Note di Matematica
Note Mat. 29 (2009), n. 1, 145-155
ISSN 1123-2536, e-ISSN 1590-0932
DOI 10.1285/i15900932v29n1p145
http://siba-ese.unisalento.it, © 2009 Università del Salento

Spread-Theoretic Dual of a Semifield

Vikram Jha
Mathematics Dept., University of Iowa,
Iowa City, Iowa 52242, USA;
jha@math.uiowa.edu

Norman L. Johnson
Mathematics Dept., University of Iowa,
Iowa City, Iowa 52242, USA;
njohnson@math.uiowa.edu

Received: 25/06/2008; accepted: 27/06/2008.

Abstract. Given a finite pre-semifield $(S, +, \circ)$, the dual pre-semifield $(S, +, *)$ has multiplication $a * b = b \circ a$. In this article, a characterization is given of the dual pre-semifield in terms of the associated spreads. This is then used to give a new proof that shows that self-dual pre-semifield spreads when transposed and dualized construct self-transpose semifield spreads. When the self-dual pre-semifield is actually commutative then the transpose-dual spread is symplectic. We also give a spread-only description of the six semifields arising from a given semifield.

Keywords: semifields, dual semifields, symplectic spreads

MSC 2000 classification: 51E23 (primary), 51A40.

1 Introduction

Given a finite semifield $(S, +, \circ)$, various related semifields may be constructed. For example, another semifield, called the 'dual semifield' $(S, +, *)$ may be defined by the multiplication $a * b = b \circ a$. Furthermore, if

$$x = 0, y = x, y = xM, \text{ for } M \in S_{Mat}$$

is a matrix spread set for a semifield plane then

$$x = 0, y = x, y = xM^t, \text{ for } M \in S_{Mat}$$

where M^t denotes the transpose of the matrix M, also gives a semifield. It is mentioned in Johnson [4], that the spread arising from the dual space of the associated vector space is isomorphic to this 'transposed spread'. Actually, the connection between transposed spreads and polarities of the associated spread was recognized in a somewhat oblique manner. Given a derivable net D, let T be a transversal to D, then there is a associated translation plane (the dual of the dual translation plane constructed using Ostrom's extension theory). On the other hand, Bruen [3] developing the notion of an 'indicator set', realized that the affine planes constructed using an indicator set were equivalent to those obtained using the extension of a derivable net but the two spreads were related by a polarity of the projective space. Since the two spreads were connected by transposing the associated matrix spread sets as above, the connection was then noted. The reader interested in the development of both of these methods is referred to the Handbook [5], Chapters 49 and 50. These ideas also arise in [1], [2], etc.

In this article, we first give a spread characterization of the spread arising from the dual semifield as above. We call this the 'companion spread' of the associated semifield spread S. We show that with semifield spreads of order p^n written over the prime field $GF(p)$, the rows of an associated matrix spread set are given in terms of linear transformations C_i of the n-dimensional $GF(p)$-vector space. That is, we show that a semifield spread may be represented in the form:

$$y = x \begin{bmatrix} wC_1 \\ wC_2 \\ wC_3 \\ \vdots \\ wC_n \end{bmatrix}, \text{ for all } n\text{-vectors } x \text{ over } GF(p),$$

where w is an arbitrary t-vector and C_i are non-singular $n \times n$ matrices over $GF(p)$. The semifield corresponding to the dual semifield is then shown to be

$$x = 0, y = x \left[\sum_{i=1}^{n} \alpha_i C_i \right], \text{ for all } n\text{-vectors } x \text{ over } GF(p), \text{ for all } \alpha_i \in GF(p).$$

