50 Years of translation structures

Guglielmo Lunardon

In memoriam Adriano Barlotti

Abstract. In this paper the term translation structure will denote any geometric object canonically constructed from an elementary abelian group. Hence, translation weak affine spaces, translation planes, linear sets, translation ovoids of polar spaces, translation generalized quadrangles and linear MRD-codes are examples of translation structures. I will present my personal excursus in the theory of finite translation structures, from the pioneering times of B. Segre, A. Barlotti and G. Tallini to these days. My aim is not to give a complete survey of the known results but to describe the influence of translation structures in proofs or disproofs of some conjectures in different areas of Finite Geometries and how valuable tool they were giving significant contributions in different areas of Discrete Mathematics.
1. Introduction

The 1960s of the past century were a “golden age” for Finite Geometries, and translation structures played a fundamental role in the researches of that period. In André [2] introduced parallel structures, i.e. incidence point-line structures with an equivalence relation in the set of lines. In Sperner [92] introduced the weak affine spaces, which are a particular case of structures with a parallelism. In Bruck and Bose [21] rediscovered the André construction of translation planes via a planar spread of a projective space (see [1]) and proved that a plane is a Moufang plane if and only if the associated planar spread is regular. In Tits [97] and [98] constructed the famous Suzuki–Tits ovoid, whose geometry was thoroughly studied in Lüneburg’s lecture notes [77] (see, also, [78]). In Segre [89] gave a complete classification of normal spreads of a finite projective space. Finally, in Barlotti and Cofman [11], generalizing André’s results, constructed a large class of translation weak affine spaces by using a spread of a projective space proving that, if the spread is not planar, then the associated translation structure is a desarguesian affine space if and only if the spread is normal.

I was introduced in the world of translation structures by my supervisor, Adriano Barlotti, who proposed me to characterize translation weak affine spaces constructed by using a spread. After we have proved that all finite central translation weak affine spaces are of Barlotti–Cofman type (see [14] and [19]), I did not work anymore on weak affine spaces until Thas [94] constructed some ovoids of the orthogonal quadrangle \(Q(4, q)\) from a semifield flock of the quadratic cone of \(PG(3, q)\). For proving that Thas ovoids are translation ovoids (see [64]), I used the representation of the projective plane \(PG(2, q^n)\) via a normal spread of \(PG(3n - 1, q)\). I tried to construct some new translation ovoids intersecting a normal spread of \(PG(3n - 1, q)\) by a transversal space: no ovoids have been found but linear blocking sets were introduced.

It Ball et al. [8] have proved a complete characterization of the small Rédei blocking sets and it was conjectured that all small blocking sets were of Rédei type. But, from the results of [8] it easily followed that any small Rédei blocking set is linear, and discussing with my PhD students, Polito and Polverino, we constructed the first example of small linear blocking set not of Rédei type (see [83]). After such a result, linear sets were widely investigated from many different points of view.

Generalizing the relationship between semifield flocks and Thas ovoids of \(Q(4, q)\), introduced in [94] and developed in [64], I used the new tool of linear sets for the study of semifield planes two dimensional over their left nucleus. (see [64]). The large number of new finite semifield planes constructed by using such a relationship (see, e.g., the survey papers [56] and [66]) proved that there were few chance to have a complete classification of finite semifield planes even of small dimensions over their nuclei.

Associated with a semifield flock of the quadratic cone of \(PG(3, q)\) there is a generalized quadrangle of order \((q^2, q)\) whose dual is a translation generalized quadrangle (see [48] and [93]). It has been proved in [87] that any translation
generalized quadrangle of order \((q, q^2)\) can be canonically constructed from a particular \((n-1)\)-partial spread \(E\) of \(\text{PG}(4n-1, s)\), \(q = s^n\), called an egg. Denote by \(T(E)\) the generalized quadrangle associated with \(E\). If \(\perp\) is a polarity of \(\text{PG}(4n-1, s)\) then \(E_{\perp} = \{X_{\perp} | X \in E\}\) is still an egg and the associated translation quadrangle is called the translation dual of \(T(E)\) (see [86]). In Thas [95] proved some strong results on the structure of the translation dual of the dual of a semifield flock and conjectured that the only semifield flocks were linear flocks, Kantor flocks, and Ganley flocks. By using the isomorphism criterion for translation structures of Barlotti–Cofman type, in [6] it has been proved that the sporadic flock constructed in [6] from the Pentilla–Williams ovoid of \(Q(4, 243)\) disproves the Thas’ conjecture, even though it is presently the only known counterexample.

Finally, let \(C\) be a set \(m \times n\) matrices over \(\mathbb{F}_q\) such that the rank \(A - B\) is at least \(d = d(C)\). It is well-known that
\[
|C| \leq q^{\max\{m,n\}(\min\{m,n\} - d + 1)},
\]
which is the Singleton bound for the rank metric distance (see [29]). When equality holds, we call \(C\) a maximum rank distance (MRD for short) code. Maximum rank distance codes, introduced by Delsarte [29], have been recently rediscovered by Kötter and Kschischang [47] as network codes for networks with close topology. The first examples of MRD-codes over the finite field \(\mathbb{F}_q\) for every \(k, n\) have been constructed by Delsarte [29] and Gabidulin [32]. An MRD-code \(C\) is linear if \(C\) is closed under addition. By using the relationship between matrices of order \(n \times n\) and linearized polynomials, which is very well studied in the theory of finite semifields, Sheekey [90] made a breakthrough in theory of linear MRD-codes constructing some new examples of linear MRD-codes. In [75], it has been proved that any MRD-code defines a translation structure with parallelism of Barlotti–Cofman type and, by using some particular collineation groups of such a structure, some relevant invariants for MRD-codes have been introduced.

The paper is organized as follows.

In Sect. 2 we recall the general theory of translation structures with parallelism paying specific attention to central translation weak affine spaces of Barlotti–Cofman type, proving Segre’s theorem on the uniqueness, up to isomorphisms, of normal spreads of \(\text{PG}(rn-1, q)\). Generalizing the Barlotti–Cofman construction, we construct a translation structure with parallelism from a general family of \((n-1)\)-dimensional subspaces of a finite projective space \(\text{PG}(rn-1, q)\). From the results of André [2], we obtain an isomorphism criterion for such structures.

Section 3 is devoted to linear sets. We use an alternative construction of the projective space \(\text{PG}(r-1, q^n)\) from a normal spread of \(\text{PG}(rn-1, q)\) for defining linear sets of \(\text{PG}(r-1, q^n)\). We discuss some applications of linear sets to the theory of blocking sets, mifield planes, symplectic spreads of \(\text{PG}(3, q)\), and translation generalized quadrangles.

In Sect. 4 we point out that, applying the Knuth cubical array, the classification of finite semifields of dimension \(n\) over one of their nuclei is equivalent to that of
finite semifields of dimension $n$ over their left nucleus, whilst the classification of commutative semifields of dimension $n$ over their middle nucleus $N_m = \mathbb{F}_q$ is equivalent to that of symplectic semifield spreads of $\text{PG}(2n-1,q)$.

Section 5 is dedicated to linear MRD-codes. We present the relationship between linear sets of linearized polynomials and linear MRD-codes studied in [67] discussing some generalizations of Sheekey’s constructions. Finally, we associate to an MRD-code a translation structure with parallelism of Barlotti–Cofman type and, applying the isomorphism criterion for such structures, we introduce the kernel, the left and the right idealizer of a linear MRD-code.

I would like to thank H. Havlicek and A. Kreuzer, Editors in Chief of Journal of Geometry, for inviting me to submit an article to this special issue, which allowed me to retrace a remarkable part of my research work, paying special attention to its geometric perspective, according to the teachings of my master Adriano Barlotti.

2. Translation weak affine spaces

2.1. Structures with parallelism

An incidence structure $\mathcal{A} = (P, L)$ is a pair of sets such that $P \neq \emptyset$, whose elements will called points, and $L$ is a family of subsets of $P$, whose elements are called lines, such that:

(I) any line contains at least two points,

(II) any point belongs to at least two lines.

An incidence structure $\mathcal{A}$ is a structure with parallelism if it is defined a equivalence relation $||$ on the set of lines $L$, called a parallelism, such that parallel lines are disjoint.

We point out that, in general, disjoint lines are not necessarily parallel.

For $i = 1, 2$ let $\mathcal{A}_i = (P_i, L_i)$ be two structures with parallelism. An isomorphism between $\mathcal{A}_1$ and $\mathcal{A}_2$ is a bijection $\sigma : P_1 \cup L_1 \longrightarrow P_2 \cup L_2$ which maps points to points, lines to lines and preserves the incidence and the parallelism.

If $\mathcal{A}_1 = \mathcal{A}_2$, we say that $\sigma$ is a collineation.

Let $\mathcal{A}$ be a structure with parallelism. A dilation of $\mathcal{A}$ is a collineation $\tau$ such that $L\tau||L$ for all lines $L$ of $\mathcal{A}$. The dilations of $\mathcal{A}$ form a group $D$.

A translation is a dilation which either is the identity or does not fix any point. Of course, the inverse of a translation is a translation.

If $\sigma$ and $\tau$ are two translations, then $\sigma\tau$ is a translation if and only if either $\sigma\tau$ is the identity or $\sigma(P) \neq \tau^{-1}(P)$ for any point $P$. Hence, the set $T$ of all translations is a subgroup of $D$ if and only if given two points $Q$ and $R$, there is at most one translation $\sigma$ such that $\sigma(Q) = R$. This implies that $T$, in general, is not a subgroup of $D$.

We call $\mathcal{A}$ a translation structure with parallelism if

(a) the set $T$ of all translations of $\mathcal{A}$ is a subgroup of $D$ which acts sharply transitively on the points of $\mathcal{A}$;

(b) if $L$ is a line of $\mathcal{A}$, then the stabilizer $T_L$ of $L$ in $T$ is transitive on the points of $L$. 

The group $T$ is called the translation group of $A$.
We recall the canonical construction of a translation structure with parallelism from its translation group due to André (see [2]).

Let $A$ be a translation structure with parallelism. Let $x$ be a fixed point and let $L_0, L_1, \ldots, L_s$ be the lines of $A$ incident with $x$. Define $T_{L_i} = \{ \tau \in T \mid L_i \tau = L_i \}$ and put $P = \{ T_{L_i} \mid i = 0, 1, \ldots, s \}$. We will say that $P$ is the congruence of $T$ associated with $A$. As $T$ is transitive on the points of $A$, the congruence $P$ is uniquely defined up to conjugation.

For each line $M$ of $A$ there is an element $\tau$ of $T$ and an index $i \in \{0, 1, \ldots, s\}$ such that $M = L_i \tau$. Therefore the coset $T_{L_i} \tau$ is the set of the elements of $T$ which map $x$ to a point of $M$ and for each point $y$ of $M$ there is exactly one element $\mu$ of $T_{L_i} \tau$ such that $x \mu = y$.

Let $S(T, P)$ be the point-line structure whose points are the elements of $T$ and whose lines are the cosets of elements of $P$.

For each point $y$, let $\tau_y$ be the element of $T$ which maps $x$ to $y$ and let $\beta_x$ be the map from $A$ to $S(T, P(A))$ defined by $y \mapsto \tau_y$ and $M \mapsto T_{L_i} \tau$ if and only if $M = L_i \tau$. Then $\beta_x$ is an isomorphism between $A$ and $S(T, P)$.

When $T$ is abelian, the kernel $K$ of $P$ is the set of all automorphisms $k$ of $T$ such that $T_{L_i}^k \subset T_{L_i}$ for all $i \in \{0, 1, \ldots, s\}$. As $T$ is abelian, $K$ with the following operations forms a ring. We will use the exponential notation so that the sum and the multiplication of $K$ are defined by $\tau^{k+h} = \tau^k \tau^h$ and $\tau^{kh} = (\tau^h)^k$ for all $\tau \in T$. Hence, the group $T$ is a $K$-module and each element of $P$ is a submodule of $T$.

For $i = 1, 2$ let $A_i = (P_i, L_i)$ be a translation structure with parallelism. Denote by $T_i$ the translation group of $A_i$, and by $P_i$ the congruence of $T_i$ associated with $A_i$. If $\sigma$ is an isomorphism from $A_1$ to $A_2$, then for any translation $\tau \in T_1$ the map $\sigma^\tau = \sigma^{-1} \tau \sigma$ is an element of $T_2$ and $\alpha : T_1 \to T_2$ is which map $P_1$ to $P_2$.

If $T_i$ is an abelian group, denote by $K_i$ the kernel of $P_i$. The map

$$\alpha : K_1 \to K_2, \quad k \mapsto k^\alpha = \sigma^{-1} k \sigma$$

is an isomorphism of rings. Therefore $\alpha$ is a non-singular linear map between $T_1$ and $T_2$ regarded as modules over their kernel. Hence we have proved the following lemma.

**Lemma 1.** (André [2]). For $i = 1, 2$ let $A_i = (P_i, L_i)$ be two translation structures with parallelism. Denote by $T_i$ the translation group of $A_i$ and let $P_i$ be the congruence associated with $A_i$. Suppose that $T_i$ is abelian.

The translation structures with parallelism $A_1$ and $A_2$ are isomorphic if and only if there is a non-singular map between $T_1$ and $T_2$ regarded as modules over their kernels, which maps $P_1$ into $P_2$.

### 2.2. Weak affine spaces

A structure with parallelism $A$ is a weak affine space if the following axioms are satisfied:

(A1) Two points are incident with exactly one common line;

(A2) Any line is incident with the same cardinal number $s \geq 2$ of points;
(A3) If the point $x$ is not incident with the line $L$, there is a unique line $M$ incident with $x$ and parallel to $L$.

We say that a weak affine space $A$ is an affine geometry when the following further axiom hold:

(A4) Let $L_1$ and $L_2$ two lines incident with a common point $O$. Denote by $x_1, y_1$ two points of $L_1$ and by $x_2, y_2$ two points of $L_2$ different from $O$. If the line $M_1$, joining $x_1$ and $y_1$, and the line $M_2$, joining $x_2$ and $y_2$, are not parallel, then there exists a point $z$ incident with $M_1$ and $M_2$.

We say that a weak affine space $A$ is an affine plane when

(A5) Two lines either are parallel or are incident with a common point.

Let $\tau$ be a translation of the weak affine space $A$, i.e. a dilation which either is the identity or has no fixed points. If $L = L^\tau$ and $M || L$ imply $M^\tau = M$, we say that $\tau$ is a central translation. If the translation group $T$ of $A$ acts sharply transitively on the points of $A$, we say that $A$ is a translation weak affine space.

The translation weak affine space $A$ is called central if any translation of $T$ is central. The next theorem, due to J. André, gives a characterisation of central translation weak affine spaces.

**Theorem 1.** [2, Satz 2.4]. A translation weak affine space is central if and only if its translation group is abelian.

In Barlotti and Cofman [11] have constructed a large class of central translation weak affine spaces generalizing the construction of a translation plane via a spread of a projective space due to André [1].

Let $K$ be a skewfield, $A$ partial spread of $\mathrm{PG}(V, K)$ is a family $S$ of mutually skew isomorphic subspaces. When $S$ is a partition of the point-set of $\mathrm{PG}(V, K)$, we say that $S$ is a spread of $\mathrm{PG}(V, K)$. If all elements of $S$ have dimension $h - 1$ we say that $S$ is an $(h - 1)$-spread.

Let $S$ be a spread of $\mathrm{PG}(V, K)$ and let $V'$ be a $K$-vector space such that $V' = V \oplus \langle v_0 \rangle$ for some $v_0$. Hence $V$ is a vector subspace of $V'$ of codimension 1 and $\Sigma' = \mathrm{PG}(V', K)$ is a hyperplane of $\Sigma' = \mathrm{PG}(V', K)$. Define a point-line geometry $A(\Sigma', \Sigma, S)$, briefly $A(S)$, in the following way. The points of $A(S)$ are the points of $\Sigma'$ not incident with $\Sigma$. The lines of $A(S)$ are the subspaces $X'$ of $\Sigma'$ non contained in $\Sigma$ such that $X = X' \cap \Sigma$ is an element of $S$. The incidence is inherited from $\Sigma'$. Two lines of $A(S)$ are parallel if and only if they contain the same element of $S$.

We recall that an central collineation $\sigma$ of $\Sigma'$ with axis $\Sigma$ and center $O$ is a collineation of $\Sigma'$ which fixes all points of $\Sigma$ and all the line incident with $O$. We say that $\sigma$ is an elation if either $\sigma = \text{id}$ or $O \in \Sigma$. The elation with axis $\Sigma$ form an abelian group sharply transitive on the points of $\Sigma' \setminus \Sigma$ (see, e.g., [30, Chapter 1.4]).

It is easy to prove that $A(S)$ is a central translation weak affine space whose translation group is the elation group of the projective space $\Sigma'$ whose axis is $\Sigma$. If $\delta$ is a central collineation of $\Sigma'$ with axis $\Sigma$ and center $O \not\in \Sigma$, then $\delta$ defines a dilation of $A(S)$ and the automorphism of $T$ defined by $\tau \mapsto \delta^{-1} \tau \delta$ belongs to the kernel of $A(S)$, i.e. the kernel of $A(S)$ contains, up to isomorphism, the subfield $K$. 
A central weak affine space is said to be of \textit{Barlotti–Cofman type} if it is isomorphic to \( \mathcal{A}(S) \) for some spread \( S \).

The spread \( S \) is \textit{planar} if for any two distinct elements \( X \) and \( Y \) of \( S \), the subspace joining \( X \) and \( Y \) is \( \Sigma \), i.e. \( \langle X, Y \rangle = \Sigma \). If \( \Sigma = \text{PG}(n-1, \mathbb{K}) \), then a \((t-1)\)-spread of \( \Sigma \) is planar if and only if \( n = 2t \). If \( S \) is a planar spread, then the structure \( \mathcal{A}(S) \) is an affine translation plane \([1]\).

We say that a spread \( S \) is desarguesian if the weak affine space \( \mathcal{A}(S) \) is a desarguesian affine space.

\textbf{Example 1. (Field reduction).} We will say that an element \( X \) of the projective space \( \text{PG}(V, \mathbb{K}) \) has \textit{rank} \( r \) and \textit{dimension} \( d = r - 1 \) if \( X \), as vector subspace of \( V \), is spanned by \( r \) vectors.

Let \( \mathbb{F} \) be a subskewfield of \( \mathbb{K} \). A left vector space \( V \) over \( \mathbb{K} \) can be regarded as a vector space over \( \mathbb{F} \). Let \( \Sigma = \text{PG}(V, \mathbb{F}) \) be the projective space defined by the lattice of the \( \mathbb{F} \)-subspaces of \( V \). Each \( \mathbb{K} \)-vector subspace of rank 1, say \( \langle v \rangle \), of \( V \) defines an \( \mathbb{F} \)-vector subspace, say \( L(v) \), of rank \([\mathbb{K} : \mathbb{F}]\).

