The dimension of a subplane of a translation plane

V. Jha N.L. Johnson*

Abstract

It is shown that the commutative binary Knuth semifield planes of order 2^n, for $n = 5k$ or $7k$ and k odd, their transposes and transpose-duals admit subplanes of order 2^2. In addition, many of the Kantor commutative semifield planes of order 2^{5k} or 2^{7k} also admit subplanes of order 4.

Furthermore, a large number of maximal partial spreads of order p^k and deficiency at least $p^k - p^{k-1}$ or translation planes of order p^k are constructed using direct sums of matrix spreads sets of different dimensions. Given any translation plane π_0 of order p^d, there is either a proper maximal partial spread of order p^{c+d} whose associated translation net contains a subplane of order p^d isomorphic to π_0 or there is a translation plane of order p^{c+d} admitting a subplane of order p^d. Other than the semifield planes mentioned above and a few sporadic planes of even order, there are no other known translation planes of order p^{c+d} admitting a subplane of order p^d, where d does not divide c.

1 Introduction.

In this article, we are interested in the so-called "subplane dimension question," which concerns finite translation planes π of order p^t. If π_0 is an affine subplane, it follows that it is a translation plane of order p^k. The question that is considered here is whether k divides t. For example, if π is a Desarguesian plane coordinatized by a finite field isomorphic to $GF(p^t)$ then any affine subplane π_0 is also Desarguesian and may be coordinatized by a subfield isomorphic to $GF(p^k)$, so k

*The authors are grateful to the referee for many helpful comments and suggestions regarding the writing and style of this article.

Received by the editors October 2008 - In revised form in January 2009.

Communicated by J. Thas.

does divide t in this case. More generally, if a finite translation plane π of order p^t admits a collineation of order p that fixes an affine subplane π_0 of order p^k pointwise, then Foulser [2] has shown that k must, in fact, divide t.

Consider now the subplane dimension question in finite semifield planes of order p^t. In this setting, G.P. Wene [8] pointed out to the authors that there is a semifield plane of order 2^5 that admits subplanes of order 4. Furthermore, in very recent work, Wene has found several sporadic semifields of various orders 2^j, for $j = 5, 7, 9, 11$, that admit subplanes of order 4. On the other hand, in spite of the fact that there are a wide variety of semifield planes and, of course, a much wider variety of translation planes, these few examples are the only known translation planes where the subplane dimension question cannot be answered in the affirmative. Therefore, in this article, we concentrate on the question for semifield planes and ask if there is an infinite class of semifield planes or whether there are just these few examples that violate the subplane dimension principle.

The background required to read this article takes two forms. First of all, we will be dealing with coordinate systems 'quasifields' of translation planes. A semifield plane has a coordinate quasifield that is a non-associated division ring called a 'semifield'. The first part of the paper deals with semifields. In particular, we shall be working in semifields of even order of order 2^t, t odd, when showing that there are interesting and unusual subsemifields of order 2^2 that occur in two well known infinite classes. The second part of this paper deals with the more geometric aspects of semifield planes. Translation planes coordinatized by semifields admit (necessarily elementary Abelian) an elation group E which fixes one parallel class and acts transitively on the remaining parallel classes. What this means is that the associated 'spread' is additive. We exploit ideas of 'additive partial' spreads to show how exotic subplanes might be constructed. So, before we discuss our results, we offer a little background detailing the ideas of spreads and quasifields.

Definition 1. *Let V_{2t} denote a $2t$-dimensional vector space over a field K isomorphic to $GF(q)$, where $q = p^r$, for p a prime and r a positive integer. Then a 'partial t-spread' of V_{2t} is a set of mutually disjoint (as subspaces) t-dimensional vector subspaces. A 't-spread' of V_{2t} is a partial spread consisting of $\frac{q^{2t}-1}{q^t-1} = q^t + 1$ t-dimensional vector subspaces, which then forms an exact cover of the non-zero vectors of V_{2t}. The terms 'partial spread' and 'spread' are used when the context is clear.*

Definition 2. *Given a partial spread $\mathcal{P}$ in V_{2t}, the point-line geometry of 'points' as vectors and 'lines' as vector translates of the subspaces of $\mathcal{P}$ is said to be a 'vector translation net' or a 'translation net', if the context is clear. If the partial spread is a spread, the translation net becomes an affine plane of order q^t; a 'translation plane' of order q^t.*

The elements of a partial spread or spread are called 'components'.

Remark 1. *In this article, a 'subplane' of a translation net or translation plane is always considered to be an affine subplane and a translation net or translation plane is always considered to be an affine structure (plane).*

However, there is a major exception to the convention in the previous remark.

Definition 3. *If an affine translation plane π is extended to a projective plane π^+ by the natural adjunction of line ℓ_∞ (line at infinity), the projective plane π^+ is now said to be a 'translation plane with respect to ℓ_∞.*

Considering the dual projective plane of π^+, $D(\pi^+)$, we use the terminology 'dual translation plane with respect to (∞)', where (∞) is ℓ_∞ considered as a point.

Now we consider the special situation where π is a semifield plane.

Remark 2. *If π is a semifield plane then the projective extension π^+ admits 'elation groups' with center any infinite point of π and axis ℓ_∞ and if π is not Desarguesian, there is a unique infinite point (∞) on ℓ_∞, such that the projective plane admits elation groups with axis any line incidence with (∞) and with center (∞). Therefore, in the dualization process if we allow that (∞) is interchanged with ℓ_∞, it is then clear that the dual projective plane of a projective semifield plane is also a projective semifield plane.*

Furthermore, is also possible to consider the 'dual semifield plane' in the following way.

