Note di Matematica
Note Mat. 1(2008), 125-140
ISSN 1123-2536, e-ISSN 1590-0932
DOI 10.1285/i15900932v28n1p125
http://siba2.unile.it/notemat

Subgeometry partitions from cyclic semifields

Vikram Jha

Mathematics Dept., Caledonian University,
Cowcadden Road,Glasgow, Scotland
vjha267@googlemail.com

Norman L. Johnson

Mathematics Dept., University of Iowa,
Iowa City, Iowa 52242, USA
njohnson@math.uiowa.edu

Received: 15/02/2007; accepted: 20/02/2007.

Abstract. New cyclic semifield planes of order $q^{\mathrm{lcm}(m,n)}$ are constructed. By varying m and n, while preserving the $\mathrm{lcm}(m,n)$, necessarily mutually non-isomorphic semifield planes are obtained. If $\mathrm{lcm}(m,n)/m = 3$, new $GL(2,q^m) - q^{3m}$-planes are constructed. If m is even, new subgeometry partitions in $PG(\mathrm{lcm}(m,n) - 1, q^2)$, by subgeometries isomorphic to either $PG(\mathrm{lcm}(m,n)/2 - 1, q^2)$ or $PG(\mathrm{lcm}(m,n) - 1, q)$ are constructed. If the 2-order of m is strictly larger than the 2-order of n then 'double' retraction is possible producing two distinct subgeometry partitions from the same semifield plane. If m is even and $\mathrm{lcm}(m,n)/m = 3$, new subgeometry partitions may be constructed from the $GL(2,q^m) - q^{3m}$-planes.

Keywords: subgeometry partition, cyclic semifield

MSC 2000 classification: primary 51E23, secondary 51A40

1 Introduction

Let $\boldsymbol{P}$ be a projective space and let $\boldsymbol{S}$ denote a subset of the points. Given any two distinct points A and B of $\boldsymbol{S}$, and let the unique line incident with A and B be denoted by line $\langle A, B\rangle$. Form an incidence geometry of 'points' the elements of $\boldsymbol{S}$ and 'lines' the sets of points $\langle A, B\rangle \cap \boldsymbol{S}$. If this incidence geometry defines a projective space, we say that $\boldsymbol{S}$ is (or becomes) a 'subgeometry' of $\boldsymbol{P}$. A 'subgeometry partition' is a partition of the points of $\boldsymbol{P}$ by a set of subgeometries, mutually disjoint on points.

In this article, we construct various classes of new subgeometry partitions from cyclic semifields. In general, we partition $PG(2kn - 1, q^2)$, into subgeometries of two types, isomorphic to either $PG(kn - 1, q^2)$ or $PG(2kn - 1, q)$.

We recall that a *finite semifield* $\mathbb{S}$ is a finite algebraic structure satisfying all the axioms for a skewfield except (possibly) associativity. The subsets

$$\begin{aligned} N_l &= \{a \in \mathbb{S} \,|\, (ab)c = a(bc),\ \forall b, c \in \mathbb{S}\}, \\ N_m &= \{b \in \mathbb{S} \,|\, (ab)c = a(bc),\ \forall a, c \in \mathbb{S}\}, \\ N_r &= \{c \in \mathbb{S} \,|\, (ab)c = a(bc),\ \forall a, b \in \mathbb{S}\} \end{aligned}$$

and

$$\mathcal{K} = \{a \in N_l \cap N_m \cap N_r \,|\, ab = ba,\ \forall b \in \mathbb{S}\}$$

are fields and are known, respectively, as the *left nucleus*, *middle nucleus*, *right nucleus* and *center* of the semifield. A finite semifield is a vector space over its nuclei and its center (for more details on semifields see [1]). Every semifield is a vector space over the left nucleus, which means that we may switch consideration to the associated 'spread'. The set of lines of the associated affine semifield plane incident with the zero vector. Each such line is uniquely determined by a linear transformation over the left nucleus.

In the present work, we shall be mostly interested in 'cyclic semifields'.

Assume that T is an element of $\Gamma L(m, q)$, which is strictly semilinear and irreducible over $GF(q)$. Then, there is a non-identity automorphism σ of $GF(q)$ such that

$$\alpha T = T\alpha^{\sigma}, \forall \alpha \in GF(q)$$

Let x and y be m-vectors. Then the following defines an additive spread set

$$\begin{aligned} \{\, x = 0, y = x(\alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_{n-1} T^{m-1}); \\ \alpha_i \in GF(q),\ i = 0, 1, 2, \ldots, m-1 \,\}. \end{aligned}$$

When such a spread set occurs, the associated coordinate system becomes a semifield and in this case, we call the structure a 'cyclic semifield plane'. The idea of this construction is due to Jha-Johnson [5, 4].