For any point \( x \) of \( \Sigma \) there is a vector \( v \) of \( V \) such that \( x = \{ av \mid a \in \mathbb{F} \} \), i.e. \( x \in L(v) \). Moreover \( L(v) \cap L(w) \neq \emptyset \) implies \( v = \alpha w \) for some \( \alpha \) in \( \mathbb{K} \), i.e. \( L(v) = L(w) \). Hence \( \Sigma = \{ L(v) \mid v \in V \} \) is a spread of \( \Sigma = \text{PG}(V, \mathbb{F}) \), called the \( \mathbb{F} \text{-linear representation} \) of \( \text{PG}(V, \mathbb{K}) \).

The map from the desarguesian affine space \( \text{AG}(V, \mathbb{K}) \) to \( \mathcal{A}(\mathcal{L}) \), which maps the point \( x \) of \( \text{AG}(V, \mathbb{K}) \) to the point \( \langle v_0 + x \rangle \) of \( \mathcal{A}(\mathcal{L}) \) and the line \( x + (y) \) of \( \text{AG}(V, \mathbb{K}) \) to the line \( \langle v_0 + x + L(y) \rangle \) of \( \mathcal{A}(\mathcal{L}) \), is an isomorphism. Hence \( \mathcal{L} \) is a desarguesian spread of \( \Sigma \).

\textbf{Example 2. (Segre’s spread \([89]\)).} The original Segre’s construction involves some properties of grassmannians. Here we present an equivalent construction and we refer to \([62]\) for more details.

Let \( \mathbb{F} \) be a field and let \( \mathbb{K} \) be a Galois extension of \( \mathbb{F} \) with finite degree \( t \). Hence the group \( G \) of automorphisms of \( \mathbb{K} \) fixing \( \mathbb{F} \) elementwise has order \( t \); put \( G = \{ \sigma_0 = id, \sigma_1, \ldots, \sigma_{t-1} \} \). If \( x = (x_1, x_2, \ldots, x_r) \) belongs to \( \mathbb{K}^r \), we still denote by \( \sigma_i \) the semilinear map of \( \mathbb{K}^r \) into itself defined by \( \sigma_i^\alpha = (x_1^\alpha, x_2^\alpha, \ldots, x_r^\alpha) \).

Let \( V^* = \mathbb{K}^r = \mathbb{K}^r \times \mathbb{K}^r \times \cdots \times \mathbb{K}^r \) and let \( \tau_i \), with \( i = 0, 1, \ldots, t - 1 \), be the \( \mathbb{F} \)-semilinear map defined by \( \tau_i : (x_1, x_2, \ldots, x_t) \mapsto (x_1^{\sigma_i}, x_2^{\sigma_i}, \ldots, x_t^{\sigma_i}) \). Then \( V = \mathbb{F}^r = \mathbb{F}^r \times \mathbb{F}^r \times \cdots \times \mathbb{F}^r = \cap_{i=0}^{t-1} \text{Fix} \tau_i \) is the set of fixed vectors of all \( \tau_i \) (\( i = 0, 1, \ldots, t - 1 \)), and \( V^* = V \otimes \mathbb{K} \). Hence \( \Sigma = \text{PG}(V, \mathbb{F}) = \text{PG}(rt - 1, \mathbb{F}) \), \( \Sigma^* = \text{PG}(V^*, \mathbb{K}) = \text{PG}(rt - 1, \mathbb{K}) \) and \( \Sigma \) is a canonical subgeometry of \( \Sigma^* \) (see Section 3 for the definition).

Let \( f(x) \) be an irreducible polynomial over \( \mathbb{F} \) of degree \( t \) such that \( \mathbb{K} \) is the splitting extension of \( f(x) \). Denote by \( \alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{K} \) the roots of \( f(x) \). Let \( \Pi_i = \{ (x, \alpha_1 x, \alpha_2 x, \ldots, \alpha_i x^{t-1}) \mid x \in \mathbb{K}^r \} \). Then \( \Pi_i \) is an \((r-1)\)-dimensional subspace of \( \Sigma^* \). Note that if \((x^{\sigma_i}, x_i^{\sigma_i} x_j^{\sigma_i}, (\alpha_i^0)^{\sigma_j} x_j^{\sigma_j}, \ldots, (\alpha_i^{t-1})^{\sigma_j} x_j^{\sigma_j}) = \lambda (x, \alpha_1 x, \alpha_2 x, \ldots, \alpha_i x^{t-1}) \) for some \( \lambda \in \mathbb{K} \), then \( x^{\sigma_i} = \lambda x \) and \( \alpha_i^{\sigma_j} x_j^{\sigma_j} = \lambda \alpha_i x_j \), i.e. \( \alpha_i^{\sigma_j} = \alpha_i \) because \( x \neq 0 \). Hence, if a point \((x, \alpha_1 x, \alpha_2 x, \ldots, \alpha_i x^{t-1}) \) of \( \Pi_i \) belongs to \( \Sigma \) then it is fixed by \( \tau_j \) for \( j = 0, 1, \ldots, t - 1 \), and \( \alpha_i^{\sigma_j} = \alpha_i \) for \( j = 0, 1, \ldots, t - 1 \) Thus \( \alpha_i \)
Let \( \Sigma \) and \( F \) belongs to \( \mathbb{F} \). By construction this is impossible and therefore \( \Pi_i \) and \( \Sigma \) are disjoint.

In a similar way we can prove that \( \Pi_i \) and \( \Pi_j \) are disjoint when \( i \neq j \), hence \( \Sigma^* = \langle \Pi_1, \Pi_2, \ldots, \Pi_t \rangle \) and \( \Pi_1^{\sigma_t} = \Pi_j \).

We can reorder the \( \alpha \)'s in such a way that \( \alpha_j = \alpha_1^{\sigma_j} \) for \( j = 2, \ldots, t \). For any point \( v = (x, \alpha_1 x, \alpha_1^2 x, \ldots, \alpha_1^{t-1} x) \) of \( \Pi_1 \) let

\[
S^*(v) = \langle v, v^{\sigma_1}, \ldots, v^{\sigma_{t-1}} \rangle.
\]

Then \( S^*(v) \) has dimension \( t - 1 \) because \( \Sigma^* = \langle \Pi_1, \Pi_2, \ldots, \Pi_t \rangle \). Also

\[
S(v) = S^*(v) \cap \Sigma = \{ \lambda v + (\lambda v)^{\sigma_1} + \cdots (\lambda v)^{\sigma_{t-1}} \mid \lambda \in \mathbb{K} \}
\]
is a \((t-1)\)-dimensional subspace of \( \Sigma \). By construction two different subspaces \( S(v) \) and \( S(w) \) are disjoint.

Moreover, for any point \( \langle w \rangle \) of \( \Sigma \) there is a unique point \( \langle v_i \rangle \) in \( \Pi_i \) such that \( w = v_1 + v_2 + \cdots + v_t \). As the Galois group is transitive on the subspaces \( \Pi_i \), and \( \langle w \rangle \) is fixed by any element of \( G \), we have \( w = v_1 + v_1^{\sigma_1} + \cdots + v_1^{\sigma_{t-1}} \), which belongs to \( S(v_i) \).

Hence \( \mathcal{F} = \{ S(v) \mid v \in \Pi_1 \} \) is a spread of \( \Sigma = \text{PG}(rt - 1, \mathbb{F}) \), called the Segre spread \([89]\) of \( \text{PG}(rt - 1, \mathbb{F}) \).

If \( r = 2 \), then \( \mathcal{F} \) is a planar spread. When \( r \) is bigger than 2, then the subspace \( \langle S(x), S(y) \rangle \) of \( \Sigma \) consists of all elements of \( \mathcal{F} \) of the type \( S(\alpha x + \beta y) \) with \( \alpha, \beta \in K \).

The \((r-1)\)-dimensional subspaces \( \Pi_i \) for \( i = 1, 2, \ldots, t \) are called the transversal \((r-1)\)-subspaces of \( \mathcal{F} \).

**Theorem 2.** The Segre spread \( \mathcal{F} \) of \( \text{PG}(rt - 1, \mathbb{F}) \) is desarguesian.

**Proof.** Let \( \mathcal{F}' \) be the Segre spread of \( \Lambda = \text{PG}((r + 1)t - 1, \mathbb{F}) \) and let \( \Pi'_i, \) \( i = 1, 2, \ldots, t \), be the transversal subspaces of \( \mathcal{F}' \). Then each \( \Pi'_i \) has dimension \( r \). We can suppose that each \( \Pi_i \) is a subspace of the relevant \( \Pi'_i \). Hence \( \Sigma = \text{PG}(rt - 1, \mathbb{F}) \) is a subspace of \( \Lambda \) and \( \mathcal{F} \) is contained in \( \mathcal{F}' \), i.e. \( \mathcal{F} = \{ X \in \mathcal{F}' \mid X \cap \Sigma \neq \emptyset \} \).

Let \( \Sigma' \) be a subspace of \( \Lambda \) of dimension \( rt \), which contains \( \Sigma \). Let \( \text{AG}(r, \mathbb{K}) \) be the affine geometry whose points are the elements of \( \Pi'_1 \setminus \Pi_1 \). For any point \( v \) of \( \Pi'_1 \setminus \Pi_1 \) and for any line \( L \) not contained in \( \Pi_1 \) define

\[
\phi : \langle v \rangle \mapsto S(v) \cap \Sigma'
\]

and

\[
\phi : L = \langle v, w \rangle \mapsto \langle S(v), S(w) \rangle \cap \Sigma'.
\]

Then \( \phi \) is an isomorphism from \( \text{AG}(r, \mathbb{K}) \) to \( A(\Sigma', \Sigma, \mathcal{F}) \). \( \square \)

**Example 3.** We present an example of weak affine space which is not a translation weak affine space.

We recall that a spread of \( \text{PG}(3, q) \) is set of \( q^2 + 1 \) mutually disjoint lines. A parallelism \( \mathbb{P} \) of \( \text{PG}(3, q) \) is a set of \( q^2 + q + 1 \) mutually disjoint spreads. As \( \text{PG}(3, q) \) has \((q^2 + 1)(q^2 + q + 1) \) lines, any line belongs to exactly one spread of \( \mathbb{P} \). We can define a weak affine space \( \mathcal{A}_\mathbb{P} \) in the following way. The points
and the lines of $A_P$ are, respectively, the points and the lines of $PG(3, q)$. The incidence is the natural one. Two lines of $A_P$ are parallel if and only if they belongs to the same spread of $\mathbb{P}$.

We recall that three mutually disjoint lines $L_1, L_2, L_3$ of $PG(3, q)$ $q > 2$ define a unique hyperbolic quadric $Q^+(3, q)$ containing such lines. Denote by $R(L_1, L_2, L_3)$ the regulus of $Q^+(3, q)$ containing $L_1, L_2, L_3$. The other regulus of $Q^+(3, q)$ will be called the opposite regulus to $R(L_1, L_2, L_3)$.

The desarguesian spread $S$ of $PG(3, q)$, $q > 2$, has the following properties. If $L_1, L_2, L_3$ are lines of $S$, then the regulus $R(L_1, L_2, L_3)$ is contained in $S$ (see [21]). If $\mathcal{R}$ is a regulus contained in $S$ and $\mathcal{R}'$ is its opposite regulus, then $S' = (S \setminus \mathcal{R}) \cup \mathcal{R}'$ is a spread of $PG(3, q)$ called a Hall spread. It is well known that a Hall spread does not have a collineation group which acts transitively on the line of $S'$ (see, e.g., [30, pp. 234–235]).

R. H. Bruck has constructed a parallelism $B$ of $PG(3, q)$, $q > 2$, which contains a desarguesian spread and $q^2 + q$ Hall spreads (see, also, [13]). By way of contradiction suppose that $A_B$ is a translation weak affine space. As any collineation of $A_B$ is defined by a collineation of $PG(3, q)$, there is a collineation group $T$ of $PG(3, q)$ of size $(q^2 + 1)(q + 1)$ which acts regularly on the points of $PG(3, q)$.

If $\tau$ is a translation, then for any line $L$ we have $L^\tau \parallel L$, i.e. $L^\tau$ and $L$ belong to the same spread of $B$. As $T_L$ is transitive on the points of $L$, the subgroup $T_L$ has order $q + 1$ and $\{L^\tau \mid \tau \in T\}$ is a class of parallelism of $A_B$, i.e. a spread of $B$. This implies that $T$ acts transitively on any spread of $B$. Since this is not possible for the Hall spread, we have the required contradiction.

It has been proved by André [1] that all translation planes can be constructed in such a way. It was a natural question to ask if any central translation weak affine space is of Barlotti–Cofman type. The answer is negative and, to explain the results, we are going back to the canonical construction of a translation structure with parallelism explained in Sect. 2.1.

Let $A$ be a translation weak affine space. Denote by $T$ its translation group and by $\mathcal{P}$ the congruence of $T$ associated with $A$. By axioms (A1) and (A3), the congruence $\mathcal{P}$ has the following properties:

1. The components of $\mathcal{P}$ are nontrivial subgroups of $T$, i.e. they are different from $\{id\}$ and $T$;
2. The components of $\mathcal{P}$ have the same cardinality;
3. Two components of $\mathcal{P}$ have trivial intersection;
4. Any element of $T$ belongs to a unique component of $\mathcal{P}$.

We will call such a family a (nontrivial) partition of $T$. By the results of Sect. 2.1, $A$ is isomorphic to $A(T, \mathcal{P})$. The next theorem, due to J. André, gives a characterisation of the kernel of a central translation weak affine space.

**Theorem 3.** [2, Satz 4.3]. The kernel of a partition $\mathcal{P}$ of an abelian group $T$ is a ring without zero-divisors.

Next, we review some known results from the point of view of the relationships between spreads and translation affine weak structures we have just discussed.
Theorem 4. [19]. Let $\mathcal{P}$ be a partition of an abelian group $T$ and let $K$ be the kernel of $\mathcal{P}$. The translation weak affine space $\mathcal{A}(T, \mathcal{P})$ is a desarguesian affine geometry if and only if $K$ is a skewfield and any component of $\mathcal{P}$ has dimension one over $K$.

Example 4. We can regard $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space of rank $n$. If $\varphi$ is a generator of the multiplicative group of $\mathbb{F}_{q^n}$, the $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$ into itself, which maps $x$ to $x\varphi$, defines a collineation $\tau_\varphi$ of $\text{PG}(n-1, q) = \text{PG}(\mathbb{F}_{q^n}, \mathbb{F}_q)$ of order $q^{n-1} + q^{n-2} + \cdots + q + 1$ and the collineation group $G = \langle \tau_\varphi \rangle$ acts sharply transitively on the points of $\text{PG}(n-1, q)$. The group $G$ is called a Singer cycle of $\text{PG}(n-1, q)$; for further details, see e.g. [40, Sect. II.10].

If $n = mr$, then $\mathbb{F}_{q^r}$ is a subfield of $\mathbb{F}_{q^n}$. Let $U = \langle \mathbb{F}_{q^r} \rangle$ be the $(r-1)$-dimensional subspace of $\text{PG}(n-1, q)$ associated with $\mathbb{F}_{q^r}$ and define

$$S = \{U^\tau \mid \tau \in G\}.$$ 

As $\varphi' = \varphi^{q^n-1}$ is a generator of $\mathbb{F}_{q^r}$, the group $H = \langle \tau_{\varphi'} \rangle$ fixes the subspace $U$.

We note that if $\tau = (\tau_{\varphi})^i$, then $U^\tau = \langle \mathbb{F}_{q^r} \varphi^i \rangle$. Hence $U \cap U^\tau \neq \emptyset$ if and only if there are two elements $\alpha$ and $\beta$ in $\mathbb{F}_{q^r}$ such that $\alpha = \beta \varphi^i$, i.e. $\varphi^i \in \mathbb{F}_{q^r}$. Hence $\varphi^i$ belongs to $\mathbb{F}_{q^r}$ and this implies $U = U^\tau$, thus two elements of $S$ are disjoint. Also, as $H$ is the stabilizer of $U$ in $G$, $S$ contains $\frac{q^n-1}{q^r-1}$ subspaces, i.e. $S$ is an $(r-1)$-spread of $\text{PG}(n-1, q)$.

Theorem 5. If $n = mr$, then $S$ is a desarguesian $(r-1)$-spread of $\text{PG}(n-1, q)$.

Proof. The spread $S$ is defined by the partition $\mathcal{P} = \{\mathbb{F}_{q^r} \varphi^i\}$ of the additive group of $\mathbb{F}_{q^n}$ and $\mathcal{A}(S)$ is isomorphic to $\mathcal{A}(\mathbb{F}_{q^n}, \mathcal{P})$. As $\mathcal{A}(\mathbb{F}_{q^n}, \mathcal{P})$ is finite, the kernel of $\mathcal{P}$ is a field.

If $\mu \in H$, then $\mu(x) = x\alpha$ with $\alpha \in \mathbb{F}_{q^r}$. Hence

$$\langle \mathbb{F}_{q^r} \varphi^i \rangle^\mu = \langle \mathbb{F}_{q^r} \varphi^i \alpha \rangle = \langle \mathbb{F}_{q^r} \alpha \varphi^i \rangle = \langle \mathbb{F}_{q^r} \varphi^i \rangle.$$

This proves that $H$ fixes all the elements of $\mathcal{P}$. Therefore the kernel of $\mathcal{P}$ has order $q^r$. By Theorem 4, $\mathcal{A}(S) \sim AG(m, q^r)$ is a desarguesian spread. \qed

A partition $\mathcal{P}$ of an abelian group $T$ is said to be homogeneous if

(a) the kernel of $\mathcal{P}$ contains a subskewfield;

(b) the elements of $\mathcal{P}$ are mutually isomorphic.

Let $\mathcal{P}$ be a homogeneous partition. For any subskewfield $\mathbb{F}$ of the kernel of $\mathcal{P}$, let $\Sigma = \text{PG}(T, \mathbb{F})$. As any component of $\mathcal{P}$ is an $\mathbb{F}$-vector subspace of $\Sigma$, the family $\mathcal{P}(\mathbb{F}) = \{\langle X \rangle \mid X \in \mathcal{P}\}$ is a spread of $\Sigma$ and $\mathcal{A}(\mathcal{P}(\mathbb{F}))$ is isomorphic to $S(T, \mathcal{P})$.

Two spreads $S_1$ and $S_2$ of $\Sigma$ are isomorphic if there is a collineation $\sigma$ of $\Sigma$ such that $S_1^\sigma = S_2$.

The central translation weak affine space of Barlotti- Cofman type have been independently characterized by Biliotti [14] and Bonetti and the author in [19], who proved the following theorem.
Theorem 6. [14,19]. Let $A = S(T, P)$ be a translation weak affine space whose translation group is abelian. There is a spread $S$ such that $A$ is isomorphic to $A(S)$ if and only if $P$ is a homogeneous partition and there is a subskewfield $\mathbb{F}$ of $\ker P$ such that $S$ and $P(\mathbb{F})$ are isomorphic.

Proof. For a proof see, e.g., [5, Corollary 12]. □

Theorem 6 gives the required characterisation of the weak affine space constructed by a spread. As an application we have the following corollary.

Corollary 1. Any finite central weak affine space $A$ is of Barlotti–Cofman type.

Proof. We recall that a finite ring without zero-divisors is a field. Hence any partition $P$ of a finite abelian group $T$ is homogeneous because the kernel $K$ of $P$ is a field and the elements of $P$ are $K$-vector subspaces of the same dimension because they have the same order.

