SUBSPACES INTERSECTING IN AT MOST A POINT

SASCHA KURZ

ABSTRACT. We improve on the lower bound of the maximum number of planes in $\operatorname{PG}(8,q) \cong \mathbb{F}_q^9$ pairwise intersecting in at most a point. In terms of constant dimension codes this leads to $A_q(9,4;3) \ge q^{12}+2q^8+2q^7+q^6+2q^5+2q^4-2q^2-2q+1$. This result is obtained via a more general construction strategy, which also yields other improvements.
Keywords: constant dimension codes, finite projective geometry, network coding
MSC: Primary 51E20; Secondary 05B25, 94B65.

1. INTRODUCTION

Let $V \cong \mathbb{F}_q^v$ be a v-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. We call each k-dimensional linear subspace of V a k-space, also using the terms points, lines, and planes for 1-, 2-, and 3-spaces, respectively. Two k-spaces U, W are said to trivially intersect or to be disjoint if $\dim(U\cap W)=0$, i.e., U and W do not share a common point. Sets of k-spaces that are pairwise disjoint are called partial k-spreads, see [10] for a recent survey on bounds for their maximum possible sizes. In finite projective geometry they are a classical topic. Here we study the rather similar objects of sets of k-spaces which pairwise intersect in at most a point and have large cardinality. More generally, we can use the subspace distance $\mathrm{d_s}(U,W)=\dim(U+W)-\dim(U\cap W)=\dim(U)+\dim(W)-2\dim(U\cap W)$ to define $A_q(v,d;k)$ as the maximum number of k-spaces in $\mathbb{F}_q^v$ that have minimum subspace distance d, i.e., that intersect in a subspace of dimension at most $k-d/2$. Since those sets, which are also called constant dimension codes, have applications in error correcting random network coding, see e.g. [11], bounds for $A_q(v,d;k)$ have been studied intensively in the literature. For the currently best known lower and upper bounds we refer to the online tables `http://subspacecodes.uni-bayreuth.de` and the associated survey [7]. Due to this connection, we also call sets of k-spaces codes and call their elements codewords.

Due to combinatorial explosion, it is in general quite hard to obtain improvements for $A_q(v,d;k)$ when the dimension v of the ambient space is small, say $v \le 11$. Our main motivation for this paper is the recently improved parametric lower bound $A_q(9,4;3) \ge q^{12}+2q^8+2q^7+q^6+q^5+q^4+1$, see [2, Theorem 3.13]. Here, we give a further improved construction for $A_q(9,4;3)$ and generalize the underlying ideas to a more general combination of constant dimension codes. The latter constitutes our main Theorem, see Theorem 3, which allows to conclude also other improved parametric constructions.

2. PRELIMINARIES

For two matrices $U,W \in \mathbb{F}_q^{m\times n}$ we define the rank distance $\mathrm{d_r}(U,W) := \operatorname{rk}(U-W)$. A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is called a rank metric code.

Theorem 1. *(see [4]) Let $m,n \ge d$ be positive integers, q a prime power, and $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ be a rank metric code with minimum rank distance d. Then, $\#\mathcal{C} \le q^{\max\{n,m\}\cdot(\min\{n,m\}-d+1)}$.*

Codes attaining this upper bound are called maximum rank distance (MRD) codes. They exist for all choices of parameters. A construction can e.g. be described using so-called linearized polynomials, see e.g. [11, Section V]. If $m<d$ or $n<d$, then only $\#\mathcal{C}=1$ is possible, which can be achieved by a zero

matrix and may be summarized to the single upper bound $\#\mathcal{C} \le \left\lceil q^{\max\{n,m\}\cdot(\min\{n,m\}-d+1)}\right\rceil$. Using an $m \times m$ identity matrix as a prefix one obtains the so-called lifted MRD codes.

