Innovations in Incidence Geometry
Volume 2 (2005), Pages 101–107
ISSN 1781-6475

The two sets of three semifields associated with a semifield flock

Michel Lavrauw*

Abstract

In 1965 Knuth [4] showed that from a given finite semifield one can construct further semifields manipulating the corresponding cubical array, and obtain in total six semifields from the given one. In the case of a rank two commutative semifield (the semifields corresponding to a semifield flock) these semifields have been investigated in [1], providing a geometric connection between these six semifields and it was shown that they give at most three non-isotopic semifields. However, there is another set of three semifields arising in a different way from a semifield flock, hence in total six semifields arise from a rank two commutative semifield (see [1]). In this article we give a geometrical link between these two sets of three semifields.

Keywords: semifields, translation planes, finite geometry

MSC 2000: 12K10, 51E15

1 Introduction and motivation

Throughout the article we will use the terminology and the notation from [1]. A semifield coordinatises a semifield plane, which corresponds to a semifield spread via the Andre-Bruck-Bose construction, see [3, Section 3.1]. A flock of a quadratic cone gives rise to a line spread of three-dimensional projective space (and hence to a translation plane) via the Thas-Walker construction, see [1], [6]. In case the flock is a semifield flock, the resulting translation plane is a semifield plane.

*This research has been supported by a VENI grant, part of the Innovational Research Incentives Scheme of the Netherlands Organisation for Scientific Research (NWO).

Remark 1.1. Two semifield planes are isomorphic if and only if the corresponding semifields are isotopic. Usually we are only interested in the number of non-isomorphic planes corresponding to a semifield plane and hence in the number of isotopy-classes arising from a semifield. Out of convenience we will often talk about the number of semifields, (for instance in the title) instead of the number of isotopy-classes of semifields.

Starting with a semifield flock, one can also construct a rank two commutative semifield, by coordinatising the projective space of the flock, in order to obtain a so-called Cohen-Ganley pair of functions (f, g). Following [1], let $\mathcal{S}$ denote the semifield obtained from a semifield flock using the Thas-Walker construction. As shown in [1] the six semifields associated to $\mathcal{S}$ under the Knuth-operations give three isotopy classes of semifields, which can geometrically be generated dualising the semifield plane ($\mathcal{S} \mapsto \mathcal{S}^*$) and dualising the semifield spread ($\mathcal{S} \mapsto \mathcal{S}^\dagger$). The three isotopy classes can be represented by $\mathcal{S} \cong \mathcal{S}^\dagger, \mathcal{S}^*, \mathcal{S}^{*\dagger} \cong \mathcal{S}^{*\dagger*}$. The rank two commutative semifield is $\hat{\mathcal{S}}^{*\dagger}$, where $\hat{\mathcal{S}}$ is the semifield corresponding to the symplectic spread, arising from the translation ovoid of $Q(4, q)$ associated to the semifield flock. As shown in [1] the six semifields associated to $\hat{\mathcal{S}}$ under the Knuth-operations give three isotopy classes of semifields, which can be represented by $\hat{\mathcal{S}} \cong \hat{\mathcal{S}}^\dagger, \hat{\mathcal{S}}^*, \hat{\mathcal{S}}^{*\dagger} \cong \hat{\mathcal{S}}^{*\dagger*}$. Here we provide a geometric link for the operation $\mathcal{S} \mapsto \hat{\mathcal{S}}$.

2 Dualising the ovoid of the Klein quadric

The key idea is to use a particular representation of the Klein quadric due to Lunardon [5], denoted by $T_4(Q^+(3, q^n))$ and construct the *translation dual* (see [5]) of the translation ovoid. First we introduce some notation. If $r(x)$ is a linearized q-polynomial over $\mathrm{GF}(q^n)$, i.e.,

$$r(x) = \sum_{i=0}^{n-1} r_i x^{q^i},$$

for some $r_i \in \mathrm{GF}(q^n)$, then we define $\hat{r}(x)$ by

$$\hat{r}(x) = \sum_{i=0}^{n-1} (r_i x)^{1/q^i}.$$

Consider the pre-semifield of rank two over its left nucleus $\mathrm{GF}(q^n)$ with multiplication

$$(x, y) \circ (u, v) = (xf(v) + yu + yg(v), xu + yv),$$

where f and g are linearized q-polynomials in $\mathrm{GF}(q^n)[X]$ as in [1], satisfying the conditions for a so called Cohen-Ganley pair that $g(x)^2 + 4xf(x)$ is a non-square for all $x \in \mathrm{GF}(q^n)^*$. The corresponding spread set is

$$\left\{ \begin{pmatrix} f(v) & u \\ u + g(v) & v \end{pmatrix} \parallel u, v \in \mathrm{GF}(q^n) \right\}.$$

