms a metric space with respect to the *rank distance* defined by $\mathrm{d_r}(\mathbf{A},\mathbf{B})=\mathrm{rk}(\mathbf{A}-\mathbf{B})$. As shown in [**4, 12, 21**], the maximum size of a code of minimum distance d, $1\leq d\leq\min\{m,n\}$, in $(\mathbb{F}_q^{m\times n},\mathrm{d_r})$ is $q^{n(m-d+1)}$ for $m\leq n$ and $q^{m(n-d+1)}$ for $m\geq n$. A code $\mathcal{A}\subseteq\mathbb{F}_q^{m\times n}$ meeting this bound with equality is said to be a q-ary

[12] The k-flats fall into $\genfrac{[}{]}{0pt}{}{n}{k}_q$ parallel classes, each consisting of $q^{m(n-k)}=q^{mn}/q^{mk}$ flats.

[13] Note, however, that in contrast with the classical case $m=1$ of projective geometry over fields, points of $\mathscr{H}$ need not be either "finite" or "infinite": The pivots of the associated m-dimensional subspace of $\mathbb{F}_q^{m+n}$ may involve both parts of the coordinate partition $\{1,\dots,m\}\uplus\{m+1,\dots,m+n\}$.

[14] Since $\mathbf{A}$ is required to have k zero columns ("above the pivots of $\mathbf{Z}$"), the number of different choices for $\mathbf{A}$ is indeed $q^{m(n-k)}$.

(m,n,k) *maximum rank distance (MRD) code*, where $k=m-d+1$ for $m\leq n$ and $k=n-d+1$ for $m\geq n$ (i.e. $\#\mathcal{A}=q^{nk}$ resp. $\#\mathcal{A}=q^{mk}$).[15]

From now on we will always assume that $m\leq n$.[16] Examples of MRD codes are the *Gabidulin codes*[17], which can be defined as follows: Consider the $\mathbb{F}_q$-space $V=\mathrm{End}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ of all $\mathbb{F}_q$-linear endomorphisms of the extension field $\mathbb{F}_{q^n}$. Then V is also a vector space over $\mathbb{F}_{q^n}$ (of dimension n), and elements of V are uniquely represented as linearized polynomials ("polynomial functions") $x\mapsto a_0x+a_1x^q+a_2x^{q^2}+\cdots+a_{n-1}x^{q^{n-1}}$ with coefficients $a_i\in\mathbb{F}_{q^n}$ and q-degree $<n$. The (n,n,k) Gabidulin code $\mathcal{G}$ consists of all such polynomials of q-degree $<k$. The usual matrix representation of $\mathcal{G}$ is obtained by choosing coordinates with respect to a fixed basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$. This gives rise to an isomorphism $(V,\mathrm{d_r})\cong(\mathbb{F}_q^{n\times n},\mathrm{d_r})$ of metric spaces, showing that the choice of basis does not matter and the coordinate-free representation introduced above is equivalent to the matrix representation. Rectangular (m,n,k) Gabidulin codes (where $m<n$) are then obtained by restricting the linear maps in $\mathcal{G}$ to an m-dimensional $\mathbb{F}_q$-subspace W of $\mathbb{F}_{q^n}$.

EXAMPLE 1. *Our main interest is in the case $m=n=3$, $d=2$. Here $\mathcal{G}=\{a_0x+a_1x^q;a_0,a_1\in\mathbb{F}_{q^3}\}$. The $2(q^3-1)$ monomials ax and ax^q, $a\in\mathbb{F}_{q^3}^\times$, have rank 3. The remaining nonzero elements of $\mathcal{G}$ are of the form $a(x^q-bx)$ with $a,b\in\mathbb{F}_{q^3}^\times$ and have*

$$\mathrm{rk}\bigl(a(x^q-bx)\bigr)=\begin{cases}2 & \text{if } b^{q^2+q+1}=1,\\ 3 & \text{if } b^{q^2+q+1}\neq 1.\end{cases}$$

This is easily seen by looking at the corresponding kernels: $x^q-bx=0$ has a nonzero solution iff $b=u^{q-1}$ for some $u\in\mathbb{F}_{q^3}^\times$, in which case $\mathrm{Ker}(x^q-bx)=\mathbb{F}_qu$. The rank distribution of $\mathcal{G}$ is shown in Table 2.

rank	0	1	2	3
#codewords	1	0	$(q^3-1)(q^2+q+1)$	$(q^3-1)(q^3-q^2-q)$

TABLE 2. Rank distribution of the q-ary $(3,3,2)$ Gabidulin code

Now we return to the case of arbitrary MRD codes and state one of their fundamental properties.[18]

[15]MRD codes form in some sense the q-analogue of maximum distance separable (MDS) codes. For more on this analogy see [**4, 27**] and Lemma 5 below.

[16]The case $m\geq n$ readily reduces to $m\leq n$ by transposing $\mathbf{A}\to\mathbf{A}^\mathsf{T}$, which maps $(\mathbb{F}_q^{m\times n},\mathrm{d_r})$ isometrically onto $(\mathbb{F}_q^{n\times m},\mathrm{d_r})$.

[17]Although this name is commonly used now, it should be noted that the examples found in [**4, 21**] are essentially the same.

[18]This property is analogous to the fact that for an $[n,k]$ MDS code every set of k coordinates forms an information set. One might say that every k-dimensional subspace of $\mathbb{F}_q^m$ forms an "information subspace" for $\mathcal{A}$.

LEMMA 5 (cf. [**27**, Lemma 2.4]). *Let $\mathcal{A} \subseteq \mathbb{F}_q^{m\times n}$ be an (m,n,k) MRD code, where $m \leq n$, and $\mathbf{Z} \in \mathbb{F}_q^{k\times m}$ of full rank k. Then $\mathcal{A} \to \mathbb{F}_q^{k\times n}$, $\mathbf{A} \mapsto \mathbf{ZA}$ is a bijection.*[19]

The matrix-free version of this easily proved lemma says that restriction to an arbitrary k-dimensional $\mathbb{F}_q$-subspace $U \subseteq W \subseteq \mathbb{F}_{q^n}$ maps an (m,n,k) MRD code $\mathcal{A} \subseteq \operatorname{Hom}_{\mathbb{F}_q}(W, \mathbb{F}_{q^n})$ isomorphically onto $\operatorname{Hom}_{\mathbb{F}_q}(U, \mathbb{F}_{q^n})$.

2.5. Lifted Maximum Rank Distance Codes. By a *lifted maximum rank distance (LMRD) code* we mean a subspace code obtained from an MRD code $\mathcal{A} \subseteq \mathbb{F}_q^{m\times n}$ by the so-called *lifting construction* of [**23**], which assigns to every matrix $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ the subspace $U = \langle(\mathbf{I}_m|\mathbf{A})\rangle$ of $\mathbb{F}_q^{m\times(m+n)}$. The map $\mathbf{A} \mapsto \langle(\mathbf{I}_m|\mathbf{A})\rangle$ defines an isometry with scale factor 2 from $\left(\mathbb{F}_q^{m\times n}, \mathrm{d_r}\right)$ into $\left(\left[\begin{smallmatrix}V\\m\end{smallmatrix}\right], \mathrm{d_s}\right)$, $V = \mathbb{F}_q^{m+n}$; cf. [**23**, Prop. 4].

Rewriting everything in terms of the subspace code parameters v, d, and k, a q-ary $(v,M,d;k)$ constant-dimension subspace code $\mathcal{L}$ is an LMRD code if $\mathcal{L} = \left\{\langle(\mathbf{I}_k|\mathbf{A})\rangle; \mathbf{A} \in \mathcal{A}\right\}$ for some MRD code $\mathcal{A} \subseteq \mathbb{F}_q^{k\times(v-k)}$ of minimum distance $d/2$. If $v \geq 2k$ (the case of interest to us) then the MRD code parameters of $\mathcal{A}$ are $(m,n,k') = (k, v-k, k-d/2+1)$, and $M = \#\mathcal{L} = \#\mathcal{A} = q^{(v-k)(k-d/2+1)}$.

