Evasive subspaces

Daniele Bartoli[†], Bence Csajbók [**], Giuseppe Marino[‡], and Rocco Trombetti[‡]

[†]Department of Mathematics and Informatics, University of Perugia, Perugia, Italy, *daniele.bartoli@unipg.it*

[*]ELKH–ELTE Geometric and Algebraic Combinatorics Research Group, ELTE Eötvös Loránd University, Budapest, Hungary, Department of Geometry, 1117 Budapest, Pázmány P. stny. 1/C, Hungary, *csajbokb@cs.elte.hu*

[‡]Dipartimento di Matematica e Applicazioni "R. Caccioppoli", Università degli Studi di Napoli "Federico II", Via Cintia, Monte S.Angelo I-80126 Napoli, Italy, *giuseppe.marino@unina.it, rtrombet@unina.it*

Abstract

Let V denote an r-dimensional vector space over $\mathbb{F}_{q^n}$, the finite field of q^n elements. Then V is also an rn-dimension vector space over $\mathbb{F}_q$. An $\mathbb{F}_q$-subspace U of V is $(h,k)_q$-evasive if it meets the h-dimensional $\mathbb{F}_{q^n}$-subspaces of V in $\mathbb{F}_q$-subspaces of dimension at most k. The $(1,1)_q$-evasive subspaces are known as scattered and they have been intensively studied in finite geometry, their maximum size has been proved to be $\lfloor rn/2 \rfloor$ when rn is even or $n = 3$.

We investigate the maximum size of $(h,k)_q$-evasive subspaces, study two duality relations among them and provide various constructions. In particular, we present the first examples, for infinitely many values of q, of maximum scattered subspaces when $r = 3$ and $n = 5$. We obtain these examples in characteristics 2, 3 and 5.

Keywords: evasive set, scattered subspace, q-polynomial

---

[*]Corresponding author.

1 Introduction

Let $\mathcal{F}$ be a set of subsets of a set A and let $S \subseteq A$. In [23, Definition 1] Pudlák and Rödl called S *c-evasive for $\mathcal{F}$* if for all $W \in \mathcal{F}$

$$|W \cap S| \leq c.$$

In their work A was then taken to be the set of vectors of an r-dimensional vector space V over $\mathbb{F}_2$, the finite field of two elements, and $\mathcal{F}$ was the set of all d-dimensional affine subspaces of V for some positive integer d. The authors of [23] also showed how such evasive sets can be used to construct explicit Ramsey graphs. Later, these objects were called *subspace evasive*, see Guruswami [13, Section 4], [14, Definition 2] or Dvir and Lovett [12, Definition 3.1] and were studied intensively since they can be used to obtain explicit list decodable codes with optimal rate and constant list-size. More precisely, following Guruswami, let V be an r-dimensional vector space over the (usually but not necessarily finite) field $\mathbb{F}$. Then $S \subseteq V$ is called (d, c)-*subspace evasive* if for every d-dimensional linear subspace H of V we have $|S \cap H| \leq c$.

Note that Dvir and Lovett used the term (d, c)-subspace evasive to denote c-evasive sets for the set of all d-dimensional affine subspaces. The two concepts do not coincide, however, they are strongly related as the next two paragraphs show.

Every d-dimensional affine subspace is contained in a $(d+1)$-dimensional linear subspace. Thus if S is c-evasive for the set of all $(d+1)$-dimensional linear subspaces then it is c-evasive for the set of all d-dimensional affine subspaces.

Also, if $\mathbb{F}$ is a finite field, say $\mathbb{F}_{p^s}$, for some p prime, and S is additive (or equivalently, S is an $\mathbb{F}_p$-linear subspace of V), then S is c-evasive for the set of all d-dimensional linear subspaces if and only if it is c-evasive for the set of all d-dimensional affine subspaces. To see this, consider any d-dimensional affine subspace A and a vector $x \in S \cap A$. For a set B we denote by $B - x$ the difference set $\{b - x : b \in B\}$. Then

$$|S \cap A| = |(S - x) \cap (A - x)| = |S \cap (A - x)|,$$

where $S - x = S$ follows from the additivity of S, and $A - x$ is a d-dimensional linear subspace of V.

In [14] additive subspace evasive sets were constructed, that is, subspace evasive sets which are also linear subspaces of V over some subfield $\mathbb{F}_{p^t}$ of $\mathbb{F}_{p^s}$, $t \mid s$. Clearly, if $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{p^s}$, then $p^s = q^n$ for some integer n. The aim of this paper is to study these evasive sets. Note that, if S is linear over $\mathbb{F}_q$ then intersections of S with linear (or affine) $\mathbb{F}_{q^n}$-subspaces of V are also linear (or affine) $\mathbb{F}_q$-subspaces. From now on, we will denote by $V = V(r, q^n)$ an r-dimensional vector space over the finite field $\mathbb{F}_{q^n}$. Note that V is also an rn-dimensional vector space over $\mathbb{F}_q$.

Definition 1.1. *An $\mathbb{F}_q$-subspace U of V will be called $(h, k)_q$-evasive if $\langle U \rangle_{\mathbb{F}_{q^n}}$ has dimension at least h over $\mathbb{F}_{q^n}$ and the h-dimensional $\mathbb{F}_{q^n}$-subspaces of V meet U in $\mathbb{F}_q$-subspaces of dimension at most k.*

Note that in the definition above the condition on the dimension of $\langle U \rangle_{\mathbb{F}_{q^n}}$ is to exclude trivial examples for which some of our results would not apply. So, take an $\mathbb{F}_q$-subspace U

of V such that the condition $\dim_{q^n}\langle U\rangle_{q^n} \geq h$ holds. Then it is easy to find an h-dimensional $\mathbb{F}_{q^n}$-subspace meeting U in an $\mathbb{F}_q$-subspace of dimension at least h and hence for an $(h,k)_q$-evasive subspace $h \leq k$ must hold. Clearly, if $\dim_q U \leq k$ then U is an $(h,k)_q$-evasive subspace. The $(r,k)_q$-evasive subspaces are the $\mathbb{F}_q$-subspaces of dimension at most k which span V over $\mathbb{F}_{q^n}$. Note that an $(h,k)_q$-evasive subspace is also $(h',k')_q$-evasive for any $h' \leq h$ and $k' \geq k$.

If S is c-evasive for $\mathcal{F}$ then the same holds for every subset $S' \subseteq S$. Thus there are two natural questions to ask:

(A) For given c and $\mathcal{F}$, what is the size of the largest c-evasive set for $\mathcal{F}$? We will call evasive sets of this size *maximum*.

(B) For given c and $\mathcal{F}$, determine the smallest c-evasive sets for $\mathcal{F}$ which are not contained in a larger one. We will call these evasive sets *maximal*.

For example if $\mathcal{F}$ is the set of edges of a graph $\mathcal{G}$ and $c = 1$ then (A) asks for the size of a maximum independent set in $\mathcal{G}$ and (B) asks for the size of a minimum vertex cover in $\mathcal{G}$.

The concept of evasive sets is well known in finite geometry as well. Denote by Σ a finite projective space isomorphic to $\mathrm{PG}(d,q)$. A *cap of kind h* is an h-evasive set for the set of $(h-1)$-dimensional projective subspaces of Σ, cf. [27]. The most studied examples are the *arcs* ($h = d$), *caps* ($h = 2$) [15] and *tracks* ($h = d-1$) [11]. To arcs and tracks correspond the MDS and almost MDS codes, respectively ([1], [16]). One can weaken further these conditions and consider point sets meeting each hyperplane in at most n points. For example (k,n)-*arcs* are the n-evasive point sets of size k for the set of lines in a projective plane of order q. There are many famous conjectures regarding the size of a maximum evasive set in this setting. For example the maximal arc conjecture, which was proved by Ball, Blokhuis and Mazzocca [4, 2]. The main conjecture for MDS codes is equivalent to ask the maximum size of an arc in Σ [1, Section 7].

Recently, in [24] Randrianarisoa introduced q-systems. A q-*system* U over $\mathbb{F}_{q^n}$ with parameters $[m,r,d]$ is an m-dimensional $\mathbb{F}_q$-subspace generating over $\mathbb{F}_{q^n}$ a r-dimensional $\mathbb{F}_{q^n}$-vector space V, where

$$d = m - \max\{\dim(U \cap H) : H \text{ is a hyperplane of } V\}.$$

With our notation, it is equivalent to say that U is $(r-1, m-d)_q$-evasive in $V(r,q^n)$ and it is not $(r-1, m-d+1)_q$-evasive. These objects are in one-to-one correspondence with $\mathbb{F}_{q^n}$-linear $[m,r,d]$-rank metric codes, cf. [24, Theorem 2].

In [10] the authors investigated the following subspace analogue of caps of kind h: for $0 < h < r$ an $\mathbb{F}_q$-subspace U of $V = V(r,q^n)$ is called h-*scattered* if U generates V over $\mathbb{F}_{q^n}$ and any h-dimensional $\mathbb{F}_{q^n}$-subspace of V meets U in an $\mathbb{F}_q$-subspace of dimension at most h. With the notation of this paper, the h-scattered subspaces are the $(h,h)_q$-evasive subspaces generating V over $\mathbb{F}_{q^n}$.

A t-*spread* of V is a partition of $V \setminus \{\mathbf{0}\}$ by $\mathbb{F}_q$-subspaces of dimension t. In particular $\mathcal{D} := \{\langle \mathbf{u}\rangle_{\mathbb{F}_{q^n}} \setminus \{\mathbf{0}\} : \mathbf{u} \in V\}$ is the so called Desarguesian n-spread of V. An $\mathbb{F}_q$-subspace

3

U of V is called *scattered with respect to a spread* $\mathcal{S}$ if U meets each element of $\mathcal{S}$ in at most a one-dimensional $\mathbb{F}_q$-subspace, i.e. when U is q-evasive for $\mathcal{S}$. In [6] Blokhuis and Lavrauw proved that $rn/2$ is the maximum dimension of a scattered subspace of V w.r.t. a Desarguesian n-spread. In other words, the dimension of a maximum $(1, 1)_q$-evasive subspace is at most $rn/2$. After a series of papers it is now known that this bound is sharp when rn is even, cf. Result 2.3. Note that the 1-scattered subspaces are the scattered subspaces generating V over $\mathbb{F}_{q^n}$.