Theorem 2. [13, Proposition 4] *For positive integers k, d, v with $k \le v$, $d \le 2\min\{k, v-k\}$, and d even, the size of a lifted MRD code in $\left[\begin{smallmatrix} V \\ k \end{smallmatrix}\right]$ with subspace distance d is given by $q^{\max\{k,v-k\}\cdot(\min\{k,v-k\}-d/2+1)}$.*

3. COMBINING SUBSPACES

Theorem 3. *Let $\mathcal{C}_1$ be a set of k-spaces in $\mathbb{F}_q^{v_1}$ mutually intersecting in at most a point, $\mathcal{C}_1^C$ be a subset of $\mathcal{C}_1$ such that all elements are pairwise intersecting trivially, and $\mathcal{C}_2$ be a set of k-spaces in $\mathbb{F}_q^{v_2}$ mutually intersecting in at most a point, where $v_2 \ge 2k$ and $\#\mathcal{C}_2 \ge 1$. If $\mathbb{F}_q^{v_2}$ admits a (v_2-k)-space S, such that exactly Λ elements of $\mathcal{C}_2$ are contained in S and all others intersect S in at most a point, then*

$$A_q(v_1+v_2-k, 2k-2; k) \ge \#\mathcal{C}_1 \cdot q^{2(v_2-k)} + \#\mathcal{C}_1^C \cdot \left(\#\mathcal{C}_2 - q^{2(v_2-k)} - \Lambda\right) + \Lambda.$$

PROOF. We embed $\mathcal{C}_1$ in $\mathbb{F}_q^{v_1+v_2-k}$ and choose a (v_2-k)-space S disjoint to the span $\langle \mathcal{C}_1 \rangle$. For each $U \in \mathcal{C}_1$ we consider the v_2-space $K = \langle U, S \rangle$. If $U \in \mathcal{C}_1^C$, we embed $\mathcal{C}_2$ minus the Λ codewords contained in S in K such that the embedding contains the k-space U and all codewords intersect S in at most a point. If $U \notin \mathcal{C}_1^C$, we embed a lifted MRD code in K such that the embedding contains the k-space U and all codewords are disjoint to S. If we additionally add Λ codewords inside S, then we obtain a set $\mathcal{C}$ of k-spaces in $\mathbb{F}_q^{v_1+v_2-k}$ of cardinality $\#\mathcal{C}_1^C \cdot (\#\mathcal{C}_3 - \Lambda) + \left(\#\mathcal{C}_1 - \#\mathcal{C}_1^C\right) \cdot q^{2(v_2-k)} + \Lambda$, since the matching lifted MRD code has cardinality $q^{2(v_2-k)}$. For two different $W, W' \in \mathcal{C}$ we have to show that they do intersect in at most a point. By construction, there exist $U, U' \in \mathcal{C}_1$ such that $W \le K := \langle U, S \rangle$ and $W' \le K' := \langle U', S \rangle$. We have $S \le K \cap K'$ and $v_2 - k \le \dim(K \cap K') = v_2 - k + \dim(U \cap U') \le v_2 - k + 1$. If $U = U'$, which we can assume w.l.o.g. for $W \le S$ or $W' \le S$, then $\dim(W \cap W') \le 1$. If $U, U' \in \mathcal{C}_1^C$, then $W \cap W' \le S$, so that $\dim(W \cap W') \le 1$. Otherwise we have $\dim(W \cap W' \cap S) = 0$, so that also $\dim(W \cap W') \le 1$. $\square$

If we choose $v_2 = 2k$ and $\mathcal{C}_2$ such that there are two disjoint codewords, then S can be chosen as a codeword, i.e., $\Lambda = 1$, and all codewords except S itself intersect S in at most a point. For brevity, we will calls sets of k-spaces that are trivially intersecting and are a subset of a some set $\mathcal{C}_1$ of k-spaces, a clique.

