Des. Codes Cryptogr. (2007) 44:39–48
DOI 10.1007/s10623-007-9054-9

Simplectic spreads and finite semifields

Guglielmo Lunardon

Received: 17 November 2006 / Revised: 17 November 2006 /
Accepted: 26 February 2007 / Published online: 8 May 2007

Abstract It is well known that associated with a translation plane π there is a family of equivalent spreads. In this paper, we prove that if one of these spreads is symplectic and π is finite, then all the associated spreads are symplectic. Also, using the geometric intepretation of the Knuth's cubical array, we prove that a symplectic semifield spread of dimension n over its left nucleus is associated via a Knuth operation to a commutative semifield of dimension n over its middle nucleus.

Keywords Symplectic spreads · Finite semifields · Nuclei

AMS Classifications 51A40 · 17A35

1 Introduction

Many new interesting results on symplectic spreads of $PG(2n-1, q)$ have been recently found. In [13], an internal criterion for a translation plane to be symplectic has been proved when q is even. New examples of symplectic spreads have been constructed in [3,8]. The geometric interpretation of Knuth's cubical array explained [2] and in [7] produces a bijection between planes associated with a symplectic spread and planes coordinatized by a commutative semifield. Using such a bijection, a new family of commutative semifields of even order has been constructed in [7].

Nevertheless some questions about symplectic spreads seem not to have been studied.

The first one is the following.

G. Lunardon (✉)
Dipartimento di Matematica e Applicazioni,
Complesso di Monte S. Angelo — Edificio T,
Via Cintia, I-80126 Napoli, Italy
e-mail: lunardon@unina.it

Associated with a translation plane π there is a family of equivalent spreads. If $\mathcal{S}$ is symplectic, is any spread equivalent to $\mathcal{S}$ still symplectic? The question arises in a natural way for deciding how many spreads of a hyperbolic quadric $Q^+(4t-1,2^e)$ have a slice isomorphic to a symplectic spread equivalent to $\mathcal{S}$, and seems not to have been studied. The characterization of the translation planes of even order associated with symplectic spreads given in [13] suggested to the author that the property of a spread to be symplectic should be invariant under equivalence of spreads. In this paper we give a positive answer to the above question proving that all spreads equivalent to a symplectic one are symplectic.

A second question concerns the nuclei of the semifields produced by a cubical array. We know that the collineation groups of the six semifield planes obtained in such a way have the same order. As any nucleus of a semifield defines a particular group of homologies, it is natural asking if the six semifield planes have groups of homologies of the same order and this question too seems not to have been studied. Using the geometric interpretation of the cubical array given in [2,7] we prove that the orders of the nuclei are permuted with given rules. Applying these rules, we are able to prove that a symplectic semifield of dimension n over its left nucleus defines a commutative semifield of the same dimension over its middle nucleus.

2 Preliminary results

We refer to [4] for the standard background concerning translation planes and their kernels and duals, as well as quasi-fields, semifields, and isotopisms.

A *spread* of $PG(2n-1,q)$ is a partition $\mathcal{S}$ of the pointset of $PG(2n-1,q)$ into $(n-1)$-dimensional subspaces. We denote by $A(\mathcal{S})$ the translation plane of order q^n associated with $\mathcal{S}$.

Let $\pi=(P,L)$ be a finite translation plane and let O be a fixed point of π. Let T be the translation group of π. For each line l of π incident with O, denote by T_l the stabilizer of l in T and denote by $\mathbb{P}$ the family of all the subgroups T_l of T. By the theory of affine planes, we know that T is elementary abelian, T_l is transitive on the points of the line l, and $T=T_l+T_m$ whenever l and m are different lines of π incident with the point O. The *kernel* K of π is the set of all the endomorphisms α of T such that $T_l^\alpha \subset T_l$ for all $T_l \in \mathbb{P}$. It has been proved by André [1] that K is a field. Hence T is a vector space over K and each element of $\mathbb{P}$ is a vector subspace of T. If $F \simeq GF(q)$ is a subfield of K, then T has rank $2n$ over F and all the elements of $\mathbb{P}$ have rank n. Denote by $PG(T,F)=PG(2n-1,q)$ the $(2n-1)$-dimensional projective space associated with T as an F-vector space and by $S(\mathbb{P},F)$ the partition of $PG(2n-1,q)$ into $(n-1)$-dimensional subspaces defined by $\mathbb{P}:\ S(\mathbb{P},F)$ is a spread of $PG(2n-1,q)$.

The relationship between translation planes and the planes constructed from $(n-1)$-spreads has been given by André [1]: *for each subfield $F=GF(q)$ of K, the planes π, and $A(S(\mathbb{P},F))$ are isomorphic.*

If $\mathcal{S}$ is a spread of $PG(2n-1,q)$, the kernel of the translation plane $A(\mathcal{S})$ contains a subfield F isomorphic to $GF(q)$ and the spreads $\mathcal{S}$ and $S(\mathbb{P},F)$ are isomorphic (i.e., there is a collineation τ of $PG(2n-1,q)$ such that $\mathcal{S}^\tau=S(\mathbb{P},F)$ see, e.g. [11] Chapt. 1).

