Scattered spaces with respect to a spread in $PG(n, q)$

Aart Blokhuis
Technische Universiteit Eindhoven,
Postbox 513, 5600 MB Eindhoven,
The Netherlands
and
Division of Mathematics and Computer Science,
Vrije Universiteit
de Boelelaan 1081a
1081 HV Amsterdam
The Netherlands

and

Michel Lavrauw
Technische Universiteit Eindhoven,
Postbox 513, 5600 MB Eindhoven,
The Netherlands

January 14, 2004

Abstract

A scattered subspace of $PG(n-1, q)$ with respect to a $(t-1)$-spread S is a subspace intersecting every spread element in at most a point. Upper and lower bounds for the dimension of a maximum scattered space are given. In the case of a normal spread new classes of two intersection sets with respect to hyperplanes in a projective space are obtained using scattered spaces.

1. Introduction

Let $V(n, q)$ be the n-dimensional vector space over the finite field of order q, $GF(q)$, where $q = p^h$, p prime, $h \geq 1$, and let $PG(n-1, q)$ be the corresponding $(n-1)$-dimensional Desarguesian projective space over $GF(q)$. To avoid confusion, we use the word *rank* for vector space dimension and *dimension* for the dimension of the corresponding projective space, following P. J. Cameron [4]. So we say that a subspace of $PG(n-1, q)$ has rank t and dimension $t-1$. Let S be a set of $(t-1)$-dimensional subspaces of $PG(n-1, q)$. Then S is called a $(t-1)$-*spread* of $PG(n-1, q)$ if every point of $PG(n-1, q)$ is contained in exactly one element of S. If S is a set of subspaces of $V(n, q)$ of rank t, then S is called a t-*spread* of $V(n, q)$ if every vector of $V(n, q) - \{\vec{0}\}$ is contained in exactly one element of S. Sometimes we work in $V(n, q)$, sometimes in $PG(n-1, q)$, but since the problems are equivalent, it will be clear what we mean. As has been proved by Segre [12], by counting the number of spread elements, a $(t-1)$-spread of $PG(n-1,q)$ exists if and only if $n=rt$. The existence of a t-spread in $V(rt,q)$ follows from the trivial 1-spread in $V(r,q^t)$. We abuse notation and use S for a spread in $PG(n-1,q)$ as well as in $V(n,q)$.

Let S be a spread in $V(n,q)$. A subspace of $V(n,q)$ is called *scattered with respect to* S if it intersects each spread element in a subspace of rank at most one. Projectively, if S is a spread in $PG(n-1,q)$, a subspace of $PG(n-1,q)$ is called *scattered with respect to* S if it intersects each spread element in at most one point. It is clear that both definitions are consistent with each other and give rise to equivalent problems.

For example, if S is a spread of lines in $PG(3,q)$, then a line not contained in the spread is a scattered space with respect to S. It intersects $q+1$ spread elements in a point. This is the highest dimension a scattered space can have in this example, since a plane of $PG(3,q)$ necessarily contains a line of S. A scattered space of highest possible dimension is called a *maximum* scattered space. So in this case it is clear what the dimension of a maximum scattered space is with respect to a spread of lines. However the problem is not always so easy. In this paper we prove some upper and lower bounds for the dimension of a maximum scattered space. Note that if $t=1$, the space itself $PG(rt-1,q)$ is scattered to every $(t-1)$-spread in $PG(rt-1,q)$, since then the spread elements are just the points of the projective space. From now on we assume that $t \geq 2$.

2. A lower bound on the dimension of a maximum scattered subspace

Giving a procedure to enlarge a scattered subspace, whenever this is possible, we get a lower bound on the dimension of a maximum scattered space.

Theorem 2.1 *Let S be a $(t-1)$-spread of $PG(rt-1,q)$ and let T be an m-dimensional scattered subspace with respect to S. If*

$$m < \frac{rt-t}{2}$$

then T is contained in an $(m+1)$-dimensional scattered subspace with respect to S. Moreover, the dimension of a maximum scattered subspace with respect to S is at least $\lceil \frac{rt-t}{2} \rceil$.

Proof : Let S be a t-spread in $V(rt,q)$ and $T = < \vec{w}_0, \vec{w}_1, \ldots, \vec{w}_m >$ be scattered with respect to S. For $\vec{w}_{m+1} \notin T$, $< T, \vec{w}_{m+1} >$ will be scattered with respect to S if

$$w_{m+1} \notin \tilde{T} := \bigcup_{Q:(Q\in S)\wedge(Q\cap T\neq\{\vec{0}\})} < Q,T > .$$

So T is contained in a larger scattered subspace if

$$q^{rt} > (q^{t+m} - q^{m+1})(q^m + q^{m-1} + \ldots + 1) + q^{m+1}.$$

Hence this allows us to extend T to a scattered subspace of rank $m+2$ if $m < \frac{rt-t}{2}$. It follows that the maximum dimension of a scattered subspace with respect to S is at least $\lceil \frac{rt-t}{2} \rceil$. This concludes the proof. □

3. An upper bound on the dimension of a scattered subspace

Let S be a $(t-1)$-spread in $PG(rt-1,q)$. The number of spread elements is $(q^{rt}-1)/(q^t-1)$ $= q^{(r-1)t} + q^{(r-2)t} + \ldots + q^t + 1$. Since a scattered subspace can contain at most one point of every spread element, the number of points in a scattered space must be less than or equal to the number of spread elements. So we have the following trivial upper bound.