By Theorem 6, $A$ is of Barlotti–Cofman type. □

Corollary 2. [19]. Let $S_1$ and $S_2$ be two spreads of a projective space. The weak affine spaces $A(S_1)$ and $A(S_2)$ are isomorphic if and only if the spreads $S_1$ and $S_2$ are isomorphic.

Proof. For $i = 1, 2$ let $S_1 \sim P_i(\mathbb{F})$. We can suppose that they have the same translation group $T$ and the same kernel $K$ containing the subskewfield $\mathbb{F}$. If $A(S_1)$ and $A(S_2)$ are isomorphic, by Lemma 1 there is a semilinear collineation $\tau$ of $T$ as $K$-module which maps $P_i$ to $P_2$. As we can regard $\tau$ as an $\mathbb{F}$-semilinear map of $T$ as vector space over $\mathbb{F}$, $\tau$ induces a collineation of $\text{PG}(T, \mathbb{F})$ which maps $P_i(\mathbb{F})$ into $P_2(\mathbb{F})$. Therefore $S_1 \simeq P_1(\mathbb{F}) \simeq P_2(\mathbb{F}) \simeq S_2$. □

2.3. Normal spreads

A non-planar spread $S$ of $\Sigma$ is normal when, for all components $X$ and $Y$ of $S$, any element of $S$ is either disjoint from $\Lambda = \langle X, Y \rangle$ or it is contained in it. Hence

$$S_\Lambda = \{Z \in S \mid Z \subset \Lambda\}$$

is a spread of $\Lambda$. Therefore for any subspace $\Lambda' = \langle \Lambda, P \rangle$ of $\Sigma'$ not contained in $\Sigma$, the translation plane $A(\Lambda', \Lambda, S_\Lambda)$ is a subplane of $A(S)$.

Theorem 7. [11]. A non-planar spread $S$ of $\Sigma$ is desarguesian if and only if it is a normal spread.

Proof. Note that the definition of normal spread is equivalent to axiom (A4) for central translation weak affine spaces. As $S$ is non-planar, $A(S)$ is not a plane. Hence $A(S)$ is isomorphic to a desarguesian affine space. □

In Segre [89] has proved that a normal spread of a finite projective space is isomorphic to the Segre spread of $\text{PG}(rn - 1, q)$ by using some arguments of classical algebraic geometry. By Theorem 7 we can give a simple proof a Segre’s Theorem.

Corollary 3. [89]. If $r > 2$, there is, up to isomorphism, a unique normal spread of $\text{PG}(rn - 1, q)$. 


Proof. By Theorem 7, a normal spread is desarguesian. As \( r > 2 \) there is, up to isomorphism, a unique affine space \( AG(r, q^n) \) and a unique desarguesian spread by Corollary 2.

We conclude this section with an example of non-normal spread and, hence, non-desarguesian by Theorem 7.

Example 5. Let \( \mathcal{L} \) be the \( \mathbb{F}_q \)-linear representation of the desarguesian plane \( PG(2, q^n) = PG(V, \mathbb{F}_q^n) \) in \( PG(3n - 1, q) \).

For each \( \lambda \in \mathbb{F}_q^n \) let \( \tau_\lambda \) be the collineation of \( PG(2, q^n) \), defined by the linear mapping of \( V \) in itself which maps \( v \mapsto \lambda v \) for all vectors \( v \) of \( V \). We notice that \( \tau_\lambda \) fixes all the points of \( PG(2, q^n) \). Also \( E = \{ \tau_\lambda : \lambda \in \mathbb{F}_q^n \} \) defines a subgroup of \( PGL(3n - 1, q) \) of order \( (q^n - 1)/(q - 1) \), which fixes all the elements \( L(x) \) of \( \mathcal{L} \) and acts sharply transitively on the points of \( L(x) \).

Let \( U \) be a \((n - 1)\)-dimensional subspace of \( PG(3n - 1, q) \) such that each element of \( \mathcal{L} \) either is disjoint from \( U \) or intersects \( U \) in exactly one point.\(^1\)

Let \( D \) be the set of all the elements of \( \mathcal{L} \) containing a point of \( U \) and let \( D^* = \{ U^\tau : \tau \in E \} \).

Theorem 8. [20]. If \( \mathcal{L}(U) = (\mathcal{L}\setminus D) \cup D^* \), then \( \mathcal{L}(U) \) is a non-desarguesian \((n - 1)\)-spread of \( PG(3n - 1, q) \).

Proof. The case \( n = 3 \) has been studied in [20]. Here we give a proof for the general case.

As \( E \) is transitive on the points of each element of \( \mathcal{L} \), the set \( D^* \) contains \( q^{n-1} + q^{n-2} + \cdots + q + 1 \) elements. By construction, if \( L(x) \in D \) and \( T \in D^* \), then \( L(x) \cap T \) is a point, and for each point \( y \) of \( L(x) \) there is an element \( W \) of \( D^* \) incident with \( y \).

If \( T_1 \) and \( T_2 \) are elements of \( D^* \) containing a common point \( x \), then there is an element \( D \) incident with \( x \). As \( T_2 = T_1^\tau \) for some \( \tau \in E \), then \( x^\tau = x \).

This implies \( \tau = 1 \) and \( T_1 = T_2 \). Hence \( D^* \) is a partial spread. As \( L(x) \) is not disjoint from all elements of \( D^* \) if and only if \( L(x) \) belongs to \( D \), we have proved that \( \mathcal{L}(U) \) is a \((n - 1)\)-dimensional spread of \( PG(3n - 1, s) \).

Let \( T \) be an element of \( \mathcal{L}\setminus D \), and \( U \) an element of \( D^* \). Denote by \( W = \langle T, U \rangle \) the \((2n - 1)\)-dimensional subspace joining \( T \) and \( U \). Suppose that an element of \( \mathcal{L}(U) \) either is disjoint from \( W \) or is contained in \( W \). Then the elements of \( \mathcal{L}(U) \) contained in \( W \) define an \((n - 1)\)-spread of \( W \). As \( q^n > (q^n - 1)/(q - 1) \), the subspace \( W \) contains at least two elements of \( \mathcal{L} \). This implies that an element \( X \) of \( \mathcal{L} \) either is disjoint from \( W \) or is contained in \( W \). Therefore all the elements of \( D \) are subspaces of \( W \). Choosing an element \( T'' \) of \( \mathcal{L}\setminus D \) disjoint from \( W \), then \( W'' = \langle T'', U \rangle \) is a \((2n - 1)\)-dimensional subspace of \( PG(3n - 1, s) \). If \( \{ X \cap W' : X \in \mathcal{L}(U) \} \) is an \((n - 1)\)-spread of \( W' \), then all the elements of \( D \) are subspaces of \( W' \), i.e. \( W = W' \). As this is impossible, we conclude that there is a \((2n - 1)\)-dimensional subspace \( W' \) of \( PG(3n - 1, s) \) containing two elements of \( \mathcal{L}(U) \) such that \( \{ X \cap W' : X \in \mathcal{L}(U) \} \) is not a spread of \( W' \).

\(^1\)We will prove in the next sections the existence of subspaces \( U \) of \( PG(3n - 1, q) \) such that each element of \( \mathcal{L} \) either is disjoint from \( U \) or intersects \( U \) in a point.
This proves that $L(U)$ is not a normal $(n - 1)$-spread. □

2.4. A generalization of the Barlotti–Cofman construction

The Barlotti–Cofman construction can be generalized as follows.

Let $\mathcal{B}$ be a family of subspaces of $\text{PG}(m, q)$ of dimension $< m - 1$. We note that the elements of $\mathcal{B}$ are not necessarily of the same dimension. Define an incidence structure $\mathfrak{A}(\mathcal{B})$ in the following way. The points of $\mathfrak{A}(\mathcal{B})$ are the points of $\text{PG}(m, q) \setminus \text{PG}(m - 1, q)$. The lines are the subspaces of $\text{PG}(m, q)$ not in $\text{PG}(m - 1, q)$ and intersecting $\text{PG}(m - 1, q)$ in an element of $\mathcal{B}$. We can define a parallelism $\parallel$ on $\mathfrak{A}(\mathcal{B})$ by saying that two lines of $\mathfrak{A}(\mathcal{B})$ are parallel if they contain the same element of $\mathcal{B}$.

We can define a parallelism $\parallel$ on $\mathfrak{A}(\mathcal{B})$ by saying that two lines of $\mathfrak{A}(\mathcal{B})$ are parallel if they contain the same element of $\mathcal{B}$. Then any elation of $\text{PG}(m, q)$ with axis $\text{PG}(m - 1, q)$ defines a translation of $\mathfrak{A}(\mathcal{B})$. Therefore, $\mathfrak{A}(\mathcal{B})$ has an elementary abelian group $T$ of translations, which acts regularly on the points of $\mathfrak{A}(\mathcal{B})$.

Any central collineation $\delta$ of $\text{PG}(m, q)$ with axis $\text{PG}(m - 1, q)$ and centre $O \notin \text{PG}(m - 1, q)$ defines an isomorphism $k_\delta : T \rightarrow T, \tau \mapsto \delta^{-1} \tau \delta$.

Hence the kernel of $\mathfrak{A}(\mathcal{B})$ contains a subfield isomorphic to $\mathbb{F}_q$. Applying the Lemma 1 we have the following theorem.

**Theorem 9.** Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two families of subspaces of $\text{PG}(m - 1, q)$. The translation structures with parallelism $\mathfrak{A}(\mathcal{B}_1)$ and $\mathfrak{A}(\mathcal{B}_2)$ are isomorphic if and only if there is a collineation of $\text{PG}(m - 1, q)$ which maps $\mathcal{B}_1$ into $\mathcal{B}_2$.

**Corollary 4.** Any finite translation structure with parallelism, whose translation group is abelian, is of Barlotti–Cofman type.

*Proof.* Let $T$ be the translation group, $p$ a fixed point, and let $\mathcal{P} = \{ T_L \mid L \ni p \}$ be the associated family of subgroups of $T$. As $T$ is finite, its kernel is finite. Therefore, there is a subfield $\mathbb{F}_q$ of the kernel of $\mathcal{P}$ and all elements of $T_L$ are $\mathbb{F}_q$-subspaces of $T$ as vector space over $\mathbb{F}_q$. If $\mathcal{B} = \{ T_L \mid L \ni p \}$, then $\mathcal{B}$ is a family of subspaces of $\text{PG}(m - 1, q) = \text{PG}(T, \mathbb{F}_q)$ and $\mathfrak{A}(\mathcal{B})$ is isomorphic to $\mathfrak{A}(T, \mathcal{P})$ via the map

$$\text{PG}(m, q) \setminus \text{PG}(m - 1, q) \rightarrow T, \langle c + w \rangle \mapsto \tau_w$$

where $p = \langle c \rangle$ is a fixed point of $\text{PG}(m, q)$ not incident with $\text{PG}(m - 1, q)$ and $\tau_w$ is the translation of $T$ which maps $p$ to $w$. □

3. Normal spreads and linear sets

3.1. Linear sets

We recall the definition of linear set by using a normal spread as originally introduced in [62] and [63].

Let $\text{PG}(r - 1, q^n) = \text{PG}(V, \mathbb{F}_{q^n})$ be the projective geometry of the $\mathbb{F}_{q^n}$-subspaces of $V$, where $V$ is a vector space of rank $r$ over the field $\mathbb{F}_{q^n}$.

Denote by $\mathfrak{L}$ be the $\mathbb{F}_q$-linear representation of $\text{PG}(r - 1, q^n)$ in $\text{PG}(rn - 1, q)$. We have proved in Example 1 that $\mathfrak{L}$ is a desarguesian spread of $\text{PG}(rn - 1, q)$. 
Hence by Theorem 7, $\mathcal{L}$ is a normal spread of $\text{PG}(rn - 1, q)$. If $T$ is a $(2n - 1)$-dimensional subspace containing two elements of $\mathcal{L}$, then an element of $\mathcal{L}$ either is contained in $T$ or is disjoint from $T$. For any $(2n - 1)$-dimensional subspace $T$ containing two elements of $\mathcal{L}$, denote by $\mathcal{L}_T$ the desarguesian planar spread of $T$ induced by $\mathcal{L}$, i.e. $\mathcal{L}_T = \{X \in S \mid X \subset T\}$.

We can construct a new incidence structure $P(\mathcal{L})$ in the following way. The points are the elements of $\mathcal{L}$ and the lines are the planar spreads $\mathcal{L}_T$ induced by $\mathcal{L}$ over a $(2n - 1)$-dimensional subspace $T$ containing two elements of $\mathcal{L}$. Let $\alpha$ be the map from $\text{PG}(r - 1, q^n)$ to $P(\mathcal{L})$ which maps the point $\langle v \rangle$ to the $(n - 1)$-subspace $L(v)$ and the line $m$ joining the points $\langle v \rangle$ and $\langle w \rangle$ to the spread induced on the $(2n - 1)$-dimensional subspace of $\text{PG}(rn - 1, q)$ joining $L(v)$ and $L(w)$. It easy to prove that $\alpha$ is an isomorphism.

Let $S$ be a subspace of $\text{PG}(rn - 1, q)$ not contained in any element of $\mathcal{L}$. The set

$$L(S) = \{L(v) \in \mathcal{L} \mid L(v) \cap S \neq \emptyset\}$$

is a linear set of $P(\mathcal{L})$. If $S$ is the subspace defined by the $\mathbb{F}_q$-linear space $W$ of $V$, by using the isomorphism $\alpha: \text{PG}(r - 1, q^n) \longrightarrow P(\mathcal{L})$ we have that

$$\alpha^{-1}(L(S)) = \{\langle v \rangle \mid L(v) \in L(S)\} = \{\langle w \rangle \mid w \in W\}.$$ 

Therefore, a set $\Lambda$ of points of $\text{PG}(r - 1, q^n)$ is an $\mathbb{F}_q$-linear set of $\text{PG}(r - 1, q^n)$ if there exists a subset $W$ of $V$, which is an $\mathbb{F}_q$-vector subspace of $V$, such that a point of $\text{PG}(r - 1, q^n)$ belongs to $\Lambda$ if and only if it is defined by a vector of $W$. We will write $\Lambda = \Lambda(W)$.

This is the present commonly used definition of linear sets. For more details we referer to [63].

If $W$ has rank $m$ as vector space over $\mathbb{F}_q$ we say that $\Lambda(W)$ has rank $m$. If $\Lambda(W)$ has rank $r$ and $\langle W \rangle = V$, then $\Lambda(W) \simeq \text{PG}(W, \mathbb{F}_q) = \text{PG}(r - 1, q)$ is said to be a (canonical) subgeometry of $\text{PG}(V, \mathbb{F}_q^n) = \text{PG}(r - 1, q^n)$. We note that linear sets are the natural generalization of notion of subgeometries of a projective geometry.

**Example 6.** The non-normal spread in Example 5 was constructed by using an $(n - 1)$-subspace $U$ of $\text{PG}(3n - 1, q)$ such that each element of $\mathcal{L}$ either is disjoint from $U$ or intersects $U$ in exactly one point. We are able to give an example of such a space by using the linear sets.

Suppose $n = 3$ and let $\pi = \text{PG}(2, q)$ be a subspace of $\text{PG}(2, q^3)$. If $\mathcal{L}$ is the $\mathbb{F}_q$-linear representation of $\text{PG}(2, q^3)$ in $\text{PG}(8, q)$, then $\pi = \Lambda(U)$ where $U$ is a plane of $\text{PG}(8, q)$ with the required property because $\pi$ has size $q^2 + q + 1$.

Denote by $\bot$ the polarity of $\text{PG}(r - 1, q^n)$ defined by a non-singular bilinear form $< ; >$ of $V$. If $Tr$ is the trace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, the bilinear form $b(x, y) = Tr(< x; y >)$ on $V$, as vector space over $\mathbb{F}_q$, defines a polarity $\omega$ of $\text{PG}(rt - 1, q)$. Let $\Omega$ be an $\mathbb{F}_q$-linear set of rank $h$ of $\text{PG}(r - 1, q^l) = \text{PG}(V, \mathbb{F}_q^n)$. If $U$ is an $(h - 1)$-dimensional subspace of $\text{PG}(rt - 1, q)$ such that $\Omega = \{\langle x \rangle \in \text{PG}(r - 1, q^n) \mid L(x) \cap U \neq \emptyset\}$, and $U^\omega$ is the polar space of $U$ with respect to $\omega$, then $\Omega^\perp = \{\langle x \rangle \in \text{PG}(rn - 1, q) \mid L(x) \cap U^\perp \neq \emptyset\}$ is an $\mathbb{F}_q$-linear set of
rank $rt - h$ of $\PG(r-1, q)$. We call $\Omega^\perp$ the dual of $\Omega$. We note that $\Omega^\perp$ does not depend, up to collineations, on the chosen polarity of $\PG(r-1, q^n)$.

### 3.1.1. Subgeometries

We recall that if $\Sigma = \PG(m - 1, q) = \PG(V, \mathbb{F}_q)$ and $\Sigma^* = \PG(m - 1, q^n) = \PG(V^*, \mathbb{F}_{q^n})$, then $\Sigma$ is a subgeometry of $\Sigma^*$ if and only if $V^* = \mathbb{F}_{q^n} \otimes V$, i.e. linearly independent vectors of $V$ are linearly independent in $V^*$. Let $S$ be a subspace of $\Sigma^*$. Suppose that $S$ is defined by the $\mathbb{F}_{q^n}$-vector subspace $W$ of $V^*$, i.e. $S = \langle W \rangle$. Then $\bar{S} = S \cap \Sigma$ is a subspace of $\Sigma$ defined by the $\mathbb{F}_q$-vector subspace $\bar{W} = \langle W \cap V \rangle$. We say that $S$ is an extended subspace of $\Sigma$ if and only if $W = \mathbb{F}_{q^n} \otimes \bar{W}$ if and only if $\bar{S}$ is a subgeometry of $S$. If $\sigma$ is the collineation of $\Sigma^*$ defined by the semilinear map of $V^*$ to itself, which maps $\lambda \otimes v$ to $\lambda^q \otimes v$, then a subspace $S$ of $\Sigma^*$ is a subspace of $\Sigma$ if and only if $S^\sigma = S$ (see, e.g., [62]).

### 3.1.2. Projections and Embeddings of a Subgeometry

In a conference held in Rome in 1981, I presented some results on indicator sets and, at the end of my talk, I made a conjecture on such sets. After my talk, F. Buekenhout suggested me to check the paper of Limbos [58] which had connections with my conjecture. The idea of Limbos was the following. Let $\Gamma = \PG(m - 1, q)$ be a fixed canonical subgeometry of $\Sigma^* = \PG(m - 1, q^n)$. Suppose that $\Gamma^*$ is an $(m - r - 1)$-dimensional subspace of $\Sigma^*$ disjoint from $\Sigma$ such that no extended planes of $\Sigma$ intersect $\Gamma^*$. Let $\Gamma = \PG(r - 1, q^n)$ be an $(r - 1)$-dimensional subspace of $\Sigma^*$ disjoint from $\Gamma^*$, and let

$$\Lambda = \{\langle \Gamma^*, P \rangle \cap \Gamma : P \in \Sigma\}$$

be the projection of $\Sigma$ from $\Gamma^*$ onto $\Lambda$. Denote by $p_{\Gamma^*, \Gamma}$ the map from $\Sigma$ to $\Lambda$ defined by $P \mapsto \langle \Gamma^*, P \rangle \cap \Gamma$ for each point $P$ of $\Sigma$. By definition $p_{\Gamma^*, \Gamma}$ is a bijection and $\Lambda = p_{\Gamma^*, \Gamma}(\Sigma)$.

