Discrete Mathematics 310 (2010) 3096–3107

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Linear sets in finite projective spaces

Olga Polverino

Seconda Università degli Studi di Napoli, Dipartimento di Matematica, via Vivaldi 43, I-81100 Caserta, Italy

ARTICLE INFO

Article history:
Received 3 September 2008
Accepted 6 April 2009
Available online 13 May 2009

Keywords:
Finite field
Projective space
Subgeometry

ABSTRACT

In this paper linear sets of finite projective spaces are studied and the "dual" of a linear set is introduced. Also, some applications of the theory of linear sets are investigated: blocking sets in Desarguesian planes, maximum scattered linear sets, translation ovoids of the Cayley Hexagon, translation ovoids of orthogonal polar spaces and finite semifields. Besides "old" results, new ones are proven and some open questions are discussed.

1. Introduction

A *linear set* of a projective space $\Omega = PG(V, \mathbb{F}_q)$ is a set of points whose defining vectors belong to an additive subgroup of V. Linear sets generalize the concept of subgeometry of a projective space; in fact, they can be characterized by mean of projection of subgeometries and preserve many of their properties. The term *linear* (used with this meaning) first appears in [40], where G. Lunardon constructs some examples of blocking sets, in the linear representation of Galois planes. These blocking sets were called, for this reason, linear blocking sets.

Probably, the very first example of linear set, which is not a subgeometry, appearing in the literature, can be found in [17] where Brouwer and Wilbrink construct, by using the André/Bruck and Bose representation of a projective Galois plane, examples of blocking sets of Rédei type which, in fact, are linear sets.

Linear sets have been intensively used in recent years to construct or characterize a wide variety of geometrical objects: blocking sets or multiple blocking sets in projective finite spaces [41,58,59,47,5,48,60,15], two-intersection sets in projective finite spaces [11,12], translation spreads of the Cayley Generalized Hexagon $H(q)$ [19,49,16], translation ovoids of polar spaces [50,23,3], semifield flocks [6,20,37] and finite semifields [42,21,51,33,34,52,43,25,26].

Although, it seems to us that, so far, the theory of linear sets has never been homogeneously treated in a proper way anywhere. Section 2 of this article fills this gap by presenting all the known results in a uniform and homogeneous way and generalizing some of them. Also, we will study dual linear sets obtained from a given linear set of a projective space by using polarities of the space.

In the other sections we deal with some applications of the theory: blocking sets in Desarguesian planes, maximum scattered linear sets, translation ovoids of the Cayley Hexagon, translation ovoids of orthogonal polar spaces and finite semifields.

Besides "old" results, new ones will be proven and some open questions will be discussed.

2. Linear sets and dual linear sets

Let $\Omega = PG(V, \mathbb{F}_{q^n}) = PG(r-1, q^n)$, $q = p^h$, p prime, and let L be a set of points of Ω. The set L is said an $\mathbb{F}_q$-*linear* set of Ω of rank t if it is defined by the non-zero vectors of an $\mathbb{F}_q$-vector subspace U of V of dimension t, i.e.,

$$L = L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}.$$

E-mail addresses: olga.polverino@unina2.it, opolveri@unina.it.

0012-365X/$ – see front matter
doi:10.1016/j.disc.2009.04.007

Let $PG(rn-1,q)=PG(V,\mathbb{F}_q)$ and note that each point P of Ω defines an $(n-1)$-dimensional subspace X_P of $PG(rn-1,q)$ and that $\mathcal{S}=\{X_P : P\in\Omega\}$ is a Desarguesian spread[1] of $PG(rn-1,q)$ (see, e.g., [40]). Also, the incidence structure $(\mathcal{S},\mathcal{L})$ whose points are the elements of $\mathcal{S}$ and whose lines are the $(2n-1)$-dimensional subspaces spanned by two elements of $\mathcal{S}$ is isomorphic to Ω; $(\mathcal{S},\mathcal{L})$ is the so called *linear representation* of Ω over $\mathbb{F}_q$. A t-dimensional $\mathbb{F}_q$-vector subspace U of V defines in $PG(rn-1,q)$ a $(t-1)$-dimensional projective subspace $P(U)$ and the linear set L_U of Ω can be seen as the set of points P of Ω such that $X_P\cap P(U)\neq\emptyset$, i.e. $L_U=\{P\in\Omega : X_P\cap P(U)\neq\emptyset\}$.

Any subspace of Ω is an $\mathbb{F}_q$-linear set; precisely, if $\Lambda=PG(W,\mathbb{F}_{q^n})$ is a subspace of Ω of dimension s, then Λ is an $\mathbb{F}_q$-linear set of Ω of rank $(s+1)n$. Also, if L_U is an $\mathbb{F}_q$-linear set, then $L_U\cap\Lambda=L_{W\cap U}$ is an $\mathbb{F}_q$-linear set as well and $L_U=L_{\lambda U}$ for each non-zero $\lambda\in\mathbb{F}_{q^n}$. The following property can be easily verified.

Property 2.1. *If f is an invertible semilinear map of V and ϕ is the collineation of Ω induced by f, then $L_U^{\phi}=L_{f(U)}$, i.e. the linear sets L_U and $L_{f(U)}$ are projectively equivalent.*

If L_U is an $\mathbb{F}_q$-linear set of Ω of rank t and $\Lambda=PG(W,\mathbb{F}_{q^n})$ is a subspace of Ω of dimension s, we say that Λ has *weight* i with respect to L_U if $\dim_{\mathbb{F}_q}(W\cap U)=i$ (i.e., the $\mathbb{F}_q$-linear set $L_{W\cap U}=\Lambda\cap L_U$ has rank i), and we write $w_{L_U}(\Lambda)=i$ or $w(\Lambda)=i$ for short. Note that $0\le w(\Lambda)\le\min\{t,(s+1)n\}$ and that a point P of Ω belongs to L_U if and only if $w(P)\ge 1$. Denoting by x_i the number of points of L_U of weight i, we easily get the following proposition.

Proposition 2.2. *If L_U is an $\mathbb{F}_q$-linear set of $\Omega=PG(r-1,q^n)$ of rank $t>0$, then*

$$|L_U|=x_1+x_2+\cdots+x_n, \tag{1}$$

$$x_1+(q+1)x_2+\cdots+(q^{n-1}+\cdots+q+1)x_n=q^{t-1}+q^{t-2}+\cdots+q+1, \tag{2}$$

$$|L_U|\le q^{t-1}+q^{t-2}+\cdots+q+1, \tag{3}$$

$$|L_U|\equiv 1\ (\mathrm{mod}\ q). \tag{4}$$

Hence, if Λ is a subspace of Ω and $L_U\cap\Lambda\neq\emptyset$, then

$$|L_U\cap\Lambda|\equiv 1\ (\mathrm{mod}\ q). \tag{5}$$

Also, the following property concerning the weight of subspaces holds true.

Property 2.3. *Let L_U be an $\mathbb{F}_q$-linear set of $\Omega=PG(r-1,q^n)=PG(V,\mathbb{F}_{q^n})$ of rank t and let $\Lambda=PG(W,\mathbb{F}_{q^n})$ be a subspace of Ω of dimension s. Then $\Lambda\subseteq L_U$ if and only if the weight of Λ with respect to L_U is at least $sn+1$.*

Proof. Let $s>0$. If $\Lambda\subseteq L_U$, then $\Lambda\subseteq L_{U\cap W}$. Indeed, if $P\in\Lambda\subseteq L_U$, then there exist $\mathbf{w}\in W\setminus\{\mathbf{0}\}$ and $\mathbf{u}\in U\setminus\{\mathbf{0}\}$ such that $P=\langle\mathbf{w}\rangle_{\mathbb{F}_{q^n}}=\langle\mathbf{u}\rangle_{\mathbb{F}_{q^n}}$. Hence $\mathbf{w}=\lambda\mathbf{u}$ for some $\lambda\in\mathbb{F}_{q^n}^*$ and this implies that $P\in L_{\lambda(U\cap W)}=L_{U\cap W}$. Suppose, by way of contradiction, that $w(\Lambda)\le sn$. Then by (3) of Proposition 2.2 we get

$$q^{ns}+q^{n(s-1)}+\cdots+q^n+1=|\Lambda|\le|L_{W\cap U}|\le q^{sn-1}+q^{sn-2}+\cdots+q+1,$$

which gives a contradiction. Conversely, suppose that $w(\Lambda)\ge sn+1$ and let $P=\langle\mathbf{w}\rangle_{\mathbb{F}_{q^n}}$ be a point of Λ with $\mathbf{w}\in W\setminus\{\mathbf{0}\}$. Note that $\langle\mathbf{w}\rangle_{\mathbb{F}_{q^n}}\cap U=\langle\mathbf{w}\rangle_{\mathbb{F}_{q^n}}\cap(W\cap U)$. Since $\langle\mathbf{w}\rangle_{\mathbb{F}_{q^n}}$ and $W\cap U$ are $\mathbb{F}_q$-subspaces of W of dimension n and at least $sn+1$ respectively, their intersection has dimension at least one, i.e. $w(P)\ge 1$, hence $P\in L_U$. □

If $\dim_{\mathbb{F}_q}U=\dim_{\mathbb{F}_{q^n}}V=r$ and $\langle U\rangle_{\mathbb{F}_{q^n}}=V$, we will say that $L_U\cong PG(U,\mathbb{F}_q)$ is a *canonical subgeometry* of $\Omega=PG(V,\mathbb{F}_{q^n})$. Note that in such a case each point of L_U has weight 1 and hence $|L_U|=q^{r-1}+q^{r-2}+\cdots+1$.

In [50], Lunardon and Polverino, generalizing the results of [41,46], give a characterization of $\mathbb{F}_q-$linear sets in terms of projection of canonical subgeometries.

Let $\Sigma=PG(m,q)$ be a canonical subgeometry of $\Sigma^*=PG(m,q^n)$ and suppose there exists an $(m-r)$-dimensional subspace Ω^* of Σ^* disjoint from Σ. Let $\Omega=PG(r-1,q^n)$ be an $(r-1)$-dimensional subspace of Σ^* disjoint from Ω^*, and let Γ be the *projection* of Σ from Ω^* to Ω, i.e.

$$\Gamma=\{y=\langle\Omega^*,x\rangle\cap\Omega \mid x\in\Sigma\}.$$

We call Ω^* and Ω the *center* and the *axis* of the projection respectively.