Corollary 4.

$$A_q(9,4;3) \ge q^{12} + 2q^8 + 2q^7 + q^6 + 2q^5 + 2q^4 - 2q^2 - 2q + 1$$

PROOF. For $k = 3$ and $v = 6$ we choose $\mathcal{C}_1$ and $\mathcal{C}_2$ as a set of $q^6 + 2q^2 + 2q + 1$ planes in $\mathbb{F}_q^6$ pairwise intersecting in at most a point [3, Theorem 2.1]. By [2, Theorem 3.12] we can choose a subset $\mathcal{C}_1^C \subseteq \mathcal{C}_1$ of cardinality $q^3 - 1$. $\square$

We remark that this improves the very recent lover bound $A_q(9,4;3) \ge q^{12} + 2q^8 + 2q^7 + q^6 + q^5 + q^4 + 1$ [2, Theorem 3.13]. As $\mathcal{C}_2$ we might also have chosen the construction from [9] of the same size.[1] In our setting we always have $\#\mathcal{C}_1^C \le A_q(6,6;3) = q^3 + 1$. If we replace $\mathcal{C}_2$ in Corollary 4 by the set of $q^8 + q^5 + q^4 - q - 1$ planes in $\mathbb{F}_q^7$ from [8, Theorem 3], then the conditions of Theorem 3 are satisfied for $\Lambda = 0$ and we obtain

$$A_q(10,4;3) \ge q^{14} + 2q^{10} + 2q^9 + 2q^8 + q^7 - q^5 - 2q^4 - q^3 + q + 1. \tag{1}$$

However, [12, Proposition 4.4] gives a better lower bound.

For a general application of Theorem 3 the presumably hardest part is to analytically determine $\mathcal{C}_1^C$, i.e., a clique in $\mathcal{C}_1$. If $\mathcal{C}_1$ itself is obtained via Theorem 3 and a lower bound on the clique size of the corresponding part $\mathcal{C}_2$ is known, then can recursively determine suitably large cliques.

[1] The same applies to $\mathcal{C}_1$, i.e., we can avoid to use [2, Theorem 3.12], see the subsequent Footnote 3.

Lemma 5. *If $\mathcal{C}$ is obtained from the construction of Theorem 3 and the corresponding part $\mathcal{C}_2$ contains a clique $\mathcal{C}_2^C$ whose elements are disjoint from S, then $\mathcal{C}$ admits a subset $\mathcal{C}'$ such that all elements are pairwise intersecting trivially and $\#\mathcal{C}' = \#\mathcal{C}_1^C \cdot \#\mathcal{C}_2^C$.*

PROOF. Using the notation from Theorem 3 we construct $\mathcal{C}'$. For each $U \in \mathcal{C}_1^C$ we consider $K := \langle U, S\rangle$ and choose a clique of cardinality $\#\mathcal{C}_2^C$ in K and add the elements to $\mathcal{C}'$. Using the analysis of the proof of Theorem 3 again and the fact that the elements of $\mathcal{C}'$ all are disjoint to S, we conclude that the elements of $\mathcal{C}'$ are pairwise intersecting trivially. □

If we choose $\mathcal{C}_2$ according to [3, Theorem 2.1], we can use [2, Theorem 3.12] to conclude $\#\mathcal{C}_2^C \geq q^3 - 1$.

Proposition 6. $A_q(6+3t, 4; 3) \geq \left(q^6 + 2q^2 + 2q + 1\right) \cdot q^{6t} + \frac{q^{6t}-1}{q^6-1} + \sum_{i=1}^{t} (2q^2+2q) \cdot \left(q^3-1\right)^i \cdot q^{6(t-i)}$ *for all* $t \geq 0$.

PROOF. For the induction start $t = 0$ we choose $\mathcal{C}^{(0)}$ as a set of $q^6 + 2q^2 + 2q + 1$ planes in $\mathbb{F}_q^6$ pairwise intersecting in at most a point according to [3, Theorem 2.1], which admits a clique of cardinality $q^3 - 1$. For the induction step $\mathcal{C}^{(i)} \to \mathcal{C}^{(i+1)}$ we apply Theorem 3 with $v_2 = 2k$, $\Lambda = 1$, $\mathcal{C}_1 = \mathcal{C}^{(i)}$, and $\mathcal{C}_2 = \mathcal{C}^{(0)}$. By induction, see Lemma 5, $\mathcal{C}^{(i)}$ admits a clique $\mathcal{C}_1^C$ of cardinality $\left(q^3-1\right)^{i+1}$. The induction hypothesis for the cardinality of $\mathcal{C}^{(i)}$ is

$$\#\mathcal{C}^{(i)} = \left(q^6 + 2q^2 + 2q + 1\right) \cdot q^{6i} + \frac{q^{6i}-1}{q^6-1} + \sum_{j=1}^{i} (2q^2+2q) \cdot \left(q^3-1\right)^i \cdot q^{6(i-j)} \tag{2}$$

and the induction step, see Theorem 3, gives $\#\mathcal{C}^{(i+1)}$ as the right hand side of Equation (2), where i is replaced by $i+1$. □