Remark 3. *If a coordinate structure $(Q, +, \cdot)$ for a semifield plane π is given, then it turns out that a coordinate structure for the affine semifield plane obtained from the natural affine restriction of the dual projective semifield plane π^+ is $(Q, +, \circ)$, where the two multiplications are related as $a \cdot b = b \circ a$.*

Therefore, when we consider the 'dual' of a semifield plane, we may consider this as an 'affine' semifield plane.

We shall also consider the 'transpose' of a semifield plane, which is also a semifield plane. This concept originates implicitly with Knuth [5] and furthermore explicated by Johnson in [3]. Also, see Maduram [6].

Definition 4. *Let π be a translation plane of order q^t obtained from a spread S of V_{2t} over K isomorphic to $GF(q)$. Given three components S, T, U, a basis may be chosen for the V_{2t} so that representing vectors in the form $(x_1, x_2, ..., x_t, y_1, y_2, ..., y_t)$, for $x_i, y_i \in K$ and such that*

S is the space of vectors where $x_1 = x_2 ... = x_t = 0$,

T is the subspace of vectors where $y_1 = y_2 ... = y_t = 0$, and

U is the subspace of vectors where $x_i = y_i$, for $i = 1, 2, ..., t$.

When a basis is so chosen, the remaining components of S may be represented in the form $\{(x, xM); x \text{ is any } t\text{-vector}\}$, where M is a non-singular $t \times t$-matrix with entries from K. Furthermore, given any two distinct $t \times t$-matrices corresponding to components, the difference is also non-singular. Hence, we may represent the spread for π in the form

$$(*) : \{(0, y); y \text{ is any } t\text{-vector}\}, \{(x, 0); x \text{ is any } t\text{-vector}\} \text{ and}$$
$$\{(x, y); y = xM, \text{for all } t\text{-vectors}\}, \text{ where } M \in S_{mat},$$

where S_{mat} is a set of $q^t - 1$ non-singular matrices that contains I_t (the identity matrix) and such that the difference of any distinct pair of matrices is also non-singular.

Remark 4. *If we represent the spread using $(*)$ of Definition 4, we shall say that the spread has a 'standard -matrix representation'. In this case, we also shall use a shorthand version of the spread as*

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

In the above setting, for a spread S of a translation plane π, an associated set S_{mat} of $t \times t$-matrices is said to be a 'matrix spread set' of π. When π is a semifield plane, and $\{(0, y); y \text{ is any } t\text{-vector}\}$ is the axis for an elation group (unique if π is not Desarguesian), it is customary to include the zero matrix 0_t in the set S_{mat} since $S_{mat} \cup \{0_t\}$ is an elementary Abelian p-group of order q^t, for $q = p^r$, in this case.

Remark 5. *Using the representation in $(*)$ of Definition 4, the transposed semifield plane is obtained by replacing the matrices in S_{mat} by their transposed matrices. Therefore, we refer to this semifield plane as the 'transposed semifield plane' of the original semifield plane.*

Considering the projective space corresponding to the lattice of subspaces of the associated vector space, it is also known that the transposed plane corresponds to a polarity of the corresponding projective space (see e.g. Johnson [3]).

Remark 6. *It is straightforward to show that given any semifield plane of order 2^r admitting a subplane of order 2^k, then the transposed semifield plane and the transposed dual semifield plane also admit affine subplanes of order 2^k.*

In this article, we show that there are at least two infinite classes of semifield planes of order 2^n, for n odd that admit Desarguesian subplanes of order 2^2, thus resolving the question in the even order case. All of the examples are for semifield planes of even order that may be coordinatized by commutative semifields. In particular, we show that there are isotopes of the commutative binary Knuth presemifields of orders 2^{tk}, for k odd and $t = 5$ or 7 that admit subfields of order 2^2. The Kantor commutative semifields [4] are generalizations of the binary Knuth commutative semifields and many of the isotopes of the Kantor commutative semifields of orders 2^{5k} or 2^{7k}, for k odd, also admit fields of order 4.

For a finite translation plane, the set of lines through the origin is called the 'spread' for the plane and if p^t is the order of the plane we may use the term 't-spread' for clarity and all elements of the spread are t-dimensional $GF(p)$-vector subspaces. It is, of course, possible if s divides t, that the spread can be an s-spread, as well. A 'maximal partial t-spread' is then simply a set of mutually disjoint t-dimensional subspaces that cannot be extended to a partial t-spread.

For this article, apart from the semifield planes mentioned above, if we take as an assumption that the subplane dimension question can always be answered affirmatively, we then are able to show how this assumption leads to a large variety of maximal partial spreads. An 'additive partial spread' is a partial spread with coordinatization into a set of matrices S_{Mat}, which is an elementary Abelian p-group. If the group has order p^k then the number of partial spread elements is $p^k + 1$. In this article, we give a simple construction of additive partial spreads of $1 + p^d$ elements, of order p^{d+c}, where d does not divide c, such that the partial spread contains a semifield subplane of order p^d. We show that any such additive

partial spread can be extended to an additive maximal partial spread or can be extended to a semifield. Note in the latter case, this would construct a semifield plane of order p^{d+c} that contains a semifield subplane of order p^d, where d does not divide c.