Remark 2.1. As mentioned before, we are only interested in the number of isotopy classes of semifields, and hence we need to choose a representative of each class. (Ideally we would like to have a canonical form for each isotopy class.) The multiplications listed in [1, Table 1] are often corresponding to a pre-semifield instead of a semifield. In Section 3 we provide a table representing the six isotopy classes, such that each multiplication corresponds to a semifield with $(1, 0)$ as unit element.

Following the above remark, we will continue with the spread set

$$\left\{ \begin{pmatrix} u & v \\ f(v) & u + g(v) \end{pmatrix} \parallel u, v \in \mathrm{GF}(q^n) \right\}.$$

Note that the condition for this to be a spread set is the same as before. The corresponding multiplication in the semifield is

$$(x, y) \circ (u, v) = (ux + yf(v), xv + yu + yg(v)).$$

Since $f(0) = g(0) = 0$, it immediately follows that $(1, 0)$ is the unit element in this semifield. The corresponding ovoid $\mathcal{O}$ of $Q^+(5, q^n) : X_0X_5 + X_1X_4 + X_2X_3 = 0$ is the set of points

$$\langle 1, u, v, -f(v), u + g(v), vf(v) - u^2 - ug(v) \rangle,\ u, v \in \mathrm{GF}(q^n),$$

and the point $\langle 0, 0, 0, 0, 1 \rangle$. By looking at $Q^+(5, q^n)$ as $T_4(Q^+(3, q^n))$ (see [5]) we obtain the $(2n - 1)$-space

$$U = \{\langle 0, u, v, -f(v), u + g(v), 0 \rangle \parallel (u, v) \in (\mathrm{GF}(q^n)^2)^*\}$$

over $\mathrm{GF}(q)$ skew from $Q^+(3, q^n)$ with equation $X_1X_4 + X_2X_3 = 0$ in the three-dimensional space with equation $X_0 = X_5 = 0$. Note that the condition for U to be skew from $Q^+(3, q)$ is exactly the condition for the set of matrices to be a spread set. Dualising with respect to the duality defined by the bilinear form over $\mathrm{GF}(q)$

$$(a, b) = \mathrm{tr}(a_1b_4 + a_4b_1 + a_2b_3 + a_3b_2),$$

where $\mathrm{tr}(x) = \sum_{i=0}^{n-1} x^{q^i}$ we obtain the $(2n - 1)$-space skew from $Q^+(3, q^n)$ inducing again a translation ovoid of $Q^+(5, q^n)$. When calculating the dual space of U one sees that U^D consists of points $\langle 0, x, y, z, w, 0 \rangle$ for which

$$\mathrm{tr}(x(u + g(v)) - yf(v) + zv + wu) = 0,\ \forall u, v \in \mathrm{GF}(q^n).$$

Putting $v = 0$ gives $w = -x$, and putting $u = 0$ gives $\mathrm{tr}(xg(v) - yf(v) + zv) = 0$, $\forall v \in \mathrm{GF}(q^n)$. This implies that $z = -\hat{g}(x) + \hat{f}(y)$ (since $\mathrm{tr}(yr(x)) = \mathrm{tr}(x\hat{r}(y))$ for any q-linearized polynomial r) and we may conclude that

$$U^D = \{\langle 0, x, y, -\hat{g}(x) + \hat{f}(y), -x, 0\rangle \parallel (x, y) \in (\mathrm{GF}(q^n)^2)^*\}.$$

By construction U^D is skew from the quadric $Q^+(3, q^n)$, and this is the exact same condition that $-x^2 - y\hat{g}(x) + y\hat{f}(y) = 0$ implies $(x, y) = 0$, as for the set of matrices

$$\left\{ \begin{pmatrix} u & v \\ v & \hat{f}(u) - \hat{g}(v) \end{pmatrix} \parallel u, v \in \mathrm{GF}(q^n) \right\}.$$

to be a spread set. The multiplication in the corresponding pre-semifield is

$$(x, y) \mathbin{\hat{\circ}} (u, v) = (xu + yv, xv + y\hat{f}(u) - y\hat{g}(v)).$$

Let $\hat{\pi}$ denote the semifield plane corresponding to the pre-semifield $\hat{\mathcal{S}}$ as in [1, Table 1].