As for ordinary MRD codes, it is sometimes more convenient to use a coordinate-free representation of LMRD codes, obtained as follows: Suppose V, W are vector spaces over $\mathbb{F}_q$ with $\dim(V) = n$, $\dim(W) = m$ and $\mathcal{A} \subseteq \operatorname{Hom}(W,V)$ is an (m,n,k) MRD code. Let $\mathcal{L}$ be the subspace code with ambient space $W \times V$ and members $G(f) = \{(x, f(x)); x \in W\}$ for all $f \in \mathcal{A}$ ("graphs" of the functions in $\mathcal{A}$). Since each $f \in \mathcal{A}$ is $\mathbb{F}_q$-linear, it is obvious that $\mathcal{L}$ consists of m-dimensional subspaces of $W \times V$. Moreover, choosing bases of V and W and representing linear maps $f\colon W \to V$ by $m \times n$ matrices $\mathbf{A}$ (acting on row vectors) with respect to these bases, induces an $\mathbb{F}_q$-isomorphism $V \times W \to \mathbb{F}_q^{m+n}$ sending $G(f)$ to $\langle(\mathbf{I}_m|\mathbf{A})\rangle$. The induced isometry $\mathrm{L}(V \times W) \to \mathrm{L}(\mathbb{F}_q^{m+n})$ maps $\mathcal{L}$ to an LMRD code with ambient space $\mathbb{F}_q^{m+n}$, showing that both views are equivalent.

EXAMPLE 2. *The q-ary $(3,3,2)$ Gabidulin code $\mathcal{G}$ of Example 1 lifts to a $(6,q^6,4;3)_q$ constant-dimension subspace code $\mathcal{L}$. In the coordinate-free representation, the members of $\mathcal{L}$ are the subspaces $G(a_0,a_1) = \{(x, a_0x + a_1x^q); x \in \mathbb{F}_{q^3}\} \in \mathrm{L}(\mathbb{F}_{q^3} \times \mathbb{F}_{q^3})$, where $a_0, a_1 \in \mathbb{F}_{q^3}$. The ambient space $\mathbb{F}_{q^3} \times \mathbb{F}_{q^3}$ is considered as a vector space over $\mathbb{F}_q$.*

A (coordinate-dependent) representation of $\mathcal{L}$ by 3×6 matrices over $\mathbb{F}_q$ is obtained by choosing a basis (b_1,b_2,b_3) of $\mathbb{F}_{q^3}/\mathbb{F}_q$ and writing a_0x+

[19]In particular, if $\mathcal{A}$ is linear (i.e. an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{m\times n}$) then $\mathbf{A} \mapsto \mathbf{ZA}$ is an isomorphism of $\mathbb{F}_q$-vector spaces.

$a_1x^q \in \mathcal{G}$ with respect to this basis. For example, if $q=2$ then we can choose the basis (β,β^2,β^4), where $\beta^3+\beta^2+1=0$ (the unique normal basis of $\mathbb{F}_8/\mathbb{F}_2$). Then

$$\beta \leftrightarrow \mathbf{B} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \qquad x^2 \leftrightarrow \mathbf{\Phi} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

and $\mathcal{L}$ consists of the 64 subspaces $\langle(\mathbf{I}_3|\mathbf{A})\rangle$ of $\mathbb{F}_2^6$ corresponding to $\mathbf{A} = \mathbf{0}$, $\mathbf{B}^i$, $\mathbf{B}^i\mathbf{\Phi}$, $\mathbf{B}^i+\mathbf{B}^j\mathbf{\Phi}$ with $0 \le i,j \le 6$.

Viewed as point sets in $\mathrm{PG}(v-1,q)$, the members of a q-ary $(v,M,d;k)$ LMRD code are disjoint from the special $(v-k-1)$-flat $S = \langle \mathbf{e}_{k+1}, \mathbf{e}_{k+2}, \dots, \mathbf{e}_v\rangle$. Delving further into this, one finds that under the hypothesis $v \ge 2k$ LMRD codes with $d = 2k$ partition the points of $\mathrm{PG}(v-1,q)$ outside S, and LMRD codes with $d < 2k$ form higher-dimensional analogs of such partitions:

LEMMA 6. *Let $\mathcal{L}$ be a q-ary $(v,M,d;k)$ LMRD code with $v \ge 2k$ and set $t = k-d/2+1$ (so that $\mathcal{L}$ arises from a q-ary $(k,v-k,t)$ MRD code $\mathcal{A}$ by the lifting construction). Then the members of $\mathcal{L}$ cover every $(t-1)$-flat in $\mathrm{PG}(v-1,q)$ disjoint from the special flat S exactly once.*

PROOF. If a $(t-1)$-flat in $\mathrm{PG}(v-1,q)$ were covered twice, we would have $\mathrm{d_s}(\mathcal{L}) \le 2k-2t = d-2$, a contradiction. Now suppose F is a $(t-1)$-flat in $\mathrm{PG}(v-1,q)$ disjoint from S. Since the pivot columns of $\mathrm{cm}(F)$ are within $\{1,\dots,k\}$, we must have $\mathrm{cm}(F) = (\mathbf{Z}|\mathbf{B})$ for some canonical matrix $\mathbf{Z} \in \mathbb{F}_q^{t\times k}$ and some matrix $\mathbf{B} \in \mathbb{F}_q^{t\times(v-k)}$. By Lemma 5, $\mathbf{B} = \mathbf{Z}\mathbf{A}$ for some $\mathbf{A} \in \mathcal{A}$. Hence $\mathrm{cm}(F) = (\mathbf{Z}|\mathbf{Z}\mathbf{A}) = \mathbf{Z}(\mathbf{I}_k|\mathbf{A})$, so that F is covered by the codeword $\langle(\mathbf{I}_k|\mathbf{A})\rangle \in \mathcal{L}$. □

Returning to Example 2, the lemma says that the q^6 planes in $\mathrm{PG}(5,q)$ obtained by lifting the q-ary $(3,3,2)$ Gabidulin code cover each of the $q^6(q^2+q+1)$ lines in $\mathrm{PG}(5,q)$ disjoint from the special plane $S = \langle \mathbf{e}_4, \mathbf{e}_5, \mathbf{e}_6\rangle$ exactly once (and thus in particular the number of lines in $\mathrm{PG}(5,q)$ disjoint from S equals $q^6(q^2+q+1)$). As an immediate consequence of this we have that the $(6,q^6,4;3)_q$ LMRD code $\mathcal{L}$ formed by these planes cannot be enlarged, without decreasing the minimum distance, by adding a new plane E with $\dim(E\cap S) \le 1$. Indeed, such a plane would contain a line disjoint from S, and hence already covered by $\mathcal{L}$, producing a codeword $U \in \mathcal{L}$ with $\mathrm{d_s}(E,U) = 2$. Since lines contained in S are covered by at most one codeword of $\mathcal{C}$, we obtain for any $(6,M,4;3)_q$ subspace code $\mathcal{C}$ containing $\mathcal{L}$ the upper bound $M \le q^6+q^2+q+1$ (a special case of [**7**, Th. 11]). This shows already that optimal $(6,M,4;3)_2$ subspace codes, which have $M > 71$, cannot contain an LMRD subcode.

3. The Computer Classification

For the classification of optimal $(6, M, 4; 3)_2$ subspace codes, we are facing a huge search space, making a direct attack by a depth-first search or an integer linear program infeasible. We will bring this under control by using certain substructures of large $(6, M, 4; 3)_2$ subspace codes as intermediate classification steps. Furthermore, we make use of the group $\mathrm{GL}(6, 2)$ of order 20158709760, which is acting on the search space. The canonization algorithm in [**10**] (based on [**9**], see also [**11**]) will be used to reject isomorphic copies at critical points during the search, keeping us from generating the "same" object too many times. The same method allows us to compute automorphism groups of network codes, and to filter the eventual list of results for isomorphic copies.

Given a $(6, M, 4; 3)_2$ constant-dimension code $\mathcal{C}$ with ambient space $V = \mathbb{F}_2^6$, we define the *degree* of a point $P \in \begin{bmatrix} V \\ 1 \end{bmatrix}$ as

$$r(P) = \#\{E \in \mathcal{C} \mid P \subset E\}.$$

By the discussion in Section 2.1, $r(P) \leq 9$ for all P.