Theorem 3.1 *If T is a m-dimensional scattered space with respect to $(t-1)$-spread in $PG(rt-1,q)$ then*

$$m \leq rt - t - 1.$$

A spread S is called *normal* if and only if the space generated by two spread elements is partitioned by a subset of S. From this it follows that the space generated by any number of elements from a normal spread is partitioned by elements of S. If $r = 1, 2$ then every spread is normal. There is a large variety of spreads and there is not much that can be said about the possible dimension of a scattered subspace with respect to an arbitrary spread. We start by showing that we can always find a spread such that the upper bound in Theorem 3.1 is obtained. A spread is called *a scattering spread with respect to a subspace*, if this subspace is scattered with respect to the spread.

Theorem 3.2 *For an $(rt-t-1)$-dimensional subspace W in $PG(rt-1,q)$, $r \geq 2$, there exists a scattering $(t-1)$-spread S with respect to W.*

Proof : We remark that since all $(rt-t-1)$-dimensional subspaces in $PG(rt-1,q)$ are projectively equivalent, it suffices to prove that we can find a spread S and an $(rt-t-1)$-dimensional subspace W, such that W is scattered with respect to S. In Lemma 4.1 we will show that there exists a scattered $(t-1)$-dimensional subspace with respect to a normal $(t-1)$- spread in $PG(2t-1,q)$. Assume $r > 2$. Let S' be a normal $(t-1)$-spread in $PG(rt-1,q)$ and U a $(rt-2t-1)$-dimensional subspace of $PG(rt-1,q)$ partitioned by elements of S'. Now we consider the quotient geometry of U in $PG(rt-1,q)$. This is isomorphic with $PG(2t-1,q)$. Moreover, the $(t-1)$-spread in $PG(rt-1,q)$ induces a normal $(t-1)$-spread in this quotient geometry. The spread elements in the quotient geometry correspond with the $(rt-t-1)$-dimensional subspaces of $PG(rt-1,q)$ obtained by taking the span of U and a spread element not intersecting U. Since S' is a normal spread, it is clear that two such subspaces are either equal or only have U in their intersection. By Lemma 4.1, we can find a $(t-1)$-dimensional scattered space with respect to this spread in the quotient geometry. This induces a $(rt-t-1)$-dimensional space W containing U which intersects spread elements outside U in at most a point. Let W' be a $(rt-t-1)$-dimensional subspace obtained by taking the space spanned by U and a spread element of S' not intersecting W. By induction on r, we can change the spread locally in W' in order to find a spread S which is scattering with respect to U. The new spread S is a scattering spread with respect to W. □

4. Scattered spaces with respect to a normal spread

Consider $PG(r-1,q^t)$. The points of $PG(r-1,q^t)$ are the subspaces of rank 1 of $V(r,q^t)$. If we look at $GF(q^t)$ as being a vector space of rank t over $GF(q)$ then a subspace of rank 1 in $V(r,q^t)$ induces a subspace of rank t in $V(rt,q)$. So the points of $PG(r-1,q^t)$ induce subspaces of rank t in $V(rt,q)$. The lines of $PG(r-1,q^t)$, which are subspaces of rank 2 of $V(r,q^t)$, induce subspaces of rank $2t$ in $V(rt,q)$. So it is clear that the points of

$PG(r-1,q^t)$, seen as $(t-1)$-dimensional subspaces in $PG(rt-1,q)$, form a normal spread S of $PG(rt-1,q)$. Moreover, for $r>2$ every normal spread can be constructed in that way (see [9]).