2 Subfields of order 4 in the Commutative Binary Knuth Semifields.

Let $x, y \in GF(2^n)$, for n odd, then the following defines the multiplication for a commutative pre-semifield due to Knuth, called the "commutative binary Knuth pre-semifield of order 2^n." We wish to consider if there could be a subplane of the corresponding Knuth semifield plane of order 2^n of order 2^2. This becomes something of a problem since we need to determine a semifield corresponding to a defined pre-semifield, which requires the determination of a unit element. Furthermore, our calculations do not work in commutative pre-semifields, so we consider instead a corresponding isotopic pre-semifield.

Our main result that sets up our examples given in the next section is as follows. In the statement of the theorem, the pre-semifield multiplication when $b = c = 1$ produces the commutative binary Knuth pre-semifield:

$$x \circ y = xy + (xT(y) + yT(x))^2, \forall x, y \in GF(2^n).$$

Theorem 1. *Consider the pre-semifield multiplication*

$$x \circ y = xbyc + (xbT(yc) + ycT(xb))^2,$$

where b and c are constants in $GF(2^n)$, for n odd, and T is the trace function from $GF(2^n)$ to $GF(2)$. Choose any nonzero element e and form the semifield

$$(x \circ e) * (e \circ y) = x \circ y.$$

If

$$T(ec) = T(b) = T(eb) = 0,$$
$$T(c) = 1, \frac{e^2}{e+1} = \frac{b}{c} + 1,$$

then there exists a subfield isomorphic to $GF(4)$ in $(S, +, *)$.

The corresponding semifield plane is the commutative binary Knuth semifield plane of order 2^n and would then admit a subsemifield plane of order 2^2.

Proof. In the semifield with multiplication $(x \circ e) * (e \circ y) = x \circ y$, we assume the following conditions: $T(ec) = T(b) = T(eb) = 0$, $T(yc) = 1$. Let $x = 1$ then we have $y = 1 + e\frac{b}{c}$. This forces $T(yc) = T(c + eb) = T(c) = 1$. The elements e, b and c will satisfy

$$(*) : 1 \circ y = 1 \circ (1 + e\frac{b}{c}) = (1 \circ e) * (1 \circ e) = 1 \circ e + e \circ e = (1 + e) \circ e.$$

This would say that considering juxtaposition to be $*$-multiplication and realizing that $e \circ e$ becomes the "1" in the associated semifield, letting $d = 1 \circ e$, we would have then $d^2 = d + 1$. Then $\{0, 1, d, d^2\}$ becomes a subfield isomorphic to $GF(4)$ in the semifield $(S, +, *)$. Since it straightforward to verify that $(*)$ is satisfied, this completes the proof. ∎

When n is divisible by 5 or 7, then the results of the previous theorem show that there are subplanes of order 4 in the commutative binary Knuth semifield planes of order 2^n, n odd.

Corollary 1. *Every commutative binary Knuth semifield plane of order 2^{5k} or 2^{7k}, for k odd, admits a Desarguesian subplane of order 4.*

Proof. (1) Let $n = 5k$, for k odd, and in $GF(2^5)$, let $x^5 + x^2 + 1 = 0$, be the irreducible polynomial. If $e = 1 + x + x^3, b = x^2, c = x^3$ then the semifield $(S, +, *)$ of order 2^{5k} admits a subfield isomorphic to $GF(4)$.

(2) Let $n = 7k$, for k odd, and in $GF(2^7)$, let $x^7 + x^4 + x^3 + x^2 + 1$ be the irreducible polynomial. If $e = 1 + x^7$, $b = x^7$ and $c = x^3$ then the semifield $(S, +, *)$ of order 2^{7k} admits a subfield isomorphic to $GF(4)$.

We shall give most of the details of part (1). For part (2), we leave some of the straightforward calculations to the reader.

First consider situation (1). We claim that if z is in $GF(2^5)$ then $T(z) = kT_5(z)$, where T_5 is the trace function of $GF(2^5)$ over $GF(2)$. Recall that we are working in $GF(2^{5k})$, so k is 1 modulo 2. $T(z) = \sum_{i=0}^{5k-1} z^{2^i}$. But, if $z \in GF(2^5)$ then $\sum_{i=0}^{5-1} z^{2^i} = T_5(z)$ is in $GF(2)$. And,

$$\begin{aligned}\sum_{i=0}^{5k-1} z^{2^i} &= T_5(z) + (z^{2^5} + z^{2^6} + z^{2^7} + z^{2^8} + z^{2^9}) + \\ &\quad ... + (z^{2^{5(k-1)}} + z^{2^{5k-4}} + z^{2^{5k-3}} + z^{2^{5k-2}} + z^{2^{5k-1}}) \\ &= kT_5(z) = T(z), \text{ for } k \equiv 1 \bmod 2.\end{aligned}$$

If, for elements e, b, c in $GF(2^5)^*$, we have:

$$\begin{aligned}T_5(ec) = T_5(b) = T_5(eb) = 0,\\ T_5(c) = 1, \frac{e^2}{e+1} = \frac{b}{c} + 1\end{aligned}$$