The spread $\mathcal{S}_1$ of $PG(2n-1,q)$ and the spread $\mathcal{S}_2$ of $PG(2m-1,s)$ are *equivalent* if the planes $A(\mathcal{S}_1)$ and $A(\mathcal{S}_2)$ are isomorphic. We note that, when $n=m$, two spreads are equivalent if and only if they are isomorphic, i.e., there is a collineation which maps one spread into the other one.

We say that the spread $\mathcal{S}$ is *symplectic* if there is a symplectic polarity $\perp$ of $PG(2n-1,q)$ such that all subspaces of $\mathcal{S}$ are totally isotropic with respect to $\perp$.

Let Q be a quasi-field of dimension n over a subfield $F = GF(q)$ of its kernel. Then $V = Q \times Q$ is a $2n$-dimensional vector space over F and $\Sigma = PG(V,F) = PG(2n-1,q)$. Define

$$\begin{aligned} F(\infty) &= \{(0,b) \mid b \in Q\}, \\ F(b) &= \{(a,ab) \mid a \in Q\}, \\ \mathcal{S}(Q,F) &= \{F(b) \mid b \in Q\} \cup \{F(\infty)\} \end{aligned}$$

then $\mathcal{S}(Q,F)$ is a spread of $PG(2n-1,q)$.

For any spread $\mathcal{S}$ of $PG(2n-1,q)$, there is a quasi-field Q, whose kernel contains a subfield F of order q such that $\mathcal{S}$ is isomorphic to $\mathcal{S}(Q,F)$ (see, e.g. [4] Sect. 5.1).

For each element b of Q, let L_b be the $GF(q)$-linear map from Q to itself defined by $x \mapsto xb$. The set $\mathbb{L} = \mathbb{L}(Q) = \{L_b \mid b \in Q\}$ has the following properties:

(1) $|\mathbb{L}| = q^n$,
(2) the zero map $0 = L_0$ and the identity $I = L_1$ belong to $\mathbb{L}$,
(3) if L_b and L_c are different elements of $\mathbb{L}$, then $L_b - L_c$ is non-singular.

Then each element of $\mathbb{L}$ different from 0 is non-singular,

A set $\mathbb{C}$ of F-linear maps of Q satisfying Properties (1)–(3) is called a *spread set* and $\mathbb{L}$ is the spread set associated with Q. We note that Q is a semifield if and only if $\mathbb{L}$ is closed under the sum. The quasi-field Q is a field if and only if $\mathbb{L}$ is closed under the sum and under the multiplication (for more details, see [4] Sect. 5.1).

The spread $\mathcal{S}(Q,F)$ is a *semifield spread* with respect to $F(\infty)$ if and only if $\mathbb{L}$ is closed under the sum, i.e., Q is a semifield. The spread $\mathcal{S}$ is desarguesian if and only if $\mathbb{L}$ is closed under the sum and under the multiplication (for more details, see [4] Sect. 5.1).

Let S be a semifield. The subsets

$$\begin{aligned} N_l &= \{a \in Q \mid (ab)c = a(bc), \forall b,c \in Q\}, \\ N_m &= \{b \in Q \mid (ab)c = a(bc), \forall a,c \in Q\}, \\ N_r &= \{c \in Q \mid (ab)c = a(bc), \forall a,b \in Q\}, \\ Z &= \{a \in N_l \cap N_m \cap N_r \mid ab = ba, \forall b \in Q\} \end{aligned}$$

are known, respectively, as the *left nucleus*, *middle nucleus*, *right nucleus* and *center* of the semifield S. The nuclei are skewfields, and it is straightforward to prove that S is a vector space both over each of its nuclei and over its center. A nucleus N is *central* if $ab = ba$ for all $a \in N$ and $b \in S$.

Let $\mathbb{C}$ be a spread set of a vector space Q over $GF(q)$. If e is a fixed non-zero vector of Q, then for each vector b of Q there is a unique element $C(b)$ of $\mathbb{C}$ such that $eC(b) = b$. If we define a multiplication on Q by $ab = aC(b)$, then $Q = Q(+,\cdot)$ is a quasifield with identity e and $F = \{\lambda e \mid \lambda \in GF(q)\}$ is a subfield of order q of the kernel of Q.

Suppose that $\mathbb{C}$ is closed under the sum. Then Q is a semifield whose left nucleus contains $GF(q)$. An element b of Q belongs to N_m if and only if $C(b)C(c) = C(bc)$ for all c in Q. Hence $\mathbb{N}_m = \{C(b) \mid b \in N_m\}$ is a field of linear maps and $\mathbb{C}$ is a left vector space over $\mathbb{N}_m$. An element c of Q belongs to N_r if and only if $C(b)C(c) = C(bc)$ for all b in Q. Hence $\mathbb{N}_r = \{C(c) \mid c \in N_r\}$ is a field of linear maps and $\mathbb{C}$ is a right vector

space over $\mathbb{N}_r$. If $N_l = GF(q)$, then the center of Q is the biggest subfield $Z = GF(s)$ of $N_l = GF(q)$ such that $\lambda X \in \mathbb{C}$ for all $\lambda \in Z$ and $X \in \mathbb{C}$.