In [10] the authors generalized the Blokhuis–Lavrauw bound and proved that the dimension of an h-scattered subspace is at most $rn/(h+1)$. They also introduced a relation, called *Delsarte duality*, on $\mathbb{F}_q$-subspaces of V and proved that the Delsarte dual of an $rn/(h+1)$-dimensional h-scattered subspace is h'-scattered with dimension $r'n/(h'+1)$ in some vector space $V'(r', q^n)$. For the precise statement see [10, Theorem 3.3]. Delsarte duality is a well known concept in the theory of rank metric codes. There is a correspondence between maximum $(r-1)$-scattered subspaces, also called *scattered subspaces w.r.t. hyperplanes*, and certain MRD (maximum rank metric) codes, see [19, 26]. In fact, if $\mathcal{C}$ is the MRD-code correspoinding to an n-dimensional $(r-1)$-scattered subspace U then the Delsarte dual $\mathcal{C}^\perp$ of $\mathcal{C}$ is the MRD-code corresponding to the Delsarte dual $\bar{U}$ of U which is again maximum scattered w.r.t. hyperplanes; see [10, Remark 4.11].

In Section 2 we collect existing constructions and present some new ones to obtain large $(h, k)_q$-evasive subspaces. In particular we study the direct sum of an $(h_1, k_1)_q$-evasive and an $(h_2, k_2)_q$-evasive subspace under various conditions. In Section 3 we investigate the "ordinary" duality (induced by a non-degenerate reflexive sesquilinear form) and Delsarte duality on evasive subspaces. In Section 4 we present (in some cases sharp) upper bounds on the size of maximum evasive subspaces. In this direction the first open problem is to determine the size of a maximum scattered (i.e. $(1, 1)_q$-evasive) subspace in $V(3, q^5)$. From the Blokhuis–Lavrauw bound it follows that scattered subspaces of $V(3, q^5)$ have dimension at most $\lfloor (3 \cdot 5)/2 \rfloor = 7$. In Section 5 we present scattered subspaces with this dimension for infinite many values of q. We obtain these examples in characteristics 2, 3 and 5. Note that these are the first non-trivial examples (i.e. $n > 3$) for scattered subspaces of dimension $\lfloor rn/2 \rfloor$ in $V(r, q^n)$ when rn is odd. To obtain these examples we use MAGMA and combine q-subresultants [8] with the strategy of Ball, Blokhuis and Lavrauw from [3] where the authors construct maximum scattered subspaces of dimension 6 in $V(3, q^4)$. Thanks to the dualities described in Section 3, our examples yield maximum evasive subspaces for many other parameters as well.

2 General properties and existence results

In this section we prove basic properties of evasive subspaces and present some construction methods. Some of these results are inductive and depend on already existing constructions as an input. We start by presenting the simplest construction of scattered subspaces w.r.t. hyperplanes. They correspond to MRD-codes known as Gabidulin codes, see [25, Section 3.2].

Example 2.1. *If $n \geq r$, then the n-dimensional $\mathbb{F}_q$-subspace*

$$\{(x, x^q, \ldots, x^{q^{r-1}}) : x \in \mathbb{F}_{q^n}\}$$

is maximum $(r-1, r-1)_q$-evasive in $\mathbb{F}_{q^n}^r$.

The following example defines subgeometries $\mathrm{PG}(r, q^m)$ in $\mathrm{PG}(r, q^n)$.

Example 2.2. *If $m \mid n$ then the mr-dimensional $\mathbb{F}_q$-subspace*

$$\{(x_1, x_2, \ldots, x_r) : x_i \in \mathbb{F}_{q^m}\}$$

is $(h, mh)_q$-evasive in $\mathbb{F}_{q^n}^r$ for each h.

Next we collect what is known about maximum $(h, h)_q$-evasive subspaces.

Result 2.3. *1. If $h + 1 \mid r$ and $n \geq h + 1$, then maximum $(h, h)_q$-evasive subspaces of $V(r, q^n)$ have dimension $rn/(h+1)$, cf. [10, Theorem 2.7];*

2. if rn is even, then maximum $(1, 1)_q$-evasive subspaces of $V(r, q^n)$ have dimension $rn/2$, cf. [3, 5, 6, 9];

3. if rn is even, then maximum $(n-3, n-3)_q$-evasive subspaces of $V(r(n-2)/2, q^n)$ have dimension $rn/2$, cf. [10, Corollary 3.5];

4. in $V(r, q^n)$ the h-scattered subspaces of dimension $rn/(h+1)$ are $(r-1, rn/(h+1) - n + h)_q$-evasive, cf. [6] for $h = 1$ and [10] for $h > 1$.

Next recall Examples 2.4 and 2.5 of Guruswami [14, Section B] which are special (linear) cases of the construction of Dvir and Lovett [12, Theorem 3.2]. Suppose $n \geq r$ and take distinct elements $\gamma_1, \gamma_2, \ldots, \gamma_r \in \mathbb{F}_{q^n}^*$. For $1 \leq i \leq h$ define

$$f_i(x_1, x_2, \ldots, x_r) = \sum_{j=1}^{r} \gamma_j^i x_j^{q^{r-j}}.$$

Example 2.4. *The $\mathbb{F}_q$-subspace*

$$V_{\mathbb{F}_{q^n}}(f_1, f_2, \ldots, f_h) := \{(x_1, x_2, \ldots, x_r) : f_i(x_1, x_2, \ldots, x_r) = 0 \text{ for } i = 1, \ldots, h\}$$

is $(k, (r-1)k)_q$-evasive of dimension $n(r-h)$ for every $1 \leq k \leq h < r$ in $\mathbb{F}_{q^n}^r$. The fact that $\langle V_{\mathbb{F}_{q^n}}(f_1, f_2, \ldots, f_h) \rangle_{\mathbb{F}_{q^n}} = \mathbb{F}_{q^n}^r$ is left as an exercise. Note that when $r = 2$ (and hence $h = k = 1$) then $V_{\mathbb{F}_{q^n}}(f_1)$ is equivalent to Example 2.1.

Example 2.5. *The direct sum of s copies of $V_{\mathbb{F}_{q^n}}(f_1, f_2, \ldots, f_h)$ in $\mathbb{F}_{q^n}^r \oplus \ldots \oplus \mathbb{F}_{q^n}^r \cong V(rs, q^n)$ is a $(k, (r-1)k)_q$-evasive subspace of dimension $sn(r-h)$ for every $1 \leq k \leq h < r$.*

Thus for every divisor m of r', in $V(r', q^n)$ there exist $(k, (m-1)k)_q$-evasive subspaces of dimension $nr' - hnr'/m$ for every $1 \leq k \leq h < m$.

Note that when $m = 2$ (and hence $h = k = 1$) we obtain maximum scattered subspaces of $V(r, q^n)$, r even, which are direct sum of the maximum scattered subspaces of $V(2, q^n)$ arising from Example 2.1. It is equivalent to the construction of Lavrauw [17, pg. 26].

Proposition 2.6. *If U is a $(h, k)_q$-evasive subspace in $V(r, q^n)$, then it is also $(h-s, k-s)_q$-evasive.*

Proof. It is enough to prove the result for $s = 1$ and then apply induction. Suppose for the contrary that there exists an $(h-1)$-dimensional $\mathbb{F}_{q^n}$-subspace H meeting U in at least q^k vectors. Since $\langle U \rangle_{\mathbb{F}_{q^n}}$ is not contained in H, there exists $\mathbf{u} \in U \setminus H$ and hence $\langle \mathbf{u}, H \rangle_{q^n}$ meets U in at least q^{k+1} vectors, a contradiction. $\square$

Proposition 2.7. *If there exists an $(h, k)_q$-evasive subspace U of dimension t in $V(r, q^n)$, then there also exists an $(h, k+s)_q$-evasive subspace of dimension $t+s$ for each $0 \le s \le rn-t$.*

Proof. Take $\mathbf{w} \notin U$. The $\mathbb{F}_q$-subspace $\langle U, \mathbf{w} \rangle_{\mathbb{F}_q}$ is $(h, k+1)_q$-evasive of dimension $t+1$. Indeed, suppose for the contrary that there exist $\mathbf{u_i} \in U$ such that

$$\mathbf{w} + \mathbf{u_1}, \mathbf{w} + \mathbf{u_2}, \ldots, \mathbf{w} + \mathbf{u_{k+2}},$$

are $\mathbb{F}_q$-linearly independent elements contained in the same h-dimensional $\mathbb{F}_{q^n}$-subspace H of V. Then $\mathbf{u_1} - \mathbf{u_{k+2}}, \mathbf{u_2} - \mathbf{u_{k+2}}, \ldots, \mathbf{u_{k+1}} - \mathbf{u_{k+2}}$ are $k+1$ $\mathbb{F}_q$-linearly independent elements of U in H, contradicting the fact that U is $(h, k)_q$-evasive. The result follows by induction. $\square$

In Proposition 2.7, starting from an evasive subspace of $V(r, q^n)$, we construct another evasive subspace in the same vector space. In the next result we construct an evasive subspace by enlarging an evasive subspace lying in a hyperplane of $V(r, q^n)$.