If $l$ is an extended line of $\Sigma$, then $\langle \Gamma^*, l \rangle \cap \Gamma$ is a line of $\Gamma$ containing $q + 1$ points of $\Lambda$. Hence if

$$\mathcal{L} = \{\langle \Gamma^*, l \rangle \cap \Gamma \mid l is an extended line of \Sigma\},$$

then $(\Lambda, \mathcal{L})$ is isomorphic to $\Sigma$ as a point line-geometry, but is not a canonical subgeometry of $\Gamma$.

This disproved my conjecture, but a more interesting consequence is the following. If $\Gamma$ and $\Gamma^*$ are disjoint, then the map $p_{\Gamma^*, \Gamma}$ is still defined and we can prove that $\Lambda = p_{\Gamma^*, \Gamma}(\Sigma)$ is an $\mathbb{F}_q$-linear set of rank $m$. (see [63]). The following characterisation of $\mathbb{F}_q$-linear sets has been proved by Lunardon et al. [71] and [73].

**Theorem 10.** [71] and [73]. Let $m > r > 1$. For any $\mathbb{F}_q$-linear set $\Lambda$ of rank $m$ of $\PG(r-1, q^n)$ there are

1. A canonical subgeometry $\Sigma = \PG(m-1, q)$ of $\Sigma^* = \PG(m-1, q^n)$,
2. An $(r-1)$-dimensional subspace $\Gamma$ of $\Sigma^*$ and
3. An $(n-r-1)$-dimensional subspace $\Gamma^*$ of $\Sigma^*$ disjoint from $\Gamma$ such that $\Lambda = p_{\Gamma^*, \Gamma}(\Sigma)$. 

In the same hypotheses of Theorem 10, if any \((r - 1)\)-dimensional extended subspace of \(\Sigma\) is disjoint from \(\Gamma^*\) we say that \(\Lambda\) is an \((r - 1)\)-embedding of \(\Sigma = \text{PG}(m - 1, q)\). This is equivalent to saying that, if \(P_1, P_2, \ldots, P_r\) are points of \(\Sigma\) whose span has dimension \(r - 1\) and \(P'_i = \text{pr}_{\Gamma^*, \Gamma}(P_i) \in \Lambda\) for all \(i = 1, 2, \ldots, r\), then \(\langle P'_1, P'_2, \ldots, P'_r \rangle = \Gamma\).

We note that \(\Lambda\) is an \((r - 1)\)-embedding if and only if \(\text{pr}_{\Gamma^*, \Gamma}\) induces an injective map from the set of all subspaces of \(\Sigma\) of dimension \(h < r - 1\) to the set of all subspaces of \(\Gamma\) of the same dimension \(h\).

Suppose that \(H\) is a hyperplane of \(\Gamma\). The subspace \(\langle \Gamma^*, H \rangle\) has dimension \(m - 2\). As \(\text{pr}_{\Gamma^*, \Gamma}(\langle \Gamma^*, H \rangle) = H\) and any \((r - 1)\)-dimensional extended subspace of \(\Sigma\) is disjoint from \(\Gamma^*\), any extended subspace contained in the hyperplane \(\langle \Gamma^*, H \rangle\) has dimension \(< r - 1\), and \(\Lambda \cap H = \text{pr}_{\Gamma^*, \Gamma}(\Sigma \cap \langle \Gamma^*, H \rangle)\) is an \(\mathbb{F}_q\)-linear set of rank \(< r\).

An \((r - 1)\)-scattered linear set of \(\text{PG}(r - 1, q^n)\) is an \(\mathbb{F}_q\)-linear set \(\Lambda\) of rank \(m\) such that any hyperplane of \(\text{PG}(r - 1, q^n)\) intersects \(\Lambda\) in an \(\mathbb{F}_q\)-linear set of rank \(< r\). Hence we have proved that

**Theorem 11.** An \(\mathbb{F}_q\)-linear set of \(\text{PG}(r - 1, q^n)\) of rank \(m\) is \((r - 1)\)-scattered if and only if it is an \((r - 1)\)-embedding of \(\text{PG}(m - 1, q)\).

Therefore the \((r - 1)\)-embeddings of \(\text{PG}(n - 1, q)\) in \(\text{PG}(r - 1, q^n)\) studied in [67, Section 3.4] and the \((r - 1)\)-scattered linear set of \(\text{PG}(r - 1, q^n)\) introduced in [91] are equivalent objects.

### 3.1.3. Embeddings of \(\text{PG}(n - 1, q)\)

Let \(\Sigma^* = \text{PG}(n - 1, q^n)\). If \(X_0, X_1, \ldots, X_{n-1}\) are the homogenous coordinates of \(\Sigma^*\), let \(\sigma\) be the collineation of \(\Sigma^*\) defined by the semilinear map

\[
(X_0, X_1, \ldots, X_{n-1}) \mapsto (X_{n-1}^q, X_0^q, \ldots, X_{n-2}^q)
\]

of order \(n\). Then \(\Sigma = \{(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}) \mid \alpha \in \mathbb{F}_q^n\} \simeq \text{PG}(n - 1, q)\) is the subgeometry of \(\Sigma^*\) pointwise fixed by \(\sigma\). For any point \(P\) of \(\Sigma^*\), let \(L(P)\) the subspace of \(\Sigma^*\) defined by \(L(P) = \langle P, P^\sigma, \ldots, P^{\sigma^{n-1}} \rangle\).

By definition, \(L(P)^\sigma = L(P)\), i.e. \(L(P)\) is an extended subspace of \(\Sigma\). We note that for any extended subspace \(S\) of \(\Sigma\) there is a point \(P^*\) of \(\Sigma^*\) such that \(S = L(P)\). We say that a point \(P = (a_0, a_1, \ldots, a_{n-1})\) of \(\Sigma^*\) is of \(\text{type} r\) if and only if the subspace \(L(P)\) has rank \(r\) if and only if the matrix

\[
M(a_0, a_1, \ldots, a_{n-1}) = \begin{pmatrix}
P \\
P^\sigma \\
\vdots \\
P^{\sigma^{n-1}}
\end{pmatrix}
= \begin{pmatrix}
a_0 & a_1 & \cdots & a_{n-1} \\
a_0^q & a_1^q & \cdots & a_{n-1}^q \\
\vdots & \vdots & \ddots & \vdots \\
a_0^{q^{n-1}} & a_1^{q^{n-1}} & \cdots & a_{n-1}^{q^{n-1}}
\end{pmatrix}
\]

has rank \(r\).

**Theorem 12.** [67, Theorem 6]. The \(\mathbb{F}_q\)-linear set \(\Lambda = \text{pr}_{\Gamma^*, \Gamma}(\Sigma)\) of rank \(n\) is an \((r - 1)\)-embedding of \(\Sigma\) if and only if all points of \(\Gamma^*\) are of type \(\geq r + 1\).

**Proof.** By definition \(\Lambda\) is an \((r - 1)\)-embedding if and only if \(\Gamma^*\) is disjoint from any subspace of \(\Sigma\) of rank \(r\). This is equivalent to saying that for any point \(P\)
of $\Gamma^*$ the subspace $L(P)$ has rank $\geq r + 1$, i.e. the point $P$ is of type $\geq r + 1$. □

Let $\perp$ be the polarity of $\text{PG}(n - 1, q^n)$ defined by the bilinear form

$$B((X_0, X_1, \ldots, X_{n-1}), (Y_0, Y_1, \ldots, Y_{n-1})) = \sum_{i=0}^{n-1} X_iY_i.$$ 

If $\text{PG}(n - 1, q) = \{ (\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}) \mid \alpha \in \mathbb{F}_{q^n} \}$ is the fixed canonical subgeometry of $\text{PG}(n - 1, q^n)$, then $\perp$ induces on $\text{PG}(n - 1, q)$ the polarity defined by the bilinear form

$$B((\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}), (\beta, \beta^q, \ldots, \beta^{q^{n-1}})) = \text{Tr}_{q^{-1}}(\alpha\beta).$$ 

Therefore $\perp$ maps a subspace of $\text{PG}(n - 1, q)$ of rank $n - k$ to a subspace of $\text{PG}(n - 1, q)$ of rank $k$.

**Corollary 5.** If $\Lambda = pr_{\Gamma^*} (\Sigma)$ is an $(r - 1)$-embedding, and $\Gamma^* = \Gamma^{\perp}$, then $pr_{\Gamma^*} (\Sigma)$ is an $(n - r - 1)$-embedding.

### 3.2. Blocking sets of Desarguesian planes

A **blocking set** in a projective plane is a set of points which intersects every line. A blocking set is **trivial** if it contains a line, and it is **minimal** if no proper subset of it is a blocking set. Two blocking sets are **equivalent** if there is a collineation of the plane which maps one to the other. In the projective plane over the Galois field of order $q$, a blocking set $B$ is **small** if its size is less than $3(q + 1)/2$, and is called of **Rédei type** if there is a line $l$ such that $|B|/|l| = q$; the line $l$ is a **Rédei line** of $B$.

If $\Lambda$ is an $\mathbb{F}_q$-linear set of rank $n + 1$ of the desarguesian plane $\text{PG}(2, q^n)$, then $\Lambda$ intersects any line of $\text{PG}(2, q^n)$. Hence $\Lambda$ is a blocking set, called a $\mathbb{F}_q$-linear blocking set.

**Theorem 13.** [83]. Let $\Lambda$ be a $\mathbb{F}_q$-linear blocking set of rank $n + 1$ of the desarguesian plane $\text{PG}(2, q^n)$. If $\Lambda$ does not contain a line of $\text{PG}(2, q^n)$, then $\Lambda$ is a small minimal blocking set whose size is at most $q^n + q^{n-1} + \cdots + q + 1$.

**Proof.** We note that the blocking set $\Lambda$ is minimal if and only if for any point $P$ there is a line of $\text{PG}(2, q^n)$ intersecting $\Lambda$ in exactly the point $P$.

Let $\Lambda = \Lambda(L)$ where $L$ is an $\mathbb{F}_q$-vector subspace of rank $n + 1$. If $\Lambda$ is not minimal, then there exists a point $P = \langle v \rangle$, $v \in L$, such that $|\ell \cap \Lambda| \geq 2$ for all line $\ell$ of $\text{PG}(2, q^n)$ incident with $P$. Denote by $\ell_1, \ell_2, \ldots, \ell_{q^n+1}$ the lines of $\text{PG}(2, q^n)$ incident with $P$, and denote by $Q_i = \langle w_i \rangle$, $w_i \in L$, a point of $\ell_i \cap \Lambda$ different from $P$. Then

$$L_i = \{ \alpha v + \beta w_i \mid \alpha, \beta \in \mathbb{F}_q \}$$

is an $\mathbb{F}_q$-vector subspace of rank two contained in $L$. As $\langle L_i \rangle$ is contained in $\ell_i$, for $i \neq j$ we have

$$L_i \cap L_j = \{ \alpha v \mid \alpha \in \mathbb{F}_q \} = \langle v \rangle_{\mathbb{F}_q}.$$
Therefore, the \( \mathbb{F}_q \)-vector space \( L \) contains \( q^n + 1 \) \( \mathbb{F}_q \)-vector subspace of rank two whose intersection is the \( \mathbb{F}_q \)-vector subspace \( \langle v \rangle_{\mathbb{F}_q} \) of rank 1. As \( L \) is an \( \mathbb{F}_q \)-vector space of rank \( n + 1 \), this is impossible.

We note that \( L \) has exactly \( q^n + q^{n-1} + \cdots + q + 1 \) \( \mathbb{F}_q \)-vector subspace of rank 1. If \( \langle w \rangle \) is a point of \( \Lambda \), then \( \langle w \rangle \cap L \) is an \( \mathbb{F}_q \)-vector subspace of rank \( \geq 1 \). This implies that \( |\Lambda| \leq q^n + q^{n-1} + \cdots + q + 1 \).

Let \( B \) be a minimal blocking set of Rédei type in the plane \( \text{PG}(2, s) \). Let \( \ell \) be a Rédei line of \( B \) and let \( P \) be a point of \( \ell \setminus B \). Suppose without loss of generality that \( l \) has equation \( X_2 = 0 \), that \( P \) has coordinates \((0, 1, 0)\), and that \((0, 0, 1) \in B \). Let

\[
B \setminus \ell = \{(a_i, b_i, 1) : i = 1, \ldots, s\}
\]

and define the following map

\[
f : a_i \in \mathbb{F}_s \longrightarrow b_i \in \mathbb{F}_s.
\]

So, \( B \setminus \ell \) is the graph \( G_f \) of the map \( f \) in the affine plane \( \text{AG}(2, s) = \text{PG}(2, s) \setminus \ell \) and the points of \( l \setminus B \) are all the points determined by the secants of the graph of \( f \).

**Theorem 14.** \([7]\) and \([8]\). Let \( B \) be a small minimal blocking set in \( \text{PG}(2, s) \) (\( s = p^n \), \( p \) any prime) of Rédei type and let \( \ell \) be a Rédei line of \( B \). Then, there is a divisor \( q \) of \( s \) such that \( f \) is an \( \mathbb{F}_q \)-linear map.

In \([62]\) it has been proven that a blocking set defined by an additive function is a linear blocking set. So, by Theorem 14, it follows:

**Theorem 15.** \([7, 8]\) and \([62]\). In the hypotheses of Theorem 14, \( B \) is an \( \mathbb{F}_q \)-linear blocking set.

It was conjectured by Blokhuis \([16]\) that all small minimal blocking sets of the desarguesian plane were of Rédei type. This implies that all linear blocking sets are of Rédei type. This conjecture was disproved in \([83]\) where the first example of linear blocking set not of Rédei type was constructed. We conclude this section by giving an example of linear blocking set of minimal size which is not of Rédei type.

**Example 7.** If \( \pi = \text{PG}(2, q^n) = \text{PG}(V, \mathbb{F}_{q^n}) \) and \( w_0, w_1, w_2 \) is an \( \mathbb{F}_{q^n} \)-basis of \( V \), denote by \( (X_0, X_1, X_2) \) the homogeneous coordinates of the point \( \langle X_0 w_0 + X_1 w_1 + X_2 w_2 \rangle \) of \( \pi \). Let \( \xi \) be a primitive element of \( \mathbb{F}_{q^n} \) and let \( W \) be the set of all vectors of \( V \) with coordinates

\[
(x_0 + x_1 \xi + \cdots + x_{n-4} \xi^{n-4}, y_0 + y_1 \xi, z_0 + z_1 \xi)
\]

where \( x_0, x_1, \ldots, x_{n-4}, y_0, y_1, z_0, z_1 \in \mathbb{F}_q \). It has been proved in \([72]\) that if \( n \geq 5 \), then \( L = \{ \langle w \rangle \mid w \in W \} \) is an \( \mathbb{F}_q \)-linear blocking set of size \( q^n + q^{n-1} + 1 \) not of Rédei type.

At the moment all known small minimal blocking sets are linear.
3.3.1. Rédei blocking sets of maximal size. Let $B = \{(a, x, f(x)) \mid a \in F_q, x \in F_q^n\}$ be an $F_q$-linear blocking set of Rédei type of PG$(2, q^n)$, i.e., $f : F_q^n \rightarrow F_q^n$ is an $F_q$-linear map. If $B$ has maximal size, then $\Lambda = \{(0, x, f(x)) \mid x \in F_q^n\}$ is a linear set of size $q^{n-1} + \cdots + q + 1$. We will say that $\Lambda$ is scattered and the $f$ is a scattered function.

If $\mathcal{L}$ is the linear representation of PG$(2, q)$ into PG$(3n - 1, q)$ and $T$ is the $(2n - 1)$-dimensional subspace of PG$(3n - 1, q)$ containing both $L(0, 1, 0)$ and $L(0, 0, 1)$ of $\mathcal{L}$, then there is an $(n - 1)$-dimensional subspace $U \subset T$ such that $\Lambda = L(U)$ and any element of $\mathcal{L}$ either is disjoint from $U$ or intersects $U$ in exactly a point. Hence, the subspace $U$ satisfies the hypotheses required in Example 5.

For long time the only known scattered functions were:

- $x \mapsto x^q$ (see [17] and [83])
- $x \mapsto \lambda x^q + x^{q^{n-1}}$ with $N(\lambda) \neq 1$, $q > 3$ and $n \geq 4$ [72, Thereom 4]

but, due to a relationship between scattered linear sets and maximum rank distance codes discovered by Sheekey [90] (see Sect. 5 for more details), such linear sets have been studied from different points of view and many new examples have been recently discovered from different authors (see, e.g., [12, 25–27, 59–61, 84]).

3.3. Semifields and semifield spreads

3.3.1. Spreads of PG$(2n - 1, q)$. A spread $S$ of PG$(2n - 1, q)$ is a semifield spread with respect to an element $A \in S$ if there is a collineation group $G$ fixing $A$ pointwise and acting regularly on $S \setminus \{A\}$. If $S$ is a semifield spread of PG$(2n - 1, q)$, then the affine plane $A(S)$ belongs the Lenz–Barlotti class V.

A spread $S$ of PG$(2n - 1, q)$ is a symplectic spread if any line of PG$(3, q)$ is totally isotropic with respect to a given symplectic polarity of PG$(2n - 1, q)$.

If $q = 2^h$ is even, the desarguesian spread is the only symplectic semifield spread of PG$(3, 2^h)$ (see [23] and [28]).

3.3.2. Semifields and presemifields. A semifield $S$ is an algebra satisfying the axioms for a skewfield except (possibly) associativity. The subsets

$$N_l = \{a \in S \mid (ab)c = a(bc), \forall b, c \in S\},$$
$$N_m = \{b \in S \mid (ab)c = a(bc), \forall a, c \in S\},$$
$$N_r = \{c \in S \mid (ab)c = a(bc), \forall a, b \in S\},$$
$$Z = \{a \in N_l \cap N_m \cap N_r \mid ab = ba, \forall b \in S\}$$

are known, respectively, as the left nucleus, middle nucleus, right nucleus and center of the semifield $S$. It is straightforward to prove that $N_l, N_m, N_r$ are skewfields and $Z$ is a field. Moreover, $S$ is a vector space over each of its nuclei and over its center.

Throughout this paper, the term semifield will always be used to denote a finite semifield.

A presemifield $S(+, \cdot)$ is a semifield if there is an identity element. Premifields coordinatize planes of Lenz–Barlotti class V.
Let $e$ be a non-zero element of $S$. Define a new multiplication $\circ$ on $S$ by $ae \circ eb = ab$. Then $S(\cdot, \circ)$ is a semifield with identity $ee$, which coordinatizes a projective plane isomorphic to that coordinatized by $S(\cdot, \cdot)$ (see [30, § 5.3]).

Two presemifields $S$ and $S'$ are said isotopic if the coordinatized planes are isomorphic. The nuclei and the center are invariant under isotopism.