This characterization is another example of an algebraic construction considered strictly in spread-theoretic terms. We then show that beginning with the spread of a (commutative) semifield spread

$$y = x[C_1w^t, C_2w^t, C_3w^t, \ldots, C_nw^t], \tag{1}$$

where w^t is an arbitrary column, is a general matrix for the matrix spread set then the transpose-dual is symplectic as the matrices C_i are symmetric. The transposed semifield field is

$$x = 0, \ y = x \begin{bmatrix} wC_1 \\ wC_2 \\ wC_2 \\ \vdots \\ wC_n \end{bmatrix}, \text{ for all } n\text{-vectors } x \text{ over } GF(p),$$

which dualizes to

$$x = 0, y = x\left[\sum_{i=1}^{n} \alpha_i C_i\right], \text{ for all } n\text{-vectors } x \text{ over } GF(p), \text{ for all } \alpha_i \in GF(p).$$

The commutativity of the original semifield ultimately shows that $C_i^t = C_i$, and this is equivalent to $[\sum_{i=1}^{n} \alpha_i C_i]^t = [\sum_{i=1}^{n} \alpha_i C_i]$.

This result explicates the original result of Kantor [6]. These ideas also give a spread description of the six semifields arising from a given semifield.

2 The Semifield Spread of a dual Pre-Semifield

Any finite semifield spread of order p^n, for p a prime, may be written in the form

$$x = 0, \ y = xM,$$

for M in an additive set $\mathcal{S}$ of $n \times n$ matrices, including the zero matrix and such that all non-zero matrices are non-singular, and where x and y are n-vectors (considered as row vectors). The set of non-zero elements of $\mathcal{S}$ is a sharply transitive set acting on the set of all n-vectors. Fix a row vector w_0. Then given any non-zero n-vector w, there is a unique matrix M_w that maps w_0 to w. Hence, there is a bijection between the set of all n-vectors and the elements of $\mathcal{S}$ that maps the zero vector to the zero matrix. More generally, we have a (pre)semifield defined by any bijection $\phi : V \to \mathcal{S}$ (which maps zero to zero) in which multiplication has the form $x \circ w = xM_w$, where M_w denotes the matrix $\phi(w)$. The translation plane π is regarded as being coordinatized by the (pre)-semifield $(V, +, \circ)$, as well as by the spreadset $\mathcal{S}$.

The projection maps A_i that maps each matrix $M_w \in \mathcal{S}$ onto its i-th row are, of course, linear. Thus we may regard each A_i as a matrix such that the map $w \mapsto A_i w$ coincides with the i-th row of M_w. Hence, the spreadset $\mathcal{S}$ coincides with the set of matrices:

$$\{M_w \in \mathcal{S}\} = \left\{ y = x \begin{bmatrix} wA_1 \\ wA_2 \\ wA_3 \\ \vdots \\ wA_n \end{bmatrix}, \text{ for all } n\text{-vectors } w \text{ (rows) over } GF(p) \right\}.$$

Moreover, since the non-zero S_w are required to be non-singular, it follows that the additive group generated by the matrices A_i, $\mathcal{A} = \langle A_1, A_2, \ldots A_n \rangle$ consists entirely of non-singular elements (and zero), hence $\mathcal{A}$ is a spreadset. Actually, this is the spreadset of the plane π', dual to π, coordinatized by the pre-semifield with multiplication $w \odot x := x \circ w$. Letting $x = (x_1, x_2, \dots, x_n)$, we have

$$w \odot x := x \circ w = x \begin{bmatrix} wA_1 \\ wA_2 \\ wA_3 \\ \vdots \\ wA_n \end{bmatrix} = \sum_{i=1}^{n} x_i w A_i = w(\sum_{i=1}^{n} x_i A_i).$$

This means that the spread

$$x = 0, y = x(\sum_{i=1}^{n} \alpha_i A_i), \text{ for all } \alpha_i \in GF(p),$$

is the semifield spread given by the dual presemifield.

1 Remark. The translation plane coordinatized by the 'projected spreadset' $\mathcal{A} = \langle A_1, \dots, A_n \rangle$ of a given spreadset $\mathcal{S}$ is the plane coordinatized by the dual of the plane coordinatized by the spreadset $\mathcal{S}$.