If $n = 3$, there are connections with a related type of spreads called 'generalized Desarguesian spreads'. Such spreads may be defined as follows: If S_3 is a cyclic semifield plane of order q^3, consider the group G isomorphic to $GL(2, q)$ acting canonically as a matrix group:

$$\left\langle \begin{bmatrix} a & b \\ c & d \end{bmatrix};\ ad - bc \neq 0, a, b, c, d \in GF(q) \right\rangle .$$

If T defines S_3 as above, the following becomes a spread set:

$$\{\, x = 0, y = x\alpha; \alpha \in GF(q) \,\} \cup \{\, (y = xT)g\, ;\ g \in G \,\}.$$

Subgeometry partitions of projective spaces were originally used to construct spreads and therefore translation planes by a 'lifting' process. In particular, in

1976, A. Bruen and J.A. Thas [2] showed that, indeed, it was possible to find subgeometry partitions of the points of $PG(2n-1,q^2)$ by projective subgeometries isomorphic to $PG(n-1,q^2)$'s and $PG(2n-1,q)$'s, sometimes called 'mixed subgeometry partitions'. Bruen and Thas furthermore showed that there is an associated translation plane of order q^{2n} and kernel containing $GF(q)$. Furthermore, there is also a construction using Segre varieties given in Hirschfeld and Thas [3] which generalizes this process and includes what are called 'Baer subgeometry partitions' of $PG(2n,q^2)$, which are partitions of the projective space by only one isomorphism type of projective space, namely by $PG(2s,q)$'s. In this latter case, there is an associated translation plane of order q^{2s+1} and kernel containing $GF(q)$. In either of these situations, we say that the translation plane has been 'lifted' from the subgeometry partition. Since the term 'lifting' is also used in other contexts to mean something entirely different, often the term 'geometric lifting' is used to describe the process of going from a projective subgeometry partition to the translation plane.

The problem is, of course, how to recognize when a finite translation plane has been geometrically lifted from a subgeometry partition of a projective space. It turns out that everything turns on the existence of a certain type of collineation group of order q^2-1 in the translation plane. In Johnson [7], there is an interpretation of the above construction from the viewpoint of the translation plane. That is, starting with a translation plane of a certain type, a 'retraction' method is possible which reverses the construction and produces either a mixed or a Baer subgeometry partition of a projective space. The main consideration is that a group isomorphic to $GF(q^2)^*$ acts as a collineation group of the translation plane, is fixed-point-free (no element fixes any non-zero vector) and the subgroup of order $q-1$ is contained in the kernel of the translation plane. That is, this subgroup fixes each component of the translation plane. Then, if such a collineation groups exists, one may 'retract' to a subgeometry partition of a corresponding projective space that in turn geometrically lifts back to the same translation plane.

Recently, in two articles by Johnson, Marino, Polverino and Trombetti [9, 8], all cyclic semifield spreads of order q^{2n}, are determined, where n is odd, the kernel (left nucleus) is isomorphic to $GF(q^n)$, and the right and middle nuclei are isomorphic to $GF(q^2)$. We may represent any translation plane of order q^{2n}, which contains $GF(q)$ in the kernel of the plane as follows and associated spread $\mathcal{S}$ as follows:

Let V_{4n} be a $4n$-dimensional vector space over $GF(q)$, and let x and y be $2n$-vectors over $GF(q)$. Then the 'points' of the plane are the vectors (x,y) and the lines of the plane are vector translates of the following subspaces:

$$x=0, y=xT;\ T\in\mathcal{S}\,.$$

If we have a semifield spread, the left nucleus corresponds to the zero mapping and collineations of the following form:

$$(x, y) \longmapsto (dx, dy).$$

The right and middle nuclei correspond to the zero mapping and collineations of the following two forms, respectively:

$$(x, y) \longmapsto (x, ya) \text{ and } (x, y) \longmapsto (xb, y),$$

where d, a, b may be considered relative to an inherent coordinate structure or as linear transformations over $GF(q)$. Furthermore, when the right and middle nuclei are equal and isomorphic to $GF(q^2)$, the product of

$$(x, y) \longmapsto (x, ya) \text{ and } (x, y) \longmapsto (xa, y), \text{ for all } a \in GF(q^2),$$

elements define the group elements of a group of order $q^2 - 1$ with exactly the properties required for retraction. However, this is not the only group of order $q^2 - 1$ with the same properties, for we may take the product of

$$(x, y) \longmapsto (x, ya^q) \text{ and } (x, y) \longmapsto (xa, y), \text{ for all } a \in GF(q^2).$$

In particular, call

$$\left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}; \alpha \in GF(q^2)^* \right\rangle = K_\alpha$$

and

$$\left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^q \end{bmatrix}; \alpha \in GF(q^2)^* \right\rangle = K_{\alpha^q}.$$

Both of these groups may be utilized to produce subgeometry partitions of $PG(2n-1, q^2)$, where the subgeometry partitions are necessarily not isomorphic. Furthermore, when $n = 3$, there are two other classes of subgeometry partitions constructed.

All of the particular cyclic semifields used in our constructions are generalizations from similar cyclic semifields of Jha-Johnson [4] of order q^{2kn}, which admit right and middle subnuclei isomorphic to $GF(q^2)$, where the left nucleus contains $GF(q)$. All of these cyclic semifields also produce subgeometry partitions. Furthermore, there are new $GL(2, q) - q^3$-planes that also produce new subgeometry partitions.