Proposition 2.8. *If there exists an $(r-1, k)_q$-evasive subspace of dimension d in $V(r, q^n)$, then for a positive integer s with $d-k \le s \le n$ in $V(r+1, q^n)$ there exists an $(r, k+s)_q$-evasive subspace of dimension $d + s$.*

Proof. Let W be an $(r-1, k)_q$-evasive subspace of dimension d in $V(r, q^n)$. Embed $V(r, q^n)$ as a hyperplane of $V(r+1, q^n)$ and take a vector $\mathbf{v} \notin V(r, q^n)$. Let W' be an $\mathbb{F}_q$-subspace of $\langle \mathbf{v} \rangle_{q^n}$ of dimension s. The $\mathbb{F}_q$-subspace $W \oplus W'$ of $V(r+1, q^n)$ will be sufficient for our purposes. $\square$

Theorem 2.9. *If U_i is an $(h, k_i)_q$-evasive subspace of $V_i = V(r_i, q^n)$ for $i = 1, 2$, then $U = U_1 \oplus U_2$ is $(h, k_1 + k_2 - h)_q$-evasive in $V = V_1 \oplus V_2$.*

Proof. Recall that $k_i \ge h$, for $i = 1, 2$, as we explained after Definition 1.1. By way of contradiction suppose that there exists an h-dimensional $\mathbb{F}_{q^n}$-subspace W of V such that

$$\dim_q(W \cap U) \ge k_1 + k_2 - h + 1. \tag{1}$$

Clearly, W cannot be contained in V_i since U_i is $(h, k_i)_q$-evasive in V_i and $k_1 + k_2 - h + 1$ is larger than both k_1 and k_2. Let $W_1 := W \cap V_1$ and $s := \dim_{q^n} W_1$. Then $s < h$ and by Proposition 2.6, the $\mathbb{F}_q$-subspace U_1 is $(s, k_1 - h + s)_q$-evasive in V_1, thus

$$\dim_q(U_1 \cap W_1) \le k_1 - h + s. \tag{2}$$

Denoting $\langle U_1, W \cap U \rangle_{\mathbb{F}_q}$ by $\bar{U}_1$, the Grassmann formula yields

$$\dim_q \bar{U}_1 - \dim_q U_1 = \dim_q(W \cap U) - \dim_q(W \cap U_1)$$

6

and hence by (1) and (2)

$$\dim_q \bar{U}_1 - \dim_q U_1 \geq (k_1 + k_2 - h + 1) - (k_1 - h + s) = k_2 + 1 - s. \tag{3}$$

Consider the subspace $T := W + V_1$ of the quotient space $V/V_1 \cong V_2$. Then $\dim_{q^n} T = h - s$ and T contains the $\mathbb{F}_q$-subspace $M := \bar{U}_1 + V_1$. Since M is also contained in the $\mathbb{F}_q$-subspace $U + V_1 = U_2 + V_1$ of V/V_1, then M is $(h, k_2)_q$-evasive in V/V_1 and hence also $(h - s, k_2 - s)_q$-evasive. Hence $\dim_q(M \cap T) \leq k_2 - s$.

On the other hand,

$$\dim_q(M \cap T) = \dim_q M = \dim_q \bar{U}_1 - \dim_q(\bar{U}_1 \cap V_1) \geq$$

$$\dim_q \bar{U}_1 - \dim_q(U \cap V_1) = \dim_q \bar{U}_1 - \dim_q U_1,$$

and hence, by (3),

$$k_2 - s \geq \dim_q(M \cap T) \geq k_2 + 1 - s;$$

a contradiction. $\qquad\square$

Note that Example 2.5 is obtained from Example 2.4 by considering direct sum of $(h, (r - 1)h)_q$-evasive subspaces so that their sum is evasive with the same parameters. By Theorem 2.9 we would get only an $(h, (r - 1)h + (r - 2)h)_q$-evasive subspace. The reason behind this is the additional property of Example 2.4, i.e. the fact that it is $(k, (r - 1)k)_q$-evasive for each $1 \leq k \leq h$. Assuming a similar hypothesis, and copying either the proof of Theorem 2.9 or the proof of [12, Claim 3.4] one can prove the following.

Theorem 2.10. *If U_i is a $(t, \lambda t)_q$-evasive subspace of $V_i = V(r_i, q^n)$ with $i = 1, 2$ for each $1 \leq t \leq h$ and for some positive integer λ, then $U = U_1 \oplus U_2$ is $(t, \lambda t)_q$-evasive in $V = V_1 \oplus V_2$ for each $1 \leq t \leq h$.*

With $V = 1$ then the result above states that the direct sum of two t-scattered subspaces is again t-scattered, see [10, Theorem 2.5]. When $h = 1$ then Theorem 2.10 is just a special case of the following result, which also improves on Theorem 2.9.

Theorem 2.11. *If U_i is a $(1, k_i)_q$-evasive subspace of $V_i = V(r_i, q^n)$ for $i = 1, 2$, then $U = U_1 \oplus U_2$ is a $(1, \max\{k_1, k_2\})_q$-evasive subspace of $V = V_1 \oplus V_2$.*

Proof. W.l.o.g. assume $k_2 \geq k_1$ and put $\dim_q U_i = d_i$ for $i = 1, 2$. Suppose for the contrary that in V there exists a one-dimensional $\mathbb{F}_{q^n}$-subspace X such that $\dim_q(U \cap X) \geq k_2 + 1$. Clearly, $X \notin V_1 \cup V_2$. Consider the $(r_1 + 1)$-dimensional $\mathbb{F}_{q^n}$-subspace $T := \langle V_1, X \rangle_{\mathbb{F}_{q^n}}$. Then $Y := T \cap V_2$ is a one-dimensional $\mathbb{F}_{q^n}$-subspace. Now consider the $\mathbb{F}_q$-subspace $T' := \langle U_1, X \cap U \rangle_{\mathbb{F}_q}$. By our assumption on X, $\dim_q T' \geq d_1 + k_2 + 1$. Then

$$\dim_q \langle T', U_2 \rangle + \dim_q(T' \cap U_2) = \dim_q T' + \dim_q U_2.$$

Since $\langle T', U_2 \rangle_{\mathbb{F}_q} = U$, this yields $\dim_q(T' \cap U_2) \geq k_2 + 1$. Also, from $T \geq T'$ and $V_2 \geq U_2$, we have $Y = T \cap V_2 \geq T' \cap U_2$ and hence the one-dimensional $\mathbb{F}_{q^n}$-subspace Y meets U_2 in an $\mathbb{F}_q$-subspace of dimension at least $k_2 + 1$, a contradiction. $\qquad\square$

3 Dualities on evasive subspaces

3.1 "Ordinary" dual of evasive subspaces

Let $\sigma : V \times V \longrightarrow \mathbb{F}_{q^n}$ be a non-degenerate reflexive sesquilinear form on $V = V(r, q^n)$ and define

$$\sigma' : (\mathbf{u}, \mathbf{v}) \in V \times V \to \mathrm{Tr}_{q^n/q}(\sigma(\mathbf{u}, \mathbf{v})) \in \mathbb{F}_q, \tag{4}$$

where $\mathrm{Tr}_{q^n/q}$ denotes the trace function of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then σ' is a non-degenerate reflexive sesquilinear form on V, when V is regarded as an rn-dimensional vector space over $\mathbb{F}_q$. Let τ and τ' be the orthogonal complement maps defined by σ and σ' on the lattices of the $\mathbb{F}_{q^n}$-subspaces and $\mathbb{F}_q$-subspaces of V, respectively. Recall that if R is an $\mathbb{F}_{q^n}$-subspace of V and U is an $\mathbb{F}_q$-subspace of V then $U^{\tau'}$ is an $\mathbb{F}_q$-subspace of V, $\dim_{q^n} R^\tau + \dim_{q^n} R = r$ and $\dim_q U^{\tau'} + \dim_q U = rn$. It easy to see that $R^\tau = R^{\tau'}$ for each $\mathbb{F}_{q^n}$-subspace R of V (for more details see [28, Chapter 7]).

Also, $U^{\tau'}$ is called the *dual* of U (w.r.t. τ'). Up to $\Gamma\mathrm{L}(r, q^n)$-equivalence, the dual of an $\mathbb{F}_q$-subspace of V does not depend on the choice of the non-degenerate reflexive sesquilinear forms σ and σ' on V. For more details see [22]. If R is an s-dimensional $\mathbb{F}_{q^n}$-subspace of V and U is a t-dimensional $\mathbb{F}_q$-subspace of V, then

$$\dim_q(U^{\tau'} \cap R^\tau) - \dim_q(U \cap R) = rn - t - sn. \tag{5}$$

From the previous equation the next result immediately follows.

Proposition 3.1. *Let U be a t-dimensional $(h, k)_q$-evasive subspace in $V = V(r, q^n)$, with $k < hn$. Then $U^{\tau'}$ is an $(rn - t)$-dimensional $(r - h, (r - h)n + k - t)_q$-evasive subspace in V.*

Proof. From (5) it follows that the $(r - h)$-dimensional $\mathbb{F}_{q^n}$-subspaces meet $U^{\tau'}$ in subspaces of dimension at most $(r - h)n + k - t$. The only thing to prove is the fact that $\langle U^{\tau'} \rangle_{\mathbb{F}_{q^n}}$ has dimension at least $r - h$. If this was not true then one could find an $(r - h - 1)$-dimensional $\mathbb{F}_{q^n}$-subspace containing $U^{\tau'}$ and hence also an $(r - h)$-dimensional $\mathbb{F}_{q^n}$-subspace containing $U^{\tau'}$. Such a subspace would meet $U^{\tau'}$ in an $\mathbb{F}_q$-subspace of dimension $rn - t$ which is larger than $(r - h)n + k - t$, a contradiction. $\qquad\square$

Note that in Proposition 3.1 the condition $k < hn$ is not very restrictive since with $k \geq hn$ each $\mathbb{F}_q$-subspace of V is $(h, k)_q$-evasive.