Similarly, we may consider a partition of the spreadset $\mathcal{S}$ into its column vectors. If a semifield is represented in the form

$$x = 0,\ y = x[C_1 w^t, C_2 w^t, \dots, C_n w^t], \tag{2}$$

where x and w are row vectors. then the semifield spread for the dual semifield is

$$x = 0,\ y = x[C_1^t w^t, C_2^t w^t, \dots, C_n^t w^t]. \tag{3}$$

As before, we exclude the possibility that the matrix $\sum_{i=1}^{n} \xi_i C_i$ is singular unless all ξ are zero. Thus, singularity implies the existence of a non-zero vector e such that $\sum_{i=1}^{n} \xi_i e^t C_i$, which means the spread element $S_e = \left[C_1 e^t, C_2 e^t, \dots, C_n e^t\right]$ is singular, a contradiction. Hence, the additive group $\langle C_1, \dots, C_n \rangle$ forms a spreadset $\mathcal{C}$. We compute its connection with the (pre)-semifield $(V, +, \circ)$ coordinatizing the plane associated with the original spread $\mathcal{S}$. Repeating the previous argument, and letting $\odot$ be the dual of $\circ$:

$$\begin{aligned} w \odot x :&= x \circ w \\ &= x \left[C_1 w^t, C_2 w^t, \dots, C_n w^t\right] \\ &= \left[x C_1 w^t, x C_2 w^t, \dots, x C_n w^t\right], \\ &= \left[w C_1^t x^t, w C_2^t x^t, \dots, w C_n^t x^t\right], \text{since } x^t C_i y \text{ are scalars, they may} \\ &\qquad\qquad\qquad\qquad\qquad\qquad \text{be transposed,} \\ &= w \left[C_1^t x^t, C_2^t x^t, \dots, C_n^t x^t\right]. \end{aligned}$$

and we notice that $\left[C_1^t x^t, C_2^t x^t, \ldots, C_n^t x^t\right]$ is the slope map of some element of the spreadset generated by $\{C_1^t, \ldots, C_n^t\}$, i.e. in the transpose spread of the initial spreadset $\mathcal{S}$. Thus, the slope T_w, for any $w \in (V, +, \odot)$, coincides with the slope map of the spreadset generated by the transpose of the spreadset associated with the 'column matrices' for the initial spreadset $\mathcal{S}$. This completes the proof of the following theorem.

2 Theorem. *(1) Let π denote a semifield spread of order p^n written in the form*

$$x = 0,\ \ y = x \begin{bmatrix} wA_1 \\ wA_2 \\ wA_3 \\ \vdots \\ wA_n \end{bmatrix}, \text{ for all } n\text{-vectors } x \text{ over } GF(p),$$

Then the following is the semifield spread corresponding to the dual pre-semifield of π.

$$x = 0, y = x(\sum_{i=1}^{n} \alpha_i A_i),\ \text{for all } \alpha_i \in GF(p).$$

(2) Let the semifield spread be written in the form

$$x = 0,\ \ y = x[C_1 w^t, C_2 w^t, \ldots, C_n w^t], \tag{4}$$

then the semifield spread for the dual pre-semifield is

$$x = 0,\ \ y = x[C_1^t w^t, C_2^t w^t, \ldots, C_n^t w^t]. \tag{5}$$

3 Transpose and Dual Iterates

From the previous section, we recall that every semifield spread of order p^n may be written in the form:

$$(*) : y = x[C_1 w^t, C_2 w^t, \ldots, C_n w^t], \tag{6}$$

for all n-vectors w, where $C_1, C_2, \ldots, C_n$ are non-singular $n \times n$ matrices over $GF(p)$. The transposed semifield spread then represented as

$$x = 0, y = x \begin{bmatrix} wC_1 \\ wC_2 \\ wC_3 \\ \vdots \\ wC_n \end{bmatrix}; w \text{ a } n\text{-vector}.$$

We have shown in Theorem 2, that the dual of the semifield spread may be given by

$$y = x\left(\sum_{i=1}^{n} \alpha_i C_i\right), \text{ for all } \alpha_i \in GF(p).$$

These steps clearly also reverse. Hence, we have the following description of the transpose and dual of a semifield spread (here "dual" refers to the dual of the semifield). This gives a spread-description of the six semifields arising from the six permutations of the subscripts of the original method that Knuth used with cubical arrays (see also the next section for "cubical arrays").