3.1. Classification of 9-configurations.

A subset of $\mathcal{C}$ consisting of 9 planes passing through a common point P will be called a 9-*configuration*. Obviously, points of degree 9 in $\mathrm{PG}(V)$ correspond to 9-configurations in $\mathcal{C}$.

LEMMA 7. *If* $\#\mathcal{C} \geq 73$ *then* $\mathcal{C}$ *contains a* 9-*configuration.*

PROOF. Assuming $r(P) \leq 8$ for all points P and double counting the pairs (P, E) with points $P \in \begin{bmatrix} V \\ 1 \end{bmatrix}$ and codewords $E \in \mathcal{C}$ passing through P yields $7 \cdot \#\mathcal{C} \leq 8 \cdot 63$ and hence the contradiction $\#\mathcal{C} \leq 72$. □

Lemma 7 implies that for the classification of optimal $(6, M, 4; 3)_2$ codes $\mathcal{C}$, we may assume the existence of a 9-configuration in $\mathcal{C}$. By Section 2.1, the derived code $\mathcal{C}_P$ in any point P of degree 9 is one of the four isomorphism types of partial spreads in $\mathrm{PG}(V/P) \cong \mathrm{PG}(4, 2)$ and will accordingly be denoted by X, E, $\mathrm{I}\Delta$ or $\mathrm{I}\Delta'$.

The above discussion shows that for our classification goal, we may start with the four different 9-configurations and enumerate all extensions to a $(6, M, 4; 3)_2$ code with $M \geq 77$. However, the search space is still too large to make this approach feasible. Consequently, another intermediate classification goal is needed.

3.2. Classification of 17-configurations.

A subset of $\mathcal{C}$ of size 17 will be called a 17-*configuration* if it is the union of two 9-configurations. A 17-configuration corresponds to a pair of points (P, P') of degree 9 that is connected by a codeword in $\mathcal{C}$. The next lemma shows that large $(6, M, 4; 3)_2$ codes are necessarily extensions of a 17-configuration.

LEMMA 8. *If* $\#\mathcal{C} \geq 74$ *then* $\mathcal{C}$ *contains a* 17*-configuration.*

PROOF. By Lemma 7 there is a point P of degree 9. The 9-configuration through P covers $9 \cdot 6 = 54$ points $P' \neq P$, since two of its planes cannot have more than a single point in common. Under the assumption that there is no 17-configuration, we get that those 54 points are of degree ≤ 8. Double counting the set of pairs (Q, E) of points Q and codewords E passing through Q shows that

$$7 \cdot \#\mathcal{C} \leq 54 \cdot 8 + (63 - 54) \cdot 9$$

and hence $\#\mathcal{C} \leq \frac{513}{7} < 74$, a contradiction. □

For the classification of 17-configurations, we start with the four isomorphism types of 9-configurations. In the following, $\mathcal{N}$ denotes a 9-configuration, $P = \bigcap \mathcal{N}$ the intersection point of its 9 planes and $M = \bigcup \mathcal{N} \setminus \{P\}$ the set of 54 points distinct from P covered by a block in $\mathcal{N}$. Up to isomorphism, the possible choices for the second intersection point P' are given by the orbits of the automorphism group of $\mathcal{N}$ on M. This orbit structure is shown in Table 3. For example, for type E the 48 points in M fall into 4 orbits of length 12 and a single orbit or length 6, so up to isomorphism, there are 5 ways to select the point P'. For each Type $T \in \{\mathrm{X}, \mathrm{E}, \mathrm{I}\Delta, \mathrm{I}\Delta'\}$, the different types for the choice of P' will be denoted by $T_1, T_2, \ldots$, enumerating those coming from larger orbits first, see Table 4.

$\mathcal{N}$	$\#\,\mathrm{Aut}(\mathcal{N})$	orbit structure on M
X	48	$48^1 6^1$
E	12	$12^4 6^1$
$\mathrm{I}\Delta$	12	$12^2 6^5$
$\mathrm{I}\Delta'$	12	$12^2 6^5$

TABLE 3. Orbit structure on the points covered by a 9-configuration $\mathcal{N}$

These $2+5+7+7 = 21$ different *dotted* 9*-structures* (9-structures together with the selected point P') are fed into a depth-first search enumerating all extensions to a 17-configuration by adding blocks through P'. For each case, the number of extensions is shown in Table 4. Filtering out isomorphic copies among the resulting 575264 17-configurations, we arrive at

LEMMA 9. *There are* 12770 *isomorphism types of* 17*-configurations.*

Each 17-configuration contains two dotted 9-configurations. The exact distribution of the pairs of isomorphism types of dotted 9-configurations is shown in Table 5. For example, there are 68 isomorphism types of 17-configurations such that both dotted 9-configurations are of isomorphism type X_1.

dotted 9-conf.	orbit size	#extensions
X_1	48	28544
X_2	6	23968
E_1	12	28000
E_2	12	28544
E_3	12	28000
E_4	12	27168
E_5	6	25632
$\mathrm{I}\Delta_1$	12	28544
$\mathrm{I}\Delta_2$	12	28000
$\mathrm{I}\Delta_3$	6	27168
$\mathrm{I}\Delta_4$	6	27680
$\mathrm{I}\Delta_5$	6	27680
$\mathrm{I}\Delta_6$	6	25632
$\mathrm{I}\Delta_7$	6	28256
$\mathrm{I}\Delta'_1$	12	28544
$\mathrm{I}\Delta'_2$	12	28000
$\mathrm{I}\Delta'_3$	6	27168
$\mathrm{I}\Delta'_4$	6	27680
$\mathrm{I}\Delta'_5$	6	27680
$\mathrm{I}\Delta'_6$	6	25632
$\mathrm{I}\Delta'_7$	6	27744
		575264

TABLE 4. Extension of dotted 9-configurations to 17-configurations

	X_1	X_2	E_1	E_2	E_3	E_4	E_5	$\mathrm{I}\Delta_1$	$\mathrm{I}\Delta_2$	$\mathrm{I}\Delta_3$	$\mathrm{I}\Delta_4$	$\mathrm{I}\Delta_5$	$\mathrm{I}\Delta_6$	$\mathrm{I}\Delta_7$	$\mathrm{I}\Delta'_1$	$\mathrm{I}\Delta'_2$	$\mathrm{I}\Delta'_3$	$\mathrm{I}\Delta'_4$	$\mathrm{I}\Delta'_5$	$\mathrm{I}\Delta'_6$	$\mathrm{I}\Delta'_7$
X_1	68	10	120	132	120	120	58	132	120	60	59	59	56	60	132	120	60	59	59	56	60
X_2		3	16	10	16	12	8	10	16	7	8	8	6	10	10	16	7	8	8	6	10
E_1			64	120	124	114	54	120	124	57	60	60	56	60	120	124	57	60	60	56	64
E_2				68	120	120	58	132	120	60	59	59	56	60	132	120	60	59	59	56	60
E_3					64	114	54	120	124	57	60	60	56	60	120	124	57	60	60	56	64
E_4						62	54	120	114	60	58	58	58	60	120	114	60	58	58	58	48
E_5							14	58	54	27	32	32	20	32	58	54	27	32	32	20	28
$\mathrm{I}\Delta_1$								68	120	60	59	59	56	60	132	120	60	59	59	56	60
$\mathrm{I}\Delta_2$									64	57	60	60	56	60	120	124	57	60	60	56	64
$\mathrm{I}\Delta_3$										17	29	29	29	31	60	57	31	29	29	29	24
$\mathrm{I}\Delta_4$											17	32	31	32	59	60	29	32	32	31	28
$\mathrm{I}\Delta_5$												17	31	32	59	60	29	32	32	31	28
$\mathrm{I}\Delta_6$													13	24	56	56	29	31	31	23	28
$\mathrm{I}\Delta_7$														23	60	60	31	32	32	24	23
$\mathrm{I}\Delta'_1$															68	120	60	59	59	56	60
$\mathrm{I}\Delta'_2$																64	57	60	60	56	64
$\mathrm{I}\Delta'_3$																	17	29	29	29	24
$\mathrm{I}\Delta'_4$																		17	32	31	28
$\mathrm{I}\Delta'_5$																			17	31	28
$\mathrm{I}\Delta'_6$																				13	28
$\mathrm{I}\Delta'_7$																					27