Then

$$\begin{aligned}T(ec) = T(b) = T(eb) = 0,\\ T(c) = 1.\end{aligned}$$

So, if we have a subfield isomorphic to $GF(4)$ of the sub-semifield of order 2^5, we then have a subfield isomorphic to $GF(4)$ of the semifield of order 2^{5k}, for k odd. We first note that if $e = 1 + x + x^3, b = x^2, c = x^3$ then $\frac{e^2}{e+1} = \frac{b}{c} + 1$. This follows by an easy calculation. We now verify

$$\begin{aligned}T_5(ec) = T_5(b) = T_5(eb) = 0,\\ T_5(c) = 1.\end{aligned}$$

First,

$$T_5(ec) = T_5((1+x+x^3)x^3) = T_5(x^3+x^4+x^6) =$$
$$T_5(x^3+x^4+x(x^2+1)) = T_5(x^3+x^4+x^3+x) = T_5(x^4)+T_5(x)$$

and since $T_5(x^{2^a}) = T_5(x)$, we see that $T_5(ec) = 0$. Then, we see that

$$\begin{aligned} T_5(x^3) &= x^3+x^6+(x^6)^2+(x^6)^4+(x^6)^8 \\ &= x^3+(x+x^3)+(x+x^2+x^3)+(x+x^2+x^3+x^4)+ \\ &(x^2+x^4+x+x^3+1+x^2+x^3) = 1. \end{aligned}$$

Also,

$$\begin{aligned} T_5(eb) &= T_5((1+x+x^3)x^2) = T_5(x^2+x^3+x^5)) \\ &= T_5(x^2+x^3+x^2+1) \\ &= 0, \text{ since } T_5(x^3) = T_5(1) = 1. \end{aligned}$$

$$T_5(b) = T_5(x^2) = x^2+x^4+x^8+x^{16}+x^{32}.$$

We are working in $GF(2^5)$, so $x^{32} = x$. Then we obtain:

$$x^2+x^4+(1+x^2+x^3)+(1+x+x^3+x^4)+x = 0.$$

This completes the proof of (1).

Now consider part (2). Assume that we have a binary Knuth commutative semifield of order 2^7, and let $x^7+x^4+x^3+x^2+1$ be the irreducible polynomial defining $GF(2^7)$. We claim that

$$T(x) = 0, T(x^3) = T(x^5) = 1.$$

$$(*) : T(x) = x+x^2+x^4+x^8+x^{16}+x^{32}+x^{64}.$$

The reader can easily establish the following:

$$\begin{aligned} x^8 &= x^5+x^4+x^3+x \\ x^{16} &= x^3+x+1, \\ x^{32} &= x^6+x^2+1, \\ x^{64} &= x^6+x^5+x. \end{aligned}$$

Hence, $(*)$ has exactly two non-zero 1-terms, when each element in $T(x)$ is written over $span\{1,x,x^2,x^3,x^4,x^5,x^6\}$. This means that $T(x) = 0$ and so then $T(x^{2^j}) = 0 = T(x^3+x+1) = T(x^3+1)$. Hence, $T(x^3) = 1$. Also, $x^8 = x^5+x^4+x^3+x$ then $T(x^5) = T(x^3) = 1$. Let $e = 1+x^7$, $b = x^7$ and $c = x^3$. Then $T(c = x^3) = 1$ and $T(b = x^7 = x^4+x^3+x^2+1) = 0$. We claim that

$$(*) : \frac{e^2}{e+1} = \frac{b}{c}+1$$

so we need to prove that

$$(1+x^7)^2 = (x^4+1)x^7,$$

and this is also easily established and left to the reader to verify. Therefore, this proves $(*)$. We now show that

$$T(eb) = T(ec) = 0.$$

Since $eb = (1+x^7)x^7 = x^7 + x^{14}$, clearly $T(eb) = 0$. Then $ec = (1+x^7)x^3 = x^3 + x^{10} = x^3 + (x^5)^2$ and $T(x^3) = T(x^5) = T(x^{10}) = 1$. Hence, $T(ec) = 0$. This completes the proof of part (2). ∎

Considering the transposed and dualized spreads, we also obtain the following corollary

Corollary 2. (1) *The transposed commutative binary Knuth semifield planes of order 2^n, for $n = 5k$, or $7k$, for k odd, admit Desarguesian subplanes of orders 2^2.*

(2) *The transposed then dualized commutative binary Knuth semifield planes of order 2^n for $n = 5k$, or $7k$, for k odd, are symplectic and admit Desarguesian subplanes of orders 2^2.*

3 The Commutative Kantor Semifields.

There are generalizations of the binary Knuth commutative semifields due to Kantor [4]. These have the following construction. Let F be a finite field of characteristic 2, fix a subfield F_n isomorphic to $GF(q)$ and let $F = F_0 \supset F_1 \supset F_2 \supset ... \supset F_n$ such that $[F : F_n] = k$ is odd. Choose a set of elements $\zeta_i \in F^*$, for $i = 1, 2, ..., n$. Let T_i denote the trace map from F to F_i. Then

$$x \circ y = xy + (x\sum_{i=1}^{n} T_i(\zeta_i y) + y\sum_{i=1}^{n} T_i(\zeta_i x))^2$$

defines a commutative pre-semifield of order $q^k = q^{n_1 n_2 ... n_n}$, where $[F_i : F_{i+1}] = n_i$, so all n_i are odd.