Let $\mathbf{p}_{\Omega^*,\Omega,\Sigma}$ be the map from Σ to Γ defined by $x\mapsto\langle\Omega^*,x\rangle\cap\Omega$ for each point x of Σ. By definition $\mathbf{p}_{\Omega^*,\Omega,\Sigma}$ is surjective and $\Gamma=\mathbf{p}_{\Omega^*,\Omega,\Sigma}(\Sigma)$.

Theorem 2.4 (*[50]*)**.** *If Γ is a projection of $PG(m,q)$ into $\Omega=PG(r-1,q^n)$, then Γ is an $\mathbb{F}_q-$ linear set of Ω of rank $m+1$ and $\langle\Gamma\rangle=\Omega$. Conversely, if L is an $\mathbb{F}_q-$ linear set of Ω of rank $m+1$ and $\langle L\rangle=\Omega=PG(r-1,q^n)$, then either L is a canonical subgeometry of Ω or there are an $(m-r)-$ dimensional subspace Ω^* of $\Sigma^*=PG(m,q^n)$ disjoint from Ω and a canonical subgeometry Σ of Σ^* disjoint from Ω^* such that $L=\mathbf{p}_{\Omega^*,\Omega,\Sigma}(\Sigma)$.*

[1] An $(n-1)$-spread $\mathcal{S}$ of $PG(rn-1,q)$ is said to be *Desarguesian* if the $2-(q^{rn},q^n,1)$ design obtained from $\mathcal{S}$, in the Barlotti-Cofman construction, is isomorphic to $AG(r,q^n)$.

Let $\sigma : V \times V \longrightarrow \mathbb{F}_{q^n}$ be a non-degenerate reflexive sesquilinear form on the r-dimensional vector space V over $\mathbb{F}_{q^n}$ and let [2]

$$\sigma' : (\mathbf{u}, \mathbf{v}) \in V \times V \longrightarrow Tr_{q^n/q}(\sigma(\mathbf{u}, \mathbf{v})) \in \mathbb{F}_q. \tag{6}$$

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 $\perp$ and $\perp'$ be the orthogonal complement maps defined by σ and σ' on the lattices of the $\mathbb{F}_{q^n}$-subspaces and the $\mathbb{F}_q$-subspaces of V, respectively. Also, denote by τ and τ' the polarities of $PG(V, \mathbb{F}_{q^n})$ and $PG(V, \mathbb{F}_q)$ arising from σ and σ', respectively. Recall that if W is an $\mathbb{F}_{q^n}$-subspace of V and U is an $\mathbb{F}_q$-subspace of V then $\dim_{\mathbb{F}_{q^n}} W^{\perp} + \dim_{\mathbb{F}_{q^n}} W = r$ and $\dim_{\mathbb{F}_q} U^{\perp'} + \dim_{\mathbb{F}_q} U = rn$. Also, it is easy to see that $W^{\perp} = W^{\perp'}$ for each $\mathbb{F}_{q^n}$-subspace W of V (for more details see [70]).

Let L_U be an $\mathbb{F}_q$-linear set of rank t of $\Omega = PG(V, \mathbb{F}_{q^n}) = PG(r-1, q^n)$. Let σ be a non-degenerate reflexive sesquilinear form on V over $\mathbb{F}_{q^n}$ and let σ' be the associated sesquilinear form on V over $\mathbb{F}_q$ defined as in (6). Since $U^{\perp'}$ is an $\mathbb{F}_q$-linear subspace of V of dimension $rn - t$, it defines an $\mathbb{F}_q$-linear set $L_{U^{\perp'}}$ of Ω of rank $rn - t$. We will denote $L_{U^{\perp'}}$ by the symbol L_U^{τ} and we will say that L_U^{τ} is the *dual linear set of* L_U *with respect to the polarity* τ induced by σ. Such a linear set does not depend on τ. Indeed, let σ and σ_1 be non-degenerate reflexive sesquilinear forms on V over $\mathbb{F}_{q^n}$, let $\perp$ and $\perp_1$ be the associated orthogonal complement maps and let τ and τ_1 be the polarities associated with $\perp$ and $\perp_1$, respectively. Let U be an $\mathbb{F}_q$-vector subspace of V and let $\perp'$ and $\perp'_1$ be the orthogonal complement maps arising from σ' and σ'_1, respectively. Then, it is easy to see that $\perp\ \perp_1$ defines an invertible semilinear map f of V over $\mathbb{F}_{q^n}$ such that

$$f(U^{\perp'}) = (U^{\perp'})^{\perp'\perp'_1} = U^{\perp'_1}.$$

Now, recalling that $L_U^{\tau} = L_{U^{\perp'}}$ and $L_U^{\tau_1} = L_{U^{\perp'_1}}$, by Property 2.1 we have

Proposition 2.5. *The dual linear sets L_U^{τ} and $L_U^{\tau_1}$ are projectively equivalent.*

The following property provides us with a relation between the weight of a subspace with respect to a linear set and the weight of its polar space with respect to the dual linear set.

Property 2.6. *If $\Lambda_s = PG(W, \mathbb{F}_{q^n})$ is an s-dimensional projective subspace of $\Omega = PG(r-1, q^n)$ and L_U is an $\mathbb{F}_q$-linear set of Ω of rank t, then*

$$w_{L_U^{\tau}}(\Lambda_s^{\tau}) - w_{L_U}(\Lambda_s) = rn - t - (s+1)n. \tag{7}$$

Proof. Recall that $w_{L_U^{\tau}}(\Lambda_s^{\tau}) = \dim_{\mathbb{F}_q}(W^{\perp} \cap U^{\perp'})$ and that $w_{L_U}(\Lambda_s) = \dim_{\mathbb{F}_q}(W \cap U)$. Since $W^{\perp} \cap U^{\perp'} = W^{\perp'} \cap U^{\perp'} = (\langle W, U\rangle_{\mathbb{F}_q})^{\perp'}$, we get

$$\dim_{\mathbb{F}_q}(W^{\perp} \cap U^{\perp'}) = rn - \dim_{\mathbb{F}_q}\langle W, U\rangle_{\mathbb{F}_q} = rn - t - (s+1)n + \dim_{\mathbb{F}_q}(W \cap U).$$

Now, Equality (7) immediately follows. □

Finally, we explicitly note that a linear set and its dual can have very different geometric structures as shown in the following property.

Property 2.7. *Let L_U be an $\mathbb{F}_q$-linear set of $\Omega = PG(r-1, q^n)$ and let $\Lambda = PG(W, \mathbb{F}_{q^n})$ be an s-dimensional subspace of Ω. Then $L_U \subseteq \Lambda$ if and only if Λ^{τ} has maximum weight $rn - (s+1)n$ with respect to L_U^{τ}. In this case, the dual linear set L_U^{τ} is a union of $(r-s-1)$-dimensional subspaces of Ω passing through the $(r-s-2)$-dimensional subspace Λ^{τ} of Ω.*

Proof. If $L_U \subseteq \Lambda$, then $U \subseteq W$ and hence $U^{\perp'} \supseteq W^{\perp'} = W^{\perp}$. This implies that $w_{L_U^{\tau}}(\Lambda^{\tau}) = \dim_{\mathbb{F}_q}(W^{\perp} \cap U^{\perp'}) = \dim_{\mathbb{F}_q} W^{\perp} = rn-(s+1)n$, and in particular $\Lambda^{\tau} \subseteq L_U^{\tau}$. In this case, let $P \in L_U^{\tau} \setminus \Lambda^{\tau}$ and note that $w_{L_U^{\tau}}(\langle P, \Lambda^{\tau}\rangle) \geq (r-s-1)n+1$. Hence by Property 2.3, we have that $\langle P, \Lambda^{\tau}\rangle \subseteq L_U^{\tau}$. This implies that L_U^{τ} is a union of $(r-s-1)$-dimensional subspaces containing Λ^{τ}. Conversely, suppose that $w_{L_U^{\tau}}(\Lambda^{\tau}) = rn-(s+1)n$, then $W^{\perp} = W^{\perp'} \subseteq U^{\perp'}$, hence $U \subseteq W$, i.e. $L_U \subseteq \Lambda$. □

3. Application 1: Linear blocking sets and scattered linear sets

3.1. Linear blocking sets

A *blocking set* B in the projective plane $PG(2, q)$, $q = p^h$, p prime, is a set of points meeting every line of $PG(2, q)$. B is called *trivial* if it contains a line, and it is called *minimal* if no proper subset of it is a blocking set. We say B *small* when its size is less than $\frac{3(q+1)}{2}$ and we call B of *Rédei type* if there exists a line l of the plane such that $|B \setminus l| = q$. The line l is called a *Rédei line* of B. The *exponent* of B is the maximal integer e $(0 \leq e \leq h)$ such that $|l \cap B| \equiv 1 (mod\, p^e)$ for every line l in

[2] The symbol $Tr_{q^n/q}$ denotes the trace function of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

$PG(2, q)$. In [67], T. Szőnyi proves that a small minimal blocking set of $PG(2, q)$ has positive exponent. For an excellent survey on minimal blocking sets in $PG(2, q)$ we refer to [68].

For a long time all known examples of small minimal blocking sets were of Rédei type. All of these examples belong to a family of blocking sets, called linear, introduced by G. Lunardon (see [40,41]). In [58], Polito and Polverino find, in the family of linear blocking sets, the first examples of small minimal blocking sets not of Rédei type.

Let $\pi = PG(2, q) = PG(V, \mathbb{F}_q)$, let $\mathbb{F}_{q'}$ be a subfield of $\mathbb{F}_q$ with $q = q'^n$ and let U be an $\mathbb{F}_{q'}$-subspace of V of dimension $n + 1$. If $\ell = PG(W, \mathbb{F}_q)$ is a line of π, then by the Grassmann relation we get $w_{L_U}(\ell) = \dim_{\mathbb{F}_q}(W \cap U) \geq 1$, i.e. $\ell \cap L_U \neq \emptyset$ for each line ℓ of π. Hence $B := L_U$ is a blocking set of π and, by [58, Corollary 1], it is a small minimal blocking set, called *$\mathbb{F}_{q'}$-linear blocking set*. If B is an $\mathbb{F}_{q'}$-linear blocking set ($q' = p^e$, p prime), then each line of π intersects B in a number of points congruent to 1 modulo q' (see (5) of Proposition 2.2), hence the exponent of B is at least e.