TABLE 5. Pairs of dotted 9-configurations in 17-configurations

3.3. Classification of $(6, M, 4; 3)_2$ codes with $M \geq 77$. By Lemma 8, a $(6, M, 4; 3)_2$ code with $M \geq 77$ is the extension of some 17-configuration. Given a fixed 17-configuration $\mathcal{S}$, we formulate the extension problem as an integer linear program: For each plane $E \in \begin{bmatrix} V \\ 3 \end{bmatrix}$, a variable x_E is introduced, which may take the values 0 and 1. The value $x_E = 1$ indicates $E \in \mathcal{C}$. Now $\mathrm{d_s}(\mathcal{C}) \geq 4$ is equivalent to a system of linear constraints for x_E:

$$\sum_{E \in \begin{bmatrix} V \\ 3 \end{bmatrix}; L \subset E} x_E \leq 1 \qquad \text{for all lines } L \in \begin{bmatrix} V \\ 2 \end{bmatrix}.$$

The fact $r(P) \leq 9$ for all points $P \in \begin{bmatrix} V \\ 1 \end{bmatrix}$ yields the further system of linear constraints

$$\sum_{E \in \begin{bmatrix} V \\ 3 \end{bmatrix}; P \subset E} x_E \leq 9 \qquad \text{for all points } P \in \begin{bmatrix} V \\ 1 \end{bmatrix}.$$

As argued in the introduction, $\mathcal{C}$ is a $(v, M, d; k)_q$ constant-dimension code if and only if $\mathcal{C}^\perp = \{E^\perp \mid E \in \mathcal{C}\}$ is a $(v, M, d; v-k)_q$ constant-dimension code. In our case, if $\mathcal{C}$ is a $(6, M, 4; 3)_2$ code then so is $\mathcal{C}^\perp$. This allows us to add the dualized constraints

$$\sum_{E \in \begin{bmatrix} V \\ 3 \end{bmatrix}; E \subset H} x_E \leq 9 \qquad \text{for all hyperplanes } H \in \begin{bmatrix} V \\ 5 \end{bmatrix} \text{ and}$$

$$\sum_{E \in \begin{bmatrix} V \\ 3 \end{bmatrix}; E \subset S} x_E \leq 1 \qquad \text{for all solids } S \in \begin{bmatrix} V \\ 4 \end{bmatrix}.$$

The starting configuration $\mathcal{S}$ is prescribed by adding the constraints

$$x_E = 1 \qquad \text{for all } E \in \mathcal{S}.$$

Under these restrictions, the goal is to maximize the objective function

$$\sum_{E \in \begin{bmatrix} V \\ 3 \end{bmatrix}} x_E.$$

To avoid unnecessary computational branches, we add another inequality forcing this value to be ≥ 77.

For each of the 12770 isomorphism types of 17-configurations $\mathcal{S}$, this integer linear problem was fed into the ILP-solver CPLEX running on a standard PC. The computation time per case varied a lot, on average a single case took about 10 minutes. In 393 of the 12770 cases, the starting configuration $\mathcal{S}$ could be extended to a code of size 77, and it turned out that the maximum possible size of $\mathcal{C}$ is indeed 77. After filtering out isomorphic copies, we ended up with 5 isomorphism classes of $(6, 77, 4; 3)_2$ constant-dimension codes. This proves Theorem 1.

	# Aut	duality	degree dist.	pos. of S	types of 9-conf.	#17-conf.
A	168	self-dual	$5^7 9^{56}$	$0^{56} 1^{14} 2^7$	$\mathrm{X}^{28}\mathrm{E}^{28}$	1428
B	48	self-dual	$5^7 9^{56}$	$0^{48} 1^{28} 3$	$\mathrm{E}^{40}(\mathrm{I}\Delta')^{16}$	1428
C	2	self-dual	$5^7 9^{56}$	$0^{48} 1^{26} 2^3$	$\mathrm{E}^{34}(\mathrm{I}\Delta)^6(\mathrm{I}\Delta')^{16}$	1416
D	2	dual of E	$5^3 6^4 8^4 9^{52}$	$0^{48} 1^{24} 2^5$	$\mathrm{E}^{24}(\mathrm{I}\Delta)^9(\mathrm{I}\Delta')^{19}$	1222
E	2	dual of D	$5^3 6^4 8^4 9^{52}$	$0^{48} 1^{24} 2^5$	$\mathrm{E}^{24}(\mathrm{I}\Delta)^9(\mathrm{I}\Delta')^{19}$	1222

TABLE 6. Types of $(6, 77, 4; 3)_2$ constant-dimension codes

3.4. Analysis of the results. The five isomorphism types will be denoted by A, B, C, D and E. We investigated the structure of those codes by computer. The results are discussed in this section.

If $\mathcal{C} \cong \mathcal{C}^\perp$ or, equivalently, $\mathcal{C}$ is invariant under a correlation of $\mathrm{PG}(5, 2)$, we will call $\mathcal{C}$ *self-dual.*[20] The five isomorphism types fall into three self-dual cases (A, B, C) and a single pair of dual codes (D, E).

There is a remarkable property shared by all five types:

COROLLARY 1. *Let $\mathcal{C}$ be a $(6, 77, 4; 3)_2$ constant-dimension code. There is a unique plane $S \in \begin{bmatrix} V \\ 3 \end{bmatrix}$ such that all points on S have degree ≤ 6 and all other points have degree ≥ 8.*

For Type B, the plane S of Corollary 1 is a codeword, for all other types it is not. An overview of the structure is given in Table 6. The column "pos. of S" gives the frequencies of $\dim(E \cap S)$ when E runs through the codewords of $\mathcal{C}$. For example, the entry $0^{48} 1^{28} 3$ for Type B means that there are 48 codewords disjoint from S, 28 codewords intersecting S in a point and the single codeword identical to S.

For a double check of our classification, we collected all 17-configurations which appear as a substructure of the five codes, see Table 6 for the numbers. After filtering out isomorphic copies, we ended up with the same 393 types that we already saw as the ones among the 12770 17-configurations which are extendible to a $(6, 77, 4; 3)_2$ code.

4. Computer-Free Constructions

We have seen in Section 3 that the best $(6, M, 4; 3)_2$ subspace codes contain large subcodes (of sizes 56 or 48; cf. Table 6) disjoint from a fixed plane of $\mathrm{PG}(5, 2)$. Since the latter are easy to construct—for example, large subcodes of binary $(3, 3, 2)$ LMRD codes have this

[20]In general, the map $\mathrm{L}(V) \to \mathrm{L}(V)$, $U \mapsto U^\perp$ defines a particular correlation (lattice anti-isomorphism) of $\mathrm{PG}(V)$, which depends on the choice of the symmetric bilinear form. Composing $U \mapsto U^\perp$ with all collineations of $\mathrm{PG}(V)$ (on either side) yields all correlations of $\mathrm{PG}(V)$ and proves equivalence of the two conditions. Thus self-duality is a purely geometric concept and does not depend on the particular bilinear form chosen.

property—, it is reasonable to take such codes as the basis of the construction and try to enlarge them as far as possible.

We start by outlining the main ideas involved in this kind of construction, which eventually leads to a computer-free construction of a $(6, 77, 4; 3)_2$ subspace code of Type A. For this we assume $q = 2$, for simplicity. Subsequently we will develop the approach for general q.