Corollary 3.2. *Let U be a t-dimensional (h, q^h)-evasive subspace in $V = V(r, q^n)$ with $t > h$. If $\dim_{q^n} \langle U^{\tau'} \rangle_{\mathbb{F}_{q^n}} \geq r - h$, then $U^{\tau'}$ is maximum $(r - h, (r - h)n + h - t)_q$-evasive with dimension $rn - t$.*

Proof. Suppose for the contrary that there exists an $(rn - t + 1)$-dimensional $(r - h, (r - h)n + h - t)_q$-evasive subspace W in V. Then $\dim_q W^{\tau'} = t - 1$ and $W^{\tau'}$ meets the h-dimensional $\mathbb{F}_{q^n}$-subspaces of V in $\mathbb{F}_q$-subspaces of dimension at most $h - 1$. Thus $\dim_q W^{\tau'} \leq h - 1$. It means that $t \leq h$, a contradiction. $\qquad\square$

3.2 Delsarte dual of evasive subspaces

In this section we follow [10, Section 3]. Let U be a t-dimensional $\mathbb{F}_q$-subspace of a vector space $V = V(r, q^n)$, with $t > r$. By [21, Theorems 1, 2] (see also [20, Theorem 1]), there is an embedding of V in $\mathbb{V} = V(t, q^n)$ with $\mathbb{V} = V \oplus \Gamma$ for some $(t-r)$-dimensional $\mathbb{F}_{q^n}$-subspace Γ such that $U = \langle W, \Gamma \rangle_{\mathbb{F}_q} \cap V$, where W is a t-dimensional $\mathbb{F}_q$-subspace of $\mathbb{V}$, $\langle W \rangle_{\mathbb{F}_{q^n}} = \mathbb{V}$ and $W \cap \Gamma = \{\mathbf{0}\}$. Then the quotient space $\mathbb{V}/\Gamma$ is isomorphic to V and under this isomorphism U is the image of the $\mathbb{F}_q$-subspace $W + \Gamma$ of $\mathbb{V}/\Gamma$.

Now, let $\beta' \colon W \times W \to \mathbb{F}_q$ be a non-degenerate reflexive sesquilinear form on W. Then β' can be extended to a non-degenerate reflexive sesquilinear form $\beta \colon \mathbb{V} \times \mathbb{V} \to \mathbb{F}_{q^n}$. Let $\perp$ and $\perp'$ be the orthogonal complement maps defined by β and β' on the lattice of $\mathbb{F}_{q^n}$-subspaces of $\mathbb{V}$ and of $\mathbb{F}_q$-subspaces of W, respectively. For an $\mathbb{F}_q$-subspace S of W the $\mathbb{F}_{q^n}$-subspace $\langle S \rangle_{\mathbb{F}_{q^n}}$ of $\mathbb{V}$ will be denoted by S^*. In this case $(S^*)^\perp = (S^{\perp'})^*$.

The next result and definition come from [10, Proposition 3.1 and Definition 3.2].

Proposition 3.3. *Let W, V, Γ, $\mathbb{V}$, $\perp$ and $\perp'$ be defined as above. If U is a t-dimensional $(h, t-r+h-1)_q$-evasive subspace of V with $t > r$, then $W + \Gamma^\perp$ is a subspace of $\mathbb{V}/\Gamma^\perp$ of dimension at least $(t-r+h+1)$ (and at most t) over $\mathbb{F}_q$. If h is maximal with this property then $W + \Gamma^\perp$ has dimension exactly $t - r + h + 1$.*

Proof. As described above, U turns out to be isomorphic to the $\mathbb{F}_q$-subspace $W + \Gamma$ of the quotient space $\mathbb{V}/\Gamma$. Also, an h-dimensional $\mathbb{F}_{q^n}$-subspace of $\mathbb{V}/\Gamma$ corresponds to a $(t-r+h)$-dimensional $\mathbb{F}_{q^n}$-subspace of $\mathbb{V}$ containing Γ. Hence, $\dim_q(H \cap W) \leq t - r + h - 1$ for each $(t-r+h)$-dimensional subspace H of $\mathbb{V}$ containing Γ. Next we prove that the dimension of $W \cap \Gamma^\perp$ is at most $r - h - 1$. Indeed, by way of contradiction, suppose that there exists an $\mathbb{F}_q$-subspace S of dimension $r - h$ in $W \cap \Gamma^\perp$. Then the $(t-r+h)$-dimensional $\mathbb{F}_{q^n}$-subspace $(S^*)^\perp$ of $\mathbb{V}$ contains the subspace Γ and meets W in the $(t-r+h)$-dimensional $\mathbb{F}_q$-subspace $S^{\perp'}$, a contradiction. It follows that the dimension of $W + \Gamma^\perp$ is at least $t - (r - h - 1)$.

Finally, if h is maximal with the property of the statement, then there exists an $(h+1)$-dimensional $\mathbb{F}_{q^n}$-subspace M of V meeting U in an $\mathbb{F}_q$-subspace of dimension at least $t - r + h + 1$. Then M corresponds to a $(t-r+h+1)$-dimensional subspace H of $\mathbb{V}$ containing Γ such that $\dim_q(H \cap W) \geq t - r + h + 1$. Then $H^\perp$ is an $(r-h-1)$-dimensional subspace contained in $\Gamma^\perp$ and intersecting W in the $(r-h-1)$-dimensional $\mathbb{F}_q$-subspace $(H \cap W)^{\perp'}$. It follows that the dimension of $W \cap \Gamma^\perp$ is at least $r - h - 1$ and hence the dimension of $W + \Gamma^\perp$ is at most $t - (r - h - 1)$. Combining with the lower bound on the dimension of $W + \Gamma^\perp$ the result follows. $\square$

Definition 3.4. Let U be a t-dimensional $\mathbb{F}_q$-subspace of $V = V(r, q^n)$. Then the $\mathbb{F}_q$-subspace $W + \Gamma^\perp$ of the quotient space $\mathbb{V}/\Gamma^\perp = V(t - r, q^n)$ will be denoted by $\bar{U}$ and it is the *Delsarte dual* of U (w.r.t. $\perp$).

Arguing as in [10, Remark 3.7] one can show that up to $\Gamma\mathrm{L}(t - r, q^n)$-equivalence, the Delsarte dual of an $\mathbb{F}_q$-subspace of V does not depend on the choice of the non-degenerate reflexive sesquilinear forms β' and β on W and $\mathbb{V}$, respectively.

One can adapt the proof of [10, Theorem 3.3] and give the following generalization.

Theorem 3.5. *Let U be a t-dimensional $(h,k)_q$-evasive subspace of a vector space $V = V(r, q^n)$ with $r < t$, $k < t - r + h - 1$. Then the $(t - r + h - k - 1)$-dimensional $\mathbb{F}_{q^n}$-subspaces meet $\bar{U}$ in $\mathbb{F}_q$-subspaces of dimension at most $t - k - 2$. In particular, if $\langle \bar{U} \rangle_{\mathbb{F}_{q^n}}$ has dimension at least $t - r + h - k - 1$ then $\bar{U}$ is a $(t - r + h - k - 1, t - k - 2)_q$-evasive subspace of dimension at least $t - r + h + 1$ in $\mathbb{V}/\Gamma^\perp = V(t - r, q^n)$.*

Proof. By Proposition 3.3, $\bar{U} = W + \Gamma^\perp$ has dimension at least $t - r + h + 1$ in $\mathbb{V}/\Gamma^\perp$. By way of contradiction, suppose that there exists a $(t - r + h - k - 1)$-dimensional $\mathbb{F}_{q^n}$-subspace of $\mathbb{V}/\Gamma^\perp$, say M, such that

$$\dim_q(M \cap \bar{U}) \geq t - k - 1. \tag{6}$$

Then $M = H + \Gamma^\perp$, for some $(t + h - k - 1)$-dimensional $\mathbb{F}_{q^n}$-subspace H of $\mathbb{V}$ containing $\Gamma^\perp$. For H, by (6), it follows that $\dim_q(H \cap W) = \dim_q(M \cap \bar{U}) \geq t - k - 1$.

Let S be an $(t - k - 1)$-dimensional $\mathbb{F}_q$-subspace of W contained in H and let $S^* := \langle S \rangle_{\mathbb{F}_{q^n}}$. Then, $\dim_{q^n} S^* = t - k - 1$,

$$S^{\perp'} = W \cap (S^*)^\perp \quad \text{and} \quad S^{\perp'} \subset (S^*)^\perp = \langle S^{\perp'} \rangle_{\mathbb{F}_{q^n}}. \tag{7}$$

Since $S \subseteq H \cap W$ and $\Gamma^\perp \subset H$, we get $S^* \subset H$ and $H^\perp \subset \Gamma$, i.e.

$$H^\perp \subseteq \Gamma \cap (S^*)^\perp. \tag{8}$$

From (8) it follows that $\dim_{q^n} \left(\Gamma \cap (S^*)^\perp \right) \geq \dim_{q^n} H^\perp = k - h + 1$. This implies that

$$\dim_{q^n} \langle \Gamma, (S^*)^\perp \rangle_{q^n} = \dim_{q^n} \Gamma + \dim_{q^n} (S^*)^\perp - \dim_{q^n} \left(\Gamma \cap (S^*)^\perp \right) \leq t - r + h$$

and hence $\langle \Gamma, (S^*)^\perp \rangle_{\mathbb{F}_{q^n}}$ is contained in a $(t - r + h)$-dimensional T space of $\mathbb{V}$ containing Γ. Also, $\dim_q(S^{\perp'}) = \dim_q W - \dim_q S = k + 1$ and, by (7), we get

$$S^{\perp'} = W \cap (S^*)^\perp \subseteq W \cap T.$$

Then $\hat{T} := T \cap V$ is an h-dimensional subspace of V and, by recalling $U = \langle W, \Gamma \rangle_{\mathbb{F}_q} \cap V$,

$$\dim_q(\hat{T} \cap U) = \dim_q(T \cap W) \geq \dim_q(S^{\perp'}) = k + 1,$$

contradicting the fact that U is $(h, k)_q$-evasive. $\qquad \square$

Remark 3.6. *Note that $\langle \bar{U} \rangle_{\mathbb{F}_{q^n}}$ has dimension at least $t - r + h - k - 1$ whenever $\dim_q \bar{U} > t - k - 2$, which clearly holds when $k + h + 3 > r$.*

4   On the size of maximum evasive subspaces

In this section we determine upper bounds on the dimension of maximum evasive subspaces and in some cases we show the sharpness of our results.

