ON THE HUGHES-KLEINFELD AND KNUTH'S SEMIFIELDS TWO DIMENSIONAL OVER A WEAK NUCLEUS

SIMEON BALL AND MICHEL LAVRAUW

Abstract. In 1960 Hughes and Kleinfeld [4] constructed a finite semifield which is two dimensional over a weak nucleus given an automorphism σ of a finite field $\mathbb{K}$ and elements $\mu, \eta \in \mathbb{K}$ with the property that $x^{\sigma+1} + \mu x - \eta$ has no roots in $\mathbb{K}$. In 1965 Knuth [7] constructed a further three finite semifields which are also two dimensional over a weak nucleus, given the same parameter set $(\mathbb{K}, \sigma, \mu, \eta)$. Moreover, in the same article, Knuth describes operations that allow one to obtain up to six semifields from a given semifield. We show how these operations in fact relate these four finite semifields, for a fixed parameter set, and that up to isotopy there are two set of semifields, one which consists of at most two non-isotopic semifields related by Knuth operations and the other which consists of at most three non-isotopic semifields.

1. Introduction

A *finite semifield* is a set $\mathbb{S}$ with two operations, addition and multiplication ($\circ$) such that $(\mathbb{S}, +)$ is a group with identity element 0, if $a \circ b = 0$ then either a or b is zero, the distributive laws hold and there is an element 1 such that $a \circ 1 = 1 \circ a = a$ for all $a \in \mathbb{S}$. In other words $\mathbb{S}$ satisfies all the axioms of a field, except (possibly) associativity of multiplication. If the set $\mathbb{S}$ satisfies all axioms of a semifield, except that it does not have an identity element for multiplication, then $\mathbb{S}$ is called a *pre-semifield*.

For a recent survey on the known finite semifields, see [2], and for an updated version see [6].

A pre-semifield $\mathbb{S}$ is a vector space over $\mathbb{F}_p$ for some prime p and can be used to coordinatise a projective plane of prime power order $|\mathbb{S}|$. Two pre-semifields $\mathbb{S} = (V, +, \circ)$ and $\mathbb{S}' = (V', +, \cdot)$ are said to be *isotopic* if there exists a triple $(f_1,\ f_2,\ f_3)$ of $\mathbb{F}_p$-linear maps from V to V' with the property that

$$f_1(x) \cdot f_2(y) = f_3(x \circ y),$$

for all $x, y \in V$. Albert showed that the projective planes coordinatised by the pre-semifields $\mathbb{S}$ and $\mathbb{S}'$ are isomorphic if and only if the pre-semifields $\mathbb{S}$ and $\mathbb{S}'$ are isotopic. We shall write $\mathbb{S} \simeq \mathbb{S}'$. For all of this we refer to Knuth [7].

Date: 8 February 2007.

The first author acknowledges the support of the Ramon y Cajal programme and the project MTM2005-08990-C02-01 of the Spanish Ministry of Science and Education and the project 2005SGR00256 of the Catalan Research Council.

During this research the second author was supported by a VENI grant, part of the Innovational Research Incentives Scheme of the Netherlands Organisation for Scientific Research (NWO).

For any pre-semifield $\mathbb{S}$ with multiplication $\circ$ we can make another pre-semifield $\tau_1(\mathbb{S})$, whose multiplication $\cdot$ is defined by

$$a \cdot b = b \circ a.$$

The projective plane coordinatised by $\mathbb{S}$ can also be constructed from the set of subspaces

$$\{\{(y, y \circ x) \mid y \in V\} \mid x \in V\} \cup \{(0, y) \mid y \in V\},$$

of $V \times V$ via the André, Bruck-Bose construction, see [3]. These subspaces partition the non-zero vectors of $V \times V$ and such a partition is called a *spread*. The set of subspaces dual to these subspaces also forms a spread which can be used to construct a projective plane coordinatised by a pre-semifield and we shall define this pre-semifield (up to isotopy) to be $\tau_2(\mathbb{S})$. For more details on this, see [1].