2 Semifields of order q^{2kn} with right and middle nuclei $GF(q^2)$

If π is a semifield plane of order q^{2kn}, assume that both the right and middle nuclei have subfields isomorphic to $GF(q^2)$ and that the left nucleus has a subfield isomorphic to $GF(q)$. By the 'fusion' results of Jha and Johnson [6], we first fuse $GF(q)$-into the three nuclei. At this point, we have the right and middle nuclei isomorphic to $GF(q^2)$ and fusing again, we may fuse $GF(q^2)$-into these two nuclei. Hence, by fusion methods, we may assume that we have subnuclei so that the right, middle and left nucleus contains a field, which we simply denote by $GF(q)$. Furthermore, we may assume that the right and middle nuclei share a field, which we denote by $GF(q^2)$. When, this occurs, we represent the semifield plane with spread

$$x = 0,\, y = xM;\; M \in \mathcal{M}\,,$$

where $\mathcal{M}$ is an additive spread set containing the zero and identity linear transformations over $GF(q)$. The associated collineation group of the semifield plane has collineations $(x, y) \longmapsto (x\alpha, y)$ and $(x, y) \longmapsto (x, y\beta)$, where α, β are linear transformations derived from the middle and right nucleus and hence, we may assume that α, β are in the same field of matrices, which again we simply denote by $GF(q^2)$. When this occurs, we consider two groups of matrices

$$K_\alpha = \left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}; \alpha \in GF(q^2) \right\rangle$$

and

$$K_{\alpha^q} = \left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^q \end{bmatrix}; \alpha \in GF(q^2) \right\rangle .$$

Note that the mapping $(x, y) \longmapsto (x\alpha, y\alpha)$, for $\alpha \in GF(q)$, maps $y = xM$, to $y = x\alpha^{-1}M\alpha$. And, since M is a linear transformation over $GF(q)$, considering $\delta \in GF(q)$ as a scalar matrix, it follows that $\alpha^{-1}M\alpha = M$, for all $M \in \mathcal{M}$. Hence, both of the groups K_α, K_{α^q} contain the scalar group of order $q - 1$ that fixes all components of the associated semifield plane. The groups are fixed-point-free and note that $K_\alpha^+ = K_\alpha \cup \{0\}$, and $K_{\alpha^q}^+ = K_{\alpha^q} \cup \{0\}$, for 0 the zero mapping are fields isomorphic to $GF(q^2)$.

Assume that for some $\alpha_0 \in GF(q^2) - GF(q)$ and for some $M \in \mathcal{M}$ that $\alpha_0^{-1}M\alpha_0 = M$. Then write $GF(q^2)$ using α_0 so a typical element is $\alpha_0\beta + \delta$, where $\beta$and δ are in $GF(q)$. Then, it follows easily that M commutes with $GF(q^2)$. Hence, the component orbit lengths under K_α are 1 or $q+1$. Similarly, the component orbit lengths under K_{α^q} are also 1 or $q+1$ (i.e. in the latter case $\alpha_0^{-1}M\alpha_0^q = M$ then $(\alpha_0\beta+\delta)^{-1}M(\alpha_0\beta+\delta) = M$). Hence, we have proved the following theorem:

1 Theorem (Double Retraction Theorem)**.** *Let π be a finite semifield plane of order q^{2kn} whose associated middle and right nuclei contain subnuclei isomorphic to $GF(q^2)$, and whose associated left nucleus contains subnuclei isomorphic to $GF(q)$.*

(1) Then π admits retraction.

(2) If n is odd, π admits double retraction.

(3) In either case, the subgeometries isomorphic to $PG(kn-1,q)$ or $PG(2kn-1,q)$ correspond to the components fixed by the group or in an orbit of length $q+1$, respectively.

3 Cyclic semifields with $GF(q^m)$ as right and middle subnuclei

In this section, we consider cyclic semifields of order $q^{\mathrm{lcm}(m,n)=\ell}$, where it is assumed that T is an element of $\Gamma L(\ell/m, q^m)$, which is strictly semilinear and irreducible over $GF(q^m)$. Then, there is a non-identity automorphism σ of $GF(q^m)$ such that

$$\alpha T = T\alpha^{\sigma}, \forall \alpha \in GF(q^m)\,.$$

Let x and y be ℓ/m-vectors. Then the following set defines an additive spread set and hence a cyclic semifield plane of order q^ℓ:

$$\{\, x=0, y = x(\alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_{n-1}T^{\ell/m-1});\\ \alpha_i \in GF(q^m),\ i = 0,1,2,\ldots,\ell/m-1\,\}.$$