Another example of a set of planes pairwise intersecting in at most a point, where we can analytically determine a reasonably large clique, is given by [12, Proposition 4.4]: $A_q(8, 4; 3) \geq q^{10} + q^6 + q^5 + 2q^4 + 2q^3 + 2q^2 + q + 1$, which is the currently best known lower bound for $q \geq 3$. The essential key here is that the code contains a lifted MRD code of cardinality q^{10} for rank distance 2. By [5, Lemma 5] the MRD code can be chosen in such a way that it contains a subcode of cardinality q^5 and rank distance 3.[2] Thus we obtain a clique of cardinality q^5 and can use Theorem 3 with $v_2 = 6$ and $\Lambda = 1$ to conclude

$$A_q(11, 4; 3) \geq q^{16} + q^{12} + q^{11} + 2q^{10} + 2q^9 + 2q^8 + 2q^7 + 2q^6 + 1, \tag{3}$$

which strictly improves upon [12, Proposition 4.4]. Of course we can iteratively apply the combination with the $q^6 + 2q^2 + 2q + 1$ planes in $\mathbb{F}_q^6$ to obtain an infinite parametric series as in Proposition 6. The method generalizes to cases where large constant dimension codes are obtained by using lifted MRD codes as subcodes, which frequently is the case. Also the constant dimension codes showing $A_q(6, 4; 3) \geq q^6 + 2q^2 + 2q + 1$ [9, Lemma 12, Example 4] and $A_q(7, 4; 3) \geq q^8 + q^5 + q^4 + q^2 - q$ [8, Theorem 4] are closely related. They both arise by starting from a lifted MRD code, removing some planes, and then extending again with a larger set of planes, cf. [1]. Considering just the reduced lifted MRD code, we can deduce clique sizes of $q^3 - 1$ and q^4, respectively.[3] If we choose $\mathcal{C}_1$ in Theorem 3 as the mentioned code for $A_q(7, 4; 3)$ and $\mathcal{C}_2$ as the mentioned code for $A_q(6, 4; 3)$ or the code for

---

[2] Using linearized polynomials to described the lifted MRD code, a clique of matching size can be described as the set of monomials ax (including the zero polynomial).

[3] Both constructions are stated in the language of linearized polynomials. For [9, Lemma 12, Example 4] the representation $\mathbb{F}_q^6 \cong \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}$ is used and the planes removed from the lifted MRD code correspond to $ux^q - u^q x$ for $u \in \mathbb{F}_{q^3}$, so that the monomials ax for $a \in \mathbb{F}_{q^3}\backslash\{\mathbf{0}\}$ correspond to a clique of cardinality q^3-1. For [8, Theorem 4] the representation $\mathbb{F}_q^7 \cong W \times \mathbb{F}_{q^4}$, where W denotes the trace-zero subspace of $\mathbb{F}_{q^4}/\mathbb{F}_q$, is used. The planes removed from the lifted MRD code correspond to $r\,(ux^q - u^q x)$ for $r \in \mathbb{F}_{q^4}\backslash\{\mathbf{0}\}$ and $u \in \mathbb{F}_{q^4}$ with $\mathrm{tr}(u) = 1$, so that the monomial s ax for $a \in \mathbb{F}_{q^4}$ correspond to a clique of cardinality q^4.

$A_q(7,4;3) \ge q^8+q^5+q^4-q-1$, see[8, Theorem 3], then we obtain

$$A_q(10,4;3) \ge q^{14}+q^{11}+q^{10}+q^8-q^7+2q^6+2q^5+1 \qquad (4)$$

and

$$A_q(11,4;3) \ge q^{16}+q^{13}+q^{12}+q^{10}+q^8-q^5-q^4. \qquad (5)$$

Both inequalities improve upon the (for $q \ge 4$) previously best known lower bounds from [12, Proposition 4.4] and the latter improves upon Inequality (3).