In $PG(2, q)$ the only $\mathbb{F}_q$-linear blocking sets are the lines. In the planes $PG(2, q^2)$ and $PG(2, q^3)$, the $\mathbb{F}_q$-linear blocking sets are classified: in $PG(2, q^2)$ they are Baer subplanes and in $PG(2, q^3)$ they are isomorphic either to the blocking set obtained from the graph of the trace function of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$ or to the blocking set obtained from the graph of the function $x \to x^q$ (see [61]). All of these are Rédei type blocking sets. The $\mathbb{F}_q$-linear blocking sets in the plane $PG(2, q^4)$ are classified in [15], where, in the table at the end of the paper, all the $\mathbb{F}_q$-linear blocking sets of $PG(2, q^4)$, up to isomorphisms, are listed. Such a table shows that there are a lot of non-isomorphic families of $\mathbb{F}_q$-linear blocking sets in $PG(2, q^4)$, both of Rédei and of non-Rédei type.

In [66], Sziklai conjectures (Linearity Conjecture) that *every small minimal blocking set of $PG(2, q)$ is linear.*[3]

The Linearity Conjecture has been already proved in some cases. Precisely, in the plane $PG(2, p)$ (here there is no small non-trivial blocking set) (Blokhius [10]), in $PG(2, p^2)$ (Szőnyi [67]), in $PG(2, p^3)$ ($p \geq 7$) (Polverino [62]), in $PG(2, q^3)$ ($q = p^h$, p prime, $p \geq 7$) for small minimal blocking sets with exponent $e \geq h$ (Polverino–Storme [63]) and in $PG(2, q)$ ($q = p^h$, $p > 2$ prime) for small minimal blocking sets of Rédei type (Blokhius–Ball–Brouwer–Storme–Szőnyi [9], Ball [4]).

Also, in [66] the author proves that a small minimal blocking set of $PG(2, q)$ is "very close" to be a linear blocking set showing that

Theorem 3.1 (*[66, Theorem 4.16]*). *If B is a small minimal blocking set of $PG(2, q)$, $q = p^h$, with exponent e and for a certain line $|\ell \cap B| = p^e + 1$, then $\mathbb{F}_{p^e}$ is a subfield of $\mathbb{F}_q$ and $\ell \cap B$ is $\mathbb{F}_{p^e}$-linear.*

If the Linearity Conjecture held true, the classification of linear blocking sets would imply the classification of small minimal blocking sets. For this reason it can be useful to give an alternative description of the isomorphism relation between linear blocking sets.

To this aim, remind that an $\mathbb{F}_q$-linear blocking set B of $\pi = PG(2, q^n)$, $n > 2$, can be also constructed as the projection of a canonical subgeometry $\Sigma \simeq PG(n, q)$ of $\Sigma^* = PG(n, q^n)$ to π from an $(n - 3)$-dimensional subspace Λ of Σ^*, disjoint from Σ (Theorem 2.4). In this case we write $B = B_{\Lambda,\pi,\Sigma}$. Also, if π_Λ is the quotient geometry of Σ^* on Λ, then $B_{\Lambda,\pi,\Sigma}$ is isomorphic to the $\mathbb{F}_q$-linear blocking set $B_{\Lambda,\Sigma}$ in π_Λ consisting of all $(n-2)$-dimensional subspaces of Σ^* containing Λ and with non-empty intersection with Σ. In [15], the following has been proven.

Theorem 3.2 (*[15, Theorem 2.4]*). *Two $\mathbb{F}_q$-linear blocking sets, $B_{\Lambda,\Sigma}$ and $B_{\Lambda',\Sigma'}$, with exponent e of the planes π_Λ and $\pi_{\Lambda'}$ respectively, constructed in $\Sigma^* = PG(n, q^n)$ ($n > 2$), are isomorphic if and only if there exists a collineation φ of Σ^* mapping Λ to Λ' and Σ to Σ'.*

The above result leads, in [15], to a complete classification of all $\mathbb{F}_q$-linear blocking sets in $PG(2, q^4)$.

We conclude this section remarking that, as it appears from the previous discussion, the most interesting open problems in this area seem to be the following:

- Prove or disprove the Linearity Conjecture.
- Attempt a classification of some families of linear blocking sets: for instance, linear blocking sets of maximum (minimum) size.

As regards the first point, we note that there is a more general version of the Linearity Conjecture concerning t-fold blocking sets. A *t-fold blocking set* in $PG(n, q)$ with respect to k-subspaces is a set of points which intersects each k-subspace in at least t points. The Linearity Conjecture for t-fold blocking sets with respect to k-subspaces says that

In $PG(n, q)$ any t-fold blocking set B, with respect to k-dimensional subspaces, is the union of linear sets $B_1, B_2, \ldots, B_s$, where B_i is a t_i-fold blocking set with respect to k-dimensional subspaces and $t_1 + t_2 + \cdots + t_s = t$; provided t and $|B|$ are "small enough" (*i.e., $t \leq T(n, q, k)$ and $|B| \leq S(n, q, k)$ for suitable functions T and S*).

The results contained in [65,64,69,14,77,13] provide some evidence that the above conjecture holds true.

3.2. Scattered linear sets

An $\mathbb{F}_q$-linear set L_U of rank t of a projective space $\Omega = PG(V, \mathbb{F}_{q^n}) = PG(r - 1, q^n)$ is said to be a *scattered linear set* if each point of L_U has weight 1 with respect to L_U. By (1) and (2) of Proposition 2.2, L_U is a scattered linear set if and only if it has maximum size $q^{t-1} + q^{t-2} + \cdots + q + 1$. If L_U is a scattered linear set of Ω, then the projective subspace $P(U)$ of

[3] In [66] the linearity conjecture is more general and involves small blocking sets of $PG(n, q)$ with respect to k-subspaces.

$PG(V, \mathbb{F}_q) = PG(rn-1, q)$ intersects each element of the Desarguesian spread $\mathcal{S}$ of the $\mathbb{F}_q$-linear representation of Ω in at most one point. So $P(U)$ is a *scattered space with respect to* $\mathcal{S}$. Scattered spaces with respect to a spread are introduced by Blokhuis and Lavrauw in [11], where scattered spaces of highest possible dimension (*maximum scattered spaces*) are investigated. So the study of maximum scattered spaces of $PG(rn-1, q)$ with respect to a Desarguesian $(n-1)$-spread is equivalent to the study of scattered $\mathbb{F}_q$-linear sets of $PG(r-1, q^n)$ of maximum rank (*maximum scattered* $\mathbb{F}_q$*-linear sets*).

The main result obtained in [11] (see also [38]) in terms of scattered linear sets is

Theorem 3.3 (*[11]*). *If L_U is a maximum scattered $\mathbb{F}_q$-linear set of $PG(r-1, q^n)$ of rank t, then*

$$t = \frac{rn}{2} \quad \text{if } r \text{ is even},$$
$$\frac{rn-n}{2} \le t \le \frac{rn}{2} \quad \text{if } r \text{ is odd}.$$

Also, if rn is even and L_U is a maximum scattered $\mathbb{F}_q$-linear set of $PG(r-1, q^n)$ of rank $\frac{rn}{2}$, then L_U is a two-intersection set (with respect to hyperplanes) in $PG(r-1, q^n)$ with intersection numbers $q^{\frac{rn}{2}-n-1} + \cdots + q + 1$ and $q^{\frac{rn}{2}-n} + \cdots + q + 1$.

By the previous theorem if r is even there always exists a scattered subspace of rank $\frac{rn}{2}$ (see [38, Theorem 2.5.5] for an explicit example). Also, if $r = 3$ and $n = 4$ an example of scattered linear set of the plane $PG(2, q^4)$ of maximum rank 6 is constructed in [5]. All these examples produce two-intersection sets and hence two-weight codes and strongly regular graphs (see [18]). The maximum scattered linear set of $PG(2, q^4)$ constructed in [5] also produces a $(q+1)$-fold blocking set of size $(q+1)(q^4+q^2+1)$ which is not the union of $(q+1)$ disjoint Baer subplanes. More generally

Theorem 3.4 (*[11]*). *A scattered linear set of rank t of $\Omega = PG(r-1, q^n)$ is a $\frac{q^k-1}{q-1}$-fold blocking set, with respect to $(\frac{rn-t+k}{n}-1)$-dimensional subspaces, of size $\frac{q^t-1}{q-1}$, where $1 \le k \le t$ such that $n \mid (t-k)$.*

As an application of the theory of dual linear sets we are able to prove

Theorem 3.5. *If rn is even and L_U is a maximum scattered $\mathbb{F}_q$-linear set of $\Omega = PG(r-1, q^n)$ of rank $\frac{rn}{2}$, then the dual linear set L_U^τ with respect to any polarity of Ω is a maximum scattered $\mathbb{F}_q$-linear set of Ω as well.*

Proof. Let τ be a polarity of $\Omega = PG(V, \mathbb{F}_{q^n}) = PG(r-1, q^n)$ arising from the non-degenerate reflexive sesquilinear form σ on V over $\mathbb{F}_{q^n}$. By Theorem 3.3 the hyperplanes of Ω have weight $\frac{rn}{2}-n$ or $\frac{rn}{2}-n+1$ with respect to L_U. Then by Equality (7) the points of Ω have weight 0 or 1 with respect to L_U^τ, i.e. L_U^τ is a scattered linear set. Also, since $\dim_{\mathbb{F}_q} U^{\perp'} = rn - \frac{rn}{2} = \frac{rn}{2}$, the linear set L_U^τ has rank $\frac{rn}{2}$. Hence L_U^τ is a maximum scattered $\mathbb{F}_q$-linear set of Ω. □

By Proposition 2.5, L_U^τ does not depend on the polarity τ and we will say that L_U^τ is the *dual maximum scattered linear set* of the maximum scattered linear set L_U.

Hence, by Theorem 3.5 any known example of maximum scattered linear set produces another example of maximum scattered linear set by "duality".

In light of the previous results, one can ask whether examples of maximum scattered linear sets of rank $\frac{rn}{2}$ exist when r is odd. Also, it would be interesting to understand whether the examples produced under duality are isomorphic to the starting ones.