Remark. Although we shall not take this point of view, one can also construct a normal spread as follows. Consider the field automorphism

$$\begin{array}{rccl} \sigma: & GF(q^t) & \to & GF(q^t), \\ & x & \mapsto & x^q. \end{array}$$

Put $\Sigma^* = PG(rt-1,q^t)$ and extend σ to a collineation of Σ^*, also denoted by σ, by coordinatizing Σ^* and letting σ act on the coordinates of the points. If P is a point of Σ^* then we denote P^σ as it's image under the collineation σ. Let $\Sigma = PG(rt-1,q)$ be the canonical subgeometry of Σ^* whose points are fixed by σ. If U is a subspace of dimension m then U is fixed by σ if and only if U intersects Σ in a subspace of dimension m. See [6] for more details. For every point P of Σ^*, define the subspace

$$L(P) :=< P, P^\sigma, \ldots, P^{\sigma^{t-1}} > .$$

Clearly $L(P)^\sigma = L(P)$, which implies that $L(P)$ intersects Σ in a subspace of dimension equal to the dimension of $L(P)$. If the dimension of $L(P)$ is $t-1$ then P is called an *imaginary point*. For an imaginary point P, $L(P)$ meets Σ in a $(t-1)$-dimensional space. There exists a $\pi = PG(r-1,q^t)$ disjoint from Σ, such that Σ^* is spanned by $\pi, \pi^\sigma, \ldots, \pi^{\sigma^{t-1}}$ and all points of π are imaginary. This implies that $S = \{L(P) \cap \Sigma \parallel P \text{ a point of } \pi\}$ is a normal $(t-1)$-spread of Σ, see [6, Section 6, Theorem 6.1].

Lemma 4.1 *In $PG(2t-1,q)$, there exists a $(t-1)$-dimensional scattered subspace with respect to a normal $(t-1)$-spread.*

Proof : Let S be the t-spread in $V(2t,q)$, induced by the 1-dimensional subspaces of $V(2,q^t)$. This is the set $\{< (a,b) >_{q^t} \ \parallel (a,b) \in (GF(q^t))^2 \setminus (0,0)\}$. If W is the set

$$\{(x,x^q) \| x \in GF(q^t)\}$$

then W is of rank t over $GF(q)$. If two vectors (a,b) and $\lambda(a,b)$, with $\lambda \in GF(q^t)$ in the spread element $< (a,b) >_{q^t}$ are contained in W, then $b=a^q$ and $\lambda b = (\lambda a)^q$. It follows that $\lambda^q = \lambda$, thus $\lambda \in GF(q)$. This implies that a spread element intersects W in at most one dimension. □

In [11] a similar construction is used.

If W is a subspace in $V(rt,q)$, then by $B(W)$ we mean the set of points of $PG(r-1,q^t)$, which correspond to the elements of S which have at least an intersection of rank 1 with W in $V(rt,q)$.

Remark. We say that a projective space P_2 is an *embedding* of a projective space P_1 in a projective space P_3 if

- (i) P_2 is isomorphic to P_1,
- (ii) the pointset of P_2 is a subset of the pointset of P_3 and
- (iii) the lines of P_2 are the lines of P_3 induced by the points of P_2.

The pointset $B(W)$ in $PG(r-1,q^t)$ is an embedding of the projective space corresponding to a scattered subspace W of $V(rt,q)$ if and only if all subspaces of rank $2t$ of $V(rt,q)$

corresponding to lines of $PG(r-1,q^t)$ intersect W in a subspace of rank 0,1 or 2. For more about embeddings we refer to [8].

Using the structure of $PG(r-1,q^t)$, we are able to improve the bounds for a maximum scattered space with respect to a normal $(t-1)$-spread in $PG(rt-1,q)$ in a number of cases. Put

$$\theta_n(q) = |PG(n,q)| = \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \ldots + q + 1.$$

If rt is even then we have the following theorem:

Theorem 4.2 *If $W_{\frac{rt}{2}}$ is a subspace of rank $\frac{rt}{2}$ of $V(rt,q)$, which is scattered with respect to a normal t-spread S of $V(rt,q)$, then $B(W_{\frac{rt}{2}})$ is a two intersection set in $PG(r-1,q^t)$ with respect to hyperplanes with intersection numbers $\theta_{\frac{rt}{2}-t-1}(q)$ and $\theta_{\frac{rt}{2}-t}(q)$.*

Proof : Let $rt = 2m$ and h_i $(i = 1,\ldots,m)$ be the number of hyperplanes of $PG(r-1,q^t)$, seen as subspaces of rank $rt-t$ in $V(rt,q)$, that intersect W_m in a subspace of rank i. It is clear that a subspace of rank m and $rt-t$ contained in $V(rt,q)$ necessarily meet in a subspace of rank at least $m-t$ and since W_m is scattered, such a hyperplane can not meet W_m in a subspace of rank bigger than $rt-2t$, because of the number of points contained in that hyperplane. Counting hyperplanes, incident point-hyperplane pairs, and incident point-point-hyperplane triples we get the set of equations

$$\begin{cases} \sum_{i=m-t}^{rt-2t} h_i = \theta_{r-1}(q^t); & (1) \\ \sum_{i=m-t}^{rt-2t} \theta_{i-1}(q)h_i = \theta_{m-1}(q)\theta_{r-2}(q^t); & (2) \\ \sum_{i=m-t}^{rt-2t} \theta_{i-1}(q)(\theta_{i-1}(q)-1)h_i = \theta_{m-1}(q)(\theta_{m-1}(q)-1)\theta_{r-3}(q^t). & (3) \end{cases}$$