So, Theorem 3 can yield improved constructions, but of course not all choices of the involved parameters and codes lead to improvements. If $v_1 < 2k$, then $\#\mathcal{C}_1^C \le 1$, so that no strict improvement over known constructions can be obtained. For $k > 3$ it might be necessary to use $v_2 > 2k$, since no example for $A_q(2k, 2k-2; k) > q^{2k}+1$ is known. In [6] the authors have indeed shown $A_2(8,6;4) = 2^8+1 = 257$ and conjectured $A_q(2k, 2k-2; k) = q^{2k}+1$ for all $k \ge 4$.

In principle it is also possible to generalize Theorem 3 to situations where the k-spaces can intersect in subspaces of dimension t strictly larger than one. To this end, one may partition $\mathcal{C}_1$ into subsets $\mathcal{C}_1^{(0)}$, $\mathcal{C}_1^{(1)}$, $\dots$, $\mathcal{C}_1^{(t)}$ such that every element from $\mathcal{C}_1^{(i)}$ intersects each different element from $\cup_{j=0}^{i}\mathcal{C}_1^{(j)}$ in dimension at most i, which generalizes the partition $\mathcal{C}_1^C$, $\mathcal{C}_1 \backslash \mathcal{C}_1^C$. If S is again our special subspace and $U \in \mathcal{C}_1^{(i)}$, then codewords in the code in $\langle U, S\rangle$ should intersect S in dimension at most $t-i$, where we may also put some additional codewords into S. Since we currently have no example at hand that improves upon a best known lower bound for $A_q(v,d;k)$, we refrain from giving a rigorous proof and detailed statement.

ACKNOWLEDGMENT

The author would like to thank Thomas Honold for his analysis of possible cliques sizes in the constant dimension codes from [9, Lemma 12, Example 4] and [8, Theorem 4], see Footnote 3. The main idea for Theorem 3 is inspired by [2].

REFERENCES

[1] J. Ai, T. Honold, and H. Liu. The expurgation-augmentation method for constructing good plane subspace codes. *arXiv preprint 1601.01502*, 2016.
[2] A. Cossidente, G. Marino, and F. Pavese. Subspace code constructions. *arXiv preprint 1905.11021*, 2019.
[3] A. Cossidente and F. Pavese. On subspace codes. *Designs, Codes and Cryptography*, 78(2):527–531, 2016.
[4] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.
[5] T. Etzion and N. Silberstein. Codes and designs related to lifted MRD codes. *IEEE Transactions on Information Theory*, 59(2):1004–1017, 2013.
[6] D. Heinlein, T. Honold, M. Kiermaier, S. Kurz, and A. Wassermann. Classifying optimal binary subspace codes of length 8, constant dimension 4 and minimum distance 6. *Designs, Codes and Cryptography*, 87(2-3):375–391, März 2019.
[7] D. Heinlein, M. Kiermaier, S. Kurz, and A. Wassermann. Tables of subspace codes. *arXiv preprint 1601.02864*, 2016.
[8] T. Honold and M. Kiermaier. On putative q-analogues of the Fano plane and related combinatorial structures. In *Dynamical systems, number theory and applications*, pages 141–175. World Sci. Publ., Hackensack, NJ, 2016.
[9] T. Honold, M. Kiermaier, and S. Kurz. Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4. In *Topics in finite fields*, volume 632 of *Contemp. Math.*, pages 157–176. Amer. Math. Soc., Providence, RI, 2015.
[10] T. Honold, M. Kiermaier, and S. Kurz. Partial spreads and vector space partitions. In *Network Coding and Subspace Designs*, Signals and Communication Technology, pages 131–170. Springer, Cham, Januar 2018.
[11] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.
[12] S. Kurz. A note on the linkage construction for constant dimension codes. *arXiv preprint 1906.09780*, 2019.
[13] 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, 2008.

SASCHA KURZ, UNIVERSITY OF BAYREUTH, 95440 BAYREUTH, GERMANY
Email address: sascha.kurz@uni-bayreuth.de