Theorem 2. *In some Kantor commutative semifield planes of orders 2^{5k} k odd, there are binary Knuth commutative semifields of order 2^5, respectively. In the associated Kantor commutative semifield planes, there are subfields of order 4.*

Proof. Let $F \simeq GF(2^{5k})$, for $5k = n_1 n_2 ... n_n$, k odd with sequence $(\zeta_1, \zeta_2, ...\zeta_{n-1}, 1)$ such that $F_n = GF(2)$ and $F_{n-1} \simeq GF(2^5)$. Let e, b, c be elements of $GF(2^5)^*$ such that for $x^5 + x^2 + 1$ is an irreducible polynomial for $GF(2^5)$. Let

$$e = 1 + x + x^3,$$
$$b = x^2$$
$$c = x^3$$

be elements of $GF(2^5)$. Choose the sequence $(\zeta_1, \zeta_2, ...\zeta_{n-1}, 1)$ so that

$$\sum_{i=1}^{n-1} T_i(\zeta_i) = 0.$$

Note that for $1 \leq i \leq n-1$, $T_i(\zeta_i r) = rT_i(\zeta_i)$, for $r \in F_{n-1} \simeq GF(2^5)$. If

$$\sum_{i=1}^{n-1} T_i(\zeta_i) = 0$$

then

$$\sum_{i=1}^{n} T_i(\zeta_i r) = T_n(\zeta_n r) = T_n(r).$$

This says that there is a binary Knuth commutative semifield which is a subsemifield of the Kantor commutative semifield. Hence, there is an isotope of the Kantor commutative semifield that contains a field isomorphic to $GF(4)$.These Kantor commutative semifield planes of order 2^{5k}, for k odd, admit subplanes of order 4. ∎

Example 1. (1) *Assume that we have a Kantor commutative semifield of order* $2^{5^2 \cdot 7}$. *Take* $n = 3$, $F_3 \simeq GF(2)$, $F_2 \simeq GF(2^5)$, $F_1 \simeq GF(2^{5^2})$, $F_0 = F \simeq GF(2^{5 \cdot 7})$. *Assume that* ζ_i*'s are all in* F_2. *Then* $\sum_{i=1}^{3} T_i(\zeta_i ed) = T_n(ed)$, *for* e *and* d *in* F_2. *Similarly,* $\sum_{i=1}^{n} T_i(\zeta_i c) = T_n(c)$. *To see this note that, since* $T_1(\zeta_1 ed) = \sum_{j=0}^{6} (\zeta_1 ed)^{(2^{5^2})^j} = 7(\zeta_1 ed) = (\zeta_1 ed)$, $T_2(\zeta_1 ed) = \sum_{j=0}^{34} (\zeta_1 ed)^{(2^5)^j} = 35(\zeta_1 ed) = (\zeta_1 ed)$.

(2) *More generally, if* n *is odd then there are an even number of proper subfields containing* $F_{n-1} \simeq GF(2^5)$. *So take* $F_{n-1} \simeq GF(2^5)$, *and assume that all elements* ζ_i *are in* F_{n-1}^* *and* $\zeta_n = 1$. *In this setting,*

$$\sum_{i=1}^{n-1} T_i(\zeta_i) = 0,$$

since $T_i(\zeta_i) = n_i \zeta_i = \zeta_i$, *where* n_i *is odd.*

Hence, in either of these two situations, we obtain an isotope that contains a field isomorphic to $GF(4)$.

We also obtain similar results for order 2^{7k}.

Theorem 3. *In some Kantor commutative semifield planes of orders* 2^{7k} k *odd, there are binary Knuth commutative semifields of order* 2^7, *respectively. In the associated Kantor commutative semifield planes, there are subfields of order* 4.

Proof. Let $F \simeq GF(2^{7k})$, for $7k = n_1 n_2 ... n_n$, odd, with sequence $(\zeta_1, \zeta_2, ...\zeta_{n-1}, 1)$ such that $F_n = GF(2)$ and $F_{n-1} \simeq GF(2^7)$. Let e, b, c be elements of $GF(2^7)^*$ such that $x^7 + x^4 + x^3 + x^2 + 1$ is an irreducible polynomial for $GF(2^7)$. Let

$$e = 1 + x^7$$
$$b = x^7$$
$$c = x^3$$

be elements of $GF(2^7)$. Choose the sequence $(\zeta_1, \zeta_2, ...\zeta_{n-1}, 1)$ so that

$$\sum_{i=1}^{n-1} T_i(\zeta_i) = 0.$$

Then there is a binary Knuth commutative semifield of order 2^7 contained as a sub-semifield in the corresponding Kantor commutative semifield. Hence, there is an isotope of the Kantor commutative semifield that contains a field isomorphic to $GF(4)$. The associated Kantor semifield plane of order 2^{7k} admits subplanes of order 4. ∎

Corollary 3. *The transposed and transposed-dual (symplectic) semifields of the Kantor commutative semifields corresponding to the semifields of Theorem 2 or Theorem 3 of orders 2^{jk}, for k odd, and $j = 5$ or 7 have isotopes that contain a field isomorphic to $GF(4)$. The corresponding semifield planes of order 2^{jk} admit subplanes of order 4.*

4 Maximal Additive Partial Spreads.

Definition 5. *We define an additive partial spread S to be 'additively maximal' if and only if there is not an additive partial spread properly containing S. Note that we may always consider the subspace $x = 0$ adjoined to any additive partial spread.*

We regard all partial spreads over the prime field $GF(p)$.