We will need the following Singleton-like bound of Delsarte which can be proved easily by the pigeonhole principle.

Result 4.1. *Let $\mathcal{C}$ be an additive subset of $\mathrm{Hom}_{\mathbb{F}_q}(U, V)$ where $\dim_q U = m$ and $\dim_q V = n$ such that non-zero maps of $\mathcal{C}$ have rank at least δ. Then $|\mathcal{C}| \leq q^{\min\{m,n\}(\max\{m,n\} - \delta + 1)}$.*

Theorem 4.2. *Let U be an $(r-1, k)_q$-evasive subspace of $V = V(r, q^n)$.*

    1. If $k < (r-1)n$ then $\dim_q U \le n + k - 1$.

    2. If $k < r - 2 + n/(r-1)$ then $\dim_q U \le n + k - r + 1$.

Proof. By definition, $\dim_{q^n}\langle U\rangle_{q^n} \ge r - 1$. First assume $\dim_{q^n}\langle U\rangle_{q^n} = r - 1$. Then $\dim_q U \le k \le n + k - 1$ proving the first part. Since $k \ge r - 1$, the condition of the second part implies $n > r - 1$ and hence $\dim_q U \le k < n + k - r + 1$ proving the second part.

Thus from now on we assume $\dim_{q^n}\langle U\rangle_{q^n} = r$. Fix an $\mathbb{F}_{q^n}$-basis in V and for $\mathbf{x} \in V$ denote the i-th coordinate w.r.t. this basis by x_i. For $\mathbf{a} = (a_0, \ldots, a_{r-1}) \in \mathbb{F}_{q^n}^r$ define the $\mathbb{F}_q$-linear map $G_{\mathbf{a}} \colon \mathbf{x} \in U \mapsto \sum_{i=0}^{r-1} a_i x_i \in \mathbb{F}_{q^n}$ and put $\mathcal{C}_U := \{G_{\mathbf{a}} : \mathbf{a} \in \mathbb{F}_{q^n}^r\}$.

Let d denote the dimension of U over $\mathbb{F}_q$. First we show that the non-zero maps of $\mathcal{C}_U$ have rank at least $d - k$. Indeed, if $\mathbf{a} \ne \mathbf{0}$, then $\mathbf{u} \in \ker G_{\mathbf{a}}$ if and only if $\sum_{i=0}^{r-1} a_i u_i = 0$, i.e. $\ker G_{\mathbf{a}} = U \cap H$, where H is the hyperplane $[a_0, a_1, \ldots, a_{r-1}]$ of V. Since U is $(r-1, k)_q$-evasive, it follows that $\dim \ker G_{\mathbf{a}} \le k$ and hence the rank of $G_{\mathbf{a}}$ is at least $d - k$. Next we show that any two maps of $\mathcal{C}_U$ are different. Suppose for the contrary $G_{\mathbf{a}} = G_{\mathbf{b}}$, then $G_{\mathbf{a}-\mathbf{b}}$ is the zero map. If $\mathbf{a} - \mathbf{b} \ne \mathbf{0}$, then U would be contained in the hyperplane $[a_0 - b_0, a_1 - b_1, \ldots, a_{r-1} - b_{r-1}]$, a contradiction since $\langle U\rangle_{\mathbb{F}_{q^n}} = V$. Hence, $|\mathcal{C}_U| = q^{nr}$.

The elements of $\mathcal{C}_U$ form an nr-dimensional $\mathbb{F}_q$-subspace of $\mathrm{Hom}_{\mathbb{F}_q}(U, \mathbb{F}_{q^n})$ and the non-zero maps of $\mathcal{C}_U$ have rank at least $d - k$. By Result 4.1 we get $|\mathcal{C}_U| = q^{rn} \le q^{d(n-d+k+1)}$ and hence

$$rn \le d(n - d + k + 1). \tag{9}$$

To prove the first part, suppose for the contrary $d \ge n + k$. Substituting in (9) gives $rn \le n + k$ and hence $(r-1)n \le k$, contradicting our assumption.

To prove the second part, suppose for the contrary $d \ge n + k - r + 2$. By (9) we get $rn \le rn + kr - r^2 + 2r - n - k + r - 2$ and hence $r - 2 + n/(r-1) \le k$, a contradiction. $\square$

Motivated by the proof of [24, Lemma 1], we present another bound which also implies the first bound in Theorem 4.2.

Theorem 4.3. *Let U be an $(h, k)_q$-evasive subspace of $V = V(r, q^n)$. Then*

$$|U| \le \frac{(q^k - 1)(q^{rn} - 1)}{q^{hn} - 1} + 1.$$

Proof. First note that the number of h-dimensional $\mathbb{F}_{q^n}$-subspaces of V is the Gaussian binomial coefficient

$$\binom{r}{h}_{q^n} = \frac{(q^{rn} - 1)(q^{rn} - q^n) \ldots (q^{rn} - q^{(h-1)n})}{(q^{hn} - 1)(q^{hn} - q^n) \ldots (q^{hn} - q^{(h-1)n})}.$$

The number of h-dimensional $\mathbb{F}_{q^n}$-subspaces of V containing a fixed non-zero vector $\mathbf{x}$ is

$$\binom{r}{h}_{q^n} \frac{q^{hn} - 1}{q^{rn} - 1}.$$

Consider the pairs $(\mathbf{x}, H)$, where H is an h-dimensional subspace of V and $\mathbf{x}$ is a vector of H. Then $\mathbf{0}$ is contained in every h-dimensional $\mathbb{F}_{q^n}$-subspace and hence double counting the pairs above yields

$$\binom{r}{h}_{q^n} + (|U| - 1)\binom{r}{h}_{q^n} \frac{q^{hn} - 1}{q^{rn} - 1} \leq q^k \binom{r}{h}_{q^n},$$

and the assertion follows. $\qquad\square$

Corollary 4.4 (First bound in Theorem 4.2). *Let U be $(r-1, k)_q$-evasive with $k < (r-1)n$. Then $\dim_q U \leq n + k - 1$.*

Proof. In Theorem 4.3 put $h = r - 1$. Then

$$|U| \leq \frac{(q^k - 1)(q^{rn} - 1)}{q^{rn-n} - 1} + 1$$

follows. Since $|U|$ is a q-power, to prove our assertion, it is enough to show

$$\frac{(q^k - 1)(q^{rn} - 1)}{q^{rn-n} - 1} + 1 < q^{n+k}.$$

After rearranging, this is equivalent to

$$q^{-n}\left(q^n - 1\right)\left(q^{nr} - q^{k+n}\right) > 0,$$

which clearly holds since $k < (r-1)n$. $\qquad\square$

In the next result we show that the second bound of Theorem 4.2 is sharp.

Proposition 4.5. *If $k < r - 2 + \frac{n}{r-1}$ then in $V(r, q^n)$ there exist maximum $(r-1, k)_q$-evasive subspaces of dimension $n + k - r + 1$.*

Proof. From the assumption on k, we get $k \leq n + r - 1$. Let W be an n-dimensional $(r-1, r-1)_q$-evasive subspace of $V(r, q^n)$, cf. Example 2.1 (note that $n \geq r$ follows from $k \geq r - 1$) and W' be an $\mathbb{F}_q$-subspace of dimension $k - r + 1$ contained in a 1-dimensional $\mathbb{F}_{q^n}$-subspace $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}}$ of $V(r, q^n)$, with $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} \cap W = \{\mathbf{0}\}$. Then the direct sum $W \oplus W'$ is an $(r-1, k)_q$-evasive subspace of dimension $n + k - r + 1$. $\qquad\square$

In the next result we show that the first bound of Theorem 4.2 is sharp when $k \geq (r-2)(n-1) + 1$.

Proposition 4.6. *If $k \geq (r-2)(n-1) + 1$, then in $V(r, q^n)$ there exist $(r-1, k)_q$-evasive subspaces of dimension $n + k - 1$.*

Proof. If $r = 2$ and $k = n$ then $V(2, q^n)$ is $(1, n)_q$-evasive of dimension $2n$. If $r = 2$ and $k < n$ then the result follows from Proposition 4.5. From now on assume $r > 2$. By Proposition 2.8 with $d = n$ and $s = n - 1$, starting from a maximum $(1, 1)_q$-evasive subspace in $V(2, q^n)$, we get a $(2, n)_q$-evasive subspace of dimension $2n - 1$ in $V(3, q^n)$. Continuing with this process it is possible to construct an $(r-1, (r-2)(n-1)+1)_q$-evasive subspace in $V(r, q^n)$ of dimension $(r-1)(n-1)+1$. By Proposition 2.7 the result follows for $k > (r-2)(n-1)+1$ as well. $\qquad\square$

When rn is even then we can prove the sharpness of the first bound of Theorem 4.2 also for smaller values of k.

Proposition 4.7. *If there exists a t-dimensional scattered subspace in $V(r, q^n)$ then there exists an $(r-1, (r-1)n+1-t)_q$-evasive subspace of dimension $(rn-t)$. In particular, if rn is even and $k \geq rn/2 - n + 1$ then there exist $(r-1, k)_q$-evasive subspaces of dimension $n + k - 1$.*

Proof. The first part follows from Proposition 3.1. The second part follows from the fact that when rn is even then there exist scattered subspaces of dimension $rn/2$, cf. Result 2.3, and from Proposition 2.7. □

The first case when we do not know the sharpness of Theorem 4.2 is when $r = 3$, $n = 5$ and $k = 4$. In this case our bound states that the dimension of an $(2, q^4)$-scattered subspace is at most 8. The existence of such subspaces will follow from the results of Section 5 and Proposition 4.7 for infinitely many values of q.