Next we recall Knuth's cubical array (see [9] or [4]).

A *pre-semifield* $S(+,\cdot)$ is a semifield if there is an identity element.

Let e be an element of S different from 0. Define a new multiplication $\circ$ on S by $ae \circ eb = ab$. Then $S(+,\circ)$ is a semifield whose identity is ee, whose coordinatized projective plane is isomorphic to that coordinatized by $S(+,\cdot)$ (see [4] Sect. 5.3).

The kernel K of the pre-semifield S is

$$K = \{\lambda \in S \mid (\lambda b)c = \lambda(bc), \forall b, c \in S\}.$$

It is easy to prove that K is a field and S is a left vector space over K. Note that when S is a semifield, then K is its left nucleus. Let $GF(s)$ be the maximum subfield of K such that the maps $a \mapsto ba$ of S into itself are $GF(s)$-linear, i.e., $b(\lambda a) = \lambda(ba)$ for all $a, b \in S$ and for all $\lambda \in GF(s)$. Note that, when S is a semifield, then $GF(s)$ is its center. Suppose that S has dimension t over $GF(s)$. Let $\{e_1 = 1, e_2, \ldots, e_t\}$ be a basis of S over $GF(s)$, and define $a_{ijk} \in GF(s)$ by

$$e_i e_j = \sum_{k=1}^{t} a_{ijk} e_k, \quad i, j = 1, 2, \ldots, t.$$

It follows that the *cubical array* A of the t^3 elements $a_{ijk} \in GF(s)$ uniquely determines the multiplication in S because:

$$(*) \quad \left(\sum_{i=1}^{t} x_i e_i\right)\left(\sum_{j=1}^{t} y_j e_j\right) = \sum_{i,j,k=1}^{t} x_i y_j a_{ijk} e_k.$$

As S is a semifield, $A = (a_{ijk})$ is *non-singular* in the sense that

if $C_i = (c_{jk})$ $i = 1, 2, \ldots, t$, is the matrix defined by $c_{jk} = a_{ijk}$ with $j, k = 1, 2, \ldots, t$, then the matrix $\sum_{i=1}^{t} y_i C_i$ with $y_1, y_2, \ldots, y_t \in GF(s)$ is singular if and only if $(y_1, y_2, \ldots, y_t) = 0$, i.e., *$\mathbb{C} = \{\sum_{i=1}^{t} y_i C_i \mid y_1, y_2, \ldots, y_t \in GF(s)\}$ is a spread set.*

The converse is also true

Result 1 ([9] Theorem 4.4.1)) *Let $A = (a_{ijk}), i, j, k = 1, 2, \ldots, t$ be a cubical array of elements $a_{ijk} \in GF(s)$, and define a multiplication in the vector space $S = GF(s)^t$ by* $(*)$. *This turns S into a presemifield if and only if A is non-singular.*

3 Equivalent spreads

Let $\Sigma = PG(V, GF(q)) = PG(n-1, q)$ and let $\Sigma^* = PG(V^*, GF(q^t)) = PG(n-1, q^t)$. We say that Σ is a *canonical subgeometry* of Σ^* when $V^* = GF(q^t) \otimes V$.

Let Σ be a canonical subgeometry of Σ^*. For each subspace S^* of Σ^*, the set $S = S^* \cap \Sigma$ is a subspace of Σ whose rank is at most equal to the rank of S^*. We say that a subspace S^* of Σ^* is a *subspace* of Σ whenever S and S^* have the same rank. If σ is a semilinear collineation of Σ^* of order t having as fixed points exactly the points of Σ, then S^* is a subspace of Σ if and only if S^* is fixed by σ (see, e.g. [10])

The notion of spread is generalized in the following way. An $(n-1)$-*spread* $\mathcal{F}$ of a projective space $PG(rn-1, q)$ is a family of mutually disjoint $(n-1)$-subspaces

such that each point of $PG(rn-1,q)$ belongs to an element of $\mathcal{F}$. We note that for $r=2$, $(n-1)$-spreads of $PG(2n-1,q)$ are spreads of $PG(2n-1,q)$.

Let $r>2$. An $(n-1)$-spread $\mathcal{F}$ is *normal* if it induces a spread in any subspace generated by two of its elements (i.e., if $A,B\in\mathcal{F}$, then an element of $\mathcal{F}$ either is disjoint from $T=\langle A,B\rangle$ or is contained in T). Such a spread is called *geometric* in Ref. [14].