First consider a $(6, 64, 4; 3)_2$ LMRD code $\mathcal{L}$ obtained, for example, by lifting a matrix version of the binary $(3, 3, 2)$ Gabidulin code. By Lemma 6, the 64 planes in $\mathcal{L}$ cover the $7 \cdot 64 = 448$ lines of $\mathrm{PG}(5, 2)$ disjoint from the special plane $S = \langle \mathbf{e}_4, \mathbf{e}_5, \mathbf{e}_6 \rangle$, so that no plane meeting S in a point (and hence containing 4 lines disjoint from S) can be added to $\mathcal{L}$ without decreasing the subspace distance. Therefore, in order to overcome the restriction $\#\mathcal{C} \leq 71$ for subspace codes $\mathcal{C}$ containing $\mathcal{L}$, we must remove some planes from $\mathcal{L}$, resulting in a proper subcode $\mathcal{L}_0 \subset \mathcal{L}$. Removing a subset $\mathcal{L}_1 \subseteq \mathcal{L}$ with $\#\mathcal{L}_1 = M_0$ will "free" $7M_0$ lines, i.e. lines disjoint from S that are no longer covered by $\mathcal{L}_0 = \mathcal{L} \setminus \mathcal{L}_1$. If $M_0 = 4m_0$ is a multiple of 4, it may be possible to rearrange the $28M_0 = 4 \cdot 7M_0$ free lines into $7M_0$ "new" planes meeting S in a point (each new plane containing 4 free lines), and such that the set $\mathcal{N}$ of new planes has subspace distance 4 (equivalently, covers no line through a point of S twice). The planes in $\mathcal{N}$ can then be added, resulting in a $(6, M, 4; 3)_2$ subspace code $\mathcal{C} = \mathcal{L}_0 \cup \mathcal{N}$ of size $M = 64 + 3m_0 > 64$. A detailed discussion (following below) will show that this construction with $M_0 = 8$ is indeed feasible and, even more, 7 further planes meeting S in a line can be added to $\mathcal{C}$ without decreasing the subspace distance. This yields an optimal $(6, 77, 4; 3)_2$ subspace code of Type A. Moreover, the construction generalizes to arbitrary q, producing a $(6, q^6 + 2q^2 + 2q + 1, 4; 3)_q$ subspace code.

4.1. Removing Subspaces from MRD Codes. Let $\mathcal{L}$ be a $(6, q^6, 4; 3)_q$ LMRD code, arising from a q-ary $(3, 3, 2)$ MRD code $\mathcal{A}$; cf. Section 2.5. Then, for any hyperplane H of $\mathrm{PG}(5, q)$ containing $S = \langle \mathbf{e}_4, \mathbf{e}_5, \mathbf{e}_6 \rangle$, the corresponding hyperplane section $\mathcal{L} \cap H = \{E \cap H; E \in \mathcal{L}\}$ consists of all q^6 lines in $H \setminus S$, by Lemma 6. Writing $\mathrm{cm}(H) = \left(\begin{smallmatrix} \mathbf{Z} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_3 \end{smallmatrix}\right)$, where $\mathbf{Z} \in \mathbb{F}_q^{2\times 3}$ is the canonical matrix associated with H (viewed as a line in $\mathrm{PG}(5, q)/S$), these q^6 lines are $\langle(\mathbf{Z}|\mathbf{Z}\mathbf{A})\rangle$ with $\mathbf{A} \in \mathcal{A}$. This simplifies to $\langle(\mathbf{Z}|\mathbf{B})\rangle$ with $\mathbf{B} \in \mathbb{F}_q^{2\times 3}$ arbitrary.

Our first goal in this section is to determine which subsets $\mathcal{R} \subset \mathcal{A}$ ("removable subsets") of size q^2 have the property that the corresponding hyperplane section $\mathcal{L}_1 \cap H$, $\mathcal{L}_1 = \{\langle(\mathbf{I}_3|\mathbf{A})\rangle; \mathbf{A} \in \mathcal{R}\}$, consists of the q^2 lines disjoint from S in a new plane (a plane meeting S in a single point). Assuming that $\mathcal{A}$ is linear over $\mathbb{F}_q$ will simplify the characterization of removable subsets.

Lemma 10. *Suppose $\mathcal{A}$ is a q-ary linear $(3,3,2)$ MRD code, and H is a hyperplane of* $\mathrm{PG}(5,q)$ *containing S with* $\mathrm{cm}(H)=\left(\begin{smallmatrix}\mathbf{Z} & \mathbf{0}\\ \mathbf{0} & \mathbf{I}_3\end{smallmatrix}\right)$. *For $\mathcal{R}\subseteq\mathcal{A}$ the following are equivalent:*

(i) The H-section $\mathcal{L}_1\cap H$ corresponding to $\mathcal{R}$ consists of the q^2 lines disjoint from S in a new plane N.

(ii) $\mathbf{Z}\mathcal{R}=\{\mathbf{ZA};\mathbf{A}\in\mathcal{R}\}$ is a line in $\mathrm{AG}_\ell(2,3,q)$.

(iii) $\mathcal{R}=\mathbf{A}_0+\mathcal{D}$ for some $\mathbf{A}_0\in\mathcal{A}$ and some 2-dimensional $\mathbb{F}_q$-subspace $\mathcal{D}$ of $\mathcal{A}$ with the following properties: $\mathcal{D}$ has constant rank 2, and the (1-dimensional) left kernels of the nonzero members of $\mathcal{D}$ generate the row space $\langle\mathbf{Z}\rangle$.[21]

If these conditions are satisfied then the new plane N has $\mathrm{cm}(N)=\left(\begin{smallmatrix}\mathbf{Z} & \mathbf{ZA}_0\\ \mathbf{0} & \mathbf{s}\end{smallmatrix}\right)$, *where $\mathbf{s}\in\mathbb{F}_q^3$ is a generator of the common 1-dimensional row space of the nonzero matrices in $\mathbf{Z}\mathcal{D}$. Moreover, $\mathbb{F}_q\mathbf{s}=N\cap S$ is the point at infinity of the line $\mathbf{Z}\mathcal{R}$ in (ii).*

Proof. (i) $\iff$ (ii): The lines L in the H-section have canonical matrices $\mathrm{cm}(L)=(\mathbf{Z}|\mathbf{ZA})$, $\mathbf{A}\in\mathcal{R}$. Lemma 4 (with an obvious modification) yields that $\mathbf{B}\mapsto\langle(\mathbf{Z}|\mathbf{B})\rangle$ maps the lines of $\mathrm{AG}_\ell(2,3,q)$ to the planes of H intersecting S in a point. Hence $\mathbf{Z}\mathcal{R}$ is a line in $\mathrm{AG}_\ell(2,3,q)$ iff the q^2 lines in the H-section are incident with a new plane N.

(ii) $\iff$ (iii): We may assume $\mathbf{0}\in\mathcal{R}=\mathcal{D}$. The point set $\mathcal{U}=\mathbf{Z}\mathcal{D}$ is a line in $\mathrm{AG}_\ell(2,3,q)$ iff the q^2-1 nonzero matrices in $\mathcal{U}$ have a common 1-dimensional row space, say $\mathbb{F}_q\mathbf{s}$, and account for all such matrices. If this is the case, then $\mathcal{D}$ must be an $\mathbb{F}_q$-subspace of $\mathcal{A}$ (since $\mathcal{U}$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{2\times 3}$ and $\mathcal{A}\to\mathbb{F}_q^{2\times 3}$, $\mathbf{A}\mapsto\mathbf{ZA}$ is bijective.[22]) Further, $\mathcal{D}$ must have constant rank 2 (since $\mathcal{D}\subseteq\mathcal{A}$ forces $\mathrm{rk}(\mathbf{A})\geq 2$ for all $\mathbf{A}\in\mathcal{D}$), and the left kernels of the nonzero matrices in $\mathcal{D}$ must generate $\langle\mathbf{Z}\rangle$ (since the left kernels of the nonzero matrices in $\mathcal{U}=\mathbf{Z}\mathcal{D}$ account for all 1-dimensional subspaces of $\mathbb{F}_q^2$). Conversely, suppose that $\mathcal{D}$ satisfies these conditions. Then all nonzero matrices in $\mathcal{U}$ have rank 1, and we must show that they have the same row space. Let $\mathbf{A}_1,\mathbf{A}_2$ be a basis of $\mathcal{D}$ and $\mathbf{z}_1,\mathbf{z}_2\in\mathbb{F}_q^3\setminus\{\mathbf{0}\}$ with $\mathbf{z}_1\mathbf{A}_1=\mathbf{z}_2\mathbf{A}_2=\mathbf{0}$. Then $\mathbf{z}_1$, $\mathbf{z}_2$ span $\langle\mathbf{Z}\rangle$ (otherwise all matrices in $\mathcal{D}$ would have kernel $\mathbb{F}_q\mathbf{z}_1=\mathbb{F}_q\mathbf{z}_2$), and hence there exist $\lambda,\mu\in\mathbb{F}_q$, $(\lambda,\mu)\neq(0,0)$, such that $(\lambda\mathbf{z}_1+\mu\mathbf{z}_2)(\mathbf{A}_1+\mathbf{A}_2)=\mathbf{0}$. Expanding, we find $\lambda\mathbf{z}_1\mathbf{A}_2=-\mu\mathbf{z}_2\mathbf{A}_1$, implying that $\mathbf{ZA}_1$ and $\mathbf{ZA}_2$ have the same row space $\mathbb{F}_q(\mathbf{z}_1\mathbf{A}_2)=\mathbb{F}_q(\mathbf{z}_2\mathbf{A}_1)=\mathbb{F}_q\mathbf{s}$, say. Since $\mathcal{U}=\langle\mathbf{ZA}_1,\mathbf{ZA}_2\rangle$, the other nonzero matrices in $\mathcal{U}$ must have row space $\mathbb{F}_q\mathbf{s}$ as well.