Note that the mappings $(x,y) \longmapsto (x\alpha, y)$ and $(x,y) \longmapsto (x, y\beta)$, for $\alpha, \beta \in GF(q^m)$ are collineations of the associated translation planes since $(x,y) \longmapsto (x\alpha, y)$ maps

$$\begin{aligned} y &= x(\alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_{\ell/m-1}T^{\ell/m-1}) \text{ to} \\ y &= x(\alpha^{-1}\alpha_0 + \alpha^{-1}\alpha_1 T + \alpha^{-1}\alpha_2 T^2 + \cdots + \alpha^{-1}\alpha_{\ell/m-1}T^{\ell/m-1}) \end{aligned}$$

and $(x,y) \longmapsto (x, y\beta)$ maps

$$\begin{aligned} y &= x(\alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_{n-1}T^{\ell/m-1}) \text{ to} \\ y &= x(\alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_{n-1}T^{\ell/m-1})\beta = \\ y &= x(\alpha_0\beta + \alpha_1\beta^{\sigma^{-1}}T + \alpha_2\beta^{\sigma^{-2}}T^2 + \cdots + \alpha_{n-1}\beta^{\sigma^{-(\ell/m-1)}}T^{\ell/m-1}). \end{aligned}$$

3.1 New constructions of cyclic semifield planes

In this subsection, we generalize the so-called Jha-Johnson cyclic semifields of type $S(\omega; m; n)$.

Let $\ell= lcm(m; n)$, where $m; n > 1$ are integers, neither of which divides the other, so $\ell >$max$\{m, n\}$.

Define the following mapping

$$T : xT = x^{q^n}\omega,$$

where ω is a primitive element of $GF(q^\ell)$. Then a cyclic semifield is obtained (see Jha and Johnson [4], p. 16). It turns out that the middle and right nucleus share a subfield isomorphic to properly $GF(q^{\ell/n})$ and the left nucleus (the kernel of the semifield plane) is isomorphic to $GF(q^n)$.

This class of cyclic semifields is called the 'Jha-Johnson cyclic semifields of type $S(\omega; m; n)$'.

When $m = 2$ and n is odd, this class of semifields is generalized by Johnson, Marino, Polverino and Trombetti in [8], [9], where it is shown that any mapping $T_b : xT_b = x^{q^n}b$, such that b^{q^n+1} is not in any proper subfield of $GF(q^n)$, also produces a cyclic semifield. More generally, we construct a variety of new cyclic semifields as follows.

2 Theorem. *For m and n arbitrary integers, neither of which divides the other and let $\ell = \mathrm{lcm}(m, n)$, define*

$$T_b : xT_b = x^{q^n}b;\ b^{(q^\ell-1)/(q^n-1)}$$

is not in any proper subfield of $GF(q^n)$.

(1) Then T_b is strictly semilinear and irreducible over $GF(q^m)$.

(2) Hence, T defines a cyclic semifield $S(b; m, n)$, where the right and middle nuclei share a subfield isomorphic to $GF(q^m)$, the right, middle, and left nuclei share a subfield isomorphic to $GF(q)$, and the left nucleus is isomorphic to $GF(q^n)$.

In this setting,

$$\alpha T_b = T_b\alpha^{q^n}, \textit{ for } \alpha \in GF(q^m).$$

Proof. We note that $T_b : F \to F$, where $F = GF(q^{\mathrm{lcm}(m,n)})$. Let $q = p^r$, for p a prime. We need to show that T_b is irreducible when F is considered a vector space over $GF(q^m)$. Let $\ell = \mathrm{lcm}(m, n)$. We note that

$$xT_b^{\ell/n} = xb^{(q^\ell-1)/(q^n-1)}.$$

Since $c = b^{(q^\ell-1)/(q^n-1)}$ is not in any proper subfield of $GF(q^n)$, it follows immediately that the module generated by $\langle c\rangle$ and $GF(p)$ is $GF(q^n)$. Now assume that W is a proper subspace over $GF(q^m)$ that is T_b-invariant. Then the remarks directly preceding the theorem show that W is also a $GF(q^n)$-subspace. Therefore, W is a module over the ring generated by $GF(q^n)$ and $GF(q^m)$, which is clearly $GF(q^{\mathrm{lcm}(m,n)})$. Hence, W is a F-vector space, but since W is a subset of F, it follows that $W = F$, a contradiction. Therefore, T does not admit any non-trivial irreducible $GF(q^m)$-submodules W, since $Wc = W$.

Now we may consider T as an element of $\Gamma L(\ell/m, q^m)$. This and our previous remarks complete the proof. $\boxed{QED}$

4 New $GL(2,q) - q^3$ planes

From every cyclic semifield of order q^3, it is possible to construct an associated plane of order q^3 admitting $GL(2,q)$. For integers m and n neither of which divides the other, we let $\ell = \mathrm{lcm}(m,n)$, and assume that $3 = \ell/m$. Consider one of the cyclic semifield planes $S(b;m,n)$ of order $q^\ell = q^{3m}$, with spread

$$x = 0, y = x(\alpha_0 + \alpha_1 T + \alpha_2 T^2); \alpha_i \in GF(q^m).$$

Then, there is a corresponding plane defined as follows: Let

$$G = \left\langle \begin{bmatrix} \alpha & \beta \\ \delta & \gamma \end{bmatrix}; \alpha\gamma - \beta\delta \neq 0, \alpha, \beta, \delta, \gamma \in GF(q^m)^* \right\rangle,$$

isomorphic to $GL(2,q^m)$. The following is a spread:

$$x = 0, y = x\alpha, (y = xT)g; \alpha \in GF(q^m), g \in G$$

called the $GL(2,q^m) - q^{3m}-$spread constructed from $S(b;m,n)$. The kernel of this plane is $GF(q^n)$. Let $m = 3^a m^*$, where $(3, m^*) = 1$ and $n = 3^{a+1}n^*$, then $\mathrm{lcm}(m,n) = 3^{a+1}(m^*, n^*)$. If n^* divides m^* then $\ell/m = 3$. this means that we may construct cyclic semifields of order q^{3m} with kernel $GF(q^{3^{a+1}z})$, where z divides m^*. The associated $GL(2,q^m) - q^{3m}$-spreads with different kernel are necessarily not isomorphic.