Let $\Sigma=PG(mt-1,q)$ be a canonical subgeometry of $\Sigma^*=PG(mt-1,q^t)$, and let σ be a semilinear collineation of Σ^* of order t which fixes Σ pointwise. There is a subspace $\Gamma=PG(m-1,q^t)$ disjoint from Σ such that Σ^* is spanned by $\Gamma,\Gamma^\sigma,\ldots,\Gamma^{\sigma^{t-1}}$ and, for each point x of Γ, $L(x)=\langle x^{\sigma^i}\mid i=0,1,2,\ldots,t-1\rangle\cap\Sigma$ is the unique subspace of Σ of rank t who spans a$(t-1)$-dimensional subspace of Σ^* containing x. Then it is easy to prove that $\mathcal{F}=\{L(x)\mid x\in\Gamma\}$ is a $(t-1)$-spread of $PG(mt-1,q)$ (see, e.g. [10]). If r is a line of Γ, then $\mathcal{F}_r=\{L(x)\mid x\in r\}$ is a spread of the subspace $L_r=\langle r,r^\sigma,\ldots,r^{\sigma^{t-1}}\rangle\cap\Sigma$ of dimension $2t-1$ (see, e.g. [10]). The $(t-1)$-spread $\mathcal{F}$ has the following property: if a $(2t-1)$-dimensional subspace T of $PG(mt-1,q)$ contains two elements of $\mathcal{F}$, then there is a line r of Γ such that $T=L_r$. Therefore, when $m>2$, $\mathcal{F}$ is a normal spread of Σ, and by [14] all normal spreads of Σ can be constructed in this way.

Let $K=GF(q^t)$ be the kernel of a given translation plane π. If $F=GF(q)$, is the subfield of K of order q, then $\mathcal{S}=S(\mathbb{P},K)$ is a spread of $PG(2n-1,q^t)$ equivalent to the spread $\mathcal{S}'=S(\mathbb{P},F)$ of $PG(2nt-1,q)$. Identify Γ with $PG(2n-1,q^t)$. Let $\Sigma=PG(2nt-1,q)$ be the canonical subgeometry of $\Sigma^*=PG(2nt-1,q^t)$ and let $\mathcal{F}$ be the normal $(t-1)$-spread of $PG(2nt-1,q)$ defined above by Γ.

Let $\mathcal{S}$ be an $(n-1)$-spread of Γ. For each $(n-1)$-dimensional subspace Ω of Γ, the subspace $L_\Omega=\langle\Omega,\Omega^\sigma,\ldots,\Omega^{\sigma^{t-1}}\rangle$ is a $(tn-1)$-dimensional subspace of Σ. Then $L_\mathcal{S}=\{L_\Omega\mid\Omega\in\mathcal{S}\}$ is a $(nt-1)$-spread of $\Sigma=PG(2nt-1,q)$, which is equivalent to $\mathcal{S}$ and all spreads equivalent to $\mathcal{S}$ can be constructed in this way (see [12]).

We conclude this section with a property of spreads.

Lemma 1 *Let $\Sigma=PG(2t-1,q)$, $\Sigma^*=PG(2t-1,q^t)$, and let $\mathcal{F}$ be the $(t-1)$-spread of $\Sigma=PG(2t-1,q)$ defined by $\Gamma\simeq PG(1,q^t)$. Let $\perp$ be a symplectic polarity of $\Sigma=PG(2t-1,q)$ such that $\mathcal{F}$ is a symplectic spread with respect to $\perp$. If $\perp^*$ is the unique symplectic polarity of $\Sigma^*=PG(2t-1,q^t)$ defined by $\perp$, then Γ is non-singular with respect to $\perp^*$.*

Proof We notice that the spread $\mathcal{F}$ arises from the groups embedding $PS_{P_2}(q^t)<PS_{P_{2t}}(q)$ and since the form fixed by $PS_{P_2}(q^t)$ is non-degenerate, Γ must be non-isotropic. □

4 Symplectic spreads

With the notation of Sect. 2, denote by **b** the non-singular alternating bilinear form associated with $\perp$. If $\mathcal{S}=S(\mathbb{P},F)$ is symplectic, then for each subfield $GF(s)$ of $F=GF(q)$, the alternating bilinear form $<x,y>=tr_{GF(s)}\mathbf{b}(x,y)$ defines a symplectic polarity ω of $PG(T,GF(s))$ and $S(\mathbb{P},GF(s))$ is symplectic with respect to ω (see [6]).

Conversely if $F\subset K$, where K is the kernel of π, and $S(\mathbb{P},F)$ is symplectic, is $S(\mathbb{P},K)$ still symplectic? We give a positive answer to this question proving the following:

Theorem 1 *All spreads equivalent to a symplectic spread are symplectic.*

Proof Let $\mathcal{S}'$ be a symplectic $(nt-1)$-spread of $\Sigma = PG(2nt-1,q)$ with respect to the polarity $\perp$.

Suppose that the kernel K of $A(\mathcal{S}')$ has order q^t. Let $\mathcal{S} = S(\mathbb{P},K)$ be the $(n-1)$-spread of $\Gamma = PG(2n-1,q^t)$ associated with the plane $A(\mathcal{S}')$. Hence $\mathcal{S}$ and $\mathcal{S}'$ are equivalent spreads. By the abovementioned construction of equivalent spreads, we can suppose that there is a normal $(t-1)$-spread $\mathcal{F}$ of $\Sigma = PG(2nt-1,q)$, defined by the subspace Γ of $\Sigma^* = PG(2nt-1,q^t)$, such that $\mathcal{S} = S(\mathbb{P},K)$ is a spread of $\Gamma = PG(2n-1,q^t)$, $\mathcal{S}' = L_{\mathcal{S}}$, and $\mathcal{F}$ induces a $(t-1)$-spread on each element of $\mathcal{S}'$.