A spread set $C$ is a subset of $M(n \times n, q)$ of size $q^n$ such that the difference of any two elements of $C$ is non singular. Let $e$ a fixed element of $S = F_q^n$ different from 0. For any element $b$ of $S$, there is a unique matrix $C(b)$ in $C$ such that $eC(b) = b$. Define a multiplication on $S$ by $a \cdot b = aC(b)$ for all $a, b \in S$. If $C$ is closed under the addition, then $S(\cdot, \cdot)$ is a presemifield. The left nucleus of the associated semifield contains a subfield isomorphic to $F_q$. It has been proved that, up to isotopism, presemifields of dimension $n$ over a subfield of its left nucleus can be constructed in such a way (see, e.g., [30, Section 5.3]).

If
\[
X(b) = \{(a, a \cdot b) \mid a \in S\},
\]
\[
X(\infty) = \{(0, b) \mid b \in S\},
\]
\[
S = S(S) = S(C) = \{X(i) \mid b \in S \cup \{\infty\}\}
\]
then $S$ is a semifield spread of $PG(S \times S, F_q) = PG(2n - 1, q)$, and the translation plane $A(S)$ is isomorphic to the plane coordinatized by the presemifield $S$ (see, e.g., [30, Section 5.3]).

**Example 8.** Let $K = F_q$ and let $\alpha, \beta$ be automorphisms of $K$. If $c$ is an element of $K$ such that $c \neq x^{\alpha-1}y^{\beta-1}$ for all $x, y \in K$, the multiplication $\circ$ defined by
\[
x \circ y = xy - cx^{\alpha}y^{\beta}
\]
turns $K$ into a presemifield (see, e.g., [30]). The associated semifields, introduced are called generalized twisted fields.

**Example 9.** A second fundamental class of semifields is due to Knuth [46]. Let $S$ be a 2-dimensional vector space over $F_q$ and let $\{1, \lambda\}$ be a basis of $S$ over $F_q$. Define a multiplication on $S$ by
\[
(x + y\lambda) \cdot (u + v\lambda) = xu + (xv + yu\sigma)\lambda + y^\alpha v^\beta f + (y^\gamma v^\delta g)\lambda
\]
with fixed $f, g \in GF(q)$ and $\alpha, \beta, \gamma, \delta, \sigma$ automorphisms of $F_q$. The necessary and sufficient condition for $S(\cdot, \cdot)$ to be a semifield is
(K) If $xu + y^\alpha v^\beta f = 0$ and $xv + yu\sigma + y^\gamma v^\delta g = 0$, then either $x = y = 0$ or $u = v = 0$.

We note that $F_q$ is a weak nucleus, i.e. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ whenever at least two of $x, y, z$ are in $F_q$.

All semifields, with two nuclei equal to $F_q$, can be constructed in such a way (see [30] or [46]).

If $q$ is odd, $f$ is a non-square and $g = 0$, then $S(\cdot, \cdot)$ is a semifield. As the case $\alpha = \beta \neq 1 = \sigma$ was first exhibited by Dickson in 1905, we call $S(\cdot, \cdot)$ a generalized Dickson semifield.
If $\alpha = \gamma = 1, \beta = \delta = \sigma \neq 1$ and the polynomial $x^{\sigma+1} + gx - f$ is irreducible, the condition (K) is satisfied and $S(\cdot, \cdot)$ is a semifield with $N_l = N_m = N_r = F_q$, called a Hughes–Kleinfeld semifield (see [39]).

**Example 10.** If the polynomial $x^2 + ax - b$ is irreducible over $F_q$, then

$$\mathbb{C} = \left\{ \begin{pmatrix} t \\ u + at \\ bt \end{pmatrix} \mid t, u \in F_q \right\}$$

is a spread set whose associated presemifield $S$ defines a desarguesian spread. If $\theta$ is an element of $F_{q^2}$ not in $F_q$, then

$$\mathbb{C}^L = \left\{ \begin{pmatrix} l \\ -\theta bt + (u + at) \\ l^q \end{pmatrix} \mid l \in F_{q^2}, t, u \in F_q \right\}$$

is a spread set of $M(2 \times 2, F_{q^2})$ closed under addition. The presemifield $S^L$ is lifted from a desarguesian plane. By construction $S^L$ has left nucleus $N_l = F_{q^2}$ and center $F_q$.

For more details see Hiramine et al. [36] and Johnson [49].

### 3.3.3. Semifield spreads of $PG(3, q)$. In this section we will briefly discuss the semifield spreads of $PG(3, q)$ or, equivalently, the semifields $S$ of dimension 2 over a subfield of their left nucleus or, equivalently, the spread sets $\mathbb{C}$ of $M(2 \times 2, q)$ closed under addition.

Let $\Omega(\mathbb{C}) = \{(X) \in PG(3, q) \mid X \in \mathbb{C}\}$. As $\mathbb{C}$ is closed under addition, let $\mathbb{F}_s$ be the maximal subfield $F_s$ of $F_q$ such that $\mathbb{C}$ is an $\mathbb{F}_s$-vector space. If $q = s^n$, then $\mathbb{C}$ has rank $2n$. Hence, $\Omega(\mathbb{C})$ is an $\mathbb{F}_s$-linear set of $PG(3, q) = PG(2 \times 2, F_q)$. With the above notation, the following hold.

**Theorem 16.** [64]. The spread $S = S(\mathbb{C})$ of $PG(3, q)$ is a semifield spread if and only there is a subfield $\mathbb{F}_s$ of $F_q$, $q = s^n$, such that $\Omega(\mathbb{C})$ is an $\mathbb{F}_s$-linear set of rank $2n$ disjoint from the hyperbolic quadric $Q^+(3, q)$ with equation $\det(X) = 0$.

Denote by $\perp$ the polarity of $\Sigma = PG(3, q)$ defined by the hyperbolic quadric $Q^+(3, q)$ with equation

$$\det \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = X_1 X_4 - X_2 X_3 = 0$$

and by $b$ the non-singular bilinear form of $V = F_q$ associated with $Q^+(3, q)$. If $Tr$ is the trace of $F_q$ over $F_s$, $q = s^n$, the bilinear form $Tr(b(x; y))$ on $V$, as a vector space over $F_s$, defines a polarity $\omega$ of $PG(4n-1, s)$.

Let $S = S(\mathbb{C})$ be semifield spread of $PG(3, q)$ and let $\Omega = \Omega(\mathbb{C})$ be the associate linear set of $PG(3, q)$. By Theorem 16, $\Omega$ is disjoint from $Q^+(3, q)$. If $\Omega^\perp$ is the dual of $\Omega$ with respect to the polarity defined by $Q^+(3, q)$, then $\Omega^\perp$ is an $\mathbb{F}_s$-linear set of rank $2n$ of $PG(3, q)$. As $\Omega$ is disjoint from $Q^+(3, q)$, then $\Omega^\perp$ is disjoint from $Q^+(3, q)$ too, hence it defines a new semifield spread of $PG(3, q)$, denoted $S^\perp$, called the translation dual of $S$ (see [64]). We note that the translation dual is a special case of a more general result of Delsarte on MRD codes.
Theorem 17. [64]. Two semifield spreads $S_1$ and $S_2$ of $PG(3,q)$ are isomorphic if and only if $S_1^\perp$ and $S_2^\perp$ are isomorphic.

As a consequence of this result, we have that the translation dual operation is “well defined”.

Theorem 16 has played an important role in the theory of the planes of Lenz–Barlotti class $V$ because, using such a construction, many new examples have been exhibited by different authors (S. Ball, I. Cardinali, G. L. Ebert, N. L. Johnson, M. Lavrauw, G. Marino, O. Polverino, J. Sheekey, R. Trombetti, . . .).

We briefly discuss some of those constructions and we refer to [56] for more details.

If $Z = F_s$, $q = s^n$ is the center of the semifield $S$ then the associated spread set $C$ is an $F_s$-vector space of rank $2n$ and, by Theorem 16, $C$ defines an $F_s$-linear set $\Omega$ of rank $2n$ disjoint from $Q^+(3,q)$.

Suppose that $q = s^2$. Hence $\Omega$ is a $F_s$-linear set of rank 4 of $PG(3,s^2)$ disjoint from the quadric $Q^+(3,q)$. Thus, $\Omega$ is a canonical subgeometry and the classification of semifields of dimension 2 over their left nucleus and dimension 4 over their center is equivalent to the classification of the canonical subgeometries of $PG(3,s^2)$ disjoint from the quadric $Q^+(3,s^2)$, which follows.

Theorem 18. [24]. If $S$ is a semifield of dimension 4 over its center $Z = F_s$ and dimension 2 over its left nucleus $N_l = F_q$, $q = s^2$, then $S$ is one of the following:

1. Generalized Dickson semifields ($q$ odd and $\xi \cdot a = a \cdot \xi$ for all $\xi \in N_l$ and $a \in S$).
2. Hughes–Kleinfeld semifields ($N_l = N_m = N_r = F_q$).
3. Semifields lifted from Desarguesian planes.
4. Generalized twisted fields.

Semifields $S$ such that $[S : N_l] = 2$ and $[S : Z] = 6$ are equivalent to $F_s$-linear sets $\Omega$ of rank 6 disjoint from $Q^+(3,q)$ with $q = s^3$. In this case we do not have a complete classification but it has been proved that there are 6 possible configurations invariant under isotopies, as stated in the following theorem.

Theorem 19. [81]. Let $S$ be a semifield of dimension 6 over its center $Z = F_s$ and dimension 2 over its left nucleus $N_l = GF(q)$, $q = s^2$, and let $\Omega = \{\langle X \rangle \mid X \in C\}$ be the $F_s$-linear set of rank 6 disjoint from $Q^+(6,q)$ associated with $S$. Then one of the following cases occurs:

1. $\Omega$ is a union of $q^2 + q + 1$ or $q^2 + 1$ lines of a pencil of $PG(3,q)$.
2. $\Omega$ is a union of $q^2 + q + 1$ lines in a plane not belonging to a pencil.
3. $\Omega$ is a union of $q^2 + q + 1$ lines through a point, not all lines in the same plane.
4. $\Omega$ contains a unique point of weight 2, it does not contain any line and is not contained in a plane.
5. $\Omega$ contains exactly one line which contains $s + 1$ points of weight 2.
6. Any point of $\Omega$ has weight 1 (i.e. $\Omega$ is scattered).
Theorem 20. [81]. Semifields belonging to different families $\mathcal{F}_i$ are not isotopic. If $S \in \mathcal{F}_i$ with $i = 0, 3, 4, 5$, then $S^\perp \in \mathcal{F}_1$, whereas $S \in \mathcal{F}_1$ if and only if $S^\perp \in \mathcal{F}_2$.

Theorem 8 motivated some new research which produced a number of new examples and proved that families $\mathcal{F}_3, \mathcal{F}_4,$ and $\mathcal{F}_5$ are not empty. The cyclic semifields constructed by Jha and Johnson belong to the family $\mathcal{F}_4$ (see, e.g., [50]). For such semifields we have $N_l = GF(s^3), N_m = N_r = GF(s^2)$ and $Z = GF(s)$. In [51] and [52] the authors generalized Jha–Johnson construction proving a complete classification for the semifields $S$ such that $N_l = GF(s^3), N_m = N_r = GF(s^2)$ and $Z = GF(s)$. All these semifields belong to the family $\mathcal{F}_4$. Further examples of semifields of the family $\mathcal{F}_4$ have been constructed in [31].

The Huang–Johnson semifields of type II, III, IV belong to the family $\mathcal{F}_3$ (see [38]) and it has been recently proved in [53] that it is possible to extend this construction to an infinite class of examples, all in the family $\mathcal{F}_3$. Semifields of the family $\mathcal{F}_5$ are defined by a particular geometric configuration called $F_q$-pseudoregulus. The only previously known examples in this class were generalized twisted fields and the Knuth semifields with both $N_l = N_r$ and $N_l = N_m$. New examples of such semifields have been recently constructed in [55].

For more details on semifields of dimension 2 over their left nucleus and dimension 6 over its center we refer to the survey paper [56].

The next result concerns the translation dual.

Theorem 21. [68]. Let $S = S(S)$ be the semifield spread of $PG(3, q)$ associated with the semifield $S$ two dimensional over a subfield $\mathbb{F}_q$ of its left nucleus. If $S^\perp$ is a semifield such that $S(S^\perp) = S^\perp$, then $S$ and $S^\perp$ have isomorphic nuclei.

We conclude this section with the generalization of Theorem 16 due to Lavrauw [54] for semifields of dimension $n$ over their left nucleus. The Segre variety $S_{n,n}$ of $PG(n^2 - 1, q) = PG(M(n \times n, q), \mathbb{F}_q)$ is the set of all matrices of rank 1 and the $(n - 2)$-secant variety of $S_{n,n}$ is the set of all matrices of rank less than $n$. We note that for $n = 2, Q^+(3, q) = S_{2,2}$ and coincide with its variety of secants.

Theorem 22. [54]. Let $\Omega = \Omega(\mathbb{C})$ be a linear set of rank $rn$ with $q = s^n$ of $PG(M(n \times n, q), F_q) = PG(n^2 - 1, q)$. Then $\mathbb{C}$ is a spread set of $M(n \times n, q)$ closed under the addition if and only if $\Omega$ is disjoint from the secant variety of $S_{n,n}$.

3.3.4. Semifield flocks of the quadratic cone. As stated in the introduction, Thas [94] constructed a symplectic spread of $PG(3, q)$ from a semifield flock of the quadratic cone of $PG(3, q)$ by using the $T_2(C)$ model of $Q(4, q)$. My interest in semifield spread of $PG(3, q)$ was motivated to prove that the symplectic spread with one of the known examples of semifield flocks are new. The translation dual of a semifield made clear such a relationship.
Let $K$ be a quadratic cone of $\text{PG}(3, q)$ with vertex $v$. A flock $\mathcal{F}$ of $K$ is a partition of $K \setminus \{v\}$ in $q$ conics. If all planes containing the elements of the flock $\mathcal{F}$ share a common line, then $\mathcal{F}$ is called linear. Two flocks $\mathcal{F}_1$ and $\mathcal{F}_2$ are said isomorphic if there is a collineation $\tau$ of $\text{PG}(3, q)$ which fixes $K$ and maps $\mathcal{F}_1$ onto $\mathcal{F}_2$.

Let $\mathcal{F}$ be a flock of the quadratic cone $K$ of $\text{PG}(3, q)$ with equation $x_3^2 - x_0x_1 = 0$. Then there are two functions $f$ and $g$ of $\mathbb{F}_q$ to itself such that $\mathcal{F} = \{K \cap \pi_t \mid t \in \mathbb{F}_q\}$ where $\pi_t$ is the plane with equation $tx_0 - f(t)x_1 + g(t)x_2 + x_3 = 0$. We will write $\mathcal{F} = \mathcal{F}(f, g)$ and we will say that $\pi_t$ is a plane of the flock. We can suppose $f(0) = g(0) = 0$ (see, Gaevart and Johnson [35]). Define

$$l_{t,u} = \{(a, b, c, d) \mid (c, d) = (a, b) \left(\begin{array}{c} u + g(t) \\ t \\ f(t) \\ u \end{array}\right); a, b \in \mathbb{F}_q\}$$

for $t$ and $u$ in $\mathbb{GF}(q)$ and $l_{\infty} = \{(0, 0, c, d) \mid c, d \in \mathbb{F}_q\}$. The spread of $\text{PG}(3, q)$ associated with $\mathcal{F}$ is defined by

$$S_{\mathcal{F}} = \{l_{t,u} \mid t, u \in \mathbb{GF}(q)\} \cup \{l_{\infty}\}.$$ 

We note that

$$\mathbb{C}_{\mathcal{F}} = \left\{\left(\begin{array}{c} u + g(t) \\ t \\ f(t) \\ u \end{array}\right) \mid u, t \in \mathbb{F}_q\right\}$$

is a spread set and $S_{\mathcal{F}} = S(\mathbb{C})$.

It has been proved in [35] that two flocks $\mathcal{F}_1$ and $\mathcal{F}_2$ are isomorphic if and only if the spreads $S(\mathcal{F}_1)$ and $S(\mathcal{F}_2)$ are isomorphic.

By definition $\mathcal{F}$ is a semifield flock if and only if $S_{\mathcal{F}}$ is a semifield spread with respect to $l_{\infty}$. If and only if the functions $f, g$ are $\mathbb{F}_s$-linear. Denote by $\bar{f}$ and $\bar{g}$ the adjoint maps of $f$ and $g$ (respectively) with respect to the $\mathbb{F}_s$-bilinear form defined by $(x, y) = Tr_{\mathbb{F}_s}(xy)$ for all $x, y \in \mathbb{F}_q$.

Let $\Omega = \Omega(\mathbb{C})$ be the $\mathbb{F}_s$-linear set associated with $\mathcal{F}$. Then the dual $\Omega^\perp$ is the $\mathbb{F}_s$-linear set

$$\Omega^\perp = \left\{\left(\begin{array}{c} a \bar{g}(a) - \bar{f}(b) \\ b \\ -a \end{array}\right) \mid a, b \in \mathbb{F}_q\right\}.$$

We can directly prove that the translation dual of $S_{\Omega}^\perp$ of $S_{\mathcal{F}}$ is symplectic with respect to the symplectic polarity of $\text{PG}(3, q)$ define by the bilinear form

$$\langle(x_0, x_1, x_2, x_3); (y_0, y_1, y_2, y_3)\rangle = x_0y_3 - x_3y_0 + x_1y_2 - x_2y_1,$$

i.e. $S_{\Omega}^\perp$ is the Thas symplectic spread associated with the semifield flock $\mathcal{F}$.

For $q$ even, the semifield flocks are linear (see Johnson [48]). We have just noted that a flock $\mathcal{F}$ defines a semifield spread $S_{\mathcal{F}}$ of $\text{PG}(3, q)$ if and only if $f, g$ are additive. The known additive functions $f, g : \mathbb{F}_q \mapsto \mathbb{F}_q$ such that the polynomial $\gamma X^2 + X g(\gamma) + f(\gamma)$ is irreducible over $\mathbb{F}_q$ for all $\gamma \in \mathbb{F}_q \setminus \{0\}$ are equivalent, up to isomorphism between flocks, to one the following cases: Type (F): Let $f(\gamma) = b \gamma$ and and $g(\gamma) = a \gamma$ where $X^2 + aX + b$ is irreducible over $\mathbb{F}_q$, for any prime power $q$. The flock $\mathcal{F}(f, g)$ is linear. The associated ovoid is an elliptic quadric.
Type (D): Let $q$ be odd. Let $f(\gamma) = n\gamma^\sigma$ and $g(\gamma) = 0$ where $\sigma \in \text{Aut}(\mathbb{F}_q)$ $\sigma \neq \text{id}$, and $n$ is a non-square in $GF(q)$. The flock $\mathcal{F}(f,g)$ is the Kantor semifield flock (see [41]). The associated spread is symplectic, i.e. $\mathcal{S}_\mathcal{F} = \mathcal{S}_\mathcal{F}^\perp$.