The remaining assertions are then easy consequences. □

Remark 1. *The conditions imposed on $\mathcal{D}$ in Lemma 10(iii) imply that the left kernels of the nonzero matrices in $\mathcal{D}$ form the set of 1-dimensional subspaces of a 2-dimensional subspace of $\mathbb{F}_q^3$ (viz., $\langle\mathbf{Z}\rangle$).*

[21]The term "constant-rank" has its usual meaning in Matrix Theory, imposing the same rank on all nonzero members of the subspace.

[22]Here we need the assumption that $\mathcal{A}$ is linear.

Two matrices $\mathbf{A}_1, \mathbf{A}_2 \in \mathcal{A}$ *generate a 2-dimensional constant-rank-2 subspace with this property iff* $\mathrm{rk}(\mathbf{A}_1) = \mathrm{rk}(\mathbf{A}_2) = 2$*, the left kernels* $K_1 = \mathbb{F}_q\mathbf{z}_1$*,* $K_2 = \mathbb{F}_q\mathbf{z}_2$ *of* $\mathbf{A}_1$ *resp.* $\mathbf{A}_2$ *are distinct, and* $\mathbf{z}_1\mathbf{A}_2$*,* $\mathbf{z}_2\mathbf{A}_1$ *are linearly dependent.*[23]

Since the maps $\mathcal{A} \to \mathbb{F}_q^{2\times 3}$, $\mathbf{A} \mapsto \mathbf{ZA}$ are bijections, we note the following consequence of Lemma 1. For each 2-dimensional subspace Z of $\mathbb{F}_q^3$ (representing a hyperplane H in $\mathrm{PG}(5,q)$ as described above, with $\mathbf{Z} = \mathrm{cm}(Z)$) and each 1-dimensional subspace P of $\mathbb{F}_q^3$ (representing a point of S, after padding the coordinate vector $\mathbf{s} = \mathrm{cm}(P)$ with three zeros), there exists precisely one 2-dimensional subspace $\mathcal{D} = \mathcal{D}(Z,P)$ of $\mathcal{A}$ with the properties in Lemma 10(iii). The subspace $\mathcal{D}$ consists of all $\mathbf{A} \in \mathcal{A}$ with $\langle \mathbf{ZA} \rangle = P$.

Example 3. *We determine the subspaces* $\mathcal{D}(Z,P)$ *for the* q*-ary* $(3,3,2)$ *Gabidulin code* $\mathcal{G}$*; cf. Example 1. Working in a coordinate-independent manner, suppose* $Z = \langle a, b\rangle$ *with* $a, b \in \mathbb{F}_{q^3}^\times$ *linearly independent over* $\mathbb{F}_q$ *and* $P = \langle c \rangle$ *with* $c \in \mathbb{F}_{q^3}^\times$*. Since* $x \mapsto ux^q - u^q x$*,* $u \in \mathbb{F}_{q^3}^\times$*, has kernel* $\mathbb{F}_q u$*, the maps*

$$f(x) = \frac{c(ax^q - a^q x)}{ab^q - a^q b}, \quad g(x) = \frac{c(bx^q - b^q x)}{ba^q - b^q a}$$

are well-defined, have rank 2, and satisfy $f(a) = g(b) = 0$*,* $f(b) = g(a) = c$*. Hence* $\mathcal{D}(Z,P) = \langle f, g\rangle$*. We may also write*

$$\mathcal{D}\big(Z, \mathbb{F}_q(ab^q - a^q b)\big) = \{ux^q - u^q x; u \in Z\},$$

making the linear dependence on Z *more visible. Scaling by a nonzero constant in* $\mathbb{F}_{q^3}^\times$ *then yields the general* $\mathcal{D}(Z,P)$*.*

It is obvious from Lemma 10 that $\mathcal{D}(Z_1,P_1) \neq \mathcal{D}(Z_2,P_2)$ whenever $(Z_1,P_1) \neq (Z_2,P_2)$. Hence a single coset $\mathcal{R} = \mathbf{A}_0 + \mathcal{D} \subset \mathcal{A}$ leads only to a single new plane in one particular hyperplane section determined by $\mathcal{D}$, and therefore Lemma 10 cannot be directly applied to yield $(6,M,4;3)_q$ subspace codes larger than LMRD codes. In order to achieve $\#\mathcal{N} > \#\mathcal{R}$, we should instead look for larger sets $\mathcal{R}$ having the property that the lines in the corresponding q^2+q+1 hyperplane sections can be simultaneously arranged into new planes. This requires $\mathcal{R}$ to be a union of cosets of spaces $\mathcal{D}(Z,P)$ simultaneously for all Z, for example a subspace containing a space $\mathcal{D}(Z,P)$ for each Z. Further we require that the corresponding points P are different for different choices of Z, excluding "unwanted" multiple covers of lines through P by new planes in different hyperplanes $H \supset S$.

Lemma 11. *Let* $\mathcal{R}$ *be a* t*-dimensional* $\mathbb{F}_q$*-subspace of a* q*-ary linear* $(3,3,2)$ *MRD code* $\mathcal{A}$*, having the following properties:*

[23] This is clear from the proof of the lemma.

(i) For each 2-dimensional subspace Z of $\mathbb{F}_q^3$ there exists a 1-dimensional subspace $P = Z'$ of $\mathbb{F}_q^3$ such that $\mathcal{D}(Z,P) \subseteq \mathcal{R}$.
(ii) The map $Z \mapsto Z'$ defines a bijection from 2-dimensional subspaces to 1-dimensional subspaces of $\mathbb{F}_q^3$.
(iii) $\operatorname{rk}\left(\frac{\mathbf{ZA}_1 - \mathbf{ZA}_2}{\mathbf{s}}\right) = 3$ whenever $\mathbf{A}_1$, $\mathbf{A}_2$ are in different cosets of $\mathcal{D}(Z,P)$ in $\mathcal{R}$, where $P = Z'$, $\mathbf{Z} = \operatorname{cm}(Z)$, and $\mathbf{s} = \operatorname{cm}(P)$.

Then the $(q^2+q+1)q^t$ lines covered by the planes in $\mathcal{L}$ corresponding to $\mathcal{R}$ can be rearranged into $(q^2+q+1)q^{t-2}$ new planes meeting S in a point and such that the set $\mathcal{N}$ of new planes has minimum subspace distance 4. Consequently, the remaining $q^6 - q^t$ planes in $\mathcal{L}$ and the new planes in $\mathcal{N}$ constitute a $(6, q^6 + q^{t-1} + q^{t-2}, 4; 3)_q$ subspace code.