Consider the expression

$$\sum_{i=m-t}^{rt-2t} [(\theta_{i-1}(q) - \theta_{m-t-1}(q))\ (\theta_{i-1}(q) - \theta_{m-t}(q))]\, h_i. \qquad (*)$$

We can write the coefficient of h_i in $(*)$ as

$$\theta_{i-1}(q)(\theta_{i-1}(q)-1) - [\theta_{m-t-1}(q) + \theta_{m-t}(q) - 1]\theta_{i-1}(q) + \theta_{m-t-1}(q)\theta_{m-t}(q).$$

Using the equations (1), (2) and (3), expression $(*)$ is equal to

$$\begin{aligned} & \theta_{m-1}(q)(\theta_{m-1}(q)-1)\theta_{r-3}(q^t) \\ - \ & [\theta_{m-t-1}(q) + \theta_{m-t}(q) - 1]\theta_{m-1}(q)\theta_{r-2}(q^t) + \theta_{m-t-1}(q)\theta_{m-t}(q)\theta_{r-1}(q^t). \end{aligned}$$

Replacing rt by $2m$ and $\theta_{n-1}(q)$ by it's definition, this expression is equal to

$$\begin{array}{rl} & (q^t-1)^{-1}(q-1)^{-2}\{(q^m-1)(q^m-q)(q^{2m-2t}-1) \\ - & [(q^{m-t}-1)+(q^{m-t+1}-1)-(q-1)](q^m-1)(q^{2m-t}-1) \\ + & (q^{m-t}-1)(q^{m-t+1}-1)(q^{2m}-1)\} \\ \\ = & (q^t-1)^{-1}(q-1)^{-2}\left[(q^m-1)(q^{m-t}-1)\ [(q^m-q)(q^{m-t}+1)-(q+1)(q^{2m-t}-1)\right. \\ + & \left.\big(q^{m-t+1}-1)(q^m+1)\big]\right]=0. \end{array}$$

Hence

$$\sum_{i=m-t}^{rt-2t}[(\theta_{i-1}(q)-\theta_{m-t-1}(q))(\theta_{i-1}(q)-\theta_{m-t}(q))]\,h_i=0,$$

which implies that $h_i=0$, for all $i\geq m-t+2$. Since a scattered subspace of rank i intersects $\theta_{i-1}(q)$ spread elements, this concludes the proof. □

We can solve $h_{\frac{rt}{2}-t}$ and $h_{\frac{rt}{2}-t+1}$ from (1) and (2) in order to obtain the unique solution

$$\begin{cases} h_i & = \ 0,\ i<\frac{rt}{2}-t, \\ h_{\frac{rt}{2}-t} & = \ \theta_{r-1}(q^t)-\theta_{\frac{rt}{2}-1}(q), \\ h_{\frac{rt}{2}-t+1} & = \ \theta_{\frac{rt}{2}-1}(q), \\ h_i & = \ 0,\ i>\frac{rt}{2}-t+1. \end{cases}$$

In [10], T. Penttila and G. F. Royle give a complete characterization of two-intersection sets in planes of order nine. According to their terminology the parameters of the two-intersection set obtained in Theorem 4.2 for $r=3$ are called *standard parameters.* These sets occur in planes of square order and have type $(m,m+\sqrt{q})$ in $PG(2,q)$.

The proof of Theorem 4.2 allows us to proof the following upper bound.

Theorem 4.3 *If W_m is a subspace of rank m of $V(rt,q)$, which is scattered with respect to a normal t-spread S of $V(rt,q)$ then $m\leq\frac{rt}{2}$.*

Proof : Starting with a scattered subspace of rank m with respect to a normal t-spread in $V(rt,q)$, we can write down the same set of equations as in the proof of Theorem 4.2 and get the equation

$$(q^t-1)(q-1)^2\sum_{i=m-t}^{rt-2t}[(\theta_{i-1}(q)-\theta_{m-t-1}(q))\ (\theta_{i-1}(q)-\theta_{m-t}(q))]\,h_i$$

$$\begin{array}{rl} = & (q^m-1)(q^m-q)(q^{rt-2t}-1) \\ - & [(q^{m-t}-1)+(q^{m-t+1}-1)-(q-1)](q^m-1)(q^{rt-t}-1) \\ + & (q^{m-t}-1)(q^{m-t+1}-1)(q^{rt}-1) \\ \\ = & (q^{rt-2t+1}+q^{2m-t+1}+q^{2m-t}+q^{rt})-(q^{rt-t+1}+q^{2m-2t+1}+q^{2m}+q^{rt-t}). \end{array}$$