To prove Theorem 1 it is enough to show that if $L_{\mathcal{S}}$ is symplectic with respect to some symplectic polarity $\perp$, then $\mathcal{S} = S(\mathbb{P},K)$ is symplectic.

Denote by $\perp^*$ the unique polarity of Σ^* defined by $\perp$. We note that the elements of $L_{\mathcal{S}}$ are maximal totally isotropic subspaces with respect to the polarity $\perp^*$. Hence each subspace Ω of $\mathcal{S}$ is totally singular with respect to $\perp^*$ because $\Omega = L_\Omega \cap \Gamma$ is a subspace of L_Ω.

We are proving Theorem 1 in four steps.

Step 1 Γ is either totally isotropic or non-singular.

Proof Let R be the radical of Γ and let U be a subspace disjoint from R such that $\Gamma = \langle R, U\rangle$. As U is non-singular and Γ has odd dimension, R has dimension $2h-1$ with $0 \le h \le n$ and the maximal totally isotropic subspaces of Γ have dimension $n+h-1$.

Suppose that an element Ω of $\mathcal{S}$ contains R and let Δ be an element of $\mathcal{S}$ different from Ω. Since Δ is contained in some maximal totally isotropic subspace L_Δ, the subspace Δ is totally isotropic and $\langle R,\Delta\rangle$ is a totally isotropic $(n+2h-1)$-dimensional subspace of Γ. Then $n+2h-1 \le n+h-1$, hence $h=0$, i.e., Γ is non-singular.

If Γ is singular, then no element of $\mathcal{S}$ contains R, i.e., for each element Ω of $\mathcal{S}$ the subspace $\langle R,\Omega\rangle$ has dimension at most $n+h-1$ because it is totally isotropic. This implies that $\Omega\cap R$ has dimension at least $h-1$. Hence $\mathcal{S}$ induces on R a partition into subspaces of dimension at least $h-1$. As $\mathcal{S}$ contains $q^{tn}+1$ elements, we have

$$\frac{(q^t)^{2h}-1}{q^t-1} = |R| \ge (q^{tn}+1)\frac{q^{ht}-1}{q^t-1},$$

i.e. $(q^{th}+1) \ge (q^{tn}+1)$. Since $0 \le h \le n$, we have $n=h$ and $R=\Gamma$. □

Step 2 If m is a totally isotropic line of Γ, then $L_m = \langle m, m^\sigma, \ldots, m^{\sigma^{t-1}}\rangle$ is totally isotropic.

Proof As $\mathcal{F}_m$ is a spread of $L_m \cap \Sigma$, if L_m is non-singular, the polarity $\perp^*$ induces a symplectic polarity on L_m and $\mathcal{F}_m$ is symplectic with respect to the induced polarity. By Lemma 1, m is a non-singular line.

Since m is totally isotropic by hypothesis, L_m is an isotropic subspace of Σ.

Let $R_m \neq \emptyset$ be the radical of L_m. Arguing as in Step 1, we conclude that L_m is totally isotropic. □

Step 3 Γ is non-singular.

Proof By way of contradiction, suppose that Γ is totally isotropic. Then all the lines of Γ are totally isotropic. Let U be a subspace of Γ of dimension $m-1 > n-1$. The subspace $L_U = \langle U, U^\sigma, \ldots, U^{\sigma^{t-1}}\rangle$ is a $(mt-1)$-dimensional subspace of Σ and

$\mathcal{F}_U = \{L(x) \mid x \in U\}$ is a spread of L_U. We note that all the elements of $\mathcal{F}_U$ are totally isotropic.

If y and z are elements of Σ incident with L_U, let Ω (respectively Δ) be the element of $\mathcal{F}_U$ incident with y (respectively z). If $\Omega \neq \Delta$, then $\langle \Omega, \Delta \rangle = L_m$ where m is a line of Γ. As Γ is totally isotropic, both m and L_m are totally isotropic. Hence $z \in y^\perp$ for all points y and z of L_U, i.e., L_U is a totally isotropic subspace of dimension $mt - 1 > nt - 1$. But this is impossible because $\perp$ is a polarity of Σ. □

Step 4 If θ is the symplectic polarity of Γ induced by $\perp$, then $\mathcal{S}$ is symplectic with respect to θ.

Proof As Γ is non-singular, $\perp^*$ induces a symplectic polarity θ on Γ, defined by $U^\theta = U^{\perp^*} \cap \Gamma$ for all subspaces U of Γ. For each element Ω of $\mathcal{S}$, $\Omega^\theta = \Omega^{\perp^*} \cap \Gamma$ contains $L_\Omega \cap \Gamma = \Omega$ because $\Omega \subset L_\Omega = L_\Omega^{\perp^*} \subset \Omega^{\perp^*}$. As Ω and Ω^θ have the same dimension $n - 1$, we have $\Omega = \Omega^\theta$. Hence the elements of $\mathcal{S}$ are maximal totally isotropic subspaces with respect to θ. □

5 Transposed spreads

Let $\perp$ be a symplectic polarity of $PG(2n-1, q)$. If $\mathcal{S}$ is a spread of $PG(2n-1, q)$, define a new spread $\mathcal{S}^d = \{D^\perp \mid D \in \mathcal{S}\}$. By construction $(\mathcal{S}^d)^d = \mathcal{S}$.