Type (CG): Let $q = 3^s$ ($s \geq 3$) and let $f(\gamma) = n\gamma^9 + n^{-1}\gamma$ and $g(\gamma) = \gamma^3$ where $n$ is a non-square in $\mathbb{F}_{3^s}$. The flock $\mathcal{F}(f,g)$ is the Ganley flock (see [34] and [35]). In this case, $\mathcal{S}_\mathcal{F}$ and $\mathcal{S}_\mathcal{F}^\perp$ are not isomorphic [96].

Type (S): $q = 3^5$ and $f(\gamma) = \gamma^9$ and $g(\gamma) = \gamma^{27}$. The flock $\mathcal{F}(f,g)$ is called the sporadic semifield flock and it has been constructed as the translation dual of the Pentilla–Williams translation ovoid (see [6] and [88]).

No more semifield flocks are known.

Suppose that $q = s^r$. If $f,g$ are $\mathbb{F}_s$-linear maps from $\mathbb{F}_q$ onto itself, we can suppose that

\[
\begin{align*}
    f(t) &= a_0t + a_1t^s + \cdots + a_rt^{s^r} \\
    g(t) &= b_0t + b_1t^s + \cdots + b_t^{s^r}.
\end{align*}
\]

Therefore $f$ and $g$ define two $\mathbb{F}_s$-linear functions $\tilde{f}$ and $\tilde{g}$ from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_{q^n}$. If the equality $g^2(t) + 4tf(t) = mh^2(t)$ is a polynomial identity and $n$ is odd, then $m$ is a non-square in $\mathbb{F}_{q^n}$ and, for any $u \in \mathbb{F}_{q^n}$, the element $\tilde{g}^2(u) + 4u\tilde{f}(u) = mh^2(u)$ is a non-square in $\mathbb{F}_{q^n}$. Hence $\mathcal{F}(\tilde{f},\tilde{g})$ is a semifield flock of $PG(3,q^n)$ which contains the flock $\mathcal{F}(f,g)$ of $PG(3,q)$.

If $n$ is even, then $m$ is a square in $\mathbb{F}_{q^n}$ and $\mathcal{F}(\tilde{f},\tilde{g})$ is not a flock.

In the proof of [28, Theorem 4.1], the authors assume that for $n$ big enough, $\mathcal{F}(\tilde{f},\tilde{g})$ is always a flock, but this is not true as proved above.

The proof of the next theorem, given in [4, Theorem 1 (a)], was a revised version of [28, Theorem 4.1].

**Theorem 23.** [4] and [28]. Let $f,g$ be $\mathbb{F}_s$-linear maps from $\mathbb{F}_q$ onto itself. If there is a polynomial $h(t)$ over $\mathbb{F}_q$ such that for a fixed non-square $m$ in $\mathbb{F}_q$ the equality $g^2(t) + 4tf(t) = mh^2(t)$ is a polynomial identity, then $f,g$ is of type (F), (D) or (CG).

We conclude this section with a classification theorem proved by Ball et al. [18]

**Theorem 24.** Let $\mathcal{F}(f,g)$ be a semifield flock of the quadratic cone of $PG(3,q^n)$ such that the functions $f,g$ are $\mathbb{F}_q$-linear. If $q \geq 4n^2 - 8n + 2$, then $\mathcal{F}(f,g)$ is either a linear flock or a Kantor semifield flock.

### 3.4. Translation generalized quadrangles and flocks

Here the basic notion is that of finite generalized quadrangle.

Let $s,t$ be positive integers. A point-line structure $\mathbb{Q} = (P,L)$ is a generalized quadrangle of order $(s,t)$ if the following properties hold

1. Each point is incident with exactly $t + 1$ lines,
2. Each line is incident with exactly $s + 1$ points,
3. If the point $x$ is not incident with the line $L$, there is exactly a point $y$ incident with $L$ and collinear with $x$.

Then $\mathbb{Q}$ has $(st + 1)(s + 1)$ points and $(st + 1)(t + 1)$ lines. The dual structure $\mathbb{Q}^d$ is a generalized quadrangle of order $(t,s)$. Two points are said to be at distance 4 if they are not collinear.
If \( p \) is a point of \( Q \) denote by \( p^\perp \) the set containing \( p \) and all points collinear with \( p \). An elation about \( p \) is a collineation \( \theta \) which fixes any line through \( p \) such that either \( \theta = \text{id} \) or \( \theta \) fixes no point of \( P \setminus p^\perp \). If \( \theta \) fixes all the points collinear with \( p \), then \( \theta \) is a symmetry about the point \( p \). Symmetries about lines are defined dually. The symmetries about a line form a group of order \( \leq s \). If there is a group \( G \) of elations about \( p \) acting regularly on \( P \setminus p^\perp \), we say that \( Q \) is an elation generalized quadrangle with elation group \( G \) and with base point \( p \). If \( G \) contains a full group of \( s \) symmetries about any line through \( (\infty) \), then \( Q \) is translation generalized quadrangle.

If \( Q \) is a translation generalized quadrangle, then \( G \) is an elementary abelian group (see, Thas and Payne [87, Chapter 8.7]).

An egg \( \mathcal{E} \) of \( \text{PG}(4n - 1, s) \) is a partial \((n - 1)\)-spread such that:

1. \( \mathcal{E} \) contains \( s^{2n} + 1 \) elements;
2. Every three elements of \( \mathcal{E} \) generate a \((3n - 1)\)-dimensional subspace of \( \text{PG}(3n - 1, q) \);
3. Each element \( X \) of \( \mathcal{E} \) is contained in a \((3n - 1)\)-dimensional subspace \( T_X \) having no point in common with any element of \( \mathcal{E} \) different from \( X \). The subspace \( T_X \) is called the tangent space to \( \mathcal{E} \) at \( X \).

An ovoid of \( \text{PG}(3, q) \) is an example of egg.

Embed \( \text{PG}(4n - 1, s) \) in \( \text{PG}(4n, s) \) as a hyperplane, and define an incidence structure \( T(\mathcal{E}) \) as follows.

Points are:
1. (i) the points of \( \text{PG}(4n, s) \setminus \text{PG}(4n - 1, s) \),
2. (ii) the \( 3n \)-dimensional subspaces of \( \text{PG}(4n, s) \) which intersect \( \text{PG}(4n - 1, s) \) in the tangent space at an element of \( \mathcal{E} \), and
3. (iii) a new symbol \((\infty)\).

Lines are:

(a) the \( n \)-dimensional subspaces of \( \text{PG}(4n, s) \) which are not contained in \( \text{PG}(4n - 1, s) \) and meet \( \text{PG}(4n - 1, s) \) in an element of \( \mathcal{E} \), and
(b) the elements of \( \mathcal{E} \).

Incidence is defined as follows.

A point of type (i) is incident only with lines of type (a); here the incidence is that of \( \text{PG}(4n, s) \). A point of type (ii) is incident with all the lines of type (a) contained in it and with the unique element of \( \mathcal{E} \) incident with it. The point \((\infty)\) is incident with no line of type (a) and all lines of type (b).

**Theorem 25.** [87, Section 8.7.1]. \( T(\mathcal{E}) \) is a translation generalized quadrangle of order \((s^n, s^{2n})\) with base point \((\infty)\).

Every translation generalized quadrangle of order \((q, q^2)\), is isomorphic to some \( T(\mathcal{E}) \) of \( \text{PG}(4n - 1, s) \), \( s^n = q \).

Let \( Q = T(\mathcal{E}) \) be a finite translation generalized quadrangle of order \((s^n, s^{2n})\) with base point \((\infty)\). Let \((\infty)^\perp\) the set of all points of \( Q \) collinear with \((\infty)\). The points at distance 4 from \((\infty)\), which are the points of type (i), and the lines at distance 3 from \((\infty)\), which are the lines of type (a), define a translation structure of Barlotti–Cofman type. Then we can apply Theorem 9, for proving the following.
Theorem 26. [6, Theorem]. Let $E_1$ and $E_2$ be two eggs of $\text{PG}(4n-1, s)$. The generalized quadrangles $T(E_1)$ and $T(E_2)$ are isomorphic if and only if there is a collineation $\tau$ of $\text{PG}(4n-1, s)$ such that $E_1^\tau = E_2$.

Let $\perp$ be a polarity of $\text{PG}(4n-1, s)$. If $E$ is an egg of $\text{PG}(4n-1, s)$ then it is easy to prove that $E^\perp = \{T^\perp_X \mid X \in E\}$ is still an egg of $\text{PG}(4n-1, s)$, called the translation dual of $E$, which defines a new translation generalized quadrangle $T(E^\perp)$.

Corollary 6. [6]. Let $E_1$ and $E_2$ be two eggs of $\text{PG}(4n-1, s)$. Then $E_1$ and $E_2$ are isomorphic if and only if $E_1^{\perp}$ and $E_2^{\perp}$ are isomorphic.

By using some constructions of Payne [85] and Kantor [41] of generalized quadrangles as coset geometries, it has been proved by J. A. Thas the following theorem

Theorem 27. [93]. Given a flock $F$ of a quadratic cone of $\text{PG}(3, q)$, then there is a standard construction of a generalized quadrangle $Q(F)$, associated with $F$.

The generalized quadrangles $Q(F_1)$ and $Q(F_2)$ are isomorphic if and only if the flocks $F_1$ and $F_2$ are.

Let $Q(F)$ be the generalized quadrangle of order $(q^2, q)$ associated with the flock $F$. It has been proved by Johnson [48] that if $F$ is a semifield flock, then the dual of $Q(F)$ is a translation generalized quadrangle of order $(q, q^2)$. Therefore there is an egg $E(F)$ of $\text{PG}(4n-1, s)$ $q = s^n$ such that $T(E_F)$ is isomorphic to $Q(F)$. Let $E_F^{\pm}$ be the translation dual of the egg $E_F$. If $F$ is either linear or a Kantor semifield flock, then $E_F$ and $E_F^{\pm}$ are isomorphic. If $F$ is a Ganley flock, then $E_F$ and $E_F^{\pm}$ are not isomorphic as proved by Payne [86].

An egg $E$ of $\text{PG}(4n-1, q)$ is good at an element $A \in E$ if and only if for any choice of $B, C \in E \setminus \{A\}$ the $(3n-1)$-dimensional space $\langle A, B, C \rangle$ contains exactly $s^n + 1$ elements of $E$. In Thas [95] has obtained a strong geometric characterisation of the good eggs and has proved that the translation dual $E_F^{\pm}$ is a good egg. It was common opinion that a good egg of $\text{PG}(4n-1, s)$ was isomorphic to the translation dual of $E_F$ where $F$ is a linear flock, or a Kantor flock or a Ganley flock. By Corollary 6, the construction of the sporadic flock disproved such a conjecture.

But there is another possible question. If $F$ is a semifield flock, could the translation dual of $E_F$ be the dual of a flock quadrangle? The next Theorem gives a complete answer to such a question.

Theorem 28. [6]. If $F$ is a semifield flock. If $F$ is neither linear nor a Kantor semifield flock, then $T(E_F^{\pm})$ is not the dual of a flock quadrangle.

4. Symplectic semifield spreads

Let $S$ be a semifield spread of $\text{PG}(2n-1, q)$, $S$ be a semifield such that $S \simeq S(S)$, and suppose the associated spread set $\mathbb{C}(S) = \{C(b) \mid b \in S\}$ of $M(n \times n, q)$ is closed under addition.
Let \((x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) = (x, y)\) be the homogeneous coordinates of \(\text{PG}(2n-1, q)\) and let \(\perp\) be the symplectic polarity defined by the alternating bilinear form

\[ B((x, y); (u, v)) = x \cdot v - y \cdot u \]

where \((x_1, x_2, \ldots, x_n) \cdot (v_1, v_2, \ldots, v_n) = x_1v_1 + x_2v_2 + \cdots x_nv_n\). The subspaces \(y = 0, x = 0\) and \(x = y\) are totally isotropic with respect to \(\perp\).

If \(X\) is an \(n \times n\) matrix over \(\mathbb{F}_q\), then the subspace \(\{ (x, xX) \mid x \in \mathbb{F}_q^n \}\) is totally isotropic with respect to \(\perp\) if and only if \(X\) is symmetric.

If \(\omega\) is a symplectic polarity of \(\text{PG}(2n-1, q)\) such that the subspaces \(y = 0, x = 0\) and \(x = y\) are totally isotropic with respect to \(\omega\), then there is an \(n \times n\) matrix \(M\) such that the the subspace \(\{ (x, xX) \mid x \in GF(q)^n \}\) is totally isotropic with respect to \(\omega\) if and only if the matrix \(M^{-1}XM\) is symmetric. Hence

**Lemma 2.** [43]. A semifield spread \(S\) of \(\text{PG}(2n-1, q)\) is symplectic if and only if there is a finite semifield \(S\) of dimension \(n\) over a subfield \(\mathbb{F}_q\) of its left nucleus such that all the matrices of \(\mathbb{C} = \mathbb{C}(S)\) are symmetric and the spreads \(S\) and \(S(S)\) are isomorphic.

We point out that symplectic semifield spreads are intriguing structures because they have many other different connections. In particular starting from a symplectic semifield spread of \(\text{PG}(3, q)\), \(q\) odd, we can construct a translation generalized quadrangle of order \((q^2, q)\) (see Sect. 3.4). Symplectic spreads of \(\text{PG}(5, q)\), \(q\) even, define ovoids and spreads of the orthogonal polar space \(Q^+(7, q)\) associated with a hyperbolic quadric of \(\text{PG}(7, q)\) [42]. Finally, symplectic semifield spreads of \(\text{PG}(2n-1, 2)\), \(n\) odd, define \(Z_4\)-linear codes (see [22] and [44]). We list some examples of symplectic spreads.

**Example 11.** The desarguesian spread of \(\text{PG}(2n-1, q)\) (see, e.g., [42]).

**Example 12.** Let \(q\) be odd. The semifield spread associated with a twisted field defined by the presemifield \((\mathbb{F}_q^3, +, \circ)\) where \(x \circ y = y^qx + yx^q\) (see [3]).

**Example 13.** The only known non-desarguesian symplectic semifield spreads of even order are those associated with the presemifields constructed in [44] starting from desarguesian spreads and, for this reason, the examples were called the desarguesian scions which are defined in the following way (see, also, [43]). Let \(F = \mathbb{F}_{q^m}\) for \(q\) even and \(m\) odd and let \(F = F_0 \supset F_1 \supset \cdots \supset F_n = \mathbb{F}_q\) be a chain of subfields. Denote by \(T_i\) the trace of \(F\) over \(F_i\) and by \(\zeta_i\) a fixed non zero element of \(F\) for \(i = 1, 2, \ldots, n\). Define a new multiplication \(*\) on \(F\) by

\[ x * y = xy^2 + \sum_{i=1}^n (T_i(\zeta_i x)y + \zeta_i T_i(xy)) \]

Then \(P = (F, +, * )\) is a symplectic presemifield such that \(\lambda (x * y) = (\lambda x) * y\) for all \(\lambda \in F_n\) and \(x, y \in F\). If \((x * 1) \circ (1 * y) = x * y\), then \(S = (F, +, \circ)\) is a semifield with identity \(1 * 1\) isotopic to \(P\).
Using the characterization of the left nucleus given in [79, Theorem 2.2], it has been proved that, if \( q^m > 8 \), then the left nucleus of \( S \) is isomorphic to \( F_n \) (see [44] and [70]).\(^2\)

**Example 14.** Let \( S = (\mathbb{F}_{q^3}, +, \cdot) \), \( q \) an odd prime power, with multiplication given by

\[
x \ast y = \frac{y + y^q}{2} x + \frac{1}{4} (f(y)) y^2 x y^q + \frac{1}{4} f(y) x y^q,
\]

with \( f(y) = y - y^q - y^q^2 - y^q^3 + y^q^4 + y^q^5 \). Then \( S \) is a symplectic semifield of order \( q^6 \) whose left nucleus contains \( \mathbb{F}_{q^2} \) and the associated semifield spread of \( \text{PG}(5, q^2) \) is symplectic (see [69, Theorem 5]).

### 4.1. Symplectic dual

In this Section we will suppose that \( q \) is odd.

For each matrix \( X = (a_{ij}) \) of \( M(3 \times 3, q) \) let \( Tr(X) = a_{11} + a_{22} + a_{33} \) be the trace of \( X \).

Let \( \Gamma = \text{PG}(\text{Sym}_3(q), \mathbb{F}_q) = \text{PG}(5, q) \), where \( \text{Sym}_3(q) \) is the subspace consisting of the symmetric matrices of \( M(3 \times 3, q) \). Then \( V_3 = S_{3,3} \cap \Gamma \) is a Veronese surface and its secant variety is the algebraic variety \( \mathcal{M}(V_3) \) defined by all singular symmetric matrices of \( M(3 \times 3, q) \). The planes of \( \Gamma \) which meet \( V_3 \) in a conic are called conic planes of \( V_3 \) and the planes containing all tangent lines of \( V_3 \) at a given point are called tangent planes of \( V_3 \). The variety \( \mathcal{M}(V_3) \) is the union of the conic planes and it is also the union of the tangent planes. For more details on the Veronese surface we refer to [37, § 25.1]. If \( X = \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \), define

\[
Q(X) = a^2 + d^2 + f^2 + 2b^2 + 2c^2 + 2e^2.
\]

Hence, \( Q \) is a non-singular quadratic form of \( \text{Sym}_3(q) \) whose associated bilinear form is \( b(X, Y) = Tr(XY) \). The polarity of \( \Gamma \) induced by the quadratic form \( Q \) maps the set of all conic planes of \( V_3 \) to the set of all tangent planes of \( V_3 \) (see [37, Theorem 25.1.18]).

Let \( q = s^r \). If \( \Lambda \) is an \( \mathbb{F}_s \)-linear set of rank \( 3r \) of \( \text{PG}(5, q) \) then the dual \( \Lambda^\perp \) of \( \Lambda \) with respect to the polarity \( \perp \) of \( \text{PG}(6n - 1, s) \), defined by the \( \mathbb{F}_s \)-bilinear form \( \langle X, Y \rangle = tr_{\mathbb{F}_s} b(X, Y) \), is an \( \mathbb{F}_s \)-linear set of \( \text{PG}(5, q) \) of rank \( 3r \) as well.

**Theorem 29.** [69, Theorem 3]. The \( \mathbb{F}_s \)-linear set \( \Lambda \) of \( \text{PG}(5, q) \) of rank \( 3r \) is disjoint from \( \mathcal{M}(V_3) \) if and only if \( \Lambda^\perp \) is disjoint from \( \mathcal{M}(V_3) \).

By Lemma 2, if \( \Lambda = \Lambda(\mathcal{C}) \) is an \( \mathbb{F}_s \)-linear set of rank \( 3r \) disjoint from \( \mathcal{M}(\mathcal{V}) \), then \( \mathcal{C} \) is a spread set of symmetric matrices of \( M(3 \times 3, q) \) defining a symplectic semifield spread \( S \). By Theorem 29, \( \Lambda^\perp \) is an \( \mathbb{F}_s \)-linear set disjoint from \( \mathcal{M}(\mathcal{V}) \). Therefore, there is a spread set \( \mathcal{C}^\perp \) closed under the sum, such that \( \Lambda^\perp = \)

\(^2\)If \( q^m = 8 \), then \( S \) is a field (i.e. \( N_l = S \)), because every plane of order 8 is desarguesian (see [30, p. 144]).
Λ(\mathbb{C}^\perp), and \mathbb{C}^\perp defines a new symplectic spread \( S^\perp \) called the symplectic dual of \( S \) (see [69] for more details).