We remark that these equations are are also valid for rt odd. Since the coefficient of h_i in this expression is always positive, the theorem follows. □

In [2] a construction is given of a scattered subspace of rank 6 with respect to a normal 4-spread in $V(12, q)$. Hence the obtained bound is sharp for $r = 3$ and $t = 4$. The next Theorem shows that this upper bound is in fact sharp in a lot of cases. In the proof we use the *Gaussian coefficient*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)},$$

which counts the number of subspaces of rank k in $V(n, q)$. Let U be a subspace of rank r in $V(n, q)$. Then the number of subspaces of rank k containing U in $V(n, q)$, with $r \leq k$, is equal to

$$\begin{bmatrix} n-r \\ k-r \end{bmatrix}_q.$$

Theorem 4.4 *If W_m is a maximum scattered subspace of rank m of $V(rt, q)$ with respect to a normal t-spread S of $V(rt, q)$ then $m \geq r'k$, where k is maximal such that*

$$r'k < \begin{cases} \frac{rt-t+3}{2} & \text{if } q = 2 \text{ and } r' = 1, \\ \frac{rt-t+r'+3}{2} & \text{otherwise}; \end{cases}$$

where $r' \mid r$ and $(r', t) = 1$.

Proof : Let C be the class of subspaces of $V(rt, q)$ of rank $r'k$, obtained from subspaces of $V(rt/r', q^{r'})$ of rank k, which intersect at least one spread element in a subspace of rank at least two. Let $W \in C$. Since W is a linear space over $GF(q^{r'})$, $\lambda W = W$, for all $\lambda \in GF(q^{r'}) \subset GF(q^r)$. If we look at $V(rt, q)$ as the tensor product $GF(q^r) \bigotimes GF(q^t)$, then it is clear what we mean by multiplying vectors of $V(rt, q)$ with an element λ of $GF(q)$, $GF(q^r)$ or $GF(q^t)$. For a pure tensor $v \otimes w$ for example we write $\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w)$ for $\lambda \in GF(q)$, $\lambda(v \otimes w) = (\lambda v) \otimes w$ for $\lambda \in GF(q^r)$, $\lambda(v \otimes w) = v \otimes (\lambda w)$ for $\lambda \in GF(q^t)$. This induces a linear multiplication on the tensor product $GF(q^r) \bigotimes GF(q^t)$ by elements of $GF(q^r)$ and $GF(q^t)$. To avoid confusion we write multiplication with elements of $GF(q^r)$ on the left and multiplication with elements of $GF(q^t)$ on the right. A vector $u \in GF(q^r) \bigotimes GF(q^t)$ is contained in the spread element $\{u\alpha \parallel \alpha \in GF(q^t)\}$. This implies that spread elements are fixed by elements of $GF(q^t)$. If $\beta \in GF(q^{r'}) \setminus GF(q)$ then

$$\{\beta u\alpha \parallel \alpha \in GF(q^t)\} \cap \{u\alpha \parallel \alpha \in GF(q^t)\} = \{0 \otimes 0\},$$

since $(r', t) = 1$. Moreover, the spread elements are permuted by elements of $GF(q^{r'})$. For every spread element P the set $\{\beta P \parallel \beta \in GF(q^{r'})\}$ contains exactly $\theta_{r'-1}(q)$ different spread elements. If W has an intersection of rank two with a spread element P then W will have an intersection of rank two with at least $\theta_{r'-1}(q)$ spread elements since the spaces $W \cap P$, $\lambda(W \cap P)$ and $(W \cap P)\mu$ have the same rank, for all $\lambda \in GF(q^r)^*$, $\mu \in GF(q^t)^*$. We count 4-tuples $(W, P, \vec{v}_1, \vec{v}_2)$, where $W \in C$, $P \in S$, and $\vec{v}_1$ and $\vec{v}_2$ are two independent vectors in the intersection of P and W, in two different ways. Starting with the number of spread elements, then counting the possibilities for $\vec{v}_1$ and $\vec{v}_2$ and then counting the number of elements of C containing $< \vec{v}_1, \vec{v}_2 >$, we get roughly

$$\theta_{r-1}(q^t)(q^t-1)(q^t-q) \begin{bmatrix} \frac{rt}{r'} - 2 \\ k-2 \end{bmatrix}_{q^{r'}} \simeq q^{(r'k-2r')(\frac{rt}{r'}-k)+rt+t}.$$