To prove the next result, we follow some of the ideas of the proof of [10, Theorem 2.3].

Theorem 4.8. *Suppose that there exists a d_2-dimensional $(h_1 - 1, k_2)_q$-evasive subspace W in $V(h_1, q^n)$. Let U be a d_1-dimensional $(h_1, k_1)_q$-evasive subspace of $V = V(r, q^n)$ with $d_2 + h_1 - k_2 - 1 > k_1$. Then*

$$d_1 \leq rn - \frac{rnh_1}{d_2}. \tag{10}$$

Proof. Take W in $\mathbb{F}_{q^n}^{h_1} = V(h_1, q^n)$, as in the assertion. Let G be an $\mathbb{F}_q$-linear transformation of V with $\ker G = U$. Clearly, $\dim_q \operatorname{Im} G = rn - d_1$. For each $(\mathbf{u}_1, \ldots, \mathbf{u}_{h_1}) \in V^{h_1}$ consider the $\mathbb{F}_{q^n}$-linear map

$$\tau_{\mathbf{u}_1, \ldots, \mathbf{u}_{h_1}} : (\lambda_1, \ldots, \lambda_{h_1}) \in W \mapsto \lambda_1 \mathbf{u}_1 + \ldots + \lambda_{h_1} \mathbf{u}_{h_1} \in V.$$

Consider the following set of $\mathbb{F}_q$-linear maps

$$\mathcal{C} := \{G \circ \tau_{\mathbf{u}_1, \ldots, \mathbf{u}_{h_1}} : (\mathbf{u}_1, \ldots, \mathbf{u}_{h_1}) \in V^{h_1}\}.$$

Our aim is to show that these maps are pairwise distinct and hence $|\mathcal{C}| = q^{rnh_1}$. Suppose $G \circ \tau_{\mathbf{u}_1, \ldots, \mathbf{u}_{h_1}} = G \circ \tau_{\mathbf{v}_1, \ldots, \mathbf{v}_{h_1}}$. It follows that $G \circ \tau_{\mathbf{u}_1 - \mathbf{v}_1, \ldots, \mathbf{u}_{h_1} - \mathbf{v}_{h_1}}$ is the zero map, i.e.

$$\lambda_1(\mathbf{u}_1 - \mathbf{v}_1) + \ldots + \lambda_{h_1}(\mathbf{u}_{h_1} - \mathbf{v}_{h_1}) \in \ker G = U \text{ for each } (\lambda_1, \ldots, \lambda_{h_1}) \in W. \tag{11}$$

For $i \in \{1, \ldots, h_1\}$ put $\mathbf{z}_i = \mathbf{u}_i - \mathbf{v}_i$, then $T := \langle \mathbf{z}_1, \ldots, \mathbf{z}_{h_1} \rangle_{q^n}$ with $\dim_{q^n} T = t$. We want to show that $t = 0$.

First assume $t = h_1$. By (11)

$$\{\lambda_1 \mathbf{z}_1 + \ldots + \lambda_{h_1} \mathbf{z}_{h_1} : (\lambda_1, \ldots, \lambda_{h_1}) \in W\} \subseteq T \cap U,$$

and $t = h_1$ yields $\dim_q(T \cap U) \geq \dim_q W = d_2 \geq k_1 + 1$ (because of our assumption on k_1 and from $k_2 \geq h_1 - 1$), which is not possible since T is an h_1-dimensional $\mathbb{F}_{q^n}$-subspace in V and U is $(h_1, k_1)_q$-evasive.

13

Next assume $1 \leq t \leq h_1 - 1$. W.l.o.g. we can assume $T = \langle \mathbf{z}_1, \ldots, \mathbf{z}_t \rangle_{q^n}$. Let $\Phi \colon \mathbb{F}_{q^n}^{h_1} \to T$ be the $\mathbb{F}_{q^n}$-linear map defined by the rule

$$(\lambda_1, \ldots, \lambda_{h_1}) \mapsto \lambda_1 \mathbf{z}_1 + \ldots + \lambda_{h_1} \mathbf{z}_{h_1}$$

and let $\bar{\Phi}$ be the restriction of Φ on $W \leq \mathbb{F}_{q^n}^{h_1}$. It can be easily seen that

$$\dim_{q^n} \ker \Phi = h_1 - t \quad \text{and} \quad \ker \bar{\Phi} = \ker \Phi \cap W. \tag{12}$$

Also, by (11)

$$\operatorname{Im} \bar{\Phi} \subseteq T \cap U. \tag{13}$$

By Proposition 2.6, W is also an $(h_1 - t, k_2 - t + 1)_q$-evasive subspace in $\mathbb{F}_{q^n}^{h_1}$ and hence taking (12) into account we get $\dim_q \ker \bar{\Phi} \leq k_2 - t + 1$, which yields

$$\dim_q \operatorname{Im} \bar{\Phi} \geq d_2 - (k_2 - t + 1). \tag{14}$$

By Proposition 2.6, U is also a $(t, k_1 - h_1 + t)_q$-evasive subspace in V, thus by (13) we get $\dim_q \operatorname{Im} \bar{\Phi} \leq k_1 - h_1 + t$, contradicting (14).

Thus we proved $t = 0$, i.e. $\mathbf{z}_i = \mathbf{0}$ for each $i \in \{1, \ldots h_1\}$ and hence $|\mathcal{C}| = q^{rnh_1}$. The trivial upper bound for the size of $\mathcal{C}$ is the size of $\mathbb{F}_q^{d_2 \times (rn - d_1)}$ and the result follows. $\square$

Then we obtain the following result which for $k < n$ slightly generalizes [10, Theorem 2.3].

Corollary 4.9. *If $k < n$ and U is an $(h, k)_q$-evasive subspace in $V(r, q^n)$, then*

$$\dim_q U \leq rn - \frac{rnh}{k+1}. \tag{15}$$

Proof. Note that in $V(h, q^n)$ there exist $(h-1, h-1)_q$-evasive subspaces of dimension $k+1 \leq n$, cf. Result 2.3. Then the result follows from Theorem 4.8 with $k_1 = k$, $h_1 = h$, $d_2 = k+1$ and $k_2 = h - 1$. $\square$

5 Maximum evasive subspaces of $V(3, q^n)$, $n \leq 5$

Let U be a maximum $(h, k)_q$-evasive subspace of $V = V(r, q^n)$. In this section we investigate the size of U for small values of r and n. First recall $h \leq k$. We will also assume $h < r$ and $k < nh$ since an h-dimensional $\mathbb{F}_{q^n}$-subspace has dimension nh over $\mathbb{F}_q$. If $k = nh$, then the whole vector space $V(r, q^n)$ is $(h, k)_q$-evasive.

If $r = 2$, then $h = 1$ and $k < n$. By Theorem 4.2 $\dim_q U$ is at most $n + k - 1$ and this bound is sharp, c.f. Example 4.6.

From now on assume $r = 3$. Then h is 1 or 2. First note that when $h = k = 1$, i.e. U is scattered, then the bound $3n/2$ can be reached for n even, cf. Result 2.3. If $h = 2$ and $n \leq k < 2n$, then by Theorem 4.2 the dimension of U is at most $n + k - 1$ and by Proposition 4.6 this bound can be reached. So from now on, we omit the discussion of these cases. It also means that we may assume $n \geq 3$.

Recall that if U has dimension t over $\mathbb{F}_q$ then the dual of U is $(r - h, (r - h)n + k - t)_q$-evasive of dimension $rn - t$ in $V(r, q^n)$.

- Case $n = 3$.

  If $h = k = 1$, then U has dimension at most 4 and such examples can be easily obtained by taking the $\mathbb{F}_q$-span of a maximum scattered subspace in $L = V(2, q^3) \le V$ and a vector $\mathbf{v} \in V \setminus L$.

  If $h = 1$ and $k = 2$ then Corollary 4.9 gives $\dim_q U \le 6$ and the dual of Example 2.2 with $m = 1$ reaches this bound.

  If $h = 2$ and $k = 2$ then Corollary 4.9 gives $\dim_q U \le 3$ and Example 2.2 with $m = 1$ reaches this bound.

- Case $n = 4$.

  If $h = 1$ and $k = 2$ then Corollary 4.9 gives $\dim_q U \le 8$, and this can be reached as the dual of Example 2.1.

  If $h = 1$ and $k = 3$ then Corollary 4.9 gives $\dim_q U \le 9$, and this can be reached starting from the previous example, cf. Proposition 2.7.

  If $h = 2$ and $k = 2$ then Corollary 4.9 gives $\dim_q U \le 4$, and this can be reached, see Example 2.1.

  If $h = 2$ and $k = 3$ then Theorem 4.2 gives $\dim_q U \le 6$, and it is reached by the maximum scattered subspaces of V, cf. Result 2.3.

- Case $n = 5$.

  If $h = k = 1$ then the Blokhuis–Lavrauw bound gives $\dim_q U \le 7$.

  If $h = 1$ and $k = 2$ then Corollary 4.9 gives $\dim_q U \le 10$, and this can be reached as the dual of Example 2.1.

  If $h = 1$ and $k = 3$ then Corollary 4.9 gives $\dim_q U \le 11$, and this can be reached from the previous example, cf. Proposition 2.7.

  If $h = 1$ and $k = 4$ then Corollary 4.9 gives $\dim_q U \le 12$, and this can be reached from the previous example, cf. Proposition 2.7.

  If $h = 2$ and $k = 2$ then Corollary 4.9 gives $\dim_q U \le 5$, and this can be reached, cf. Example 2.1.