4. Application 2: Translation spreads in $H(q)$

The *split Cayley hexagon* $H(q)$ has been defined by Tits in [75] as follows. Let $Q(6, q)$ be the parabolic quadric of $PG(6, q)$ with equation $X_3^2 = X_0X_4 + X_1X_5 + X_2X_6$. The points of $H(q)$ are all the points of $Q(6, q)$. The lines of $H(q)$ are those lines of $Q(6, q)$ whose Grassmann coordinates satisfy the equations $p_{34} = p_{12}$, $p_{35} = p_{20}$, $p_{36} = p_{01}$, $p_{03} = p_{56}$, $p_{13} = p_{64}$ and $p_{23} = p_{45}$. Two elements of $H(q)$ are *opposite* if they are at distance 6 in the incidence graph of $H(q)$. A *spread* of $H(q)$ is a set of q^3+1 mutually opposite lines of $H(q)$.

Let L be a fixed line of $H(q)$ and denote by E^L the group of the automorphisms of $H(q)$ generated by all the collineations fixing L pointwise and stabilizing all the lines through some point of L. The group E^L has order q^5 and acts regularly on the set of the lines of $H(q)$ at distance 6 from L (see, e.g., [76]). A spread $\mathcal{S}$ of $H(q)$ containing L is a *translation spread*, with respect to L, if for each $x \in L$ there is a subgroup of E^L which preserves $\mathcal{S}$ and acts transitively on the lines of $\mathcal{S}$ at distance 4 from M, for all lines M of $H(q)$ incident with x and different from L (see [8]). By [54] it is possible to associate to any translation spread $\mathcal{S}$ with respect to a line of $H(q)$ a subfield of $\mathbb{F}_q$, called the *kernel* of $\mathcal{S}$. If $\mathcal{S}$ is a translation spread of $H(q^n)$ with kernel $\mathbb{F}_q$, we say that $\mathcal{S}$ is an $\mathbb{F}_q$*-translation spread* of $H(q^n)$.

The known examples of $\mathbb{F}_q$-translation spreads of $H(q)$ with respect to a line are: the *Hermitian spreads* (Thas [71]), the spreads $\mathcal{S}_{[9]}$ constructed by Bloemen, Thas and Van Maldeghem in [8] for $q \equiv 1 \pmod 3$, q odd, and the spreads $\mathcal{S}_l$ constructed, independently, by Cardinali, Lunardon, Polverino and Trombetti in [19] and by Offer in [54] for $q \equiv 1 \pmod 3$, q even. The only known examples of translation spreads with proper kernel are the spreads $\mathcal{S}_\beta$ of $H(3^h)$, $h > 1$, constructed in [8].

By using the construction of $H(q^n)$ as a coset geometry the following theorem has been proven.

Theorem 4.1 (*[19,49]*). *Each translation spread $\mathcal{S}$ of $H(q^n)$ with respect to a line L and with kernel $\mathbb{F}_q$ defines an $\mathbb{F}_q$-linear set $L(\mathcal{S})$ of $PG(3, q^n)$ of rank $2n$ (having $\mathbb{F}_q$ as the maximal subfield of linearity) whose points belong to imaginary chords of a twisted cubic $\mathcal{C}$ of $PG(3, q^n)$, and conversely. Also, the automorphism group of $H(q^n)$ fixing the line L induces on $PG(3, q^n)$ the collineation group of $PGL(4, q^n)$ fixing the twisted cubic $\mathcal{C}$.*

Recall that a line of $PG(3, q)$ ($q = p^h$, p prime) is a *chord* of a twisted cubic $\mathcal{C}$ if it contains two points of $\bar{\mathcal{C}}$, where $\bar{\mathcal{C}}$ is the twisted cubic defined by $\mathcal{C}$ over the algebraic closure of $\mathbb{F}_q$. There are three possibilities: either the two points are distinct and belong to $\mathcal{C}$, or they are coincident, or they are conjugate over $\mathbb{F}_{q^2}$; the line is called a *real chord*, a *tangent* or an *imaginary chord*, respectively. Every point not belonging to $\mathcal{C}$ lies on exactly one chord. If $p \neq 3$, the tangents to $\mathcal{C}$ are self-polar lines of a non-singular symplectic polarity ω of $PG(3, q)$. An *axis* of $\mathcal{C}$ is a line l of $PG(3, q)$ whose polar line with respect to ω is a chord. We say that l is *a real axis* or *an imaginary axis* when l^ω is a real chord or an imaginary chord respectively (for more details, see [30, Section 21]). Also, the following properties hold true.

Theorem 4.2 (*[49]*). *If l is a line of $PG(3, q)$ whose points belong to imaginary chords of $\mathcal{C}$, then either l is an imaginary chord or $q \equiv 1 \pmod 3$ and l is an imaginary axis.*

Theorem 4.3 (*[16]*). *Let L be an $\mathbb{F}_q$-linear set of $PG(3, q^n)$ of rank $2n$ ($n > 2$) whose points belong to imaginary chords of $\mathcal{C}$. If $q^n \equiv 1 \pmod 3$, q odd, $q \geq 4n^2 - 8n + 2$ and $q > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime, then L is an $\mathbb{F}_{q^n}$-linear set and either L is an imaginary chord or L is an imaginary axis of $\mathcal{C}$.*

The following results on translation spreads of $H(q)$ are known.

Theorem 4.4 (*[8] for q odd, [49] for q even*). *The Hermitian spreads, the spreads $\mathcal{S}_{[9]}$ and $\mathcal{S}_l$, up to isomorphisms, are the only $\mathbb{F}_q$-translation spreads of $H(q)$.*

Theorem 4.5 (*[55]*). *A spread $\mathcal{S}$ of $H(3^h)$ which is translation spread with respect to a line, up to isomorphisms, is either Hermitian or a spread $\mathcal{S}_\beta$.*

Theorem 4.6 (*[19,49]*). *If q is even then all translation spreads of $H(q)$ are $\mathbb{F}_q$-translation spreads and, up to isomorphisms, are the Hermitian spreads, the spreads $\mathcal{S}_{[9]}$ and $\mathcal{S}_l$.*

Theorem 4.7 (*[16]*). *If $q^n \equiv 1 \pmod 3$, q odd, $n > 2$, $q \geq 4n^2 - 8n + 2$ and $q > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime, then $H(q^n)$ does not admit an $\mathbb{F}_q$-translation spread.*

The classification results in [16] and in [49] are obtained using the correspondence, established in Theorem 4.1, between translation spreads of $H(q)$ and linear sets. Indeed, if $\mathcal{S}$ is an $\mathbb{F}_q$-translation spread of $H(q)$, then the associated linear set $L(\mathcal{S})$ is a line of $PG(3, q)$ whose points belong to imaginary chords of a twisted cubic $\mathcal{C}$ of $PG(3, q)$. In particular, the Hermitian spreads correspond to imaginary chords of $\mathcal{C}$ and the spreads $\mathcal{S}_{[9]}$ and $\mathcal{S}_l$ ($q \equiv 1 \pmod 3$) correspond to imaginary axes of $\mathcal{C}$ ([19]). Hence Theorems 4.4 and 4.7 are obtained as applications of Theorems 4.2 and 4.3.

Next, by using the theory of dual linear sets introduced in Section 2, we define the *dual of a translation spread* of $H(q)$ when $q \equiv 1 \pmod 3$.

Let $\mathcal{C}$ be a twisted cubic of $PG(3, q)$. Recall that, if $q \equiv 1 \pmod 3$ and l is an imaginary axis, then all points on l belong to an imaginary chord of $\mathcal{C}$ (see [19]).

Theorem 4.8. *Let L be an $\mathbb{F}_q$-linear set of rank $2n$ of $PG(3, q^n)$ whose points belong to imaginary chords of a twisted cubic $\mathcal{C}$. If $q^n \equiv 1 \pmod 3$, then the dual L^ω of L with respect to the symplectic polarity ω associated with $\mathcal{C}$ is an $\mathbb{F}_q$-linear set of rank $2n$ whose points belong to imaginary chords of $\mathcal{C}$ as well.*

Proof. Let P be a point of L^ω and let r be a chord of $\mathcal{C}$ passing through P. Since $P \in L^\omega$, the weight of P with respect to L^ω is at least 1 and hence, by Equality (7), $w_L(r^\omega) = w_{L^\omega}(r) \geq 1$, i.e. the line r^ω contains at least a point, say T, of L. So the unique chord l of $\mathcal{C}$ through T is an imaginary chord. This means that l^ω is an imaginary axis and, since $l \cap r^\omega \neq \emptyset$, the line l^ω is not disjoint from r. Since $q^n \equiv 1 \pmod 3$, this implies that r is an imaginary chord. □

So by Theorems 4.1 and 4.8 we obtain

Corollary 4.9. *If $q^n \equiv 1 \pmod 3$, then the dual linear set L^ω (with respect to the polarity ω arising from $\mathcal{C}$) of a linear set L associated with an $\mathbb{F}_q$-translation spread $\mathcal{S}$ of $H(q^n)$, defines an $\mathbb{F}_q$-translation spread of $H(q^n)$.*

We call the $\mathbb{F}_q$-translation spread of $H(q^n)$ arising from L^ω *the dual translation spread* $\mathcal{S}^\omega$ of $\mathcal{S}$.

If the linear set arising from a translation spread $\mathcal{S}$ of $H(q)$ is a line l of $PG(3, q)$, then the dual linear set of l is the polar line of l with respect to ω. Also, we have that if l is an imaginary chord, then l^ω is an imaginary axis, and conversely. This implies that

Theorem 4.10. *If $q \equiv 1 \pmod 3$, then the dual spread of a Hermitian spread of $H(q)$ is a spread $\mathcal{S}_{[9]}$, if q is odd, a spread $\mathcal{S}_l$, if q is even, and conversely.*

The previous theorem shows that a translation spread $\mathcal{S}$ of $H(q)$ ($q \equiv 1 \pmod 3$) and its dual $\mathcal{S}^\omega$ may be not isomorphic.

5. Application 3: Translation ovoids of orthogonal polar spaces

Denote by $\mathbb{P}$ either the polar space associated with a non-singular quadric of $PG(2n, q)$ ($n \geq 2$) or the polar space associated with a non-singular quadric of $PG(2n+1, q)$ ($n \geq 1$).

An ovoid of $\mathbb{P}$ is a set of $q^n + 1$ points, no two collinear in $\mathbb{P}$. An ovoid O of $\mathbb{P}$ is a *translation* ovoid with respect to a point x of O if there is a collineation group of $\mathbb{P}$ fixing x linewise and acting sharply transitively on $O \setminus \{x\}$.