Starting with the number of elements of C, then choosing the spread element and then choosing $\vec{v}_1$ and $\vec{v}_2$ in their intersection, we get roughly

$$|C|\theta_{r'-1}(q)(q^2-1)(q^2-q) \simeq |C|q^{r'+3}.$$

The total number of subspaces of $V(rt/r', q^{r'})$ of rank k has order $q^{r'k(rt/r'-k)}$. If the order of $|C|$ is smaller than this, there must exist a scattered subspace of rank $r'k$. By computation there exists a scattered subspace of rank $r'k$ with respect to S if

$$r'k < \frac{rt - t + r' + 3}{2}.$$

By doing the computation in detail we see that there exists a scattered subspace if

$$\frac{(q^{t-1}-1)(q^{kr'}-1)(q^{kr'-r'}-1)}{(q^{r'}-1)(q^2-1)(q^{rt-r'}-1)} < 1.$$

This is satisfied if $r'k < \frac{rt-t+r'+3}{2}$ unless $r' = 1$ and $q = 2$, in which case $r'k < \frac{rt-t+r'+2}{2}$ implies the existence of a scattered subspace of rank $r'k$. This concludes the proof. □

In [3], A. Beutelspacher and J. Ueberberg give some combinatorial characterizations of normal spreads. In their paper they use the alternative name *geometric spread* for a normal spread. The following theorem follows from their results. The first part from [3, Section 2, Lemma 1], the second from their main theorem in [3]. Here we give an easier proof of the theorem.

Theorem 4.5 *Let S be a 2-spread in $V(2r, q)$ and let T be a maximum scattered subspace of rank m. Then*

$$\begin{cases} m = r & \text{if } S \text{ is a normal spread,} \\ m \geq r+1 & \text{otherwise.} \end{cases}$$

Proof : From Theorem 2.1 and Theorem 3.1 we get that $r \leq m \leq 2r-2$. Let S be a normal line-spread in $PG(2r-1, q)$ and suppose there exists a scattered r-dimensional subspace T_r. Let π be a $(r-1)$-dimensional subspace of T_r. There are $\theta_{r-1}(q)$ spread lines, say $l_1, \ldots, l_{\theta_{r-1}(q)}$, intersecting π. The numbers of r-dimensional spaces containing π in $PG(2r-1, q)$ is $\theta_{r-1}(q)$. Since T_r does not contain a spread line, there exist a pair i, j with $i \neq j$ such that $< \pi, l_i > = < \pi, l_j >$. This implies that $< \pi, l_i, l_j >$ is r-dimensional, so π intersects $< l_i, l_j >$ in a scattered plane. Since we assumed the spread to be normal this is a contradiction.

Suppose S is not a normal spread. There exist spread elements l_i, l_j, l_k such that l_k and $< l_i, l_j >$ intersect in a point P. In $< l_i, l_j >$ there are q^2+q+1 planes through P, at least $q+1$ of which must be scattered. Let π be such a scattered plane in $< l_i, l_j >$. Then it is clear that $< \pi, l_i > = < \pi, l_j >$. By Theorem 2.1 we can construct a scattered $(r-1)$-dimensional subspace T_{r-1} containing π. But then we have that $< T_{r-1}, l_i > = < T_{r-1}, l_j >$ and since the number of r-dimensional spaces containing T_{r-1} in $PG(2r-1, q)$ is equal to the number of spread lines intersecting T_{r-1} $(= \theta_{r-1}(q))$, there exists at least one r-dimensional scattered subspace containing T_{r-1}. This concludes the proof. □

We remark that for a normal spread Theorem 4.3 and Theorem 4.4 already implied the equality $m = r$ in Theorem 4.5.

5. Two intersection sets

In this section we want to say something more about the two intersection sets we obtained in Theorem 4.2. First we point out the relation between two intersection sets with respect to hyperplanes, two-weight linear codes and strongly regular graphs. For a more detailed survey of these objects we refer to [5].

A *q-ary linear code* C is a linear subspace of $GF(q)^n$. If C has dimension r, then C is called a $[n,r]$-code. A *generator matrix* G for a linear code C is an $(r \times n)$-matrix for which the rows are a basis of C. If G is a generator matrix for C then $C = \{xG \parallel x \in GF(q)^r\}$. The *weight* $w(c)$ of a codeword $c \in C$ is the number of non-zero coordinates of c or equivalently the Hamming distance between the all-zero codeword and c. If no two of the vectors defined by the columns of G are linearly dependent, then C is called *projective.*

Consider a two intersection set T with respect to hyperplanes in $PG(r-1,q)$ of size n, with intersection numbers h_1 and h_2. In [5], such a set is called a *projective* (n,r,h_1,h_2) *set.* We assume that the points of T span $PG(r-1,q)$. Put $T = \{(g_{1i},\ldots,g_{ri}) \parallel i = 1,\ldots n\}$. Let G be the $(r \times n)$-matrix with the points of T as columns. The points of T span $PG(r-1,q)$, hence the matrix G has rank r. The rows of G span an $[n,r]$-code C. Suppose that the j-th coordinate of a codeword, $c = (c_1,\ldots,c_n) = (x_1,\ldots,x_r)G$, is zero. That is

$$c_j = \sum_{i=1}^{r} x_i g_{ij} = 0.$$

This is equivalent with saying that the point with coordinates $(g_{1j},\ldots,g_{rj})$ lies on the hyperplane of $PG(r-1,q)$, with equation

$$\sum_{i=1}^{r} x_i X_i = 0.$$

Since T is a projective (n,r,h_1,h_2) set, the number of zeros in a codeword is either h_1 or h_2. This implies that C is a two-weight code with weights $w_1 = n-h_1$ and $w_2 = n-h_2$. Conversely, we can start with a two-weight linear code and obtain a two intersection set. We have the following correspondence.