If ω is any polarity of $PG(2n-1, q)$, then $\tau = \perp \omega$ is a collineation of $PG(2n-1, q)$ and $(D^\perp)^\tau = D^\omega$. Hence $\mathcal{S}^d$ does not depend, up to isomorphisms, from the choosen polarity and we call $\mathcal{S}^d$ the *transpose* of $\mathcal{S}$.

Theorem 2 *Spreads, which are trasposed of equivalent spreads, are equivalent.*

Proof Let $\Sigma = PG(2nt-1, q) = PG(V, GF(q))$, $\Sigma^* = PG(2nt-1, q^t) = PG(V^*, GF(q^t))$ with $V^* = V \otimes GF(q^t)$ and let $\mathcal{F}$ be the $(t-1)$-spread of Σ defined by $\Gamma \simeq PG(2n-1, q^t)$.

Denote by σ the collineation of Σ^* of order t fixing Σ pointwise defined by the semilinear map $v \otimes \alpha \mapsto v \otimes \alpha^q$. Let $\Gamma^{\sigma^{i-1}} = PG(W_i, GF(q^t))$, $i = 1, 2, \ldots, t$, where W_i is a $GF(q^t)$-vector subspace of V^* of dimension $2n$.

As in Sect. 4, each vector v of V^* can be written as $v = w_1 + w_2 + \cdots + w_t$ with $w_i \in W_i$, $(i = 1, 2, \ldots, t)$.

Denote by ω the sympletic polarity of Γ defined by a non-singular alternating bilinear form $\langle\,;\rangle$ of W_1. The alternating bilinear form $\langle\,;\rangle^*$ on V^* defined by

$$\langle v_1 + v_2^\sigma \cdots + v_t^{\sigma^{t-1}}; w_1 + w_2^\sigma + \cdots + w_t^{\sigma^{t-1}} \rangle^* = \sum_{i=1}^{t} \langle v_i; w_i \rangle$$

(where v_i, w_i are elements of W_i for all $i = 1, 2, \ldots, t$) is non-singular and defines a polarity ω^* of Σ^* which induces a symplectic polarity ω on Σ, because $\sigma\omega^* = \omega^*\sigma$.

By construction, all the elements of $\mathcal{F}$ are totally isotropic subspaces with respect to ω and Γ is non-singular with respect to ω^*. Moreover, for any subspace U of Γ, we have $(U^{\sigma^i})^{\omega^*} \cap \Gamma^{\sigma^i} = (U^\omega)^{\sigma^i}$.

Let $\mathcal{S}$ be a spread of $\Gamma = PG(2n-1, q)$ and let $L(\mathcal{S})$ be the linear representation of $\mathcal{S}$ in $\Sigma = PG(2nt-1, q)$.

If $\mathcal{S}'$ is a spread of Σ equivalent to $\mathcal{S}$, then $\mathcal{S}'$ is isomorphic to $L(\mathcal{S})$. As the transpose does not depend on the choosen polarity, for proving Theorem 2 it is enough to prove that $\mathcal{S}^d$ is equivalent to $L(\mathcal{S})^d$.

If Ω belongs to $\mathcal{S}$, then $L(\Omega) = \langle \Omega, \Omega^\sigma, \ldots, \Omega^{\sigma^{t-1}} \rangle$ belongs to $L(\mathcal{S})$ and

$$L(\Omega)^{\omega^*} = \Omega^{\omega^*} \cap (\Omega^\sigma)^{\omega^*} \cap \cdots \cap (\Omega^{\sigma^{t-1}})^{\omega^*} = \langle \Omega^\omega, (\Omega^\omega)^\sigma, \ldots, (\Omega^\omega)^{\sigma^{t-1}} \rangle.$$

Hence $L(\mathcal{S})^d = L(\mathcal{S}^d)$. □

Corollary 1 *The planes $A(\mathcal{S}^d)$ and $A(\mathcal{S})$ have isomorphic kernels.*

Proof By Theorem 2, we can suppose that the kernel of $A(\mathcal{S})$ is $GF(q)$ and $\mathcal{S}$ is a spread of $PG(2n-1, q)$. By construction, $GF(q)$ is a subfield of the kernel K of $A(\mathcal{S}^d)$.

If $GF(q) \neq K = GF(q^r)$, then $n = rt$ and there is a spread $\mathcal{S}_1$ of $PG(2t-1, q^r)$ equivalent to $\mathcal{S}^d$. By Theorem 2, $\mathcal{S}_1^d$ is a spread of $PG(2t-1, q^r)$ equivalent to $\mathcal{S}$. Hence the kernel of $A(\mathcal{S})$ has order at least $q^r > q$. As this is impossible, we have proved the corollary. □

Let $\mathcal{S} = \mathcal{S}(Q, K)$ where K is the kernel of Q. If $\langle\,;\rangle$ is a non-singular symmetric bilinear form of Q as a (left) vector space over K, then $V = Q \times Q$ is a left vector space over K and the non-singular alternating form

$$((x, y); (u, v)) = \langle x, v\rangle - \langle y, u\rangle$$

defines a symplectic polarity $\perp$ of $\Sigma = PG(V, K) = PG(2n-1, q)$. By construction $F(\infty) = \{(0, y) \mid y \in Q\}$ and $F(0) = \{(x, 0) \mid x \in Q\}$ are totally isotropic subspaces with respect to $\perp$.