Theorem 2.2. *The semifield plane corresponding to the pre-semifield* $(\mathrm{GF}(q^n)^2, +, \hat{\circ})$ *is isomorphic to the semifield plane* $\hat{\pi}$.

Proof. Let $F(x, y) = (y, -x)$ and $G(u, v) = (-v, u)$. Then

$$F((x, y) \mathbin{\hat{\circ}} (u, v)) = (xv + y\hat{f}(u) - y\hat{g}(v), -xu - yv)$$
$$= (y, -x) \cdot (-v, u) = F(x, y) \cdot G(u, v),$$

where $\cdot$ is the multiplication

$$(x, y) \cdot (u, v) = (yu + x\hat{f}(v) + x\hat{g}(u), xu + yv)$$

of the pre-semifield $\hat{\mathcal{S}}$ as in [1, Table 1]. This implies that the two pre-semifields are isotopic and hence that the two semifield planes are isomorphic. □

We may conclude that apart from operation $*$ (dualising the plane), operation † (dualising the spread), also the operation $\mathcal{S} \mapsto \hat{\mathcal{S}}$ has a geometric interpretation (dualising the ovoid).

3 The six semifields associated to a semifield flock

In this section we provide a table with the semifield multiplication (instead of pre-semifield multiplication), with unit element $(1, 0)$, for each of the six isotopy classes of semifields corresponding to a semifield flock.

As in Section 2 let $\mathcal{S}$ denote the semifield with multiplication

$$(x, y) \circ (u, v) = (ux + yf(v), xv + yu + yg(v)).$$

Dualising the plane we get the semifield $\mathcal{S}^*$ by reversing the multiplication, i.e.,

$$(x, y) \circ^* (u, v) = (xu + vf(y), uy + xv + vg(y)).$$

Both multiplications have $(1, 0)$ as identity element. In order to obtain the multiplication for $\mathcal{S}^{*\dagger}$ we have to dualise the semifield spread obtained from $\mathcal{S}^*$ (see [1]). We have to find all $a, b, c, d \in \mathrm{GF}(q^n)$ for which

$$tr(xa + yb + (xu + f(y)v)c + (yu + xv + g(y)v)d) = 0,\ \forall x, y \in \mathrm{GF}(q^n).$$

Putting $x = 0$ we get the condition

$$tr(yb + f(y)vc + yu + g(y)vd = 0,\ \forall y \in \mathrm{GF}(q^n).$$

This implies $b = -(\hat{f}(vc) + ud + \hat{g}(vd))$. Similarly, after putting $y = 0$ we get $a = -uc - vd$. Hence after some coordinate transformations, we get the multiplication

$$(x, y) \cdot (u, v) = (xu + yv, uy + \hat{f}(xv) + \hat{g}(yv))$$

In order for $(1, 0) = (1, 0) \cdot (1, 0)$ to be the identity we have to define a new multiplication by $((x, y) \cdot (1, 0)) \circ^{*\dagger} ((1, 0) \cdot (u, v)) = (x, y) \cdot (u, v)$ (see [4]). We get

$$(x, y) \circ^{*\dagger} (u, v) = (xu + y\hat{f}^{-1}(v), uy + \hat{f}(x\hat{f}^{-1}(v)) + \hat{g}(y\hat{f}^{-1}(v))).$$

That $\hat{f}^{-1}$ is well defined follows from the fact that the multiplication $\hat{\circ}$ from the previous section has no zero divisors. In the previous we had the following multiplication for $\hat{\mathcal{S}}$:

$$(x, y) \mathbin{\hat{\circ}} (u, v) = (xu + yv, xv + y\hat{f}(u) - y\hat{g}(v)).$$