3 Theorem. *Let S be a semifield spread of order p^n. If D and E are semifields let D^t, E^d denote the spreads corresponding to the transpose and dual for the semifields D and E respectively. Then there are non-singular matrices C_i, for $i = 1, 2, \ldots, n$ such that we have the following representations for the various spreads.*

$$S : x = 0, y = x[C_1w^t, C_2w^t, \ldots, C_nw^t] \Longleftrightarrow \textit{transpose}$$

$$S^t : x = 0, y = x\begin{bmatrix} wC_1^t \\ wC_2^t \\ wC_3^t \\ \vdots \\ wC_n^t \end{bmatrix} \Leftrightarrow \textit{dualize}$$

$$S^{td} : x = 0, y = x\left(\sum_{i=1}^{n} \alpha_i C_i^t\right), \textit{ for all } \alpha_i \in GF(p), \Longleftrightarrow \textit{transpose}$$

$$S^{tdt} : x = 0, y = x\left(\sum_{i=1}^{n} \alpha_i C_i\right), \textit{ for all } \alpha_i \in GF(p), \Longleftrightarrow \textit{dualize}$$

$$S^{tdtd} : x = 0, y = x\begin{bmatrix} wC_1 \\ wC_2 \\ wC_3 \\ \vdots \\ wC_n \end{bmatrix} \Longleftrightarrow \textit{transpose}$$

$$S^{tdtdt} : x = 0, y = x[C_1^tw^t, C_2^tw^t, \ldots, C_n^tw^t] \Longleftrightarrow \textit{dualize}$$

$$S^{tdtdtd} = S : x = 0, y = x[C_1w^t, C_2w^t, \ldots, C_nw^t].$$

Finally, we consider the connections between two representations of the same spread:

$$x = 0,\ y = x[C_1w^t, C_2w^t, \ldots, C_nw^t], \tag{7}$$

and

$$x = 0,\ y = x \begin{bmatrix} wA_1 \\ wA_2 \\ wA_3 \\ \vdots \\ wA_n \end{bmatrix},\ \text{for all } n\text{-vectors } x \text{ over } GF(p).$$

We have noted that

$$x = 0, y = x(\sum_{i=1}^{n} \alpha_i A_i),\ \text{for all } \alpha_i \in GF(p),$$

represents the spread of the dual pre-semifield and we know that

$$x = 0, y = x(\sum_{i=1}^{n} \alpha_i C_i),\ \text{for all } \alpha_i \in GF(p),$$

is also a spread, and it follows immediately that this is the "transposed-dual-transposed" spread of our spread. The question is, how are the two sets of matrices $\{A_i;\, i = 1, 2, \ldots, n\}$ and $\{C_i;\, i = 1, 2, \ldots, n\}$ related to each other.

4 Theorem. *If the semifield spread is represented both by*

$$x = 0,\ y = x[C_1 w^t, C_2 w^t, \ldots, C_n w^t], \tag{8}$$

and by

$$x = 0,\ y = x \begin{bmatrix} cwA_1 \\ wA_2 \\ wA_3 \\ \vdots \\ wA_n \end{bmatrix},\ \textit{for all } n\textit{-vectors } x \textit{ over } GF(p),$$

Then the ordered set of columns of A_j is the ordered set of transposes of the j-th rows of the C_i for $i = 1, 2, \ldots, n$. Similarly, the ordered set of rows of C_j is the ordered set of of transposes of the j-th columns of the A_i, for $i = 1, 2, \ldots, n$.