Examples of translation ovoids of $Q^+(3, q)$ are the conics contained in it. The ovoids of the Klein quadric $Q^+(5, q)$ correspond to line spreads of $PG(3, q)$ and translation ovoids are equivalent to semifield spreads. Hence, $Q^+(5, q)$ has ovoids and translation ovoids for all values of q. If $Q(4, q) = H \cap Q^+(5, q)$ is a non-singular quadric, where H is a hyperplane of $PG(5, q)$, then ovoids of $Q(4, q)$ are equivalent to symplectic spreads of $PG(3, q)$ and translation ovoids are equivalent to symplectic semifield spreads of $PG(3, q)$.

For $n > 2$ ovoids are rare objects. In [72] it is proved that $Q^-(2n+1, q)$ has ovoids only if $n = 1$. The polar space $Q(2n, q)$, with q even, has ovoids if and only if $n = 2$ and, in this case, they are equivalent to ovoids of $PG(3, q)$. If q is odd, ovoids of $Q(2n, q)$ do not exist if $n \geq 4$ (see [29]) and the only two known ovoids of $Q(6, q)$ are the unitary ovoid of $Q(6, 3^e)$ and the Ree ovoid of $Q(6, 3^{2e+1})$ (see [35] and [72]). Examples of ovoids of $Q^+(7, q)$ are known for q even, for $q \equiv 2 \pmod 3$ and for q an odd prime (see [36], [35,22] and [53]).

Let $\mathbb{P}$ be one of the following orthogonal polar spaces: $Q^+(2n+1, q)$ ($n \geq 2$), $Q(2n, q)$ ($n \geq 2$), $Q^-(2n-1, q)$ ($n \geq 3$) and denote by $\perp$ the polarity defined by $\mathbb{P}$. Let x be a point of $\mathbb{P}$ and let Ω' be a hyperplane not containing x. Denote by $\mathbb{P}^*$ the polar space obtained intersecting $\mathbb{P}$ with the hyperplane $\Omega = \Omega' \cap x^\perp$ of Ω'. Define a point-line geometry $\mathbb{P}_x$ in the following way. The points are: (i) a symbol (∞), (ii) hyperplanes of Ω' which intersect Ω in a hyperplane tangent to $\mathbb{P}^*$ and (iii) points of $\Omega' \setminus \Omega$. The lines are (I) the points of $\mathbb{P}^*$, (II) the lines of Ω' which intersect Ω in a point of $\mathbb{P}^*$ and (if $\mathbb{P} \neq Q(4, q), Q^-(5, q)$) (III) the subspaces of Ω' not contained in Ω which intersect Ω in the polar space of a line of $\mathbb{P}^*$. The point (∞) is incident only with the lines of type (I). All other incidences are inherited from Ω'.

If l and m are lines of $\mathbb{P}$ and y is a point of $\mathbb{P}$, then the map θ defined by

$$\begin{aligned}
&\theta : x \mapsto (\infty),\\
&\theta : l \mapsto l \cap \Omega, \quad \text{for } x \in l \subset x^\perp,\\
&\theta : l \mapsto l^\perp \cap \Omega', \quad \text{for } x \notin l \subset x^\perp,\\
&\theta : y \in x^\perp \setminus \{x\} \mapsto y^\perp \cap \Omega',\\
&\theta : m \not\subset x^\perp \mapsto \langle m, x\rangle \cap \Omega',\\
&\theta : y \notin x^\perp \mapsto \langle x, y\rangle \cap \Omega',
\end{aligned}$$

is an isomorphism from $\mathbb{P}$ onto $\mathbb{P}_x$.

An ovoid O of $\mathbb{P}$ containing the point x is mapped by θ to an ovoid O_x of $\mathbb{P}_x$ containing the point (∞). This means that $O_x \setminus \{(\infty)\}$ is a set of q^n points of $\Omega' \setminus \Omega$ such that the lines joining any two of them have no point in common with $\mathbb{P}^*$, i.e., the set of "directions"

$$D(O_x \setminus \{\infty\}) = \{PQ \cap \Omega : P, Q \in O_x \setminus \{(\infty)\}\}$$

of $O_x \setminus \{(\infty)\}$ in Ω is disjoint from $\mathbb{P}^*$.

Theorem 5.1 ([50]). *If O_x is a translation ovoid of $\mathbb{P}_x$ with respect to (∞), then there is a subfield $\mathbb{F}_s$ of $\mathbb{F}_q$ ($q = s^t$) such that $D(O_x \setminus \{\infty\})$ is an $\mathbb{F}_s$-linear set of rank nt of Ω disjoint from $\mathbb{P}^*$. Conversely, if L is an $\mathbb{F}_s-$ linear set of rank nt of Ω disjoint from $\mathbb{P}^*$, then there exists a translation ovoid O_x of $\mathbb{P}_x$ with respect to (∞) such that $L = D(O_x \setminus \{\infty\})$.*

By using Theorem 5.1 and the characterization of linear sets as projection of canonical subgeometries, in [50] the following theorem has been proven.

Theorem 5.2 ([50]). *Translation ovoids of $\mathbb{P}$ exist if and only if $\mathbb{P}$ is one of $Q^+(3, q)$, $Q(4, q)$, $Q^+(5, q)$.*

Consequently, the most important open problems are related to the existence and to the classification of translation ovoids of $Q(4, q)$ and $Q^+(5, q)$. But, these problems are strictly connected with the theory of semifield spreads of $PG(3, q)$ which we will deal with in the next section.

6. Application 4: Finite semifields

A *finite semifield* $\mathbb{S}$ is a finite algebraic structure satisfying all the axioms for a skewfield except (possibly) associativity. The subsets $\mathbb{N}_l = \{a \in \mathbb{S} \mid (ab)c = a(bc),\ \forall b, c \in \mathbb{S}\}$, $\mathbb{N}_m = \{b \in \mathbb{S} \mid (ab)c = a(bc),\ \forall a, c \in \mathbb{S}\}$, $\mathbb{N}_r = \{c \in \mathbb{S} \mid (ab)c = a(bc),\ \forall a, b \in \mathbb{S}\}$ and $\mathcal{K} = \{a \in \mathbb{N}_l \cap \mathbb{N}_m \cap \mathbb{N}_r \mid ab = ba,\ \forall b \in \mathbb{S}\}$ are fields and are known, respectively, as the *left nucleus*, the *middle nucleus*, the *right nucleus* and the *center* of the semifield. A finite semifield is a vector space over its nuclei and its center. A finite semifield which is not a field is a *proper semifield*. If $\mathbb{S}$ satisfies all the axioms of a semifield, except possibly the existence of the identity element of the multiplication, then $\mathbb{S}$ is called *pre-semifield*. From now on the terms semifield and pre-semifield will be always used to denote a finite semifield and a finite pre-semifield, respectively.

Semifields coordinatize certain translation planes (called *semifield planes*) and two semifield planes are isomorphic if and only if the corresponding semifields are *isotopic* (see [1]). The dimensions of a semifield $\mathbb{S}$ over its nuclei and its center are invariant under the isotopy relation. A semifield is isotopic to a field if and only if the corresponding semifield plane is Desarguesian. Also, from any pre-semifield it is possible to construct a semifield which is isotopic to the starting pre-semifield (for more details on semifields see, e.g., [24,32]).

For any subfield $\mathbb{F}$ of the left nucleus of a semifield $\mathbb{S}$, the vector subspaces of $\mathbb{S}\times\mathbb{S}$ (regarded as left vector space over $\mathbb{F}$):

$$F(\infty)=\{(0,a):\ a\in\mathbb{S}\},\qquad F(b)=\{(a,ab):\ a\in\mathbb{S}\},$$

with $b\in\mathbb{S}$, define a spread $\mathcal{S}$ of the projective space $PG(\mathbb{S}\times\mathbb{S},\mathbb{F})$, which is called *semifield spread*. By the André Spread Isomorphism Theorem (see, e.g., [32, Theorem 2.26]), two semifield spreads in projective spaces of the same dimension are isomorphic if and only if the corresponding semifields are isotopic.

A semifield $\mathbb{S}$ is *symplectic* if the associated semifield spread $\mathcal{S}$ of $PG(\mathbb{S}\times\mathbb{S},\mathbb{N}_l)$ is symplectic with respect to any polarity of $PG(\mathbb{S}\times\mathbb{S},\mathbb{N}_l)$. Symplectic semifield spreads of $PG(3,q)$ correspond, via the Plücker map, to translation ovoids of $Q(4,q)$. The known examples of proper symplectic semifields 2-dimensional over their left nucleus are: the Kantor–Knuth semifields (see, e.g., [73]), the Payne–Thas semifields of order $q=3^{2t}$ $(t>2)$ [56] and the Penttila–Williams symplectic semifield of order 3^{10} [57].

A semifield $\mathbb{S}$ of dimension at most 2 over its left nucleus is *associated with a flock*, if the corresponding semifield spread is the union of q reguli which share a common line, i.e. it arises from a flock of the quadratic cone of $PG(3,q)$ (see, e.g., [28]). The known examples of proper semifields associated with a flock are: the Kantor–Knuth semifields, the semifields of order $q=3^{2t}$ $(t>2)$ associated with the Ganley flocks [28] and the Bader–Lunardon–Pinneri semifield of order 3^{10} [2].

By [73] the only semifields which are both symplectic and associated with a flock are the fields and the Kantor–Knuth semifields. Also, if q is even, there is no proper semifield associated with a flock (see [31]).

Let b be an element of a semifield $\mathbb{S}$ with center $\mathcal{K}$; the map $\varphi_b: x\in\mathbb{S}\to xb\in\mathbb{S}$ is linear when $\mathbb{S}$ is regarded as a left vector space over $\mathbb{N}_l$. The set $S=\{\varphi_b: b\in\mathbb{S}\}$ is called the *spread set of linear maps* (*spread set* for short) of $\mathbb{S}$. A spread set S satisfies the following properties:

(i) $|S|=|\mathbb{S}|$;
(ii) S is closed under addition, contains the zero map and the identity map;
(iii) every non-zero map in S is non-singular (that is, invertible).