3 Theorem. *Let π_i be a cyclic semifield plane of order q^{3m} of type $S(b_i; m, n)$. Let $J(\pi_i)$ denote the associated $GL(2,q^m) - q^{3m}$-translation plane, for $i = 1, 2$. Then π_1 is isomorphic to π_2 if $J(\pi_1)$ is isomorphic to $J(\pi_2)$.*

Proof. Assume that T_i are the functions constructing $S(b_i; m, n)$ and form the associated $J(\pi_i)$, planes. These planes have two orbits under $GL(2,q^m)$, one orbit

$$\{\, x = 0, y = x\alpha;\ \alpha \in GF(q^m)\,\}$$

and the remaining orbit

$$\{(y = xT_i)g; g \in G\},$$

where

$$G = \left\langle \begin{bmatrix} \alpha & \beta \\ \delta & \gamma \end{bmatrix}; \alpha, \beta, \delta, \gamma \in GF(q^m); \alpha\gamma - \beta\delta \neq 0 \right\rangle \simeq GL(2, q^m).$$

It is clear that any isomorphism of $J(\pi_1)$ onto $J(\pi_2)$ must preserve the two orbits due to the action of G (that is, $SL(2, q^m)$ is generated by elations and as such is a normal subgroup of the full collineation group). Therefore, we may regard that any isomorphism necessarily maps T_1 onto T_2, thereby inducing an isomorphism from π_1 onto π_2. $\boxed{QED}$

5 New subgeometry partitions

We note the following consequences of Theorem 2.

4 Theorem. *$S(b, 2k, n)$, for neither $2k$ or n dividing the other, is a cyclic semifield of order $q^{\mathrm{lcm}(2k,n)} = q^{\ell}$.*

Generally, the right and middle nuclei contain $GF(q^{2k})$, the left nucleus is $GF(q^n)$ and the right, middle and left nuclei contain $GF(q^{(2k,n)})$.

5 Corollary. *Then the semifield admits as a collineation group*

$$G = \left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^q \end{bmatrix}; \alpha \in GF(q^2)^*. \right\rangle$$

This group is fixed-point-free, contains the kernel subgroup of order $q - 1$ and G union the zero mapping is a field isomorphic to $GF(q^2)$.

Hence, there is a corresponding subgeometry partition relative to G. In this setting, we obtain subgeometry partitions of $PG(\ell - 1, q^2)$ by subgeometries isomorphic to $PG(\ell/2 - 1, q^2)$ and $PG(\ell - 1, q)$, corresponding to orbits of lengths 1 and $q + 1$, respectively.

Proof. Certainly when α is in $GF(q)$, $\alpha^q = \alpha$, since $GF(q^{(2k,n)})$ contains $GF(q)$, this means the when $\alpha^q = \alpha$, we have the group in the kernel homology group. The rest of the proof follows immediately. $\boxed{QED}$

6 Theorem. *Under the assumptions of the previous theorem, let the maximum power of 2 dividing k be denoted by k_2. If $n_2 < m_2$ then the semifield admits double retraction to two distinct proper subgeometry partitions.*

7 Remark. The retraction partitions of the previous two theorems may occur in a variety of ways.

The particular subgeometries may be easily determined from the various cyclic subgroups.

Some examples will make the ideas clear.

8 Example. Let $m = 8$ and $n = 12$. Hence, we have a vector space of dimension 48 over $GF(q)$.

(i) There are two non-kernel groups of order $q^8 - 1$ containing a kernel subgroup of order $q^4 - 1$:

$$\begin{aligned} G_8' &= \left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}; \alpha \in GF(q^8)^* \right\rangle, \\ G_8 &= \left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{q^4} \end{bmatrix}; \alpha \in GF(q^8)^* \right\rangle. \end{aligned}$$

Both of these groups retract the semifield spread to subgeometry partitions of $PG(5, q^8)$ by subgeometries isomorphic to $PG(2, q^8)$ or $PG(5, q^4)$.

(ii) There is one non-kernel group of order $q^4 - 1$ containing a kernel subgroup of order $q^2 - 1$:

$$G_4 = \left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{q^2} \end{bmatrix}; \alpha \in GF(q^4)^* \right\rangle.$$

This group retracts the semifield spread to a subgeometry partition of $PG(11, q^4)$ by subgeometries isomorphic to $PG(5, q^4)$ or $PG(11, q^2)$.