  If $h = 2$ and $k = 3$ then the second bound of Theorem 4.2 gives $\dim_q U \le 6$ and this bound is sharp, cf. Proposition 4.5.

  If $h = 2$ and $k = 4$ then the first bound of Theorem 4.2 gives $\dim_q U \le 8$.

We can see that the first open cases are when $n = 5$ and $h = k = 1$ or $h = 2$ and $k = 4$. Note that if the bound in one of these two cases is reached then, by duality, the other bound is sharp as well. In the last part of this paper our aim is to find 7-dimensional scattered subspaces of $V(3, q^5)$. Then the dual of such a subspace is $(2, 4)_q$-evasive of dimension 8. Then by Theorem 3.5 and Remark 3.6 its Delsarte dual is an 8-dimensional 2-scattered $\mathbb{F}_q$-subspace in $V(5, q^5)$, which is maximum, by Corollary 4.9. Its dual is a $(3, 9)_q$-evasive subspace of dimension 17. Here we cannot use Corollary 4.9 since $k = 9$ and $n = 5$. However, we know that it is maximum by Corollary 3.2.

Maximum scattered subspaces of $V(3, q^5)$

In this section our aim is to construct scattered subspaces of dimension 7 in $V(3, q^5)$. To do this, we will work in $\mathbb{F}_{q^{15}}$ considered as a 3-dimensional vector space over $\mathbb{F}_{q^5}$. Then the one-dimensional $\mathbb{F}_{q^5}$-subspaces can be represented as follows: $x \in \langle u \rangle_{\mathbb{F}_{q^5}}$ if and only if $x = \lambda u$ for some $\lambda \in \mathbb{F}_{q^5}$ and hence $x^{q^5-1} = u^{q^5-1}$. In particular, x is a root of $x^{q^5} - dx$ with $d = u^{q^5-1}$. We proceed with the following steps.

(1) Find q-polynomials $P(x) = \sum_{i=0}^{7} \alpha_i x^{q^i} \in \mathbb{F}_{q^{15}}[x]$ with q^7 roots in $\mathbb{F}_{q^{15}}$. Then $U := \ker_q P$ is an $\mathbb{F}_q$-subspace of dimension 7.

(2) Apply [8, Theorem 2.1] to obtain conditions when $P(x)$ has at most q common roots with the polynomial $x^{q^5} - dx$ for each $d \in \mathbb{F}_{q^{15}}$ with $d^{1+q^5+q^{10}} = 1$. This is equivalent to ask that $\dim_q(\langle u \rangle_{\mathbb{F}_{q^5}} \cap U) \leq 1$, where $d = u^{q^5-1}$.

(3) Show that $P(x)$ can be chosen such that these conditions are satisfied.

For some $a, b \in \mathbb{F}_{q^{15}}$, $a^{q^3} b \neq a b^{q^3}$ put

$$R_{a,b}(x) = R(x) = \begin{pmatrix} x & x^{q^3} & x^{q^6} \\ a & a^{q^3} & a^{q^6} \\ b & b^{q^3} & b^{q^6} \end{pmatrix} = x^{q^6}(ab^{q^3} - a^{q^3}b) + x^{q^3}(a^{q^6}b - ab^{q^6}) + x(a^{q^3}b^{q^6} - a^{q^6}b^{q^3}).$$

Then $\ker R = \langle a, b \rangle_{\mathbb{F}_{q^3}}$ has dimension 2 over $\mathbb{F}_{q^3}$ and hence dimension 6 over $\mathbb{F}_q$. Take any $\bar{x} \notin \ker R$ and put $c = R(\bar{x})$. Define

$$P_{a,b,c}(x) = P(x) = cR(x)^q - c^q R(x). \tag{16}$$

Then P vanishes on $\langle \ker R, \bar{x} \rangle_{\mathbb{F}_q}$, i.e. on an $\mathbb{F}_q$-subspace of dimension 7. The coefficients of $P(x)$ are:
$$\alpha_0 = -c^q(a^{q^3}b^{q^6} - a^{q^6}b^{q^3}), \quad \alpha_1 = c(a^{q^4}b^{q^7} - a^{q^7}b^{q^4}), \quad \alpha_2 = 0,$$
$$\alpha_3 = -c^q(a^{q^6}b - ab^{q^6}), \quad \alpha_4 = c(a^{q^7}b^q - a^q b^{q^7}), \quad \alpha_5 = 0,$$
$$\alpha_6 = -c^q(ab^{q^3} - a^{q^3}b), \quad \alpha_7 = c(a^q b^{q^4} - a^{q^4}b^q).$$

By [8, Theorem 2.1] U is scattered if and only if for each $d \in \mathbb{F}_{q^{15}}$ with $d^{1+q^5+q^{10}} = 1$ the

following two matrices are not singular at the same time:

$$
\begin{pmatrix}
\alpha_7^{q^4} & \alpha_6^{q^4} & 0 & \alpha_4^{q^4} & \alpha_3^{q^4} & 0 & \alpha_1^{q^4} & \alpha_0^{q^4} & 0 & 0 & 0 & 0 \\
0 & \alpha_7^{q^3} & \alpha_6^{q^3} & 0 & \alpha_4^{q^3} & \alpha_3^{q^3} & 0 & \alpha_1^{q^3} & \alpha_0^{q^3} & 0 & 0 & 0 \\
0 & 0 & \alpha_7^{q^2} & \alpha_6^{q^2} & 0 & \alpha_4^{q^2} & \alpha_3^{q^2} & 0 & \alpha_1^{q^2} & \alpha_0^{q^2} & 0 & 0 \\
0 & 0 & 0 & \alpha_7^{q} & \alpha_6^{q} & 0 & \alpha_4^{q} & \alpha_3^{q} & 0 & \alpha_1^{q} & \alpha_0^{q} & 0 \\
0 & 0 & 0 & 0 & \alpha_7 & \alpha_6 & 0 & \alpha_4 & \alpha_3 & 0 & \alpha_1 & \alpha_0 \\
1 & 0 & 0 & 0 & 0 & -d^{q^6} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & -d^{q^5} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -d^{q^4} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -d^{q^3} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -d^{q^2} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -d^{q} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -d
\end{pmatrix}
$$

$$
\begin{pmatrix}
\alpha_7^{q^3} & \alpha_6^{q^3} & 0 & \alpha_4^{q^3} & \alpha_3^{q^3} & 0 & \alpha_1^{q^3} & \alpha_0^{q^3} & 0 & 0 \\
0 & \alpha_7^{q^2} & \alpha_6^{q^2} & 0 & \alpha_4^{q^2} & \alpha_3^{q^2} & 0 & \alpha_1^{q^2} & \alpha_0^{q^2} & 0 \\
0 & 0 & \alpha_7^{q} & \alpha_6^{q} & 0 & \alpha_4^{q} & \alpha_3^{q} & 0 & \alpha_1^{q} & \alpha_0^{q} \\
0 & 0 & 0 & \alpha_7 & \alpha_6 & 0 & \alpha_4 & \alpha_3 & 0 & \alpha_1 \\
1 & 0 & 0 & 0 & 0 & -d^{q^5} & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & -d^{q^4} & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -d^{q^3} & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -d^{q^2} & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -d^{q} \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{pmatrix}
$$

Theorem 5.1. *Let h be a non-negative integer. Consider $q = p^{15h+s}$, with $\gcd(s, 15) = 1$ if $p = 2, 3$ and with $s = 1$ if $p = 5$. Then in $V(3, q^5)$ there exist scattered subspaces of dimension 7.*

Proof. We will prove that there exist $a, b, c \in \mathbb{F}_{q^{15}}$ with $a^{q^3} b \neq a b^{q^3}$ and $c \in \operatorname{Im} R_{a,b} \setminus \{0\}$ such that the kernel of $P_{a,b,c}(x)$ as in (16) is scattered of dimension 7 in $\mathbb{F}_{q^{15}}$.

First consider the case $p = 2$ and $s = 1$. Choose as a generator of $\mathbb{F}_{2^{15}}$ an element ξ such that $\xi^{15} + \xi^5 + \xi^4 + \xi^2 + 1 = 0$. Then put $V = \xi^{31369}$. It can be verified with the help of the Software MAGMA [7] that $\lambda^{15} + \lambda + 1 = 0$. Then for any element $z \in \mathbb{F}_{2^{15}}$ we have $z^q = z^{2^{15h+1}} = z^2$. Set $a = \lambda^2$, $b = \lambda^4$ and

$$
c := R_{a,b}(\lambda) = \lambda^{273} + \lambda^{266} + \lambda^{161} + \lambda^{140} + \lambda^{98} + \lambda^{84} = \xi^{8539} \neq 0.
$$

Then the second matrix above, which we will call $M(d)$, reads as

$$\begin{pmatrix}
\xi^{3757} & \xi^{22429} & 0 & \xi^{17} & \xi^{20559} & 0 & \xi^{10610} & \xi^{9472} & 0 & 0 \\
0 & \xi^{18262} & \xi^{27598} & 0 & \xi^{16392} & \xi^{26663} & 0 & \xi^{5305} & \xi^{4736} & 0 \\
0 & 0 & \xi^{9131} & \xi^{13799} & 0 & \xi^{8196} & \xi^{29715} & 0 & \xi^{19036} & \xi^{2368} \\
0 & 0 & 0 & \xi^{20949} & \xi^{23283} & 0 & \xi^{4098} & \xi^{31241} & 0 & \xi^{9518} \\
1 & 0 & 0 & 0 & 0 & d^{q^5} & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & d^{q^4} & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & d^{q^3} & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & d^{q^2} & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & d^q \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{pmatrix}$$

and its determinant is

$$\det M(d) = \xi^{5977} d^{q^4+q^3+q^2+q} + \xi^{2592} d^{q^3+q^2+q} + \xi^{4799} d^{q^2+q} + \xi^{8832} d^q$$
$$+ \xi^{4161} d^{q^4+q^3+q^2} + \xi^{19121} d^{q^4+q^2} + \xi^{28007} d^{q^4} + \xi^{27801}.$$