Proof. If $A_j = [D_{j1}, D_{j2}, \ldots, D_{jn}]$, where the D_{ji} are the columns of A_j, for $i = 1, 2, \ldots, n$ and $C_j = \begin{bmatrix} E_{1j} \\ E_{2j} \\ \vdots \\ E_{nj} \end{bmatrix}$, where E_{ij} are the rows of C_j, for $i = 1, 2, \ldots, n$. Then we obtain

$$[wD_{ij}] = \left[E_{ij} w^t\right]$$

so $D_{ij} = E_{ij}^t$. Then $A_j = [E_{j1}^t, E_{j2}^t, \ldots, E_{jn}^t]$, so the set of columns of A_j is the set of transposes of the j-th rows of the C_i for $i = 1, 2, \ldots, n$. Similarly, $C_j = \begin{bmatrix} D_{1j}^t \\ D_{2j}^t \\ \vdots \\ D_{nj}^t \end{bmatrix}$, and we have that the set of rows of C_j is the set of of transposes of the j-th columns of the A_i, for $i = 1, 2, \ldots, n$. $\boxed{QED}$

4 Self-Dual/Self-Transpose

In this section, we investigate the iterative process of transpose-dual of a semifield spread with the initial assumption that the original spread is self-dual.

Again we recall that every semifield spread of order p^n may be written in the form:

$$x = 0, \ y = x[C_1 w^t, C_2 w^t, \ldots, C_n w^t], \text{ for all } w \ n\text{-vectors} \tag{9}$$

where $C_1, C_2, \ldots, C_n$ are non-singular $n \times n$ matrices over $GF(p)$, for all n-vectors w and x. Now we apply Theorem 3, that shows the spread corresponding to the dual pre-semifield is

$$x = 0, \ y = x[C_1^t w_1^t, C_2^t w_1^t, \ldots, C_n^t w_1^t], \text{ for all } w_1 \ n\text{-vectors.} \tag{10}$$

In particular if,

$$x \circ w = x[C_1 w^t, C_2 w^t, \ldots, C_n w^t], \tag{11}$$

then $*$ defines the dual pre-semifield if

$$x * w = w[C_1 x^t, C_2 x^t, \ldots, C_n x^t].$$

Now assume that the spread obtained from the dual pre-semifield is the same as the original spread then

$$x[C_1 w^t, C_2 w^t, \ldots, C_n w^t] = x[C_1^t w_1^t, C_2^t w_1^t, \ldots, C_n^t w_1^t], \tag{12}$$

where the mapping $w \to w_1$ is a bijection. This means that $\{C_1, C_2, \ldots, C_n\} = \{C_1^t, \ldots, C_n^t\}$, which we symbolize by $\{C_i; i = 1, 2, \ldots, n\}^t = \{C_i; i = 1, 2, \ldots, n\}$. If we now transpose and dualize, we see the corresponding spread is

$$x = 0, y = x\left(\sum_{i=1}^{n} \alpha_i C_i^t\right), \text{ for all } \alpha_i \in GF(p),$$

which shows that

$$\left(\sum_{i=1}^{n}\alpha_iC_i^t;\alpha_i\in GF(p)\right)^t=\left(\sum_{i=1}^{n}\beta_iC_i^t;\beta_i\in GF(p)\right).$$

In other words, the original spread is self-dual if and only if the transposed-dual spread is self-transpose. Note that a semifield spread defines a commutative pre-semifield if and only if it is "individually" self-dual and a semifield spread is symplectic if and only if it is "individually" self-transpose (symmetric).

5 Theorem. *[Compare with Kantor [6] in the symplectic case] Let $(S,+,\circ)$ be a pre-semifield (or semifield) of order p^n defining a self-dual semifield spread. Then take the semifield spread*

$$y=x[C_1w^t,C_2w^t,\ldots,C_nw^t]=x\circ w;\ \textit{for all } n\textit{-vectors } w, \tag{13}$$

where C_i is a non-singular $n\times n$ matrix.