We see that $(1, 0) \mathbin{\hat{\circ}} (u, v) = (u, v)$ and, $(x, y) \mathbin{\hat{\circ}} (1, 0) = (x, y\hat{f}(1))$, and in order for $(1, 0)$ to be the identity, we can apply one of the methods to get a semifield from a pre-semifield (see [4]) and define a new multiplication. We use the same notation $\hat{\mathcal{S}}$ for the semifield with identity $(1, 0)$ and multiplication

$$(x, y) \mathbin{\hat{\circ}} (u, v) = (xu + y\hat{f}^{-1}(1)v, xv + y\hat{f}^{-1}(1)\hat{f}(u) - y\hat{f}^{-1}(1)\hat{g}(v)).$$

Reversing this mulitplication we get the semifield $\hat{\mathcal{S}}^*$, i.e.,

$$(x, y) \mathbin{\hat{\circ}^*} (u, v) = (xu + y\hat{f}^{-1}(1)v, yu + v\hat{f}^{-1}(1)\hat{f}(x) - v\hat{f}^{-1}(1)\hat{g}(y)).$$

Finally we get the semifield $\hat{\mathcal{S}}^{*\dagger}$ by dualising the semifield spread corresponding to $\hat{\mathcal{S}}^{*}$. As before, after applying the same methods in order to obtain a multiplication with identity $(1,0)$, we get

$$(x,y)\ \hat{\circ}^{*\dagger}\ (u,v) = (xu + f(yv), xv + yu - g(yv)).$$

The following table summarizes these results.

Table 1: The six semifield multiplications with identity $(1,0)$, defined on the set of elements of $\mathrm{GF}(q^n)^2$ (addition as in $\mathrm{GF}(q^n)^2$) associated with a semifield flock. The nuclei are as in [1] with q replaced by q^n and q_0 replaced by q.

$\mathcal{S}$	$(x,y)\circ(u,v) = (ux + yf(v), xv + yu + yg(v))$
$\mathcal{S}^*$	$(x,y)\circ^*(u,v) = (xu + vf(y), uy + xv + vg(y))$
$\mathcal{S}^{*\dagger}$	$(x,y)\circ^{*\dagger}(u,v) = (xu + y\hat{f}^{-1}(v), uy + \hat{f}(x\hat{f}^{-1}(v)) + \hat{g}(y\hat{f}^{-1}(v)))$
$\hat{\mathcal{S}}$	$(x,y)\ \hat{\circ}\ (u,v) = (xu + y\hat{f}^{-1}(1)v, xv + y\hat{f}^{-1}(1)\hat{f}(u) - y\hat{f}^{-1}(1)\hat{g}(v))$
$\hat{\mathcal{S}}^*$	$(x,y)\ \hat{\circ}^*\ (u,v) = (xu + y\hat{f}^{-1}(1)v, yu + v\hat{f}^{-1}(1)\hat{f}(x) - v\hat{f}^{-1}(1)\hat{g}(y))$
$\hat{\mathcal{S}}^{*\dagger}$	$(x,y)\ \hat{\circ}^{*\dagger}\ (u,v) = (xu + f(yv), xv + yu - g(yv))$

Remark 3.1. Note that this operation (dualising the ovoid) can be extended to all finite semifields which are of rank two over their left nucleus (and so corresponding to spreads of $\mathrm{PG}(3,q^n)$ and hence ovoids of $Q(5,q^n)$). In fact this turns out to be a special case of one of the semifield operations from [2].

Acknowledgment

The author would like to thank one of the referees for simplifying the proof of Theorem 2.2.

References

[1] **S. Ball** and **M. R. Brown**, The six semifield planes associated with a semifield flock, *Adv. Math.*, **189** (2004) 68–87.

[2] **S. Ball**, **G. Ebert** and **M. Lavrauw**, A new approach to finite semifields, preprint.

[3] **P. Dembowski**, Finite Geometries, Springer, Berlin, 1968.

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

[5] **G. Lunardon**, Translation ovoids. Combinatorics, 2002 (Maratea), *J. Geom.* **76** (2003), no. 1-2, 200–215.

[6] **M. Walker**, A class of translation planes, *Geom. Dedicata* **5** (1976), 135–146.

Michel Lavrauw

DEPARTMENT OF DISCRETE MATHEMATICS, EINDHOVEN UNIVERSITY OF TECHNOLOGY, P.O.BOX 513, 5600 MB EINDHOVEN, THE NETHERLANDS,

e-mail: mlavrauw@win.tue.nl