The symplectic dual of a desarguesian spread of \( \text{PG}(5,q) \) is the symplectic semifield spread of \( \text{PG}(5,q) \) arising from a twisted field. The spread constructed in Examples 14 is self-dual (see [69] for more details).

### 4.2. Symplectic semifield spreads and commutative semifields

Let \( S = S(+, \cdot) \) be a semifield. Define a new multiplication \( \circ \) on \( S \) by \( a \circ b = b \cdot a \).

It is easy to prove that \( S^d = S(+, \circ) \) is a semifield, and the plane \( \pi(S) \) is the dual of \( \pi(S^d) \) (see, e.g., [40]).

Note that if \( S = S(+, \cdot) \) is commutative, then \( a \circ b = a \cdot b \), i.e. \( S^d = S \) and the plane \( \pi = \pi^d \) is self-dual.

We have previously noted that a spread \( S \) of \( \text{PG}(2n-1, q) \) is a semifield spread with respect to an element \( A \) of \( S \) if there exists an elementary abelian group \( E \) of order \( q^n \) which fixes \( A \) pointwise and acts regularly on \( S \setminus \{A\} \).

Let \( \perp \) be a symplectic polarity of \( \text{PG}(2n-1, q) \). Suppose that \( S \) is a semifield spread of \( \text{PG}(2n-1, q) \) with respect to \( A \) and denote by \( E \) the relevant elementary abelian group. As \( \text{PG}(2n-1, q) \) is a finite projective space, \( S^T = \{X^\perp \mid X \in S\} \) is a spread of \( \text{PG}(2n-1, q) \) and \( \overline{E} \), the conjugate of \( E \) under \( \perp \), is an elementary abelian group which fixes \( A^\perp \) pointwise and acts regularly on \( S^T \setminus \{A^\perp\} \). Hence, \( S^T \) is a semifield spread with respect to \( A^\perp \).

We note that, up to isomorphisms, \( S^T \) does not depend on the chosen polarity. Using the algebraic properties of the Knuth cubical array associated with a finite semifield, we can define a chain of six semifields starting from a given one (see, e.g., [30]). The geometric interpretation of such a construction is given in [76] (see, also, [9]) where it has been proved that the six semifield planes are associated with one of the semifield spreads

\[
S \mapsto S^d \mapsto S^{dT} \mapsto S^{dT^d} \mapsto S^{dTdT} \mapsto S^{dTdT^d} \mapsto S^{dTdTdT} = S.
\]

Let \( S \) be a finite semifield, denote by \( S^d \) the dual of \( S \) and by \( S^T \) a semifield which coordinatizes the plane \( \pi(S^T) \).

If \( N^l_d, N^m_d, N^r_d, Z^d \) are, respectively, the left nucleus, the middle nucleus, the right nucleus and the center of \( S^d \), then \( N^l_d = N_r, N^m_d = N_m, N^r_d = N_l \) and \( Z^d = Z \). Furthermore, if \( N^l_T, N^m_T, N^r_T, Z^T \) are (respectively) the left nucleus,
the middle nucleus, the right nucleus and the center of $S_T$, then $N^T_I = N_I$, $N^T_m \simeq N_r$, $N^T_T \simeq N_m$ and $Z^T = Z$ (see [65, 76] and [15]). The above properties turn out to be very useful. For instance, if $S$ is a semifield of dimension 2 over $N_I = N_m = \mathbb{F}_q$, then the dual $S^d$ has dimension 2 over $N^d_m = N^d_r = \mathbb{F}_q$ and the transpose $S^T$ has dimension 2 over $N^T_m = N^T_T = \mathbb{F}_q$.

Using the geometric interpretation of the Knuth operation on the cubical array one can prove the following theorem

**Theorem 30.** Let $S$ be a semifield and let $S = \mathcal{F}(S, GF(q))$ be the spread of $PG(2n - 1, q)$ associated with $S$.

1. The spread $S$ is symplectic if and only if the plane $\pi(S^dTd)$ is coordinatized by a commutative semifield $S^dTd$ [43].
2. If $S$ is symplectic, then $N_m = N_r = Z$ [65].
3. If $S$ is symplectic, then the semifield $S$ has dimension $n$ over its left nucleus if and only if $S^dTd$ has dimension $n$ over its middle nucleus [65].

**Example 15.** When $q$ is even, the dual of the transpose of the dual of a desarguesian scion is the only known class of commutative semifields, constructed in [43] and called generalized binary Knuth semifields, because they are a generalization of binary Knuth semifields constructed in [45].

By Theorems 21 and 30, the translation dual is not a Knuth operation and can produce a chain of length 12 which is a particular case of the semifield chain constructed by Ball et al. [10].

Hence, summarizing the above results, the classification of semifields of dimension $n$ over one of their nuclei is equivalent to that of finite semifields of dimension $n$ over their left nucleus, whilst the classification of commutative semifields of dimension $n$ over their middle nucleus $N_m = \mathbb{F}_q$ is equivalent to that of symplectic semifield spreads of $PG(2n - 1, q)$.

In the introduction of Kantor [43] observes that finite commutative semifields are painfully lacking listing all the known examples. This remark motivated new researches and some new commutative semifields have been found (see, e.g., [80] for a recent list of known examples).

5. MRD-codes and translation structures

5.1. Linear MRD-codes

A linearized polynomial over $\mathbb{F}_{q^n}$ is a polynomial of type $a_0 x + a_1 x^q + \cdots + a_{n-1} x^{q^{n-1}}$ with coefficients in $\mathbb{F}_{q^n}$. Let $E = \text{End}(\mathbb{F}_{q^n}, \mathbb{F}_q)$ be the vector space of all the endomorphisms of $\mathbb{F}_{q^n}$ as vector space over $\mathbb{F}_q$. For any element $\varphi$ of $E$, there is a unique linearized polynomial $a_0 x + a_1 x^q + \cdots + a_{n-1} x^{q^{n-1}}$ with $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_{q^n}$, such that $\varphi = \varphi_{a_0, a_1, \ldots, a_{n-1}} : x \mapsto a_0 x + a_1 x^q + \cdots + a_{n-1} x^{q^{n-1}}$. Recall that the $q$-degree of a non-zero polynomial is the maximum $i$ such that $a_i \neq 0$.

A rank metric code $C$ is a set of linearized polynomials equipped with the distance function $d(\varphi, \theta) = \text{rank}(\varphi - \theta)$. A linear rank metric code $C$ is a
A prime. Then the set

\[ \text{codes using linearized polynomials. Sheekey’s ideas is the following. Let} \ n, k, s \]

Given a linearized polynomial \( \varphi(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \), the adjoint of \( \varphi \) is defined by

\[ \hat{\varphi}(x) = \sum_{i=0}^{n-1} a_i x^{q^{n-i}}. \]

Moreover, \( rk(\hat{\varphi}) = rk(\varphi) \).

The adjoint code of an MRD-code \( \mathcal{C} \) is the code \( \hat{\mathcal{C}} = \{ \varphi \mid \varphi \in \mathcal{C} \} \), which is an MRD-code with the same distance as \( \mathcal{C} \).

Let \( \varphi(x) = a_0 x + a_1 x^q + \cdots + a_{n-1} x^{q^{n-1}} \). If \( q = p^e \), let \( \varphi^{p^h} \) the linearized polynomial defined by

\[ \varphi^{p^h}(x) = a_0^{p^h} x + a_1^{p^h} x^q + \cdots + a_{n-1}^{p^h} x^{q^{n-1}}. \]

Two linear rank metric codes \( \mathcal{C}_1 \) and \( \mathcal{C}_2 \) are equivalent if there are two non-singular linearized polynomials \( \theta, \vartheta \) such that \( \mathcal{C}_2 = \{ \vartheta \circ \varphi^{p^h} \circ \theta \mid \varphi \in \mathcal{C}_1 \} \). We say that \( \mathcal{C}_1 \) and \( \mathcal{C}_2 \) are weakly equivalent if \( \mathcal{C}_2 \) is equivalent to \( \hat{\mathcal{C}}_1 \).

Maximum rank distance codes, introduced by Delsarte [29], have been recently rediscovered by Kötter and Kschischang [47] as network codes for networks with close topology.

The first examples of linear MRD-codes over the finite field \( \mathbb{F}_q \) for every \( k, n \) have been constructed by Delsarte [29] and Gabidulin [32] in the following way. Let \( n, k, s \) be positive integers such that \( \gcd(n, s) = 1 \) and let \( s \) be a power of a prime. Then the set

\[ \mathcal{G}(k, s) = \{ a_0 x + a_1 x^{q^s} + \cdots + a_{k-1} x^{q^{s(k-1)}} \mid a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_q^n \} \]

is an \( \mathbb{F}_q \)-linear MRD code of size \( q^{nk} \). In literature these are usually called the generalized Gabidulin codes (see Gabidulin and Kshevetskiy [33]).

Recently, Sheekey [90] made a breakthrough in the construction of linear MRD-codes using linearized polynomials. Sheekey’s ideas is the following. Let

\[ \mathcal{G} = \{ a_1 x^{q^s} + a_1 x^{q^{2s}} + \cdots + a_{k-1} x^{q^{s(k-1)}} \mid a_1, \ldots, a_{k-1} \in \mathbb{F}_q^n \} \approx \mathcal{G}(k-1, s) \]

\[ \mathcal{K} = \mathcal{K}(f, g) = \{ g(b)x + f(b)x^{q^s} + \mid b \in \mathbb{F}_q^n \} \]

where \( f, g \) are \( \mathbb{F}_q \)-linearized polynomials. Denote by \( N_{q^n,q}(a) = a^{q^n-1} \) the norm function from \( \mathbb{F}_q^n \) to \( \mathbb{F}_q \). If for all \( b \in \mathbb{F}_q^n \setminus \{0\} \) we have

\[ N_{q^n,q}(f(b)) \neq (-1)^{kn} N_{q^n,q}(g(b)) \]

then \( \mathcal{C} = \mathcal{G} + \mathcal{K}(f, g) \) is an MRD-code with distance \( n - k + 1 \) (see [90, Remark 8]). The known functions \( f, g \) satisfying the above conditions are:

1. For \( s = 1 \), let \( g(b) = b \) and \( f(b) = h^\eta b^h \) where \( N_{q^n,q}(\eta) \neq (-1)^{nk} \). Then \( \mathcal{H}(\eta, k) = \mathcal{G}(k-1, 1) + \mathcal{K}(f, g) \) is an \( \mathbb{F}_q \)-linear MRD-code of size \( q^{nk} \), which is called a twisted Gabidulin code (see Sheekey [90]);

2. For \( s \neq 1 \), let \( g(a) = a \) and \( f(b) = h^{\eta b^{s^h}} \) where \( N_{q^n,q}(\eta) \neq (-1)^{nk} \). Then \( \mathcal{H}(\eta, k, s) = \mathcal{G}(k-1, s) + \mathcal{K}(f, g) \) is an \( \mathbb{F}_q \)-linear MRD-code of size \( q^{nk} \), which is called a generalized twisted Gabidulin code (see Sheekey [90]).
The proof that $\mathcal{H}(\eta, k, s)$ and $\mathcal{H}(\eta, k)$ are not equivalent has been given in [74];

(3) For $\gamma \in \mathbb{F}_{q^{2^m}}$ such that $N_{q^{2^m}, q}(\gamma)$ is a non-square in $\mathbb{F}_q$, let $g(\alpha + \gamma \beta) = \alpha$ and $f(\alpha + \gamma \beta) = \gamma \beta$. Then $D_{k,s}(\gamma) = G(k,s) + K(f,g)$ is the Trombetti–Zhou MRD-code [99, Theorem 3.1].

(4) Let $g(b) = b$ and $f(b) = \eta b^\gamma$ where $N_{q^m,q}(\eta) \neq (-1)^{nk}$. Then $A = G(k,s) + K(f,g)$ is an MRD-code called additive generalized twisted Gabidulin code (see Otal and Ozbudak [82]).

5.2. MRD-codes and linear sets
Let $\Sigma^* = \text{PG}(n - 1, q^n)$. If $X_0, X_1, \ldots, X_{n-1}$ are the homogenous coordinates of $\Sigma^*$, let $\sigma$ be the collineation of $\Sigma^*$ defined by the semilinear map

$$(X_0, X_1, \ldots, X_{n-1}) \mapsto (X_0^q, X_1^q, \ldots, X_{n-1}^q)$$

of order $n$. Then $\Sigma = \{ (\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}) \mid \alpha \in \mathbb{F}_{q^n} \} \simeq \text{PG}(n-1, q)$ is the subgeometry of $\Sigma^*$ pointwise fixed by $\sigma$. A point $P = (a_0, a_1, \ldots, a_{n-1})$ of $\Sigma^*$ is of type $r$ if and only if the matrix

$$M(a_0, a_1, \ldots, a_{n-1}) = \begin{pmatrix}
a_0 & a_1 & \cdots & a_{n-1} \\
a_0^q & a_1^q & \cdots & a_{n-2}^q \\
\vdots & \vdots & \ddots & \vdots \\
\gamma & \gamma^q & \cdots & a_0^{q^{n-1}}
\end{pmatrix}$$

has rank $r$ if and only if the linearized polynomial

$$\varphi = \varphi_{a_0, a_1, \ldots, a_{n-1}}(x) = a_0 x + a_1 x^q + \cdots + a_{n-1} x^{q^{n-1}}$$

has rank $r$ (see [57, p. 362]).

Let $C$ be a linear MRD-code of $\mathbb{E}$ with distance $d = n - k + 1$. Then $C$ has size $q^{nk}$ and there is a maximal subfield $\mathbb{F}_s$ of $\mathbb{F}_q$ with $q = s^e$ such that $C$ is an $\mathbb{F}_s$-vector space. Hence

$$\Omega(C) = \{ (a_0, a_1, \ldots, a_{n-1}) \in \text{PG}(n - 1, q^n) \mid \varphi_{a_0, a_1, \ldots, a_{n-1}} \in K \}$$

is an $\mathbb{F}_s$-linear set of $\text{PG}(n - 1, q^n)$ of rank $nk$, all points of which are of type $\geq n - k + 1$. The following relationship has been proved in [67, Theorem 1]:

**Theorem 31.** For any linear MRD-code $C \subset \mathbb{E}$ of size $q^{nk}$, there is an $\mathbb{F}_s$-linear set $\Omega$ of $\text{PG}(n - 1, q^n)$ of rank $nk$, with $q = s^e$, all points of which are of type $\geq n - k + 1$, such that $\Omega = \Omega(C)$.

5.2.1. Embedding and $\mathbb{F}_{q^n} - $linear MRD-codes. For any $\lambda \in \mathbb{F}_{q^n}$, let $\varphi_\lambda(x) = \lambda x$. We say that an MRD-code $C$ is $\mathbb{F}_{q^n}$-linear if for any element $\varphi$ of $C$ and any $\lambda \in \mathbb{F}_{q^n}$ the polynomials $\varphi_\lambda \varphi$ belongs to $C$.

If $C$ is an $\mathbb{F}_{q^n}$-linear MRD code with distance $d = n - k + 1$, then $\Omega(C)$ is a $(k - 1)$-dimensional subspace of $\Sigma^*$. We note that the generalized Gabidulin codes are $\mathbb{F}_{q^n}$-linear.

Let $\Gamma^*$ be an $(k - 1)$-dimensional subspace of $\Sigma^*$ disjoint from $\Sigma$ and let $\Gamma^* = \Omega(C)$. Denote by $\Gamma$ an $(n - k - 1)$-dimensional subspace of $\Sigma^*$ disjoint from $\Gamma^*$ and let $\Lambda = p_{\Gamma^*,\Gamma}(\Sigma)$. By Theorem 12, $C$ is an $\mathbb{F}_{q^n}$-linear MRD-code if
and only if $\Lambda$ is an $(k-1)$-embedding of $\Sigma$ if and only if $\Lambda$ is an $(k-1)$-scattered $\mathbb{F}_q$-linear set of $\Gamma$.

5.2.2. MRD-codes of Sheekey’s type. Sheekey’s ideas can be generalized in the following way.

Let $G$ be an $\mathbb{F}_{q^n}$-linear MRD-code of size $q^{n(k-1)}$ and let $K$ be a linear rank metric code of size $q$ such that $G \cap K = \emptyset$. Therefore $C = G \oplus K$ is a linear rank metric code of size $q^{nk}$.

As $G$ is $\mathbb{F}_{q^n}$-linear, $\Gamma^* = \Omega(G)$ is a $(k-2)$-dimensional subspace of $\Sigma^*$ disjoint from $\Sigma$. If $\Gamma$ is an $(n-k)$-dimensional subspace of $\Sigma^*$ disjoint from $\Gamma$, we can suppose that $\Omega = \Omega(K)$ is contained in $\Gamma$. Let $\Lambda = p_{\Gamma^*,\Gamma}(\Sigma)$. Then

**Theorem 32.** [67, Theorem 5]. The rank metric code $C$ is an MRD-code if and only if $\Omega = \Omega(K)$ is disjoint from any hyperplane of $\Gamma$ spanned by $n-k$ points of $\Lambda$.

*Proof.* By construction $p_{\Gamma^*,\Gamma}(\Omega(C)) = \Omega$. We note that $C$ is an MRD-code if and only if all points of $\Omega(C)$ are of type $\geq n-k+1$.

By way of contradiction suppose that a point $P$ of $\Omega(C)$ is of type $n-k$. Then $L(P)$ is an $(n-k-1)$-dimensional subspace of $\Sigma^*$ disjoint from $\Gamma^*$. Hence, $\langle \Gamma^*, L(P) \rangle \cap \Gamma$ is a hyperplane of $\Gamma$ spanned by $n-k$ points of $\Lambda$. As the point $P' = p_{\Gamma^*,\Gamma}(P)$ of $\Omega$ belongs to the subspace $p_{\Gamma^*,\Gamma}(L(P))$, we have the required contradiction. \hfill $\Box$

5.2.3. MRD-codes and scattered linear sets of $PG(1, q^n)$. Let $L$ be a line of $\Sigma^*$ disjoint from $\Sigma$. As $\Sigma$ has exactly $q^n-1 + \cdots + q + 1 < q^n+1$ points, there is a point of type $n$ on the line $L$. As the points of type $n$ are all equivalent, we can suppose that $(1, 0, \ldots, 0)$ belongs to $L$. If $(a_0, a_1, \ldots, a_{n-1})$ is a second point, let $f(x) = a_0x + a_1x^q + \cdots + a_{n-1}x^{q^{n-1}}$ be the associated linearized polynomial. If $C = \{\alpha x + \beta f(x) \mid \alpha, \beta \in \mathbb{F}_{q^n}\}$, then $L = \Omega(C)$. Then $C$ is an MRD-code if and only if all points of $L$ are of type $\geq n-1$.

**Theorem 33.** [90, Theorem 8]. The rank metric code $C$ is an $\mathbb{F}_{q^n}$-linear MRD-code if and only if the set $\Delta_f = \{(x, f(x)) \mid x \in \mathbb{F}_{q^n}\}$ is a scattered $\mathbb{F}_q$-linear set of $PG(1, q^n)$.