We refer to the operations τ_1 and τ_2 as the *Knuth operations*. They were described by Knuth as permutations of the subscripts in a cubical array obtained from a pre-semifield, see [7]. Together they generate a group G isomorphic to the symmetric group $Sym(3)$ acting on the set of all pre-semifields. The orbit of the pre-semifield $\mathbb{S}$ is the set of six pre-semifields $\mathbb{S}$, $\tau_1(\mathbb{S})$, $\tau_2(\mathbb{S})$, $\tau_2\tau_1(\mathbb{S})$, $\tau_1\tau_2(\mathbb{S})$ and $\tau_1\tau_2\tau_1(\mathbb{S})$, some of which may be isotopic, depending on $\mathbb{S}$. In [7] Knuth shows that the operations τ_1 and τ_2 preserve isotopy, so $\mathbb{S} \simeq \mathbb{S}'$ if and only if $\tau_i(\mathbb{S}) \simeq \tau_i(\mathbb{S}')$. Generally we are only interested in the isotopy classes of pre-semifields, and considering the action of the group G on the set of all isotopy classes of pre-semifields, we shall refer to the orbit of the isotopy class containing the pre-semifield $\mathbb{S}$ as the *Knuth orbit of* $\mathbb{S}$.

In the very same article [7] Knuth constructs four semifields, given a field $\mathbb{K}$ and an automorphism σ and elements $\mu, \eta \in \mathbb{K}$ with the property that $x^{\sigma+1} + \mu x - \eta$ has no root in $\mathbb{K}$, one of which is the Hughes-Kleinfeld semifield [4], and all of which are two dimensional over a *weak nucleus* $\mathbb{K}$, a set of elements of $\mathbb{S}$ with the property that

$$x \circ (y \circ z) = (x \circ y) \circ z,$$

whenever two of x, y or z are in $\mathbb{K}$.

The purpose of this note is to show that, for a fixed parameter set $(\mathbb{K}, \sigma, \mu, \eta)$, three of these four semifields lie in the same Knuth orbit of size at most three, and the other one has a Knuth orbit of size at most two.

2. Knuth's semifields two dimensional over a weak nucleus

Let $\mathbb{K}$ be a finite field. In [7] Knuth gave four multiplications for $(\mathbb{K}^2, +, \circ)$ all of which give semifields under the condition that $\eta, \mu \in \mathbb{K}$ and σ, an automorphism of $\mathbb{K}$, are chosen so that $x^{\sigma+1} + \mu x - \eta$ has no root in $\mathbb{K}$. They are
$\mathbb{S}_1$ defined by

$$(u, v) \circ (x, y) = (ux + \eta y^{\sigma} v^{\sigma^{-2}}, x^{\sigma} v + uy + \mu y^{\sigma} v^{\sigma^{-1}}),$$

$\mathbb{S}_2$ defined by

$$(u, v) \circ (x, y) = (ux + \eta y^{\sigma} v, x^{\sigma} v + uy + \mu y^{\sigma} v),$$

$\mathbb{S}_3$ defined by

$$(u, v) \circ (x, y) = (ux + \eta y^{\sigma^{-1}} v^{\sigma^{-2}}, x^{\sigma} v + uy + \mu y v^{\sigma^{-1}}),$$

and $\mathbb{S}_4$ defined by

$$(u,v)\circ(x,y)=(ux+\eta y^{\sigma^{-1}}v, x^\sigma v+uy+\mu yv).$$

We have already defined τ_1 as the Knuth operation that changes the order of multiplication. Considering the maps $f_1, f_2, f_3 : \mathbb{K}^2 \to \mathbb{K}^2$ defined by

$$\begin{aligned} f_1 &: (u,v)\mapsto (u^{\sigma^{-1}}+\mu^{\sigma^{-1}}v^{\sigma^{-2}}, -v^{\sigma^{-2}}), \\ f_2 &: (x,y)\mapsto (y^{\sigma^{-1}}, -x/\eta), \text{ and} \\ f_3 &: (a,b)\mapsto (b^{\sigma^{-1}}, -a/\eta), \end{aligned}$$

it is straightforward to check that $\tau_1(\mathbb{S}_2)$, which has multiplication

$$(u,v)\cdot(x,y)=(ux+\eta v^\sigma y, u^\sigma y+xv+\mu v^\sigma y),$$

is isotopic to $\mathbb{S}_3$, i.e.

$$f_1(u,v)\cdot f_2(x,y)=f_3((u,v)\circ(x,y)),$$

where $\circ$ is multiplication in $\mathbb{S}_3$. Thus $\mathbb{S}_3\simeq\tau_1(\mathbb{S}_2)$, which implies that $\mathbb{S}_2$ and $\mathbb{S}_3$ lie in the same Knuth orbit. The semifields of type $\mathbb{S}_2$ were discovered by Hughes and Kleinfeld [4] and the isotopic relation $\mathbb{S}_3\simeq\tau_1(\mathbb{S}_2)$ was already known to Knuth as it follows from [7, Theorem 7.4.1] and the fact that τ_1 interchanges the left and right nuclei.