PROOF. As before let $\mathcal{L}_1$ denote the set of q^t planes of the form $\langle(\mathbf{I}_3|\mathbf{A})\rangle$, $\mathbf{A} \in \mathcal{R}$. By (i), the q^t lines in any of the q^2+q+1 hyperplane sections $\mathcal{L}_1 \cap H$ are partitioned into q^{t-2} new planes meeting S in the same point $P = Z'$. Condition (ii) ensures that new planes in different hyperplanes have no line in common and hence subspace distance ≥ 4. Finally, if N, N' are distinct new planes in the same hyperplane section then $\operatorname{cm}(N) = \left(\begin{smallmatrix}\mathbf{Z} & \mathbf{ZA} \\ \mathbf{0} & \mathbf{s}\end{smallmatrix}\right)$, $\operatorname{cm}(N') = \left(\begin{smallmatrix}\mathbf{Z} & \mathbf{ZA}' \\ \mathbf{0} & \mathbf{s}\end{smallmatrix}\right)$ for some $\mathbf{A}$, $\mathbf{A}' \in \mathcal{R}$ with $\mathbf{A} + \mathcal{D} \neq \mathbf{A}' + \mathcal{D}$ where $\mathcal{D} = \mathcal{D}(Z,P)$. Condition (iii) is equivalent to $N + N' = H$, i.e. $N \cap N' = P$ or $\mathrm{d_s}(N, N') = 4$. $\square$

Condition (iii) in Lemma 11 is also equivalent to the requirement that the set $\mathcal{N}_H$ of q^{t-2} new planes in any hyperplane $H \supset S$ must form a partial spread in the quotient geometry $\mathrm{PG}(H/P) \cong \mathrm{PG}(3,q)$. This implies $t \leq 4$ with equality iff $\mathcal{N}_H \cup \{S\}$ forms a spread in $\mathrm{PG}(H/P)$. As $t \leq 2$ is impossible (cf. the remarks before Lemma 11), our focus from now on will be on the case $t = 3$.

EXAMPLE 4. *[Continuation of Example 3] Setting $\mathcal{R} = \{ux^q - u^q x; u \in \mathbb{F}_{q^3}\}$ and $Z' = P = \mathbb{F}_q(ab^q - a^q b)$ for a 2-dimensional subspace $Z = \langle a, b\rangle$ of $\mathbb{F}_{q^3}$, we have $\mathcal{D}(Z,P) \subset \mathcal{R}$ for any Z. Using $ab^q - a^q b = a^{q+1}\big((a^{-1}b)^q - (a^{-1}b)\big)$, the additive version of Hilbert's Theorem 90* [**14**, Satz 90] *and $\gcd(q^2+q+1, q+1) = 1$, we see that $Z \mapsto Z'$ is bijective.*[24] *Condition (iii) of Lemma 11 is equivalent to $\langle ca^q - c^q a, cb^q - c^q b, ab^q - a^q b\rangle = \mathbb{F}_{q^3}$ whenever $\langle a, b, c\rangle = \mathbb{F}_{q^3}$. This is in fact true, as we now show: a, b, c form a basis of $\mathbb{F}_{q^3}/\mathbb{F}_q$ iff*

$$\begin{vmatrix} a & b & c \\ a^q & b^q & c^q \\ a^{q^2} & b^{q^2} & c^{q^2} \end{vmatrix} \neq 0.$$

[24]In fact $Z \mapsto Z'$ defines a correlation of $\mathrm{PG}(\mathbb{F}_{q^3}) \cong \mathrm{PG}(2,q)$: The image of the line pencil through $\mathbb{F}_q a$ is the set of points on the line with equation $\operatorname{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(xa^{-q-1}) = 0$.

The adjoint determinant is

$$\begin{vmatrix} A^q & A^{q^2} & A \\ B^q & B^{q^2} & B \\ C^q & C^{q^2} & C \end{vmatrix}$$

with $A = bc^q - b^q c$, $B = ca^q - c^q a$, $C = ab^q - a^q b$. *By the same token, the adjoint determinant is* $\neq 0$ *iff* A, B, C *form a basis of* $\mathbb{F}_{q^3}/\mathbb{F}_q$. *From this our claim follows.*

Thus $\mathcal{R}$ *satisfies all conditions of Lemma 11 and gives rise to a* $(6, q^6 + q^2 + q, 4; 3)_q$ *subspace code* $\mathcal{C}$ *consisting of* $q^6 - q^3$ *"old" planes disjoint from* S *and* $q^3 + q^2 + q$ *"new" planes meeting* S *in a point,* q *of them passing through any of the* $q^2 + q + 1$ *points in* S.

In the coordinate-free model introduced in Section 2.5, $\mathcal{C}$ *consists of the* $q^6 - q^3$ *planes* $G(a_0, a_1) = \{(x, a_1 x^q - a_0 x); x \in \mathbb{F}_{q^3}\}$ *with* $a_0, a_1 \in \mathbb{F}_{q^3}$, $a_0 \neq a_1^q$ *and the* $q(q^2 + q + 1)$ *planes* $N(a, b, c) = \{(x, cx^q - c^q x + y(ab^q - a^q b); x \in Z, y \in \mathbb{F}_q\}$ *with* $Z = \langle a, b\rangle$ *any* 2*-dimensional* $\mathbb{F}_q$*-subspace of* $\mathbb{F}_{q^3}$ *and* $c \in \mathbb{F}_{q^3}/Z$.

4.2. Construction A and the proof of Theorem 2. In this section we complete the construction of an optimal $(6, 77, 4; 3)_2$ subspace code of Type A in Table 6. This will be done by adding 7 further planes to the $(6, 70, 4; 3)_2$ code $\mathcal{C}$ of Example 4. Since $\mathcal{C} = \mathcal{L}_0 \oplus \mathcal{N}$ already covers all lines disjoint from S, these planes must meet S in a line.[25] Hence the augmented $(6, 77, 4; 3)_2$ subspace code will contain precisely 56 planes disjoint from S and thus be of Type A.

In fact there is nothing special with the case $q = 2$ up to this point, and for all q we can extend the code of Example 4 by adding $q^2 + q + 1$ further planes meeting S in a line. This is the subject of the next lemma, which thereby completes the proof of Theorem 2.

Lemma 12. *The subspace code* $\mathcal{C}$ *from Example 4 can be extended to a* $(6, q^6 + 2q^2 + 2q + 1, 4; 3)_q$ *subspace code* $\overline{\mathcal{C}}$.

Proof. Our task is to add $q^2 + q + 1$ further planes to $\mathcal{C}$, one plane E with $E \cap S = L$ for each line L in S. These planes should cover points outside S at most once (ensuring that no line through a point of S is covered twice), and we must avoid adding planes that contain a line already covered by $\mathcal{N}$.

First we will determine the points outside S covered by the planes in $\mathcal{N}$. These are precisely the points covered by the "replaced" planes in $\mathcal{L}_1$. Viewed as points in $\mathrm{PG}(\mathbb{F}_{q^3} \times \mathbb{F}_{q^3})$, they have the form $(x, ux^q - u^q x)$ with $u \in \mathbb{F}_{q^3}$, $x \in \mathbb{F}_{q^3}^\times$. Since $ux^q - u^q x = -x^{q+1}\big((ux^{-1})^q - ux^{-1}\big)$, the points covered by $\mathcal{L}_1$ are the $q^2(q^2 + q + 1)$ points $\mathbb{F}_q(x, x^{q+1} v)$ with $x, v \in \mathbb{F}_{q^3}$, $x \neq 0$ and $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v) = 0$, each such point being covered

[25] The plane S itself may also be added to $\mathcal{C}$ without decreasing the subspace distance, resulting in a maximal $(6, 73, 4; 3)_2$ subspace code.

exactly q times.[26] The $q^5+q^4+q^3-(q^4+q^3+q^2)=q^5-q^2$ points outside S and not covered by $\mathcal{L}_1$ are those of the form $\mathbb{F}_q(x,x^{q+1}v)$ with $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v)\neq 0$.