If L is a K-linear map from Q into itself, the adjoint of L with respect to $\langle\,;\rangle$ is the K-linear map L^T defined by $\langle x, yL\rangle = \langle xL^T, y\rangle$ for all x and y in Q.

We recall that, for each element b of Q, L_b is the $GF(q)$-linear map of Q into itself defined by $x \mapsto xb$, and $\mathbb{L} = \mathbb{L}(Q) = \{L_b \mid b \in Q\}$ is the spread set associated with Q. Also $\mathbb{L}^d = \{L_b^T \mid b \in Q\}$ is a spread set. The *transpose* Q^d of Q is the quasi-field of unity 1 defined by the spread set $\mathbb{L}^d$.

If $\mathcal{S} = \mathcal{S}(Q, K)$, then $\mathcal{S}^d = \mathcal{S}(Q^d, K)$.

We note $\mathbb{L}$ is closed under the sum if and only if $\mathbb{L}^d$ is closed under the sum. Hence Q is a semifield if and only if Q^d is. When there is a non-singular symetric bilinear form $\langle\,;\rangle$ with respect to which $L_a = L_a^T$ for any element a of Q, the quasi-field Q is called *symplectic*. We note that Q is symplectic if and only if $\mathcal{S}$ is symplectic with respect to the symplectic polarity $\perp$.

Theorem 3 *If S is a symplectic semifield, then $N_m = N_r = Z$.*

Proof If S is symplectic, then for any element $L_b \in \mathbb{L}$ we have $L_b^T = L_b$ with respect to a given symmetric bilinear form $<\ ;\ >$.

An element b of S belongs to N_m if and only if $L_b L_c = L_{bc}$ for all c in S (i.e., $\mathbb{N}_m = \{L_b \mid b \in N_m\}$ is a field of linear maps and $\mathbb{L}$ is a left vector space over $\mathbb{N}_m$), and an element d of S belongs to N_r if and only if $L_c L_d = L_{cd}$ for all $c \in S$. Hence, for any element L_b of $\mathbb{N}_m$ we have

$$L_c L_b = (L_b L_c)^T = L_{bc}^T = L_{bc} = L_b L_c$$

for all $c \in S$. Hence $\mathbb{L}$ is a right vector space over $\mathbb{N}_m$, i.e., N_m is a subfield of N_r.

In the same way we can prove that N_r is a subfield of N_m. Thus $N_m = N_r$.

As $L_b L_c = L_c L_b$, we have

$$bc = cb$$

for all $b \in N_r$ and $c \in S$. Then N_r is central in S.

As $N_r = N_m$, for any ξ in N_r and all $x, y \in S$ we have

$$\xi(xy) = (xy)\xi = x(y\xi) = x(\xi y) = (x\xi)y = (\xi x)y.$$

Thus $N_r = N_m$ is a subfield of N_l, i.e., $Z = N_m = N_r$. □

6 Nuclei of finite semifields

Let $S = S(+, \cdot)$ be a semifield and denote by N_l, N_m, and N_r the nuclei of S as in Sect. 2.

Recall that the map $L_a : x \mapsto xa$ is a N_l-linear map of S as a left vector space over N_l and $\mathbb{L} = \{L_a \mid a \in S\}$ is a spread set. Similarly, if $R_a : x \mapsto ax$, then R_a is a N_r-linear map of S as a right vector space over N_r, and $\mathbb{R} = \{L_a \mid a \in S\}$ is a spread set.

The *dual* of S is the semifield $S^* = S(+, \star)$ defined by

$$x \star y = yx.$$

By construction $(S^*)^* = S$.

Theorem 4 *If N_l^*, N_m^*, N_r^*, Z^* are the left, the middle, the right nucleus, and the center, respectively, of the semifield S^*, then $N_l^* = N_r$, $N_m^* = N_m$, $N_r^* = N_l$, and $Z^* = Z$.*

Proof It follows directly from the definition of S^*. □

Theorem 5 *If N_l^d, N_m^d, N_r^d are the left, the middle, and the right nucleus, respectively, of S^d, then $N_l^d = N_l$, $N_m^d \simeq N_r$, and $N_r^d \simeq N_m$.*

Proof An element b of S belongs to N_m if and only if $L_b L_c = L_{bc}$ for all c in S. Hence $\mathbb{N}_m = \{L_b \mid b \in N_m\}$ is a field of linear maps and $\mathbb{L}$ is a left vector space over $\mathbb{N}_m$.