(1) Then $\{C_i;i=1,2,\ldots,n\}^t=\{C_i;i=1,2,\ldots,n\}$ and $C_i=C_i^t$ if and only the pre-semifield is commutative.

(2) Transpose the matrices of the self-dual pre-semifield spread to obtain

$$y=x\begin{bmatrix}wC_1\\wC_2\\wC_3\\\vdots\\wC_n\end{bmatrix}$$

(3) Dualize to obtain the spread

$$y=x\left(\sum_{i=1}^{n}\alpha_iC_i\right),\text{ for all }\alpha_i\in GF(p).$$

Then note that

$$\left(\sum_{i=1}^{n}\alpha_iC_i^t;\alpha_i\in GF(p)\right)^t=\left(\sum_{i=1}^{n}\beta_iC_i^t;\beta_i\in GF(p)\right).$$

So, the spread itself is self-transpose. The spread is symplectic if and only if the original spread is commutative.

(4) Conversely, if

$$\left(\sum_{i=1}^{n}\alpha_i C_i^t;\alpha_i\in GF(p)\right)^t=\left(\sum_{i=1}^{n}\beta_i C_i^t;\beta_i\in GF(p)\right).$$

defines a self-transpose semifield spread then the dual semifield spread is

$$y=x\begin{bmatrix}wC_1\\ wC_2\\ wC_3\\ \vdots\\ wC_n\end{bmatrix}$$

and the transpose of this spread is

$$y=x[C_1w^t,C_2w^t,\dots,C_nw^t]. \tag{14}$$

Now define a multiplication by

$$x\circ w=x[C_1w^t,C_2w^t,\dots,C_nw^t]$$

for all x,w n-vectors over $GF(p)$.

Since $\{C_i;i=1,2,\dots,n\}^t=\{C_i;i=1,2,\dots,n\}$, it is immediate that we obtain a self-dual pre-semifield, which is commutative if and only if $C_i^t=C_i$.

Proof. Then simply apply Theorem 2 or Theorem 3. $\boxed{QED}$

Finally, we note that in our results, we have chosen a specific representation for an initial semifield spread; either in row or column form. The column form is best suited to determine if a semifield is self-dual and the row form is ideal if asking if a semifield spread is self-transpose. Theorem 4 shows how to deal with the opposite situation.

For example, if we have a representation

$$x=0,\ y=x\begin{bmatrix}wA_1\\ wA_2\\ wA_3\\ \vdots\\ wA_n\end{bmatrix}, \text{ for all } n\text{-vectors } x \text{ over } GF(p),$$

and wish to determine if the semifield is self-dual or commutative, we note that by Theorem 4 then C_j^t is the set of ordered j-th columns of the $A_1,A_2,\dots,A_n$. Hence, the semifield is commutative if and only if the $C_j^t=C_j$ and is self-dual if and only if $\{C_j;j=1,2,\dots,n\}^t=\{C_j;j=1,2,\dots,n\}$.

References

[1] S. Ball, M. Brown: *The six semifield planes associated with a semifield flock*, Adv. Math., no. 1 **189** (2004), 68–87.

[2] M. Biliotti, V. Jha, N. L. Johnson: *Symplectic flock spreads in $PG(3, q)$*, Note di Mat., no. 1 **24** (2005), 85–110.

[3] A. Bruen: *Spreads and a conjecture of Bruck and Bose*, J. Algebra **23** (1972), 519–537.

[4] N. L. Johnson: *A note on net replacement in transposed spreads*, Bull. Canad. J. Math., (4) vol. **28** (1985), 469–471.

[5] N. L. Johnson, V. Jha, M. Biliotti: *Handbook of finite translation planes*, Pure and Applied Mathematics (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, **289** (2007), xxii+861.

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