Using this representation we can proceed as follows: We choose $v_0\in\mathbb{F}_{q^3}$ with $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v_0)\neq 0$ and connect the point $\mathbb{F}_q(x,x^{q+1}v_0)$ to the line in $S=\{0\}\times\mathbb{F}_{q^3}=\bigl\{(0,y);y\in\mathbb{F}_{q^3}\bigr\}$ with equation $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(yx^{-q-1})=0$. This gives q^2+q+1 planes $E(x)$, $x\in\mathbb{F}_{q^3}^\times/\mathbb{F}_q^\times$, which intersect S in q^2+q+1 different lines (since $\mathbb{F}_qx\mapsto\mathbb{F}_qx^{q+1}$ permutes the points of $\mathrm{PG}(\mathbb{F}_{q^3})$) and cover no point already covered by $\mathcal{L}_1$ (since the points in $E(x)$ have the form $\mathbb{F}_q\bigl(x,x^{q+1}(v_0+v)\bigr)$ with $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v)=0$ and hence $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v_0+v)\neq 0$).[27] Clearly the latter implies that $E(x)$ has no line in common with a plane in $\mathcal{N}$. Finally, projection onto the first coordinate (in $\mathbb{F}_{q^3}$) shows that distinct planes $E(x)$ and $E(x')$ do not have points outside S in common and hence intersect in a single point $P\in S$. In all we have now shown that the extended subspace code $\overline{\mathcal{C}}=\mathcal{C}\cup\bigl\{E(x);x\in\mathbb{F}_{q^3}^\times/\mathbb{F}_q^\times\bigr\}$ has the required parameters. □

5. Conclusion

We conclude the paper with a list of open questions arising from the present work.

Open Problems. *(1) Determine the maximum sizes* $\mathrm{A}_2(6,d)$ *of binary "mixed-dimension" subspace codes with packet length (ambient space dimension)* 6 *and minimum subspace distance* d, $1\leq d\leq 6$.[28]

(2) Give computer-free constructions of $(6,77,4;3)_2$ *subspace codes of Types B, C, D and E.*

(3) Find a computer-free proof of the upper bound $\mathrm{A}_2(6,4;3)\leq 77$. *A first step in this direction would be the proof that* $(6,M,4;3)_2$ *subspaces codes with* $M\geq 77$ *determine a distinguished plane* S *with the property in Corollary 1.*

(4) For $q>2$, *the best known bounds on* $\mathrm{A}_q(6,d)$ *are provided by Theorem 2 and Lemma 2:*

$$q^6+2q^2+2q+1\leq \mathrm{A}_q(6,4;3)\leq q^6+2q^3+1$$

---

[26] From this it follows that any plane in $\mathcal{L}_1$ intersects $(q-1)(q^2+q+1)=q^3-1$ further planes in $\mathcal{L}_1$, i.e., the q^3 planes in $\mathcal{L}_1$ mutually intersect in a point. This can also be concluded from the fact that the matrix space $\mathcal{R}$ has constant rank 2.

[27] It is unfortunate that we cannot use lines in S multiple times, since we are obviously able to pack the q^5-q^2 points outside S and not covered by $\mathcal{L}_1$ using $q(q^2+q+1)$ such planes, q through every line of S, by choosing q different values for $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v_0)$.

[28] Some of the values $\mathrm{A}_2(6,d)$ are already known. For example, $\mathrm{A}_2(6,1)=2825$ (the total number of subspaces of $\mathbb{F}_2^6$) and $\mathrm{A}_2(6,5)=\mathrm{A}_2(6,6)=9$ (as is easily verified).

Reduce the remaining gap of size $2(q^3 - q^2 - q)$ *by improving the lower or the upper bound.*

(5) *Generalize Construction A to packet lengths* $v > 6$ *and/or constant dimensions* $k > 3$.

(6) *Prove or disprove* $\mathrm{A}_2(7, 4; 3) = 381$ *(now the smallest open binary constant-dimension case), thereby resolving the existence question for the* 2*-analog of the Fano plane.*

Acknowledgements.

The authors wish to thank Thomas Feulner for providing us with his canonization algorithm from [**10**] and the two reviewers for valuable comments and corrections.

References

[1] A. Beutelspacher. Partial spreads in finite projective spaces and partial designs. *Mathematische Zeitschrift*, 145:211–230, 1975. Corrigendum, ibid. 147:303, 1976.

[2] G. Bonoli, N. Melone. A characterization of Grassmann and attenuated spaces as $(0, \alpha)$-geometries. *European Journal of Combinatorics*, 124:489–498, 2003.

[3] F. de Clerck and H. van Maldeghem. Some classes of rank two geometries. In F. Buekenhout, editor, *Handbook of Incidence Geometry—Buildings and Foundations*, chapter 10, pages 433–475. Elsevier Science Publishers, 1995.

[4] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25:226–241, 1978.

[5] J. Eisfeld and L. Storme. (Partial) t-spreads and minimal t-covers in finite projective spaces. Lecture notes, Ghent University, 2000.

[6] T. Etzion. Problems on q-analogs in coding theory. Preprint arXiv:13056126 [cs.IT], May 2013.

[7] T. Etzion and N. Silberstein. Codes and designs related to lifted MRD codes. *IEEE Transactions on Information Theory*, 59(2):1004–1017, Feb. 2013.

[8] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Transactions on Information Theory*, 57(2):1165–1173, Feb. 2011.

[9] T. Feulner. The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes. *Advances in Mathematics of Communications*, 3(4):363–383, Nov. 2009.

[10] T. Feulner. Canonical Forms and Automorphisms in the Projective Space. Preprint arXiv:1305.1193 [cs.IT], May 2013.

[11] 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.

[12] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–12, 1985.

[13] 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.

[14] D. Hilbert. Die Theorie der Algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 4:175–535, 1897.

[15] D. E. Knuth. Subspaces, subsets, and partitions. *Journal of Combinatorial Theory, Series A*, 10:178–180, 1971.

[16] R. Kötter and F. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, Aug. 2008.

[17] A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In J. Calmet, W. Geiselmann, and J. Müller-Quade, editors, *Mathematical Methods in Computer Science. Essays in Memory of Thomas Beth*, number 5393 in Lecture Notes in Computer Science, pages 31–42. Springer-Verlag, 2008.

[18] F. R. Kschischang. An introduction to network coding. In M. Médard and A. Sprintson, editors, *Network Coding: Fundamentals and Applications*, chapter 1, pages 1–37. Elsevier Science Publishers, 2012.

[19] V. S. Pless and W. C. Huffman, editors. *Handbook of Coding Theory*, volume I. Elsevier Science Publishers, 1998.

[20] V. S. Pless and W. C. Huffman, editors. *Handbook of Coding Theory*, volume II. Elsevier Science Publishers, 1998.

[21] R. M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, Mar. 1991. Comments by Emst M. Gabidulin and Author's Reply, ibid. 38(3):1183, 1992.

[22] R. Shaw. Subsets of $\mathrm{PG}(n, 2)$ and maximal partial spreads in $\mathrm{PG}(4, 2)$. *Designs, Codes and Cryptography*, 21(1/2/3):209–222, Oct. 2000.

[23] D. Silva, F. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, Sept. 2008.

[24] A.-L. Trautmann and J. Rosenthal. New improvements on the Echelon-Ferrers construction. In A. Edelmayer, editor, *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010)*, pages 405–408, Budapest, Hungary, 5–9 July 2010. Reprint arXiv:1110.2417 [cs.IT].

[25] Z.-X. Wan. *Geometry of Matrices.* World Scientific, 1996.

[26] S.-T. Xia and F.-W. Fu. Johnson type bounds on constant dimension codes. *Designs, Codes and Cryptography*, 50(2):163–172, 2009.

[27] S. Yang and T. Honold. Good random matrices over finite fields. *Advances in Mathematics of Communications*, 6(2):203–227, May 2012.

Thomas Honold, Department of Information and Electronic Engineering, Zhejiang University, 38 Zheda Road, 310027 Hangzhou, China
E-mail address: `honold@zju.edu.cn`

Michael Kiermaier, Mathematisches Institut, Universität Bayreuth, D-95440 Bayreuth, Germany
E-mail address: `michael.kiermaier@uni-bayreuth.de`

Sascha Kurz, Mathematisches Institut, Universität Bayreuth, D-95440 Bayreuth, Germany
E-mail address: `sascha.kurz@uni-bayreuth.de`