Theorem 4. *An additively maximal additive partial spread is a maximal partial spread. Any additive partial spread that is not maximal may be extended to an additively maximal additive partial spread.*

Proof. Let S be any additively maximal additive partial spread and assume that it is not maximal. Then again noting our remark that $x = 0$ may be adjoined to any additive partial spread, we then obtain a subspace $y = xM$, where M is non-singular, that is not in

$$x = 0, y = x\sum_{i=1}^{k} \alpha_i A_i,$$

(see standard matrix representation of $(*)$, Definition 4) where

$$S = \left\{ \sum_{i=1}^{k} \alpha_i A_i; \text{ for all } \alpha_i \in GF(p) \right\}.$$

Therefore, we have that

$$M - \sum_{i=1}^{k} \alpha_i A_i$$

is non-singular for $\alpha_i \in GF(p)$. Thus,

$$\beta M - \sum_{i=1}^{k} \alpha_i A_i$$

is non-singular for all β, $\alpha_i \in GF(p)$, where at least one of β or $\alpha_i, i = 1, 2, ..., k$ is non-zero. Hence, this means that letting $M = A_{k+1}$, then we have

$$S \cup \{M\} = \left\{ \sum_{i=1}^{k+1} \alpha_i A_i; \text{ for all } \alpha_i \in GF(p) \right\},$$

is an additive partial spread of degree p^{k+1}. This proves the theorem. ∎

Corollary 4. *Any additive partial spread (with $x = 0$ adjoined), may be extended either to a proper maximal partial spread that is additively maximal or extended to a semifield spread.*

Note we have then an algorithm for the construction of semifield spreads and maximal additive partial spreads. Choose any three mutually disjoint t-dimensional subspaces in a $2t$-dimensional vector space over $GF(p)$, for p a prime. Choose a basis for the vector space so that the three subspaces are $x = 0, y = 0, y = x$, writing vectors as $(x_1, ..., x_t, y_1, ..., y_t)$, $x = (x_1, ..., x_t)$ and $y = (y_1, ..., y_t)$. Use $y = x$ to generate an additive partial spread $y = x\ iI_t$, for all $i \in GF(p)$, where I_t is the $t \times t$ identity matrix. This partial spread with $x = 0$ adjoined is a p-regulus. Choose any t-subspace that is disjoint from this p-regulus, so must be of the form $y = xA_2$, where A_2 is non-singular. Generate an additive partial spread of degree p^2. Either, together with $x = 0$, this is a maximal partial spread or the algorithm may be continued. This process constructs all semifields and all additive maximal partial spreads, which is equivalent to all maximal partial spreads which are additive.

Corollary 5. *Suppose that S is an additive partial t-spread over $GF(p)$ that cannot be extended to a semifield spread. Then there is a maximal partial t-spread of degree $\leq p^{t-1} + 1$.*

5 Direct Sums.

In this section, we show that either we obtain abundant numbers of additive maximal partial spreads or there are semifield planes with prescribed and extremely exotic affine subplanes. Our results are actually more general than this and apply to any matrix spread for a translation plane. The ideas of direct sums allows a large degree of flexibility in the type of maximal partial spreads or translation planes that ultimately occur. We begin with a fundamental lemma.

Lemma 1. *Let π be a finite translation plane of order p^t. Then there is a set of $t \times t$ non-singular matrices $S_{Mat}^{t\times t}$ of cardinality $p^t - 1$ whose distinct differences are also non-singular and such that given any non-zero t-vector w there is a unique matrix $M_w^{t\times t}$ such that the first row of $M_w^{t\times t}$ is w.*

Proof. Most of the above lemma is well known. Note that since there are exactly $p^t - 1$ non-singular matrices whose distinct differences are also non-singular, it follows that the set $S_{Mat}^{t\times t}$ is necessarily sharply transitive on the set of non-zero vectors. A basis change, if necessary, completes the proof of the lemma. ∎

Definition 6. *Any matrix spread set for a translation plane π of order p^t chosen as in Lemma 1 shall be called a 'standard matrix spread set'. We shall use the term 'matrix t-spread set' when it is necessary to specify the dimension of the matrices. Our components for the associated translation plane are*

$$x = 0, y = 0, y = xM_w^{t\times t};\ M_w^{t\times t} \in S_{Mat}^{t\times t},$$

using the shorthand version of the standard matrix representation.

Theorem 5. *Choose any standard matrix c-spread set $S_{Mat}^{c\times c}$ of $c \times c$ matrices and any standard matrix d-spread set $S_{Mat}^{d\times d}$ of $d \times d$ matrices for $c > d$. Select any $c - d$ entries to be 0 in a c-vector, then there is a subspread set S_{Mat}^{c-d} of $S_{Mat}^{c\times c}$ of cardinality $p^d - 1$, whose matrices have their first rows with this same set of $c - d$ entries all zero. Let the d-vector w represent rows in both S_{Mat}^{c-d} and $S_{Mat}^{d\times d}$.*

Form the bijective correspondence between the subspread S_{Mat}^{c-d} of $S_{Mat}^{c\times c}$ and $S_{Mat}^{d\times d}$, by mapping $M_w^{c\times c}$ onto $M_w^{d\times d}$ in the notation of Lemma 1. Form the set

$$\mathcal{P} = \left\{ x = 0, y = 0,\ y = x \begin{bmatrix} M_w^{c\times c} & 0 \\ 0 & M_w^{d\times d} \end{bmatrix};\ w \text{ a } d\text{-vector} \right\},$$

for all $M_w^{c\times c} \in S_{Mat}^{c-d}$ and $M_w^{d\times d} \in S_{Mat}^{d\times d}$.