Theorem 5.1 *1. If the code C is a q-ary projective two-weight $[n,r]$ code, then the points defined by the columns of a generator matrix of C form a projective $(n,r,n-w_1,n-w_2)$ set that spans $PG(r-1,q)$.*

2. Conversely, if the columns of a matrix G are the points of a projective (n,r,h_1,h_2) set that spans $PG(r-1,q)$, then the code C, with G as a generator matrix, is a q-ary projective two-weight $[n,r]$ code with weights $n-h_1$ and $n-h_2$.

Applying this to the two intersection set obtained in Theorem 4.2, we get a projective

$$\left(\frac{q^{\frac{rt}{2}}-1}{q-1}, r, \frac{q^{\frac{rt}{2}-t}-1}{q-1}, \frac{q^{\frac{rt}{2}-t+1}-1}{q-1}\right)$$

set which gives rise to a two-weight $[\frac{q^{\frac{rt}{2}}-1}{q-1}, r]$ code with weights

$$\begin{cases} w_1 &= q^{\frac{rt}{2}-t}\left(\frac{q^t-1}{q-1}\right), \\ w_2 &= q^{\frac{rt}{2}-t+1}\left(\frac{q^{t-1}-1}{q-1}\right). \end{cases}$$

We remark that the condition that the two intersection set has to span $PG(r-1,q^t)$ is satisfied because of Theorem 4.3. The parameters of the obtained two-weight codes correspond to $SU2$, $CY4$ and $RT1$ in [5], which arise from two intersection sets obtained in another way. If t is even, we can take the union of $(q^{t/2}-1)/(q-1)$ subgeometries $PG(r-1,q^{t/2})$ of $PG(r-1,q^t)$. If r is even, we can take the union of $(q^t-1)/(q-1)$ spread elements of a $(r/2-1)$-spread in $PG(r-1,q^t)$. In both cases, we obtain a two intersection set with the same parameters as the intersection set obtained in Theorem 4.2.

For the correspondence between two intersection sets with respect to hyperplanes and strong regular graphs, we refer to [5] and simply state the result.

Theorem 5.2 *A projective $(n,r,n-w_1,n-w_2)$ set for which the points span $PG(r-1,q)$ is equivalent with a strong regular graph for which the parameters (N,K,λ,μ) are given by*

$$\begin{cases} N &= q^r, \\ K &= n(q-1), \\ \lambda &= K^2+3K-q(w_1+w_2)-Kq(w_1+w_2)+q^2w_1w_2, \\ \mu &= \frac{q^2w_1w_2}{q^r} = K^2+K-Kq(w_1+w_2)+q^2w_1w_2. \end{cases}$$

We remark that since strong regular graphs with these parameters exist this theorem does not give us non existence results for scattered spaces.

6. Blocking sets

Here we only consider blocking sets in projective spaces. Blocking sets in affine spaces are far from equivalent to the blocking sets in projective spaces. For results concerning blocking sets in affine spaces, we refer to S. Ball [1].

An *s-fold blocking set with respect to k-dimensional subspaces in $PG(n,q)$* is a set of points, at least s on every k-dimensional subspace of $PG(n,q)$. A point of an s-fold blocking set with respect to k-dimensional subspaces which lies on a k-dimensional subspace intersecting the blocking set in exactly s points, is called *essential*. If every point contained in the s-fold blocking set is essential, then we say that the s-fold blocking set is *minimal* or *irreducible*. This is equivalent with saying that no proper subset of the s-fold blocking set is itself an s-fold blocking set. If $k=n-1$, then we omit the words "with respect to $(n-1)$-dimensional subspaces". If $s=1$, then we simply speak of a *blocking set*, otherwise they are sometimes called *multiple blocking sets*. If a blocking set contains an $(n-k)$-dimensional subspace then we call the blocking set *trivial*. Here, we will only consider non-trivial blocking sets, and from now on with a blocking set we mean a non-trivial blocking set. One example of a blocking set in $PG(n,q)$ is a blocking set in a plane of $PG(n,q)$. On the other hand if B is a blocking set in $PG(n,q)$, then we can project B from a point not in B on to a hyperplane. Since this projection will then be a blocking set in that hyperplane, it follows that the size of the smallest blocking set with respect to hyperplanes, will be at least the size of the smallest blocking set in a plane. Moreover, this implies that the smallest blocking sets in $PG(n,q)$ are the smallest minimal blocking sets in a plane.