An element c of S belongs to N_r if and only if $L_b L_c = L_{bc}$ for all b in S. Hence $\mathbb{N}_r = \{L_c \mid c \in N_r\}$ is a field of linear maps and $\mathbb{L}$ is a right vector space over $\mathbb{N}_r$. As $(L_b L_c)^T = L_c^T L_b^T$, then $\mathbb{L}^d$ is a left vector space over $\mathbb{N}_m^d = \{L_c^T \mid c \in N_r\}$ and a right vector space over $\mathbb{N}_r^d = \{L_b^T \mid b \in N_m\}$. □

We note that if S has dimension 2 over $N_m = N_r = GF(q)$, then S^* has dimension 2 over $N_l^* = N_m^* = GF(q)$ and S^{*d} has dimension 2 over $N_l^{*d} = N_r^{*d} = GF(q)$.

In [7, Sect. 3], it has been proved that the six projective planes obtained from the Knuth's cubical array are coordinatized by the six semifields S, S^*, S^{*d}, S^{*d*}, S^{*d*d}, S^{*d*d*}, where S^{*d*d*d} and S are isotopic.

Theorem 6 *Let S be a semifield of dimension n over its left nucleus N_l. Then, S is symplectic if and only if S^{*d} is isotopic to a commutative semifield of dimension n over its middle nucleus.*

Proof By Proposition 3.8 of [7], S is symplectic if and only if S^{*d} is isotopic to a commutative semifield.

By Theorems 4 and 5, S has dimension n over its left nucleus if and only if S^{*d} has dimension n over its middle nucleus. □

We conclude with a remark on the Kantor commutative semifield constructed in Ref. [7].

Assume that we are given fields $F = F_0 \supset F_1 \supset \cdots \supset F_n = GF(q)$ of characteristic 2 with $[F : F_n]$ odd and corresponding trace maps $T_i : F \mapsto F_i$. Choose any elements $\xi_i \in F^*$, $1 \leq i \leq n$. Define $\mathbf{B} = F(+, \star)$ by

$$x \star y = xy + (x \sum_{i=1}^{n} T_i(\xi_i y) + y \sum_{i=1}^{n} T_i(\xi_i x))^2.$$

If $|F| > 8$, then $\mathbf{B}$ is a commutative semifield whose left nucleus is $GF(2)$ (see Sect. 4 of [7]).

The points of the affine plane $\mathcal{A}$ associated with $\mathbf{B}$ are the elements of F^2. The lines of $\mathcal{A}$ are the subsets of points

$$[m, b] = \{(x, xm + b) \mid x \in F\},$$
$$[a] \quad = \{(a, y) \mid y \in F\}.$$

By definition of $\mathbf{B}$, for any $k \in F_n^*$ and any $x, y \in F$, we have

$$(xk) \star (k^{-1}y) = x \star y.$$

For $k \neq 0$, the additive map $\tau_k : (x, y) \mapsto (xk, y)$ of F^2 maps $[m, b]$ to $[k^{-1}m, b]$ and fixes $[0]$ pointwise, i.e., τ_k is a homology with axis $[0]$ and center the point at infinity of the line $[0, 0]$.

Hence *the group of homologies with axis* $[0]$ *and center the point at infinity of the line* $[0, 0]$ *of* $\mathcal{A}$ *has order at least* $q - 1$.

If $\mathbf{S} = F(+, \circ)$ is the semifield constructed in Sect. 4.4 of [7] isotopic to $\mathbf{B}$ (i.e., it coordinatizes the plane $\mathcal{A}$), then the multiplicative group of the middle nucleus N_m of $\mathbf{S}$ is isomorphic to the group of homologies with axis $[0]$ and center the point at infinity of the line $[0, 0]$ (see [5] Theorem 8.2). Thus N_m has order at least q.

References

1. André J (1954) Über nicht-desarguessche ebenen mit transitive translationgruppe. Math Z 60: 156–186
2. Ball S, Brown M (2004) The six semifield planes associated with a semifield flocks. Adv Math 189: 68–87
3. Ball S, Bamberg J, Lavrauw M, Penttila T. (2004) Symplectic spreads. Des Codes Cryptogr 32: 9–14
4. Dembowski P (1968) Finite Geometries. Springer, Berlin Heidelberg New York
5. Hughes DR, Piper FC (1972) Projective planes. Springer
6. Kantor WM (1982) Spreads, translation planes and kerdock sets, I. Siam J Algebra Discr Methods 3: 151–165
7. Kantor WM (2003) Commutative semifields and symplectic spreads. J Algebra 270: 96–114
8. Kantor WM, Williams ME (2004) Symplectic semifields planes and $\mathbb{Z}_4$-linear codes. Trans Am Soc 356: 895–938
9. Knuth DE (1965) Finite semifields and projective planes. J Algebra 2: 182–217
10. Lunardon G (1999) Normal spreads. Geom Dedicata 75: 245–261
11. Lüneburg H (1980) Translation planes. Springer, Berlin Heidelberg New York
12. Mellinger KE (2003) A geometric relationship between equivalent spreads. Des Codes Cryptogr 30: 63–71
13. Maschietti A (2003) Symplectic translation planes and line ovals. Adv Geom 3: 123–143
14. Segre B (1964) Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. Ann Mat Pur Appl 64: 1–76