Then $\mathcal{P}$ is a partial spread of order p^{d+c} and degree $1 + p^d$ that contains a translation subplane of order p^d isomorphic to the translation plane given by the d-spread set $S_{Mat}^{d\times d}$.

Proof. Clearly, $M_w^{c\times c}$ is the zero matrix if and only if $M_w^{d\times d}$ is the zero matrix. Hence, we have a set of non-singular matrices $\begin{bmatrix} M_w^{c\times c} & 0 \\ 0 & M_w^{d\times d} \end{bmatrix}$. Now take the difference of two of these matrices

$$\begin{bmatrix} M_w^{c\times c} & 0 \\ 0 & M_w^{d} \end{bmatrix} - \begin{bmatrix} M_{w^*}^{c\times c} & 0 \\ 0 & M_{w^*}^{d} \end{bmatrix} = \begin{bmatrix} M_w^{c\times c} - M_{w^*}^{c\times c} & 0 \\ 0 & M_w^{d} - M_{w^*}^{d} \end{bmatrix}.$$

Since $M_w^{c\times c} - M_{w^*}^{c\times c}$ and $M_w^{d} - M_{w^*}^{d}$ are both non-singular for $w \neq w^*$ and w and w^* non-zero vectors (adjoin the zero-entries, when appropriate), we have that

$$x = 0, y = x \begin{bmatrix} M_w^{c\times c} & 0 \\ 0 & M_w^{d\times d} \end{bmatrix};\ w \text{ a } d\text{-vector}$$

is a partial spread of degree $1 + p^d$. The associated vector space is $2(d + c)$-dimensional over $GF(p)$, and let the $2(d + c)$-vectors be denoted by

$$(x_1, x_2, ..., x_{d+c}, y_1, y_2, .., y_{d+c}).$$

Now let

$$\pi_0 = \left\{ \begin{array}{c} (0, 0, ..., 0, x_{c+1}, x_{c+2}, ..., x_{c+d}, 0, 0, ..., 0, y_{c+1}, y_{c+2}, ..., y_{c+d});\ \\ x_i, y_i \in GF(p),\ i = c + 1, ...c + d \end{array} \right\}.$$

Note that π_0 is a vector space of dimension $2d$ over $GF(p)$ and intersects $x = 0$ and $y = 0$ in d-dimensional subspaces. Furthermore, the intersection with

$$y = x \begin{bmatrix} M_w^{c\times c} & 0 \\ 0 & M_w^d \end{bmatrix}$$

is

$$\begin{aligned}(0,0,...,0,y_{c+1},y_{c+2},...,y_{c+d}) &= (0,0,...,0,x_{c+1},x_{c+2},...,x_{c+d}) \begin{bmatrix} M_w^{c\times c} & 0 \\ 0 & M_w^d \end{bmatrix} \\ &= (0,0,...,0,(x_{c+1},x_{c+2},...,x_{c+d})M_w^d),\end{aligned}$$

which is also a d-dimensional $GF(p)$-subspace for each non-zero d-vector w. Hence, we have a spread of $1 + p^d$ d-dimensional subspaces of π_0, so that π_0 becomes an affine subplane of order p^d, which is isomorphic to the original d-spread. This completes the proof. ∎

Corollary 6. *Assume the conditions of Theorem 5. If the subplane dimension question is answered affirmatively then $\mathcal{P}$ cannot be extended to a matrix $(c + d)$-spread.*

Proof. Now assume that the subplane dimension question is answered affirmatively then if a partial spread of this form can be extended to a spread, we would have a translation plane of order p^{d+c} with d not dividing c, containing a subplane of order p^d, a contradiction. Hence, the partial spreads of the given form cannot be extended to a translation plane, thus completing the proof. ∎

Theorem 6. *Assume the conditions of Theorem 5. If $S_{Mat}^{c\times c}$ and $S_{Mat}^{d\times d}$ are semifield spreads (additive) then the subspread S_{Mat}^{c-d} is additive and the partial spread $\mathcal{P}$ is an additive partial spread. Furthermore, there is a semifield subplane of order p^d isomorphic to the semifield plane with matrix spread set given by $S_{Mat}^{d\times d}$.*

(a) If the subplane dimension question is answered affirmatively for order p^{d+c} semifield planes, the partial spread of Theorem 5 can be embedded in an additively maximal additive partial spread of degree $1 + p^{d+e} \leq 1 + p^{d+c-1}$, which is a maximal partial spread.

(b) One of the following situations must occur:

(i) there is a maximal partial spread of order p^{d+c} and deficiency at least $p^{d+c} - p^{d+c-1}$, or

(ii) every such partial spread may be extended to a semifield plane of order p^{d+c} that contains a subplane of order p^d, where d does not divide $d + c$.

(c) In this setting, the affirmation of the subplane dimension question also says that given any semifield plane π_0 of order p^d then there is a semifield plane of order p^{d+c}, for $c > d$, such that d does not divide c, that contains a subplane of order p^d isomorphic to the semifield plane given by the original d-spread.