In [7] U. Heim introduced a *proper blocking set* as a blocking set in $PG(n,q)$ not containing a blocking set in a hyperplane of $PG(n,q)$. In $PG(r-1,q^t)$, we can always construct a proper blocking set if $t>r-2$, with $r\geq 3$. To do this, we use Theorem 2.1, with the extra property that we always choose a vector that lies in a spread element, which corresponds with a point in $PG(r-1,q^t)$ that is independent from the points corresponding with the previously intersected spread elements, as long as that is possible. In this way we can construct a scattered t-dimensional subspace W of $PG(rt-1,q)$, with the additional property that $B(W)$ is a minimal blocking set not contained in a hyperplane.

If ℓ is a line and B a blocking set in $PG(2,q)$ then ℓ intersects B in at most $|B|-q$ points. If B is a blocking set in $PG(2,q)$ of size $q+m$, and there is a line ℓ intersecting B in exactly m points, then we say that B is *of Rédei type*, and ℓ is called a *Rédei line*. For a long time all examples of small minimal blocking sets were of Rédei type, but in 1997 O. Polito and P. Polverino [11] constructed small minimal blocking sets which are not of Rédei type. The examples they constructed are of a special type of blocking sets, namely *linear blocking sets*. They are called that way because they arise from a linear subspace of a higher dimensional space over a smaller field. The construction uses the correspondence between the points of $PG(2,q^t)$ and the spread elements of a normal $(t-1)$-spread of $PG(3t-1,q)$, which is given at the beginning of Section 4. Using the concept of linear blocking sets and scattered subspaces, S. Ball and the authors [2] constructed a class of $(q+1)$-fold blocking sets in $PG(2,q^4)$ which are not the union of $q+1$ Bear subplanes. In terms of (m,n)-sets [10] this gives rise to a set of $(q+1,q^2+q+1)$-sets in $PG(2,q^4)$. The following theorem states what type of blocking sets we get using scattered spaces.

Theorem 6.1 *A scattered subspace W of rank m, with respect to a normal t-spread, in $V(rt,q)$ induces a $(\theta_{k-1}(q))$-fold blocking set, with respect to $(\frac{rt-m+k}{t}-1)$-dimensional subspaces in $PG(r-1,q^t)$, of size $\theta_{m-1}(q)$, where $1 \le k \le m$ such that $t \mid m-k$.*

Proof : Let U be an $(\frac{rt-m+k}{t}-1)$-dimensional subspace in $PG(r-1,q^t)$. Then U induces a $(rt-m+k-1)$-dimensional subspace in $PG(rt-1,q)$, which intersects an $(m-1)$-dimensional subspace in a subspace of dimension at least $k-1$. The rest of the proof follows from the fact that W is scattered. □

Acknowledgement. The authors would like to thank Simeon Ball for helpful discussions and comments on the article.

References

[1] S. Ball, On intersection sets in Desarguesian affine spaces, manuscript.

[2] S. Ball, A. Blokhuis, M. Lavrauw, Linear $(q+1)$-fold blocking sets in $PG(2,q^4)$. *Finite Fields Appl.*, to appear.

[3] A. Beutelspacher, J. Ueberberg, A characteristic property of geometry t-spreads in finite projective spaces. *European J. Combin.* **12** (1991), 277-281.

[4] P. J. Cameron, Projective and Polar spaces. Queen Mary & Westfield College math notes 13.

[5] R. Calderbank, W. M. Kantor, The geometry of two-weight codes. *Bull. London Math. Soc.* **18** (1986), 97–122.

[6] L. R. Casse, C. M. O'Keefe, Indicator sets for t-spreads of $PG((s+1)(t+1)-1,q)$. *Boll. Un. Mat. Ital. B (7)* **4** (1990), 13–33.

[7] U. Heim, Proper blocking sets in projective spaces. *Discrete Math.* **174** (1997), 167–176.

[8] M. Limbos, A characterization of the embeddings of $PG(m,q)$ into $PG(n,q^r)$. *J. Geom.* **16** (1981), 50–55.

[9] G. Lunardon, Normal spreads. *Geom. Dedicata* **75** (1999), 245–261.

[10] T. Penttila, G. F. Royle, Sets of type (m, n) in the affine and projective planes of order nine. *Des. Codes Cryptogr.* **6** (1995), no. 3, 229–245.

[11] P. Polito, O. Polverino, On small blocking sets. *Combinatorica* **18** (1998), 1–5.

[12] B. Segre, Teoria di Galois, fibrazioni proiettive e geometrie non Desarguesiane. *Ann. Mat. Pura Appl.* **64** (1964), 1-76.