(iii) There is one non-kernel group of order $q^2 - 1$ containing a kernel subgroup of order $q - 1$:

$$G_2 = \left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{q} \end{bmatrix}; \alpha \in GF(q^2)^* \right\rangle.$$

This group retracts the semifield spread to a subgeometry partition of $PG(23, q^2)$ by subgeometries isomorphic to $PG(11, q^2)$ or $PG(23, q)$.

(iv) Let $q = p^r$. Take any subgroup of order $p^{2t} - 1$ where t divides r, then we have a vector space of dimension $48r$ over $GF(p)$, we have a kernel subgroup of order $q^6 - 1$, so we have a kernel subgroup of order $p^{(2t,6r)} - 1 = p^{2t} - 1$, we may take the group

$$G_{2t} = \left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{q} \end{bmatrix}; \alpha \in GF(q^2)^* \right\rangle.$$

This group retracts the semifield spread to a subgeometry partition of $PG(24r/t-1,p^{2t})$ by subgeometries isomorphic to $PG(12r/t-1,p^{2r})$ or $PG(24r/t-1,p^{t})$.

6 More new subgeometry partitions

From every cyclic semifield of order q^3, we constructed an associated plane of order q^3 admitting $GL(2,q)$. For integers m and n neither of which divides the other, we let $\ell = \mathrm{lcm}(m,n)$, and assume that $3=\ell/m$. Consider one of the cyclic semifield planes $S(b;m,n)$ of order $q^\ell = q^{3m}$, with spread

$$x=0, y=x(\alpha_0+\alpha_1 T+\alpha_2 T^2); \alpha_i \in GF(q^m).$$

Then, there is a corresponding plane defined as follows: Let

$$G=\left\langle \begin{bmatrix} \alpha & \beta \\ \delta & \gamma \end{bmatrix}; \alpha\gamma-\beta\delta \neq 0, \alpha,\beta,\delta,\gamma \in GF(q^m)^* \right\rangle.$$

Now, of course, when $\beta=\delta=0$, and $\gamma=\alpha^\sigma$, for all $\alpha \in GF(q^m)^*$, σ an automorphism of $GF(q^m)$. Suppose that m is even, so that

$$G_\sigma=\left\langle \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^\sigma \end{bmatrix}; \alpha \in GF(q^2)^* \right\rangle,$$

The kernel of this plane is $GF(q^n)$. Let $m=3^a m^*$, where $(3,m^*)=1$ and $n=3^{a+1}n^*$, then $\mathrm{lcm}(m,n)=3^{a+1}(m^*,n^*)$. If n^* divides m^* then $\ell/m=3$. this means that we may construct cyclic semifields of order q^{3m} with kernel $GF(q^{3^{a+1}z})$, where z divides m^*. The associated $GL(2,q^m)-q^{3m}$-spreads with different kernel are necessarily not isomorphic.

The right, and middle nuclei of the original cyclic semifield share $GF(q^m)$ and the kernel is $GF(q^n)$. In this planes, the kernel is still $GF(q^{3^{a+1}z})$. In any case, if σ is q above, then G_σ contains the kernel homology group of order $q-1$.

9 Theorem.

(1) In the above setting, if σ is q, we have a group producing retraction.

(2) If n is odd then taking $\sigma=1$, gives another group producing retraction.

(3) Also, there are many variations of smaller groups giving subgeometry partitions.

For example, if $n_2<m_2$, again at least two groups produce distinct subgeometry partitions.

Hence, we also obtain a variety of new subgeometry partitions from $GL(2,q^n)-q^{3m}$-spreads.

7 Isomorphisms

We have constructed a wide variety of new cyclic semifield planes and also new $GL(2,h)-h^3$-planes, but we have not yet discussed isomorphisms. However, we have seen that non-isomorphic $GL(2,h)-h^3$ planes lead to non-isomorphic cyclic semifield planes.

We begin with the cyclic semifield planes. For m and n arbitrary integers, neither of which divides the other and let $\ell = \mathrm{lcm}(m,n)$, define

$$T_b : xT_b = x^{q^n}b;\ b^{(q^\ell-1)/(q^n-1)}$$

Basically, there are three parameters m, n, and b. By varying m and n we may achieve the same order q^ℓ and change the kernel $GF(q^n)$ and or right and middle nuclei $GF(q^m)$. Since the order of the nuclei are invariant under isomorphisms, we would obtain a number of mutually non-isomorphic semifields simply by this observation. Furthermore, then by fixing the orders of the left, right and middle nuclei and then by varying b, we would also obtain another variety of mutually non-isomorphic semifields.

7.1 The two-dimensional cyclic semifields

For example, in the latter case, suppose that $\mathrm{lcm}(m,n) = 2n$.

For example, we may let n be odd and $m = 2$. This is the setting considered in Johnson, Marino, Polverino and Trombetti in [8, 9]. In the second article, when $n = 3$, there are associated $GL(2,q^2)-q^6$-Planes. These planes are also determined by Kantor [10], and the isomorphisms are completely determined. Since we have seen that the number of isomorphism classes of cyclic semifield planes of order q^6 with kernel $GF(q^3)$ with right and middle nuclei $GF(q^2)$ is as least as large as the number of isomorphism classes of the associated $GL(2,q^2)-q^6$-planes, we obtain an easy bound for such cyclic semifield planes.