Let us see how τ_2 relates further the semifields $\mathbb{S}_i$. Let $\alpha,\beta,\gamma,\epsilon$ be automorphisms of $\mathbb{K}$ such that the multiplication

$$(u,v)\circ(x,y)=(ux+\eta y^\alpha v^\beta, x^\sigma v+uy+\mu y^\gamma v^\epsilon)$$

defines a semifield $\mathbb{S}$. The elements of the spread constructed from the semifield $\mathbb{S}$ are

$$A_{x,y}:=\{(u,v,ux+\eta y^\alpha v^\beta, x^\sigma v+uy+\mu y^\gamma v^\epsilon)\mid u,v\in\mathbb{K}\},\ x,y\in\mathbb{K},$$

and $\{(0,0,u,v)\mid u,v\in\mathbb{K}\}$. As in Kantor [5] we use the alternating form

$$((u,v,w,z),(a,b,c,d))=Tr(cu+dv-aw-bz),$$

where Tr is the trace function from $\mathbb{K}$ to $\mathbb{F}_p$, to calculate the dual spread which consists of the subspaces

$$A^\perp_{x,y}=\{(a,b,c,d)\mid Tr(cu+dv-a(ux+\eta y^\alpha v^\beta)-b(x^\sigma v+uy+\mu y^\gamma v^\epsilon))=0 \text{ for all } u,v\in\mathbb{K}\},$$

$x,y\in\mathbb{K}$, and $\{(0,0,u,v)\mid u,v\in\mathbb{K}\}$. When $u=0$ we have the equation

$$Tr(dv-a\eta y^\alpha v^\beta-bx^\sigma v-b\mu y^\gamma v^\epsilon)=0,\ \forall v\in\mathbb{K}$$

which is equivalent to

$$Tr(v(d-(a\eta y^\alpha)^{\beta^{-1}}-bx^\sigma-(b\mu y^\gamma)^{\epsilon^{-1}}))=0,\ \forall v\in\mathbb{K}.$$

When $v=0$ we have the equation

$$Tr(cu-uax-buy)=0,\ \forall u\in\mathbb{K}.$$

Thus the subspace

$$A^\perp_{x,y}=\{(a,b,ax+by, bx^\sigma+(\eta ay^\alpha)^{\beta^{-1}}+(\mu by^\gamma)^{\epsilon^{-1}})\mid a,b\in\mathbb{K}\}.$$

This implies that the isotopy class of the semifield $\tau_2(\mathbb{S})$ is represented by the pre-semifield with multiplication

$$(u,v)\bullet(x,y)=(ux+vy, vx^\sigma+(\eta uy^\alpha)^{\beta^{-1}}+(\mu vy^\gamma)^{\epsilon^{-1}}).$$

Considering the isotopism (f_1, f_2, f_3)

$$\begin{aligned} f_1 &: (u,v) \mapsto (u\eta^{-1}, v^{\epsilon^{-1}}), \\ f_2 &: (x,y) \mapsto (x, y^{\epsilon\alpha^{-1}}), \\ f_3 &: (a,b) \mapsto (\eta^{-1}a, b^{\epsilon^{-1}}), \end{aligned}$$

we see that the semifield $\tau_2(\mathbb{S})$ is isotopic to a pre-semifield that has multiplication

$$(u,v) \star (x,y) = (ux + \eta v^{\epsilon^{-1}} y^{\epsilon\alpha^{-1}}, vx^{\epsilon\sigma} + u^{\epsilon\beta^{-1}} y^{\epsilon^2\beta^{-1}} + \mu v^{\epsilon^{-1}} y^{\gamma\epsilon\alpha^{-1}}),$$

since

$$f_1(u,v) \bullet f_2(x,y) = f_3((u,v) \star (x,y))$$

By substituting the appropriate automorphisms so that $\mathbb{S} = \mathbb{S}_2$ ($\alpha = \sigma$, $\beta = 1$, $\gamma = \sigma$ and $\epsilon = 1$) we see that

$$\mathbb{S}_4 \simeq \tau_2(\mathbb{S}_2),$$

which implies that $\mathbb{S}_2$ and $\mathbb{S}_4$ have the same Knuth orbit. By substituting the appropriate automorphisms so that $\mathbb{S} = \mathbb{S}_3$ ($\alpha = \sigma^{-1}$, $\beta = \sigma^{-2}$, $\gamma = 1$ and $\epsilon = \sigma^{-1}$) we see that