Also, $\lambda\varphi_b=\varphi_{\lambda b}$ for any $\lambda\in\mathcal{K}$, i.e. S is a $\mathcal{K}$-vector subspace of the vector space $\mathbb{V}=End(\mathbb{S},\mathbb{N}_l)$ of all $\mathbb{N}_l$-linear maps of $\mathbb{S}$. Conversely, any set S of $\mathbb{F}$-linear maps satisfying Properties (i), (ii) and (iii) defines a semifield $\mathbb{S}$ whose left nucleus contains the field $\mathbb{F}$. This means that semifields t-dimensional over their left nucleus $\mathbb{F}_{q^n}$ and with center $\mathbb{F}_q$ can be investigated via the spread sets of $\mathbb{F}_{q^n}$-linear maps of any t-dimensional vector space over $\mathbb{F}_{q^n}$. Choosing such a space as the Galois field $\mathbb{F}_{q^{nt}}$, any element φ of $\mathbb{V}=End(\mathbb{F}_{q^{nt}},\mathbb{F}_{q^n})$ can be represented in a unique way as a q^n-polynomial over $\mathbb{F}_{q^{nt}}$, that is

$$\varphi=\varphi_{a_0,a_1,\dots,a_{t-1}}: x\in\mathbb{F}_{q^{nt}}\mapsto a_0x+a_1x^{q^n}+a_2x^{q^{2n}}+\cdots+a_{t-1}x^{q^{(t-1)n}}\in\mathbb{F}_{q^{nt}}.$$

Also, $\varphi_{a_0,a_1,\dots,a_{t-1}}$ is invertible if and only if $\det(A)\neq 0$, where

$$A=\begin{pmatrix} a_0 & a_{t-1}^{q^n} & a_{t-2}^{q^{2n}} & \dots & a_1^{q^{n(t-1)}}\\ a_1 & a_0^{q^n} & a_{t-1}^{q^{2n}} & \dots & a_2^{q^{n(t-1)}}\\ a_2 & a_1^{q^n} & a_0^{q^{2n}} & \dots & a_3^{q^{n(t-1)}}\\ \vdots & \vdots & \vdots & & \vdots\\ a_{t-1} & a_{t-2}^{q^n} & a_{t-3}^{q^{2n}} & \dots & a_0^{q^{n(t-1)}} \end{pmatrix}$$

(see [39, pg. 362]). Hence, any spread set S of linear maps defining a semifield can be seen as a set of linearized polynomials satisfying Properties (i), (ii) and the above mentioned non-singularity condition.

If Ψ and Φ are invertible $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{nt}}$ and σ is an automorphism of $\mathbb{F}_{q^{nt}}$, then the set

$$S'=\Psi S^\sigma\Phi=\{\Psi\varphi^\sigma\Phi:\varphi\in S\}\qquad(*)$$

(where $\varphi^\sigma: x\mapsto a_0^\sigma x+a_1^\sigma x^{q^n}+a_2^\sigma x^{q^{2n}}+\cdots+a_{t-1}^\sigma x^{q^{(t-1)n}}$ for $\varphi=\varphi_{a_0,a_1,\dots,a_t}$ and the composition of maps is to be read from right to left) is an additive spread set of linear maps that defines on $\mathbb{F}_{q^{nt}}$ a pre-semifield $\mathbb{S}'$ isotopic to $\mathbb{S}$. Conversely, any pre-semifield $\mathbb{S}'=(\mathbb{F}_{q^{nt}},+,\circ')$ isotopic to $\mathbb{S}$ is defined by a spread set S' of type $(*)$ (see, e.g., [32, Chapter 5]). Note that the map $\Gamma:\varphi\in\mathbb{V}\longrightarrow\Psi\varphi^\sigma\Phi\in\mathbb{V}$ is an invertible semilinear map of $\mathbb{V}$ preserving the non-invertible elements of $\mathbb{V}$.

Now, we focus on semifields 2-dimensional over their left nucleus. Let $\mathbb{S}=(\mathbb{F}_{q^{2n}},+,\circ)$ be a semifield with left nucleus $\mathbb{F}_{q^n}$ and center $\mathbb{F}_q$ and let S be the set of the $\mathbb{F}_{q^n}$-linear maps defining the multiplication of $\mathbb{S}$, i.e. $x\circ y=\varphi_y(x)$ where φ_y is the unique element of S such that $\varphi_y(1)=y$. Since S is closed under $\mathbb{F}_q$-scalar multiplication, it follows that S is a $2n$-dimensional $\mathbb{F}_q$-vector subspace of the 4-dimensional vector space $\mathbb{V}=End(\mathbb{F}_{q^{2n}},\mathbb{F}_{q^n})$. Also, since an element $\varphi_{a,b}$ of $\mathbb{V}$ is non-invertible

if and only if $a^{q^n+1} = b^{q^n+1}$ and since $\mathbf{q}(\varphi_{a,b}) = a^{q^n+1} - b^{q^n+1}$ is a quadratic form of $\mathbb{V}$ over $\mathbb{F}_{q^n}$, the non-invertible elements of $\mathbb{V}$ define the hyperbolic quadric

$$\mathcal{Q} = \{\langle\varphi_{a,b}\rangle_{\mathbb{F}_{q^n}} \mid a^{q^n+1} - b^{q^n+1} = 0, (a, b) \neq (0, 0)\}$$

of the 3-dimensional projective space $\mathbb{P} = PG(\mathbb{V}, \mathbb{F}_{q^n}) = PG(3, q^n)$.

Hence, by Property (iii), the $\mathbb{F}_q$-vector subspace S of $\mathbb{V}$ defines an $\mathbb{F}_q$-linear set

$$L_S = L(\mathbb{S}) = \{\langle\varphi\rangle_{\mathbb{F}_{q^n}} : \varphi \in S, \varphi \neq 0\}$$

of $\mathbb{P}$ of rank $2n$, disjoint from the quadric $\mathcal{Q}$. The linear set $L_S = L(\mathbb{S})$ is *the* $\mathbb{F}_q$*-linear set* associated with $\mathbb{S}$. Also, any semilinear map of $\mathbb{V}$ of type

$$\Gamma: \varphi \in \mathbb{V} \mapsto \Psi\varphi^\sigma\Phi \in \mathbb{V}, \qquad (\diamond)$$

where Ψ and Φ are invertible $\mathbb{F}_{q^n}$-linear maps of $\mathbb{V}$ and $\sigma \in Aut(\mathbb{F}_{q^{2n}})$, induces a collineation of $\mathbb{P}$ preserving the reguli of $\mathcal{Q}$, and conversely (see [42,21]). Hence

Theorem 6.1 ([21]). *Two semifields $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, \circ)$ and $\mathbb{S}' = (\mathbb{F}_{q^{2n}}, +, \circ')$, 2-dimensional over their left nucleus $\mathbb{F}_{q^n}$ and with center $\mathbb{F}_q$ are isotopic if and only if there exists a collineation ϕ of the group $G \leq P\Gamma O^+(4, q^n)$ preserving the reguli of $\mathcal{Q}$ induced by a semilinear map Γ of type ($\diamond$) such that $L_S^\phi = L_{S^\Gamma} = L_{S'}$.*

Let τ be the polarity of $\mathbb{P}$ arising from the hyperbolic quadric $\mathcal{Q}$ and let L_S^τ be the dual, with respect to τ, of the linear set L_S associated with the semifield $\mathbb{S}$. By using Equality (7), it is easy to see that $L_S^\tau = L_{S^\perp}$ is disjoint from $\mathcal{Q}$ as well. So the $\mathbb{F}_q$-linear subspace $S^\perp$ of $\mathbb{V}$ of dimension $2n$ defines a pre-semifield $\mathbb{S}^\perp$ called *the translation dual* of $\mathbb{S}$ (see [42], [45, Section 3], [32, Chapter 85]). For an alternative description of the translation dual construction see [7].

The properties for a semifield to be Desarguesian, symplectic and associated with a flock, can be stated purely in terms of associated linear sets, as shown in

Proposition 6.2 ([42]). *Let $\mathbb{S}$ be a semifield with dimension at most 2 over its left nucleus and let $L(\mathbb{S})$ be its associated linear set.Then*

(I) *$\mathbb{S}$ is a field if and only if $L(\mathbb{S})$ is a line of $\mathbb{P}$.*

(II) *$\mathbb{S}$ is symplectic if and only if $L(\mathbb{S})$ is contained in a plane of $\mathbb{P}$.*

(III) *$\mathbb{S}$ is associated with a flock if and only if $L(\mathbb{S})$ has a point P of maximum weight. In this case, $L(\mathbb{S})$ is a union of lines through P.*

Hence, by Property 2.7, we have

(IV) *$\mathbb{S}$ is symplectic if and only if $\mathbb{S}^\perp$ is associated with a flock.*

The translation dual of a Kantor–Knuth semifield is a Kantor–Knuth semifield as well; the translation dual of a Payne–Thas semifield is isotopic to a Ganley semifield arising from a flock; the transaltion dual of the Penttila–Williams semifield of order 3^{10} is isotopic to the Bader–Lunardon-Pinneri semifield.

If $\mathbb{S}$ is a semifield associated with a flock with left nucleus $\mathbb{F}_{q^n}$ and center $\mathbb{F}_q$, then by (III) of the previous proposition, the associated linear set $L(\mathbb{S})$ has a point, say P, of weight n. If q is odd and τ is the polarity associated with the quadric $\mathcal{Q}$, then we get that the linear set $\mathcal{I} = P^\tau \cap L(\mathbb{S})$ has rank n and each point of $\mathcal{I}$ is an internal point of the irreducible conic $P^\tau \cap \mathcal{Q}$. Conversely, if $\mathcal{I}$ is an $\mathbb{F}_q$-linear set of rank n of a plane π of $\mathbb{P} = PG(3, q^n)$ whose points are internal points of the irreducible conic $\pi \cap \mathcal{Q}$, then the linear set obtained joining the point π^τ with $\mathcal{I}$ is an $\mathbb{F}_q$-linear set of rank $2n$, disjoint from $\mathcal{Q}$. So, the existence of semifields associated with a flock with left nucleus of order q^n (q odd) and with center $\mathbb{F}_q$ is equivalent to the existence of linear sets of rank n contained in the set of internal points of an irreducible conic of the plane $PG(2, q^n)$ (see [74], [44]). If $n = 2$, then by [8], $\mathbb{S}$ is a Kantor–Knuth semifield.

Ball, Blokhuis and Lavrauw in [6], and Lavrauw in [37] (for the case q prime), prove that

Theorem 6.3 ([6,37]). *If there is a subplane of order q contained in the set of internal points of a non-degenerate conic in $PG(2, q^n)$ ($n \geq 3$), then $q < 4n^2 - 8n + 2$ and $q \leq 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime.*

As a consequence, the following result on the existence of semifield flocks has been determined:

Theorem 6.4 ([6,37]). *If $\mathcal{F}$ is a semifield flock of a quadratic cone in $PG(3, q^n)$, q odd, with kernel containing $\mathbb{F}_q$ and $q \geq 4n^2 - 8n + 2$, and $q > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime, then $\mathcal{F}$ is linear or Kantor type.*

In terms of semifields the previous result states that if a semifield $\mathbb{S}$, arising from a semifield flock of $PG(3, q^n)$, q odd, has center containing $\mathbb{F}_q$ with $q \geq 4n^2 - 8n + 2$, and $q > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime, then $\mathbb{S}$ is either a field or a Kantor–Knuth semifield.