Theorem 33 motivated the renewed interest in scattered polynomials as explained in Sect. 3.2.

5.3. Idealisers of an MRD-code

In general, it is difficult to tell whether two rank metric codes with the same parameters are equivalent or not. Hence, it is quite natural to ask whether there are further invariants for other rank metric codes, especially for MRD codes. In this section we present the construction of left and right invariants only for the MRD-codes defined by linearized polynomials, i.e. the MRD-codes defined by square matrices. We refer the reader to [75] for the general case.

We recall that a linear rank metric code is a subgroup and, therefore, $0$ belongs to the code.

Let $C$ be a rank metric code. Let $V = \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$. For any linearized polynomial $\varphi$ let
Corollary 7. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be linear MRD-codes with distance $d < n$, then $\mathcal{C}_1$ is equivalent to $\mathcal{C}_2$.

By Theorem 9 we have the following corollary.

Corollary 7. The MRD-codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if and only if there is a collineation $\tau$ of $\mathrm{PG}(n^2 - 1, q)$ such that $\mathcal{C}_1 = \mathcal{C}_2$, $\mathcal{S}(\infty)^\tau = \mathcal{S}(\infty)$ and $\mathcal{S}(0)^\tau = \mathcal{S}(0)$ if and only if the translation structures with parallelism $\mathcal{S}(\mathcal{C}_1)$ and $\mathcal{S}(\mathcal{C}_2)$ are isomorphic via an isomorphism which fixes the lines $\mathcal{S}(\infty)$ and $\mathcal{S}(0)$.

Proof. For any semilinear non-singular map $\tau$ of $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ to itself which fixes $\mathcal{S}(\infty)$ and $\mathcal{S}(0)$, there are two non-singular linearized polynomials $\alpha$ and $\beta$ such that

$$\tau : (x, y) \mapsto (\beta^{-1}(x^{p^h}), \alpha(y^{p^h})).$$

Hence $\tau$ maps $\mathcal{S}(\varphi)$ to $\mathcal{S}(\alpha \varphi^{p^h} \beta)$. The Corollary follows from the definition of equivalent codes. \qed

If $\mathcal{C}$ is a linear metric code, the left idealiser $L(\mathcal{C})$ of $\mathcal{C}$ is defined by

$$L(\mathcal{C}) = \{ \lambda \in \mathbb{E} \mid \lambda \varphi \in \mathcal{C}, \forall \varphi \in \mathcal{C} \}$$

and the right idealiser $R(\mathcal{C})$ of $\mathcal{C}$ is defined by

$$R(\mathcal{C}) = \{ \varrho \mid \varrho \varphi \in \mathcal{C}, \forall \varphi \in \mathcal{C} \}$$

It is easy to prove that $L(\mathcal{C})$ and $R(\mathcal{C})$ are closed under addition and multiplication. We note that if $\lambda$ is a non-singular linearized polynomial, then $\lambda \in L(\mathcal{C})$ if and only if the semilinear map $(x, y) \mapsto (x, \lambda(y))$ fixes $\mathcal{C}$. Hence the non singular elements of $L(\mathcal{C})$ define the group of all collineations of $\mathcal{S}(\mathcal{C})$ fixing $\mathcal{S}(\infty)$ and inducing the identity on $\mathcal{S}(0)$. If $\varrho$ is a non-singular linearized polynomial, then $\varrho \in R(\mathcal{C})$ if and only if the collineation $(x, y) \mapsto (\varrho(x), y)$ fixes $\mathcal{S}(\mathcal{C})$. Hence the non singular elements of $R(\mathcal{C})$ define the group of all collineations of $\mathcal{S}(\mathcal{C})$ fixing $\mathcal{S}(0)$ and inducing the identity on $\mathcal{S}(\infty)$.

Theorem 35. [75, Theorem 5.4]. If $\mathcal{C}$ is a linear MRD-code, then $L(\mathcal{C})$ and $R(\mathcal{C})$ are fields and $\mathcal{C}$ is a vector space over each of them.
Corollary 8. [75]. Equivalent MRD-codes have the same dimension over $L(C)$ and over $R(C)$.

Proof. As $C_1$ is equivalent to $C_2$ if and only if there is an isomorphism
\[ \tau : (x, y) \mapsto (\beta^{-1}(x^p^h), \alpha(x^p^h)) \]
from $S(C_1)$ to $S(C_2)$, then $\tau$ maps $S(\varphi)$ to $S(\alpha \varphi x^p^h \beta)$ and the map
\[ L(C_1) \rightarrow L(C_2), \quad \lambda \mapsto \alpha \lambda \alpha^{-1} \]
is an isomorphism. In a similar way we can prove the map
\[ R(C_1) \rightarrow R(C_2), \quad \varrho \mapsto \beta^{-1} \varrho x^p^h \beta \]
is an isomorphism. \hfill \Box

Funding Open access funding provided by Università degli Studi di Napoli Federico II within the CRUI-CARE Agreement.

Open Access. This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] André, J.: Über nicht-Desarguessche Ebenen mit transitive Translationgruppe. Math. Z. 60, 156–186 (1954)
[2] André, J.: Über Parallelstrukturen—II: Translationstrukturen. Math. Z. 76, 155–180 (1961)
[3] Bader, L., Kantor, W.M., Lunardon, G.: Symplectic spreads from twisted fields. Boll. Un. Mat. Ital. 8, 383–389 (1994)
[4] Bader, L., Lunardon, G.: On non-hyperelliptic flocks. Eur. J. Combin. 15, 411–415 (1994)
[5] Bader, L., Lunardon, G.: Desarguesian spreads. Ric. Mat. 60, 15–38 (2011)
[6] Bader, L., Lunardon, G., Pinneri, I.: A new semifield flock. J. Comb. Theory Ser. A 86, 49–62 (1999)
[7] Ball, S.: The number of directions determined by a function over a finite field. J. Comb. Theory Ser A 104, 341–350 (2003)
[8] Ball, S., Blokhuis, A., Brouwer, A.E., Storme, L., Szönyi, T.: On the number of slopes of the graph of a function defined on a finite field. J. Comb. Theory Ser. A 86, 187–196 (1999)

[9] Ball, S., Brown, M.: The six semifield planes associated with a semifield flocks. Adv. Math. 189, 68–87 (2004)

[10] Ball, S., Ebert, G.L., Lavrauw, M.: A geometric construction of finite semifields. J. Algebra 311, 117–129 (2007)

[11] Barlotti, A., Cofman, J.: Finite Sperner spaces constructed from projective and affine spaces. Abh. Math. Sem. Univ. Hamburg 40, 230–241 (1974)

[12] Bartoli, D., Zanella, C., Zullo, F.: A new family of maximum scattered linear sets in $PG(1,q^6)$. Ars Math. Contemp. 19, 125–145 (2020)

[13] Beutelspacher, A.: On parallelisms in finite projective spaces. Geom. Dedicata. 3, 35–40 (1974)

[14] Biliotti, M.: Geometrie affini su un A modulo e S spazi. Atti Sem. Mat. Fis. Univ. Modena 25, 1–13 (1975)

[15] Biliotti, M., Jha, V., Johnson, N.L.: Symplectic flock spreads in $PG(3,q)$. Note di Math. 24(1), 85–110 (2005)

[16] Blokhuis, A.: Special pointsets in finite planes. CWI Q. 9, 31–36 (1997)

[17] Blokhuis, A., Lavrauw, M.: Scattered spaces with respect to a spread in $PG(n,q)$. Geom. Dedicata 81, 231–243 (2000)

[18] Blockhius, A., Lavrauw, M., Ball, S.: On the classification of semifield flocks. Adv. Math. 180, 104–111 (2003)

[19] Bonetti, F., Lunardon, G.: Sugli S spazi di traslazione. Boll. U.M.I. 14-A, 368–374 (1977)

[20] Bonetti, F., Lunardon, G.: Un esempio di S spazio di traslazione. Acc. Naz. S.L.A., Modena 59, 153–157 (1977)

[21] Bruck, R.H., Bose, R.C.: The construction of translation planes from projective spaces. J. Algebra 1, 85–102 (1964)

[22] Calderbank, A.R., Cameron, P.J., Kantor, W.M., Seidel, J.: $Z_4$-Kerdok codes, orthogonal spreads, and extremal Euclidean line-sets. Proc. Lond. Math. Soc. 75, 436–480 (1997)

[23] Cardinali, I., Lunardon, G., Polverino, O., Trombetti, R.: Spreads in $H(q)$ and 1-systems of $Q(6,q)$. Eur. J. Combin. 23, 367–376 (2002)

[24] Cardinali, I., Polverino, O., Trombetti, R.: Semifield planes of order $q^4$ with kernel $F_{q^2}$ and center $F_q$. Eur. J. Combin. 27, 940–961 (2006)

[25] Csajbók, B., Marino, G., Polverino, O.: Classes and equivalence of linear sets in $PG(1,q^n)$. J. Combin. Theory Ser. A 157, 402–426 (2018)

[26] Csajbok, B., Marino, G., Polverino, O., Zullo, F.: Maximum scattered linear sets and MRD-codes. Linear Algebra Appl. 548, 203–220 (2018)

[27] Csajbók, B., Marino, G., Zullo, F.: New maximum scattered linear sets of the projective line. Finite Fields Appl. 54, 133–150 (2018)

[28] Cohen, S.D., Ganley, M.: Commutative semifields two dimensional over their middle nucleus. J. Algebra 75, 373–385 (1982)

[29] Delsarte, P.: Bilinear forms over finite fields with application to coding theory. J. Combin. Theory Ser. A 25, 226–241 (1978)

[30] Dembowski, P.: Finite Geometries. Springer, Berlin (1968)
[31] Ebert, G.L., Marino, G., Polverino, O., Trombetti, R.: Infinite families of new semifields. Combinatorica 29, 637–663 (2009)

[32] Gabidulin, E.: Theory of codes with maximum rank distance. Probl. Inf. Transm. 21, 3–16 (1985)

[33] Gabidulin, E., Kshevetskiy, A.: The new construction of rank codes. In: International Symposium on Information Theory, ISIT 2005 Proceedings, 2105–2108

[34] Ganley, M.J.: Central weak nucleus semifields. Eur. J. Combin. 2, 339–347 (1981)

[35] Gevaert, H., Johnson, N.L.: Flocks of quadratic cones, generalized quadrangles and translation planes. Geom. Dedicata. 27, 301–317 (1988)

[36] Hiramine, Y., Matsumoto, M., Oyama, T.: On some extension of 1 spread sets. Osaka J. Math. 24, 123–137 (1987)

[37] Hirsched, J.W.P., Thas, J.A.: General Galois Geometries. Oxford University Press, Oxford (1991)

[38] Huang, H., Johnson, N.L.: Semifield of order $8^2$. Discrete Math. 80, 69–79 (1990)

[39] Hughes, D., Kleinfeld, E.: Seminuclear extensions of Galois fields. Ann. J. Math. 82, 389–392 (1960)

[40] Hughes, D., Piper, F.: Projective Planes. Springer, Berlin (1972)

[41] Kantor, W.M.: Some generalized quadrangles with parameters $(q^2, q)$. Math. Z. 192, 45–50 (1986)

[42] Kantor, W.M.: Spreads, translation planes and Kerdock sets, I. SIAM J. Alg. Disc. Methods 3, 151–165 (1982)

[43] Kantor, W.M.: Commutative semifields and symplectic spreads. J. Algebra 270, 96–114 (2003)

[44] Kantor, W.M., Williams, M.E.: Symplectic semifields planes and $Z_4$-linear codes. Trans. Am. Soc. 356, 895–938 (2004)

[45] Knuth, D.E.: A class of projective planes. Trans. Am. Math. Soc. 115, 541–549 (1965)

[46] Knuth, D.E.: Finite semifields and projective planes. J. Algebra 2, 182–217 (1965)

[47] Kötter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. IEEE Trans. Inf. Theory 54, 3579–3591 (2008)

[48] Johnson, N.L.: Semifield flocks of quadratic cones. Simon Stevin 61, 313–326 (1987)

[49] Johnson, N.L.: Sequences of derivable translation planes. Osaka J. Math. 25, 519–53 (1988)

[50] Johnson, N.L., Jha, V., Biliotti, M.: Handbook of finite translation planes. In: Pure and Applied Mathematics (Boca Raton), 289. Chapman & Hall/CRC, Boca Raton, FL (2007)

[51] Johnson, N.L., Marino, G., Polverino, O., Trombetti, R.: Semifields of order $q^6$ with left nucleus $F_{q^3}$ and center $F_q$. Finite Fields Appl. 14(2), 456–469 (2008)

[52] Johnson, N.L., Marino, G., Polverino, O., Trombetti, R.: On a generalization of cyclic semifields. J. Algebr Comb. 29, 29–34 (2009)

[53] Johnson, N.L., Marino, G., Polverino, O., Trombetti, R.: On the Huang–Johnson semifields. Preprint

[54] Lavrauw, M.: Finite semifields with a large nucleus and higher secant varieties to Segre varieties. Adv. Geom. 11, 399–410 (2011)
[55] Lavrauw, M., Marino, G., Polverino, O., Trombetti, R.: $F_{q^p}$-pseudoreguli of $PG(3,q^3)$ and scattered semifields of order $q^6$. Finite Fields Appl. 17, 225–239 (2011)

[56] Lavrauw, M., Polverino, O.: Finite semifields. In: Current Research Topics in Galois Geometry, Nova Collected Works (2011)

[57] Lidl, R., Niederreiter, H.: Finite fields. In: Encyclopedia of Mathematics and its Applications, vol. 20, 2nd edn. Cambridge University Press, Cambridge (1997)

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

[59] Longobardi, G., Marino, G., Trombetti, R., Zhou, Y.: A large family of maximum scattered linear sets of $PG(1,q^n)$ and their associated MRD-codes. Submitted

[60] Longobardi, G., Zanella, C.: Linear sets and MRD-codes arising from a class of scattered linearized polynomials. J. Algebraic Comb. 53, 639–661 (2021)

[61] Longobardi, G., Zanella, C.: Partially scattered linearized polynomials and rank metric codes. Submitted

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

[63] Lunardon, G.: Linear $k$-blocking sets. Combinatorica 21, 571–581 (2001)

[64] Lunardon, G.: Translation ovoids. J. Geom. 76, 200–215 (2003)

[65] Lunardon, G.: Symplectic spreads and finite semifields. Des. Codes Cryptogr. 44, 39–48 (2007)

[66] Lunardon, G.: Projective planes of Lenz–Barlotti class $V$. J. Geom. 101, 157–172 (2011)

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

[68] Lunardon, G., Marino, G., Polverino, O., Trombetti, R.: Translation dual of a semifield. J. Combin. Theory Ser. A 115, 1321–1332 (2008)

[69] Lunardon, G., Marino, G., Polverino, O., Trombetti, R.: Symplectic semifield spreads and Veronesean surfaces. Ric. Mat. 60, 125–142 (2011)

[70] Lunardon, G., Marino, G., Polverino, O., Trombetti, R.: A remark on symplectic semifield planes and $\mathbb{Z}_4$-linear codes. Des. Codes Cryptogr. 69, 143–149 (2013)

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

[72] Lunardon, G., Polverino, O.: Blocking sets of size $q^t + q^{t-1} + 1$. J. Combin Theory. Ser. A 90, 148–158 (2000)

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

[74] Lunardon, G., Trombetti, R., Zhou, Y.: Generalized twisted Gabidulin codes. J. Combin. Theory Ser. A 159, 79–106 (2018)

[75] Lunardon, G., Trombetti, R., Zhou, Y.: On kernels and nuclei of rank metric codes. J. Algebr. Combin. 46, 313–340 (2017)

[76] Maduram, D.M.: Transposed translation plane. Proc. Am. Math. Soc. 53, 265–270 (1975)

[77] Lüneburg, H.: Die Suzukigruppen und ihre Geometrien. In: Lectures Notes in Mathematics. Springer (1965)

[78] Lüneburg, H.: Translation Planes. Springer, Berlin (1980)

[79] Marino, G., Polverino, O.: On the nuclei of a finite semifield. Contemp. Math.
[80] Marino, G., Polverino, O.: *On isotopisms and strong isotopisms of commutative presemifields.* J. Algebraic Combin. **36**, 247–261 (2012)

[81] Marino, G., Polverino, O., Trombetti, R.: *On $\mathbb{F}_q$-linear sets of $PG(3,q^3)$ and semifields.* J. Combin. Theory Ser. A **114**, 769–788 (2007)

[82] Otal, K., Ozbudak, F.: *Additive rank metric codes.* IEEE Trans. Inf. Theory **63**, 164–168 (2016)

[83] Polito, P., Polverino, O.: *On small blocking sets.* Combinatorica **18**, 133–137 (1998)

[84] Polverino, O., Zullo, F.: *Connections between scattered linear sets and MRD-codes.* Bull. Inst. Combin. Appl. **89**, 46–74 (2020)

[85] Payne, S.E.: *A new infinite family of generalized quadrangles.* Congr. Numer. **49**, 115–128 (1985)

[86] Payne, S.E.: *An essay on skew translation generalized quadrangles.* Geom. Dedicata. **32**, 93–118 (1989)

[87] Payne, S.E., Thas, J.A.: *Finite Generalized Quadrangles.* Pitman, Trowbridge (1984)

[88] Penttila, T., Williams, B.: *Ovoids of parabolic spaces.* Geom. Dedicata. **82**, 1–19 (2000)

[89] Segre, B.: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane.* Ann. Mat. Pura Appl. **64**, 1–76 (1964)

[90] Sheekey, J.: *A new family of maximum rank distance codes.* Adv. Math. Commun. **10**, 475–488 (2016)

[91] Sheekey, J., Van de Voorde, G.: *Rank-metric codes, linear sets, and their duality.* Des. Codes Cryptogr. **88**, 655–675 (2020)

[92] Sperner, E.: *Affine Räume mit Schwacher Inzidenz und zugehörige algebraische Strukturen.* J. Reine Angew. Math. **24**, 205–215 (1960)

[93] Thas, J.A.: *Generalized quadrangles and flocks of cones.* Eur. J. Comb. **8**, 293–312 (1987)

[94] Thas, J.A.: *Generalized quadrangles of order $(s,s^2)$.* J. Combin. Theory Ser. A **67**, 140–160 (1994)

[95] Thas, J.A.: *Generalized quadrangles of order $(s,s^2)$, II.* J. Combin. Theory Ser. A **79**, 223–254 (1997)

[96] Thas, J.A., Payne, S.E.: *Spreads and ovoids in finite generalized quadrangles.* Geom. Dedicata. **52**, 227–253 (1994)

[97] Tit, J.: *Les groupes simples de Suzuki et de Ree.* Seminaire Bourbaki 210

[98] Tit, J.: *Ovoïdes et groupes de Suzuki.* Arch. Math. **13**, 187–198 (1962)

[99] Trombetti, R., Zhou, Y.: *A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$.* IEEE Trans. Inf. Theory **65**, 1054–1062 (2019)
Received: July 20, 2021.
Revised: April 6, 2022.
Accepted: April 13, 2022.