But, actually there are many other planes where $\mathrm{lcm}(m,n) = 2n$, where $m = 2^{a+1}m^*$, $(m^*,2) = 1$, and $n = 2^a n^*$, $(n^*,2) = 1$ and m^* dividing n^*. For example, for $m = 8, n = 12$, we have order q^{24}, with kernel $GF(q^{12})$ and right and middle nucleus $GF(q^8)$. The order of the associated mapping T is ℓ/m, so that again in this case, we have a $GL(2,q^8)-q^{24}$-plane.

10 Theorem. *In general, we have a complete determination of the Kantor planes of orders h^6 with kernel $GF(h^3)$ by the construction of the cyclic semifields $S(b,m,n)$, where $\mathrm{lcm}(m,n) = 2n$, for various values of b. By applying the method of Jha-Johnson to theses cyclic semifields, there are constructions of associated $GL(2,q^n)-q^{3n}$ planes.*

In an oblique way, we may count the number of mutually non-isomorphic cyclic semifields of order q^ℓ, where $\ell = \mathrm{lcm}(m,n) = 2n$ and $\ell/m = 3$ so that $2n = 3m$ by noting Theorem 3 and applying the work of Kantor [10]. This theorem is also proved for the special case that n is odd and $m = 2$ in Johnson, Polverino, Marino, Trombetti [8]. Furthermore, again when n is odd and $m = 2$, the converse to Theorem 3 is also proved in the same paper. Moreover, in general when n is odd and $m = 2$, the number of mutually non-isomorphic cyclic semifields plane is determined. For our purposes, we concentrate only on the cyclic semifield planes of cubic order. Therefore, we formally record the following.

11 Theorem. *Let* $\mathrm{lcm}(m,n) = 3m = 2n$*. Consider the class of all cyclic semifield of order* $q^{3m} = q^{2n}$ *with kernel* $GF(q^n)$ *and right and middle nuclei containing* $GF(q^m)$*. Then the number of non-isomorphic cyclic semifield planes is at least*

$$\frac{(q^{m/2}+1)q^{\frac{m}{2}}}{6s},$$

where $q = p^r$*, and* $s = \frac{rm}{2}$*.*

7.2 Mutually non-isomorphic planes by varying the nuclei

We may choose a tremendous variety of non-isomorphic cyclic semifield planes of the same order q^ℓ with kernel $GF(q^n)$ as follows: Let m and n have prime decomposition as follows:

$$m = \Pi_{i=1}^{t} p_i^{m_i},\ n = \Pi_{i=1}^{t} p_i^{n_i},$$

where m_i and n_i are non-negative integers. Noting that $\ell = \ell cm(m,n) = \Pi_{i=1}^{t} p_i^{\max(m_i,n_i)}$, we can achieve the same order q^ℓ and obtain a tremendous of mutually non-isomorphic translation planes simply by varying m and n and maintaining the $\mathrm{lcm}(m,n)$.

12 Remark. If m is even we also produce new subgeometry partitions.

13 Remark. If $\ell/m = 3$, we also construct new $GL(2,h) - h^3$-planes.

14 Remark. In addition, when m is even and $\ell/m = 3$, we may construct subgeometry partitions from the associated $GL(2,h) - h^3$-planes.

15 Remark. If we choose m and n to preserve the lcm and have the 2-order of m strictly larger than the 2-order of n, then we may retract in at least two ways to produce non-isomorphic subgeometry partitions.

So, we may choose m and n so that $\max(m_i, n_i)$ is an invariant for all m_i, $i = 1, 2, \ldots, t$ and as long as the condition that neither m nor n divide the other, we obtain a proper cyclic semifield. So, the larger the number of prime factors in

$\Pi_{i=1}^{t}p_i^{\max(m_i,n_i)}$, the larger the number of necessarily mutually non-isomorphic semifields with different orders of nuclei.

An example will be helpful here.

16 Example. (1) Suppose the idea is to construct a cyclic semifield which may be doubly retracted. Then, we would choose the 2-order of m strictly larger than the 2-order of n. Take $\mathrm{lcm}(m,n)=2^2\ \cdot 3\cdot 5\cdot 7$. Then the only restriction on m is that 4 divide m but not divide n.

Then $n=2^{n_1}\cdot 3^{n_2}\cdot 5^{n_3}\cdot 7^{n_4}$, and the n_i may be chosen in any of 2 ways (0 or 1) for each i, for 16 possible choices for n. Note that m_1 must always be 2. Whenever n_j, for j is 1, then m_j may be chosen in any of 2 ways $(0,1)$.

We choose the number of 1 for the n_i, i not 1, as follows: There are $\sum\sum_{k=1}^{3}\binom{4}{k}2^k$ ways to choose m and n to preserve the lcm when n_1 is 0 and the same number when $n_1=1$. Hence, there are

$$2\sum\sum_{k=0}^{3}\binom{3}{k}2^k=54$$

necessarily mutually non-isomorphic cyclic semifields of order $q^{2^2\cdot 3\cdot 5\cdot 7}$ obtained simply by varying the orders of the nuclei, each of which leads to mutually non-isomorphic subgeometry partitions.