In the last years the above mentioned connection between semifields and linear sets has been intensively used to construct and characterize families of semifields with given dimensions over the nuclei and the center. In what follows, we will say that a semifield $\mathbb{S}$ is *of type* $(q^{2n}, q^n, q^r, q^m, q)$ if it has order q^{2n}, left nucleus of order q^n, right nucleus of order q^r, middle nucleus of order q^m and center of order q, where r and m are divisors of $2n$ and $0 < r, m < 2n$.

In [21], Cardinali, Polverino and Trombetti classify all semifields of order q^4 with left nucleus of order q^2 and center of order q. The result is stated in terms of semifield planes.

Theorem 6.5 ([21]). *Let π be a semifield plane of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$.*

(i) *If q is odd, then π belongs to one of the following classes: Generalized Dickson semifield planes, Hughes–Kleinfeld semifield planes, semifield planes lifted from Desarguesian planes of Cordero–Figueroa type or Generalized twisted field planes.*
(ii) *If q is even, then π either belongs to one of the following classes: Hughes–Kleinfeld semifield planes, Generalized twisted field planes, or it belongs to the class of lifted planes (from Desarguesian planes) of type (b).*

In [51,33,26], semifields of order q^6, with left nucleus of order q^3 and center of order q, are studied.
The results on these semifields can be summarized in the following way:

Theorem 6.6 ([51,33]). *Let $\mathbb{S}$ be a semifield of order q^6 with left nucleus of order q^3 and center of order q. Then, there are precisely six possible geometric configurations for the corresponding linear set $L = L(\mathbb{S})$ in $\mathbb{P} = PG(3, q^3)$. The corresponding classes of semifields are partitioned into six non-isotopic families labeled $\mathcal{F}_0$, $\mathcal{F}_1$, $\mathcal{F}_2$, $\mathcal{F}_3$, $\mathcal{F}_4$ and $\mathcal{F}_5$. Also, the family $\mathcal{F}_4$ is further partitioned into three non-isotopic subfamilies denoted $\mathcal{F}_4^{(a)}$, $\mathcal{F}_4^{(b)}$ and $\mathcal{F}_4^{(c)}$.*

Using [73,6,8], in [51] the families $\mathcal{F}_i$, $i = 0, 1, 2$ are completely characterized:

$\mathcal{F}_0$: $\mathbb{S}$ belongs to the family $\mathcal{F}_0$ if and only if $\mathbb{S}$ is isotopic to a Generalized Dickson semifield with the given parameters.
$\mathcal{F}_1$: $\mathbb{S}$ belongs to the family $\mathcal{F}_1$ if and only if $q = 3$ and $\mathbb{S}$ is associated with the Payne–Thas ovoid of $Q^+(4, 3^3)$.
$\mathcal{F}_2$: $\mathbb{S}$ belongs to the family $\mathcal{F}_2$ if and only if $q = 3$ and $\mathbb{S}$ is associated with the Ganley flock of the quadratic cone of $PG(3, 3^3)$.

So far, only a few examples of semifields belonging to $\mathcal{F}_3$ are known. They are obtained by using MAGMA for small values of q ($q = 2, 4, 8$).

The subfamilies $\mathcal{F}_4^{(a)}$, $\mathcal{F}_4^{(b)}$, and $\mathcal{F}_4^{(c)}$ have been introduced in [33] and studied in [26], where the general form for the multiplication of a semifield belonging to each of such families is determined. Moreover,

$\mathcal{F}_4^{(a)}$: In [26] the authors construct, for any odd q, a new example of semifield belonging to $\mathcal{F}_4^{(a)}$ of type (q^6, q^3, q^2, q, q), called *EMPT semifield of type* (q^6, q^3, q^2, q, q), and a new example of semifield belonging to $\mathcal{F}_4^{(a)}$ of type (q^6, q^3, q, q^2, q), called *EMPT semifield of type* (q^6, q^3, q, q^2, q). Also, they prove that if q is even, semifields of type (q^6, q^3, q^2, q, q) or (q^6, q^3, q, q^2, q) not belonging to the family $\mathcal{F}_5$ do not exist; whereas, if q is odd, they prove that there exists, up to isotopy, for any value of q, a unique semifield of type (q^6, q^3, q^2, q, q) and a unique semifield of type (q^6, q^3, q, q^2, q), not belonging to $\mathcal{F}_5$, precisely, the above mentioned EMPT's semifields.

$\mathcal{F}_4^{(b)}$: In [26] it has been proved that a semifield belonging to $\mathcal{F}_4^{(b)}$ is necessarily of type (q^6, q^3, q, q, q) and one example is exhibited for $q = 3$ by MAGMA computation.

$\mathcal{F}_4^{(c)}$: A semifield belonging to $\mathcal{F}_4^{(c)}$ is either of type (q^6, q^3, q, q, q) or is of type (q^6, q^3, q^2, q^2, q) ([26]) and in [25] a class of new examples of semifields of type (q^6, q^3, q, q, q) belonging to $\mathcal{F}_4^{(c)}$ has been constructed for any value of q. On the other hand, in [33], it has been proved that any semifield of type (q^6, q^3, q^2, q^2, q) belongs to the family $\mathcal{F}_4^{(c)}$ and it is isotopic to a cyclic semifield.

Finally, semifields belonging to the family $\mathcal{F}_5$ are called *scattered semifields* because their associated linear sets are scattered. In [51] it has been proved that to any semifield $\mathbb{S}$ belonging to $\mathcal{F}_5$ is associated an $\mathbb{F}_q$-*pseudoregulus* $\mathcal{L}(\mathbb{S})$ of $\mathbb{P} = PG(3, q^3)$, which is a set of $q^3 + 1$ pairwise disjoint lines with exactly two transversal lines. An $\mathbb{F}_q$-pseudoregulus of $PG(3, q^3)$ defines a *derivation set* as the pseudoregulus of $PG(3, q^2)$ defined by Freeman in [27]. The known examples of semifields belonging to the family $\mathcal{F}_5$ are the generalized twisted fields and the two families of Knuth semifields with the involved parameters. They are also characterized in terms of the associated $\mathbb{F}_q$-pseudoreguli.

It is clear, from previous arguments, that the complete classification of semifields of order q^6, with left nucleus of order q^3 and center of order q, requires a deeper study of $\mathbb{F}_q$-pseudoreguli in $PG(3, q^3)$ in order to understand whether there exist other semifields belonging to $\mathcal{F}_5$. Moreover, a complete search for examples of semifields belonging to classes $\mathcal{F}_3$ or $\mathcal{F}_4^{(b)}$ should be achieved.

Semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, when n is odd, are investigated in [34] and in [52]. In [34], Johnson, Marino, Polverino and Trombetti determine all the cyclic semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd, generalizing some cyclic semifields previously constructed by Jha–Johnson. This wider family contains new classes of semifields not cyclic but isotopic to cyclic semifields and, for $q = 2, 4$ and $n = 5$, examples of semifields not isotopic to any previously known semifield. Furthermore, they give a lower bound for the number of isotopism classes of cyclic semifields.

In [52], Marino, Polverino and Trombetti determine, up to isotopy, the general form for the multiplication of any semifield $\mathbb{S}$ of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd. Also, by using the geometric properties of the associated spread sets of linear maps, they

prove that such semifields are partitioned into $\frac{n-1}{2}$ potentially non-isotopic families. Some of these classes seem to be likely places to search for new semifields. Indeed, computational results obtained using MAGMA, provide some new examples of semifields of type $(q^{14}, q^7, q^2, q^2, q)$, for $q = 2$.

Finally, in [25], by using linearized polynomials and the geometric approach of linear sets new infinite families of semifields are constructed. In particular, the authors construct six new mutually non-isotopic families of semifields, the families $\mathcal{F}_I$, $\mathcal{F}_{II}$, $\mathcal{F}_{III}$, $\mathcal{F}_{IV}$, $\mathcal{F}_V$ and $\mathcal{F}_{VI}$. The semifields belonging to $\mathcal{F}_I$, $\mathcal{F}_{II}$ and $\mathcal{F}_{III}$ are of type (q^{2n}, q^n, q, q, q) and are defined for all odd $n > 1$ and all odd prime powers q; while those belonging to $\mathcal{F}_{IV}$ and $\mathcal{F}_V$ are of the same type and are defined for all odd $n > 1$ and even q. The semifields belonging to $\mathcal{F}_{VI}$ are of type $(q^{2n}, q^n, q^2, q^2, q)$ and are defined for all odd prime powers q and even integers $n > 2$.

For an updated list of known finite semifields see [32, Chapter 37] and [52].

Acknowledgement

This work was supported by the Research Project of MIUR (Italian Office for University and Research) "Strutture geometriche, combinatoria e loro applicazioni".