Next we prove $\det M(d) \neq 0$ for each $d \in \mathbb{F}_{q^{15}}$ with $d^{q^{10}+q^5+1} = 1$. To do this, we define the following multivariate polynomial over the algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$:

$$F_0(D_0, \ldots, D_{14}) := \xi^{5977} D_4 D_3 D_2 D_1 + \xi^{2592} D_3 D_2 D_1 + \xi^{4799} D_2 D_1 + \xi^{8832} D_1$$
$$+ \xi^{4161} D_4 D_3 D_2 + \xi^{19121} D_4 D_2 + \xi^{28007} D_4 + \xi^{27801} \in \overline{\mathbb{F}}_2[D_0, \ldots, D_{14}].$$

Clearly, $\det M(d) = F_0(d, d^q, \ldots, d^{q^{14}})$. For $i = 1, 2, \ldots, 14$ define $F_i \in \overline{\mathbb{F}}_2[D_0, \ldots, D_{14}]$ as the polynomial obtained from F_0 by taking q^i-th powers of its coefficients and by replacing D_j by $D_{j+i \pmod{15}}$ for $j = 0, 1, \ldots, 14$. Then, by $d \in \mathbb{F}_{q^{15}}$, $\det M(d) = 0$ yields $F_i(d, d^q, \ldots, d^{q^{14}}) = 0$ for $i = 0, 1, \ldots, 14$.

We first compute the ideal I generated by the polynomials F_i, $i = 1, \ldots, 14$. Then we compute the elimination ideal of I with respect to the variable D_0, which is generated by $G(D_0) := D_0^3 + \xi^{7925} D_0^2 + \xi^{24175} D_0 + \xi^{31682}$. The three roots of $G(D_0)$ are $\xi^{15773}, \xi^{16482}, \xi^{32194}$ and therefore putative values $d \in \mathbb{F}_{q^{15}}$ for which $\det M(d) = 0$ belong to $S := \{\xi^{15773}, \xi^{16482}, \xi^{32194}\} \subset \mathbb{F}_{2^{15}}$. Recall that d should also satisfy $d^{q^{10}+q^5+1} = 1$ and, since $d \in S \subset \mathbb{F}_{2^{15}}$ and $q = 2^{15h+1}$, this equation reads $d^{2^{10}+2^5+1} = 1$. None of the elements of S is a $(2^{10}+2^5+1)$-th root of unity in $\mathbb{F}_{2^{15}}$. This shows that $\det M(d) \neq 0$ when $d^{q^{10}+q^5+1} = 1$.

A similar argument applies to all the other cases. In particular, elements $\lambda \in \mathbb{F}_{p^{15}}$ for $p = 2, 3$ and $\gcd(s, 15) = 1$ are summarized in Table 1. As a notation, if $p = 2$ then ξ satisfies $\xi^{15} + \xi^5 + \xi^4 + \xi^2 + 1 = 0$, whereas if $p = 3$ then $\xi^{15} + 2\xi^8 + \xi^5 + 2\xi^2 + \xi + 1 = 0$ holds. Finally, for $p = 5$ and $s = 1$, the element $\lambda = \xi^{24079949306}$, where $\xi^{15} + 2\xi^5 + 3\xi^3 + 3\xi^2 + 4\xi + 3 = 0$, can be chosen.

$\square$

Remark 5.2. *A computer search in MAGMA [7] shows that random 7-dimensional $\mathbb{F}_q$-subspaces in $V(3, q^5)$, for $q = 2, 3$, are in general not scattered. Indeed, we tested in total 5180000 and 3700 $\mathbb{F}_q$-subspaces of dimension 7 in $V(3, 2^5)$ and $V(3, 3^5)$, respectively, and we*

found that 332477 (6.4%) and 625 (16.9%) of them are scattered. The number of subspaces examined represents only a tiny part of the whole search space. However, our computations seem to suggest that the property of being scattered is not so rare for 7-dimensional $\mathbb{F}_q$-subspaces in $V(3, q^5)$. On the other hand, such scattered subspaces are completely random and a suitable description seems far from being reached.

Acknowledgements

References

[1] S. BALL: Finite Geometry and Combinatorial Applications, Cambridge University Press, 2015.

[2] S. BALL AND A. BLOKHUIS: An easier proof of the maximal arcs conjecture, *Proc. Amer. Math. Soc.* **126** (1998), 3377–3380.

[3] S. BALL, A. BLOKHUIS AND M. LAVRAUW: Linear $(q + 1)$-fold Blocking Sets in $PG(2, q^4)$, *Finite Fields Appl.* **6** (2000), 294–301.

[4] S. BALL, A. BLOKHUIS AND F. MAZZOCCA: Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica* **17** (1997), 31–41.

[5] D. BARTOLI, M. GIULIETTI, G. MARINO AND O. POLVERINO: Maximum Scattered Linear Sets and Complete Caps in Galois Spaces, *Combinatorica* **38** (2018), 255–278.

[6] A. BLOKHUIS AND M. LAVRAUW: Scattered Spaces with Respect to a Spread in PG(n, q), *Geom. Dedicata* **81**(1-3) (2000), 230–243.

[7] W. BOSMA, J. CANNON, AND C. PLAYOUST: The Magma algebra system. I. The user language. Computational algebra and number theory, *J. Symbolic Comput.* **24**(3–4) (1997), 235–265.

[8] B. CSAJBÓK: Scalar q-subresultants and Dickson matrices. *J. Algebra* **547** (2020), 116–128.

[9] B. CSAJBÓK, G. MARINO, O. POLVERINO AND F. ZULLO: Maximum scattered linear sets and MRD-codes, *J. Algebraic Combin.* **46** (2017), 517–531.

[10] B. Csajbók, G. Marino, O. Polverino and F. Zullo: Generalising the scattered property of subspaces, *Combinatorica* (2021). `https://doi.org/10.1007/s00493-020-4347-y`

[11] M. A. De Boer: Almost MDS Codes, *Des. Codes Cryptogr.* **9** (1996), 143–155.

[12] Z. Dvir and S. Lovett: Subspace evasive sets, in: *Proceedings of the 44th ACM Symposium on Theory of Computing*, 351—358, 2012.

[13] V. Guruswami: Linear-algebraic list decoding of folded Reed-Solomon codes, *Annual IEEE Conference on Computational Complexity*, 77–85, 2011.

[14] V. Guruswami, C. Wang and C. Xing: Explicit List-Decodable Rank-Metric and Subspace Codes via Subspace Designs. *IEEE Trans. Info. Theory* **62**(5), 2707--2718, May 2016.

[15] J. W. P. Hirschfeld: Projective Geometries over Finite Fields, second ed. Clarendon Press, Oxford, 1998.

[16] I. Landjev and A. Rousseva: The Main Conjecture for Near-MDS Codes. WCC2015 - 9th International Workshop on Coding and Cryptography 2015, Anne Canteaut, Gaëtan Leurent, Maria Naya-Plasencia, Apr 2015, Paris, France. hal-01276222

[17] M. Lavrauw: Scattered Spaces with respect to Spreads and Eggs in Finite Projective Spaces, Ph.D. Thesis, 2001.

[18] M. Lavrauw: Scattered spaces in Galois Geometry, *Contemporary Developments in Finite Fields and Applications*, 2016, 195–216.

[19] G. Lunardon: MRD-codes and linear sets, *J. Combin. Theory Ser. A* **149** (2017), 1–20.

[20] G. Lunardon, P. Polito and O. Polverino: A geometric characterisation of linear k-blocking sets, *J. Geom.* **74 (1-2)** (2002), 120–122.

[21] G. Lunardon and O. Polverino: Translation ovoids of orthogonal polar spaces, *Forum Math.* **16** (2004), 663–669.

[22] O. Polverino: Linear sets in finite projective spaces, *Discrete Math.* **310**(22) (2000), 3096–3107.

[23] P. Pudlák and V. Rödl: Pseudorandom sets and explicit constructions of ramsey graphs, *Quaderni di Matematica* **13** (2004), 327–346.

[24] T. H. Randrianarisoa: A geometric approach to rank metric codes and a classification of constant weight codes, *Des. Codes Cryptogr.* **88**, pages 1331–1348 (2020)

[25] J. SHEEKEY: MRD Codes: Constructions and Connections, in: Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications Ed. by Schmidt, Kai-Uwe and Winterhof, Arne, Series: Radon Series on Computational and Applied Mathematics 23, De Gruyter 2019.

[26] J. SHEEKEY AND G. VAN DE VOORDE: Rank-metric codes, linear sets, and their duality, *Des. Codes Cryptogr.* **88** (2020), 655–675.

[27] G. TALLINI: On caps of kind s in a Galois r-dimensional space, *Acta Arithmetica* **7**(1) (1961), 19–28.

[28] D. E. TAYLOR: The geometry of the classical groups. Sigma Series in Pure Mathematics. 9. Berlin: Heldermann Verlag. v (1992).

Table 1: Values $V \in \mathbb{F}_{p^{15}}$ for $p = 2, 3$ and $\gcd(s, 15) = 1$.

	$s=1$	$s=2$	$s=4$	$s=7$	$s=8$	$s=11$	$s=13$	$s=14$
$p=2$	ξ^{31369}	ξ^{14336}	ξ^{184}	ξ^{136}	ξ^{4102}	ξ^{16767}	ξ^{28172}	ξ^{11248}
$p=3$	$\xi^{11227515}$	$\xi^{10565258}$	$\xi^{5832991}$	$\xi^{12725576}$	$\xi^{11963627}$	$\xi^{11963627}$	$\xi^{13348604}$	$\xi^{13348604}$