(2) Suppose now that $\mathrm{lcm}(m,n)=2\cdot 3\cdot 5\cdot 7$, choose a prime to divide one of m or n but not the other in any of $4\cdot 2$ ways. Now choose n_i to be 1 so that m_i could take on any of 2 choices. Hence, in this setting there are

$$8\sum\sum_{k=0}^{3}\binom{3}{k}2^k=216$$

mutually non-isomorphic cyclic semifield planes of order $q^{2\cdot 3\cdot 5\cdot 7}$.

More generally, assume that we have a number $\ell=\Pi_{i=1}^{t}p_i^{\alpha_i}$, which is to be a $\mathrm{lcm}(m,n)$, and where is required that neither m nor n divides the other. Then the number of choices for n is $\Pi_{i=1}^{t}(\alpha_i+1)$ and m has the same number of choices and these choices for m are independent of the choices for n except for the given condition that neither m nor n divides the other. Note if n_i is not α_i, then m_i must be α_i. The number of associated mutually non-isomorphic cyclic semifields therefore grows in proportion.

For example, if all $\alpha_i's$ are 1, we may give a count. Choose a prime p_{i_0} to divide either m or n but not both, in $2t$ ways. Then choose the number of n_i equal to 1. For each such choice, there are 2 choices for m_i.

17 Theorem. *Consider cyclic semifields of order $q^{\Pi_{i=1}^{t}p_i}$, there are at least*

$$2t\sum_{k=0}^{t-1}\binom{t-1}{k}2^k$$

mutually non-isomorphic cyclic semifields of the same order.

8 Final comments

In this article, we have constructed a variety of new cyclic semifield planes of order $q^{\mathrm{lcm}(m,n)}$, where m and n are positive integers neither of which divides the other. When $\mathrm{lcm}(m,n)/m = 3$, there is a corresponding translation plane of order h^3 admitting $GL(2,h)$ as a collineation group, that is called a $GF(2,h) - h^3$-plane. When m is even, we may also construct new subgeometry partitions by finding an appropriate group of order $q^2 - 1$ containing a subkernel homology group of order $q - 1$. There are usually at least two such groups producing so-called 'double retraction' to projective spaces admitting subgeometry partitions. Often, we do not mention the groups possible, but these are easily determined. Furthermore, the orbits of lengths $q + 1$ and 1 are also easily determined, giving the numbers of subgeometries of each type. When the group is other than simply of order $q^2 - 1$, for example, $q^4 - 1$, the orbits of length $q^2 + 1$ and 1 and similarly easily determined.

What is not probably so easy is to determine the number of mutually non-isomorphic cyclic semifield planes to each other obtained. Although, some results on isomorphism classes for planes of order q^6 and order q^{2n}, for n odd, are obtained in Johnson, Marino, Polverino and Trombetti in [8], [9].

On the other hand, when $\mathrm{lcm}(m,n) = 2n$, we have given some isomorphism conditions and in general the large number of choices of m and n to achieve the same $\mathrm{lcm}(m,n)$, will produce non-isomorphic semifield planes for each choice.

What we have not then done is to consider what the isomorphisms are when b is varied in $S(b;m,n)$, leaving m and n fixed.

18 Problem. Therefore, we leave as an open problem to determine the isomorphism classes of the new cyclic semifields $S(b;m,n)$, in general, obtained by varying b and fixing m and n.

References

[1] M. Biliotti, V. Jha, N. L. Johnson: Foundations of Translation Planes, Monographs and Textbooks in Pure and Applied Mathematics, vol. 243, Marcel Dekker Inc., New York 2001.

[2] A. A. Bruen, J. A. Thas: *Partial spreads, packings and Hermitian manifolds in* $\mathrm{PG}(3,q)$, Math. Z., **151**, n. 3 (1976), 207–214.

[3] J. W. P. Hirschfeld, J. A. Thas: General Galois Geometries, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York 1991.

[4] V. Jha, N. L. Johnson: *An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem*, Algebras Groups Geom., **6**, n. 1 (1989), 1–35.

[5] V. Jha, N. L. Johnson: *Translation planes of large dimension admitting nonsolvable groups*, J. Geom., **45**, n. 1–2 (1992), 87–104.

[6] V. Jha, N. L. Johnson: *Nuclear fusion in finite semifield planes*, Adv. Geom., **4**, n. 4 (2004), 413–432.

[7] N. L. Johnson: *Retracting spreads*, Bull. Belg. Math. Soc. Simon Stevin, **8**, n. 3 (2001), 505–524.

[8] N. L. Johnson, G. Marino, O. Polverino, R. Trombetti: *On a generalization of cyclic semifield spreads*, preprint.

[9] N. L. Johnson, G. Marino, O. Polverino, R. Trombetti: *Semifield spreads of* $PG(3,q^3)$ *with center* F_q, (submitted).

[10] W. M. Kantor: *Translation planes of order* q^6 *admitting* $\mathrm{SL}(2,q^2)$, J. Combin. Theory Ser. A, **32**, n. 2 (1982), 299–302.