References

[1] A.A. Albert, Finite division algebras and finite planes, Proc. Sympos. Appl. Math. 10 (1960) 53–70.
[2] L. Bader, G. Lunardon, I. Pinneri, A new semifield flock, J. Combin. Theory, Ser. A 86 (1999) 49–62.
[3] L. Bader, G. Marino, O. Polverino, R. Trombetti, Spreads of $PG(3, q)$ and ovoids of Polar Spaces, Forum Math. 19 (6) (2007) 1101–1110.
[4] S. Ball, The number of directions determined by a function over a finite field, J. Combin. Theory, Ser. A 104 (2) (2003) 341–350.
[5] S. Ball, A. Blokhuis, M. Lavrauw, Linear $(q + 1)$-fold blocking sets in $PG(2, q^4)$, Finite Fields Appl. 6 (4) (2000) 294–301.
[6] S. Ball, A. Blokhuis, M. Lavrauw, On the classification of semifield flocks, Adv. Math. 180 (2003) 104–111.
[7] S. Ball, G.L. Ebert, M. Lavrauw, A geometric construction of finite semifields, J. Algebra 311 (2007) 117–129.
[8] I. Bloemen, J.A. Thas, H. Van Maldeghem, Translation ovoids of generalized quadrangles and hexagons, Geom. Dedicata 72 (1998) 19–62.
[9] A. Blokhius, S. Ball, A.E. Brouwer, L. Storme, T. Szőnyi, On the number of slopes of the graph of a function defined on a finite field, J. Combin. Theory, Ser. A 86 (1999) 187–196.
[10] A. Blokhuis, On the size of a blocking set in $PG(2, p)$, Combinatorica 14 (1994) 273–276.
[11] A. Blokhuis, M. Lavrauw, Scattered spaces with respect to a spread in $PG(n, q)$, Geom. Dedicata 81 (1–3) (2000) 231–243.
[12] A. Blokhuis, M. Lavrauw, On two-intersection sets with respect to hyperplanes in projective spaces, J. Combin. Theory, Ser. A 99 (2) (2002) 377–382.
[13] A. Blokhuis, L. Lovász, L. Storme, T.L. Szőnyi, On multiple blocking sets in Galois planes, Adv. Geom. 7 (1) (2007) 39–53.
[14] M. Bokler, Minimal blocking sets in projective spaces of square order, Des. Codes Cryptog. 24 (2) (2001) 131–144.
[15] G. Bonoli, O. Polverino, $\mathbb{F}_q$-linear blocking sets in $PG(2, q^4)$, Innov. Incidence Geom. 2 (2005) 35–56.
[16] G. Bonoli, O. Polverino, The twisted cubic of $PG(3, q)$ and translation spreads of $H(q)$, Discrete Math. 296 (2005) 129–142.
[17] A.E. Brouwer, H.A. Wilbrink, Blocking sets in translation planes, J. of Geom. 19 (1982) 200.
[18] R. Calderbank, W.M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. 18 (1986) 97–122.
[19] I. Cardinali, G. Lunardon, O. Polverino, R. Trombetti, Translation spreads of the classical generalized hexagon, European J. Combin. 23 (2002) 367–376.
[20] I. Cardinali, O. Polverino, R. Trombetti, On the sporadic semifield flock, Des. Codes Cryptog. 30 (2) (2003) 219–226.
[21] I. Cardinali, O. Polverino, R. Trombetti, Semifield planes of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$, European J. Combin. 27 (2006) 940–961.
[22] J.H. Conway, P.B. Kleidman, R.A. Wilson, New families of ovoids in O_8^+, Geom. Dedicata 26 (1988) 157–170.
[23] A. Cossidente, G. Lunardon, G. Marino, O. Polverino, Hermitian indicator sets, Adv. Geom. 7 (2007) 357–373.
[24] P. Dembowski, Finite Geometries, Springer Verlag, Berlin, 1968.
[25] G.L. Ebert, G. Marino, O. Polverino, R. Trombetti, Infinite families of new semifields, Combinatorica (in press).
[26] G.L. Ebert, G. Marino, O. Polverino, R. Trombetti, On the multiplication of some semifields of order q^6, Finite Fields Appl. 15 (2) (2009) 160–173. doi:10.1016/j.ffa.2008.11.003.
[27] J.W. Freeman, Reguli and pseudo–reguli in $PG(3, s^2)$, Geom. Dedicata 9 (1980) 267–280.
[28] H. Gevaert, N.L. Johnson, Flocks of quadratic cones, generalized quadrangles and translation planes, Geom. Dedicata 27 (1988) 301–317.
[29] A. Gunawardena, G.E. Moorhouse, The non-existence of ovoids in $O_9(q)$, European J. Combin. 18 (1997) 171–173.
[30] J.W.P. Hirschfeld, Finite Projective Spaces of Three Dimensions, The Clarendon Press Oxford University Press, New York, 1985.
[31] N.L. Johnson, Semifield flocks of quadratic cones, Simon Stevin 61 (3–4) (1987) 313–326.
[32] N.L. Johnson, V. Jha, M. Biliotti, Pure and Applied Mathematics, in: Handbook of Finite Translation Planes, Taylor Books, 2007.
[33] N.L. Johnson, G. Marino, O. Polverino, R. Trombetti, Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$, Finite Fields Appl. 14 (2) (2008) 456–469.
[34] N.L. Johnson, G. Marino, O. Polverino, R. Trombetti, On a generalization of cyclic semifields, Journal of Algebraic Combin. 29 (2009) 1–34.
[35] W.M. Kantor, Ovoids and translation planes, Canad. J. Math. 34 (1982) 1195–1207.
[36] W.M. Kantor, Spreads, translation planes and Kerdock sets, I, SIAM J. Algebr. Discrete Methods 3 (1982) 151–165.
[37] M. Lavrauw, Sublines of prime order contained in the set of internal points of a conic, Des. Codes Cryptog. 38 (1) (2006) 113–123.
[38] M. Lavrauw, Scattered Spaces with respect to Spreads and Eggs in Finite Projective Spaces, Ph.D. Thesis, 2001.
[39] R. Lidl, H. Niederreiter, Finite fields, in: Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (Now distributed by Cambridge University Press).
[40] G. Lunardon, Normal spreads, Geom. Dedicata 75 (1999) 245–261.
[41] G. Lunardon, Linear k-blocking sets, Combinatorica 21 (4) (2001) 571–581.
[42] G. Lunardon, Translation ovoids, J. Geom. 76 (2003) 200–215.
[43] G. Lunardon, Semifields and linear sets of $PG(1, q^t)$, Quaderni di Matematica (in press).
[44] G. Lunardon, Flocks, ovoids of $Q(4, q)$ and designs, Geom. Dedicata 66 (2) (1997) 163–173.
[45] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Translation dual of a semifield, J. Combin. Theory, Ser. A 115 (8) (2008) 1321–1332.
[46] G. Lunardon, P. Polito, O. Polverino, A geometric characterisation of linear k-blocking sets, J. Geom. 74 (2002) 120–122.
[47] G. Lunardon, O. Polverino, Blocking sets of size $q^t + q^{t-1} + 1$, J. Combin. Theory, Ser. A 90 (2000) 148–158.
[48] G. Lunardon, O. Polverino, Blocking sets and derivable partial spreads, Journal of Algebraic Combin. 14 (2001) 49–56.
[49] G. Lunardon, O. Polverino, On the twisted cubic of $PG(3, q)$, J. Algebraic Combin. 18 (2003) 255–262.
[50] G. Lunardon, O. Polverino, Translation ovoids of orthogonal polar spaces, Forum Math. 16 (2004) 663–669.
[51] G. Marino, O. Polverino, R. Trombetti, On $\mathbb{F}_q$-linear sets of $PG(3, q^3)$ and semifields, J. Combin. Theory, Ser. A 114 (2007) 769–788.
[52] G. Marino, O. Polverino, R. Trombetti, On semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd, Innov. Incidence Geom. (6–7) (2008) 271–289.

[53] G.E. Moorhouse, Root lattice constructions of ovoids, in: Finite Geometries and Combinatorics (Deinze 1992), Cambridge University Press, 1993, pp. 269–275.
[54] A.D. Offer, Translation spreads of the split Cayley hexagon, Adv. Geom. 3 (2) (2003) 105–121.
[55] A.D. Offer, Translation ovoids and spreads of the generalized hexagon $H(q)$, Geom. Dedicata 85 (1–3) (2001) 135–145.
[56] S.E. Payne, J.A. Thas, Spreads and ovoids in finite generalized quadrangles, Geom. Dedicata 52 (1994) 227–253.
[57] T. Penttila, B. Williams, Ovoids of parabolic spaces, Geom. Dedicata 82 (1–3) (2000) 1–19.
[58] P. Polito, O. Polverino, On small blocking sets, Combinatorica 18 (1) (1998) 133–137.
[59] P. Polito, O. Polverino, Blocking sets in André planes, Geom. Dedicata 75 (1999) 199–07.
[60] P. Polito, O. Polverino, On linear blocking sets in $PG(2, q^t)$, Discrete Math. 255 (2002) 343–348.
[61] O. Polverino, Blocking set nei piani proiettivi, Ph.D. Thesis, University of Naples Federico II, 1998.
[62] O. Polverino, Small blocking sets in $PG(2, p^3)$, Des. Codes Cryptog. 20 (2000) 319–324.
[63] O. Polverino, L. Storme, Small minimal blocking sets in $PG(2, q^3)$, European J. Combin. 23 (2002) 83–92.
[64] L. Storme, P. Sziklai, Linear pointsets and Rédei type k-blocking sets in $PG(n, q)$, J. Algebraic. Combin. 14 (2001) 221–228.
[65] L. Storme, Zs Weiner, Minimal blocking sets in $PG(n, q)$, $n \geq 3$., Des. Codes Cryptog. 21 (2000) 235–251.
[66] P. Sziklai, On small blocking sets and their linearity, J. Combin. Theory, Ser. A 115 (7) (2008) 1167–1182.
[67] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, Finite Fields Appl. 3 (1997) 187–202.
[68] T. Szőnyi, A. Gács, Zs. Weiner, On the spectrum of minimal blocking sets in $PG(2, q)$., J. Geom. 76 (112) (2003) 256–281.
[69] T. Szőnyi, Zs. Weiner, Small blocking sets in higher dimensions, J. Combin. Theory, Ser. A (95) (2001) 88–101.
[70] D.E. Taylor, The geometry of the classical groups, in: Sigma Series in Pure Mathematics., vol. 9, Heldermann Verlag. v, Berlin, 1992.
[71] J.A. Thas, Polar spaces, generalized hexagons and perfect codes, J. Combin. Theory Ser. A 29 (1980) 87–93.
[72] J.A. Thas, Ovoids and spreads of finite classical polar spaces, Geom. Dedicata 174 (1981) 135–143.
[73] J.A. Thas, Generalized quadrangles and flocks of cones, European J. Combin. 8 (1987) 441–452.
[74] J.A. Thas, Generalized quadrangles of order (s, s^2). II, J. Combin. Theory, Ser. A 79 (1997) 223–254.
[75] J. Tits, Sur la trialité et certains groupes qui s'en déduisent, Inst. Hautes Études Sci. Publ. Math. 2 (1959) 14–60.
[76] H. Van Maldeghem, Generalized Polygons, in: Monogr. Math., vol. 93, Birkhäuser Verlag, Basel, 1998.
[77] Zs. Weiner, Small point sets of $PG(n, q)$ intersecting each k-space in 1 modulo $\sqrt{q}$ points, Innov. Incidence Geom. 1 (2005) 171–180.