$$\tau_2(\mathbb{S}_3) \simeq \tau_1(\mathbb{S}_2),$$

which implies that the Knuth orbit of $\mathbb{S}_2$ has size at most three. Similarly when $\mathbb{S} = \mathbb{S}_1$ ($\alpha = \sigma$, $\beta = \sigma^{-2}$, $\gamma = \sigma$ and $\epsilon = \sigma^{-1}$), we get

$$\tau_2(\mathbb{S}_1) \simeq \tau_1(\mathbb{S}_1),$$

which implies that the Knuth orbit of $\mathbb{S}_1$ has size at most two. Thus we conclude that from the four semifields listed by Knuth, for a fixed parameter set $(\mathbb{K}, \sigma, \mu, \eta)$, together with the Knuth operations one can only generate (at most) five isotopy classes of semifields, contained in at most two Knuth orbits and represented by

$$\mathbb{S}_1 \simeq \tau_1\tau_2(\mathbb{S}_1) \simeq \tau_2\tau_1(\mathbb{S}_1) \text{ and } \tau_1\tau_2\tau_1(\mathbb{S}_1) \simeq \tau_2(\mathbb{S}_1) \simeq \tau_1(\mathbb{S}_1)$$

and

$$\mathbb{S}_2 \simeq \tau_1\tau_2\tau_1(\mathbb{S}_2),\ \tau_1(\mathbb{S}_2) \simeq \tau_2\tau_1(\mathbb{S}_2) \text{ and } \tau_2(\mathbb{S}_2) \simeq \tau_1\tau_2(\mathbb{S}_2),$$

since $\mathbb{S}_3 \simeq \tau_1(\mathbb{S}_2)$.

It is possible that $\tau_1(\mathbb{S}_2)$ and $\tau_2(\mathbb{S}_2)$ are both isotopic to $\mathbb{S}_2$. As proven in [4] this occurs if and only if σ^2 is the identity map and $\mu = 0$. In this case the Knuth orbit of $\mathbb{S}_2$ has size one.

If σ^2 is the identity map and $\eta^\sigma = \eta$ then $\mathbb{S}_1$ is isotopic to $\tau_1(\mathbb{S}_1)$. Explicitly the isotopism is given by

$$\begin{aligned} f_1 &: (u,v) \mapsto (u^\sigma, v), \\ f_2 &: (x,y) \mapsto (x^\sigma, y), \\ f_3 &: (a,b) \mapsto (a^\sigma, b), \end{aligned}$$

and it is a simple matter to check that

$$f_1(u,v) \diamond f_2(x,y) = f_3((u,v) \circ (x,y)),$$

where $\diamond$ is multiplication in $\tau_1(\mathbb{S}_1)$ and $\circ$ is multiplication in $\mathbb{S}_1$. There doesn't seem to be any simple argument to determine whether these are the only conditions on σ, μ and η that imply that the Knuth orbit of $\mathbb{S}_1$ has size one.

3. Final Remarks

The fact that $\mathbb{S}_4 \simeq \tau_2(\mathbb{S}_2)$ and hence that $\mathbb{S}_2$, $\mathbb{S}_3$ and $\mathbb{S}_4$ lie in the same Knuth orbit for a fixed parameter set, follows from [8, Section 6] together with [7, Theorem 7.4.1]. We are grateful to one of the referees for this observation and to both referees for their helpful suggestions.

References

[1] S. Ball and M. R. Brown, The six semifield planes associated with a semifield flock, *Adv. Math.*, **189** (2004) 68–87.
[2] M. Cordero and G. P. Wene, A survey of finite semifields, *Discrete Math.*, **208/209**, (1999), 125–137.
[3] P. Dembowski, *Finite Geometries*, Springer, Berlin, 1968.
[4] D. R. Hughes and E. Kleinfeld, Semi-nuclear extensions of Galois fields, *Am. J. Math*, **82** (1960), 389–392.
[5] W. M. Kantor, Commutative semifields and symplectic spreads, *J. Algebra*, **270** (2003) 96–114.
[6] W. M. Kantor, Finite semifields, pp. 103–114 in: Finite Geometries, Groups, and Computation (Proc. of Conf. at Pingree Park, CO Sept. 2005), de Gruyter, Berlin-New York, 2006.
[7] D. E. Knuth, Finite semifields and projective planes, *J. Algebra*, **2** (1965) 182–217.
[8] G. Lunardon, On symplectic spreads, preprint.