Proof. Assume that $S_{Mat}^{c\times c}$ and $S_{Mat}^{d\times d}$ correspond to semifield spreads, which means that adjoining the appropriate zero matrix to each, both become elementary Abelian p-groups. Then we obtain, in particular an elation subgroup of order p^d with elements

$$\begin{bmatrix} I_{d+c} & \begin{bmatrix} M_w^{c\times c} & 0 \\ 0 & M_w^{d\times d} \end{bmatrix} \\ 0 & I_{d+c} \end{bmatrix}.$$

We note that this is true since then the matrices are additive and two matrices with $c-d$ 0's in fixed locations of row 1 will add to a matrix with $c-d$ 0's in the same fixed locations. Hence, if the matrix spreads sets are additive, we obtain a semifield subplane of order p^d. If the partial spread is additive (in the sense that the original spreads used in the construction are semifield d-spreads and c-spreads, respectively) then we have a semifield subplane π_0 and if this partial spread is not maximal then there is an additive partial spread of degree $1+p^{d+1}$ containing it. If this additive partial spread is not maximal, then we may continue to form additive partial spreads using Theorem 4. So, we may continue forming additive partial spreads until we obtain either a semifield spread or an additive partial spread of order $1+p^{d+e} \leq 1+p^{d+c-1}$. This completes the proof. ∎

6 Final Remarks and Open Problems.

Based on what we know of the internal structures of the known classes of translation planes and particularly what we know of semifield planes, our results show that either there are many classes of semifield planes left to be discovered that are quite different from the known families or there are great numbers of maximal additive partial spreads of very large deficiency. Since there are no non-semifield planes that are known to satisfy the subplane dimension problem in the negative, the same statement can be made for arbitrary translation planes.

To illustrate the complexity of the situation, recall again that there are semifield planes of order 2^5 that contain semifield subplanes of order 2^2, necessarily Desarguesian and there are semifields planes of orders 2^{5k} or 2^{7k}, for k odd, that admit Desarguesian subplanes of order 2^2. So take any semifield plane of order 2^5 and let c be any integer larger than 5 such that 5 does not divide c. Then either there is an additive partial spread which is a maximal partial spread of degree $\leq 1+2^{5+c-1}$ or there is a semifield plane of order 2^{5+c} that contains a semifield subplane of order 2^2 and of order 2^5. For example, if $c=6$, either there is a semifield plane of order 2^{11} that contains subplanes of orders 2^2, 2^5 or there is an additive partial spread which is maximal of degree $\leq 1+2^{10}$ and order 2^{11}. **Now assume that we never obtain additive maximal partial spreads.** Then choose any sequence of integers $2,5,11,i_4,i_5..,i_n$ such that $i_{j+1}=i_j+t_j$, such that i_j does not divide t_j. Then there is a semifield plane of order 2^{i_n} admitting subplanes of orders $2^2, 2^5, 2^{11}, ..., 2^{i_{n-1}}$. For example, take the sequence $2,5,11,23,47$, then there is an assumed semifield plane of order 2^{47} that contains semifield subplanes of orders 2^2, 2^5, 2^{11}, 2^{23}. Similar sequences are possible for semifields of order 2^{7k}, for k odd.

In general, we have shown that given any translation plane π_o of order p^d, we may find a partial spread of order p^{d+c} and degree $1+p^d$ that contains a translation subplane of order p^d isomorphic to π_0. If this partial spread is not contained in a proper maximal partial spread then there is a translation plane of order p^{c+d} that contains a translation subplane of order p^d. This seems improbable, assuming that d does not divide c. Thus, we would expect there to be a very large number of maximal partial spreads of large orders that may be generated in this manner.

Finally, we list three open problems.

- Find examples of translation planes of order p^t that admit affine subplanes of order p^k, where t does not divide t. Show, if possible, that commutative semifields satisfy the subsemifield dimension property (i.e. the dimension of a commutative subsemifield must divide the dimension of the commutative semifield).
- Show there exist semifield planes of order 2^r, for any odd integer r that admit Desarguesian subplanes of order 2^2. (Wene [7], there are sporadic semifield planes of orders 2^j, for $j = 5, 7, 9, 11$ that do have subplanes of order 2^2.)
- Show that there exist semifield planes of order 2^t, for any integer t relatively prime to 3 that admit semifield subplanes of order 2^3.

References

[1] A. Beutelspacher, Partitions of finite vector spaces: an application of the Frobenius number in geometry, Arch. Math. (Basel) 31 (1978/79), no. 2, 202–208.

[2] D.A. Foulser, D. A. Planar collineations of order p in translation planes of order p^r, Geometriae Dedicata 5 (1976), no. 3, 393–409.

[3] N.L. Johnson, A note on the construction of quasifields, Proc. Amer. Math. Soc. 29 (1971), 138-142.

[4] W.M. Kantor, Commutative semifields and symplectic spreads. J. Algebra 270 (2003), no. 1, 96-114.

[5] D.E. Knuth, Finite Semifields and projective planes, J. Algebra 2 (1965), 182-217.

[6] D.M. Maduram, Transposed translation planes, Proc. Amer. Math. Soc. 53 (1975), no. 2 265-270.

[7] G.P. Wene, Semifields of Odd Dimension over $GF(2)$ Containing Subalgebras of Even Dimension over $GF(2)$, Preprint.

[8] G.P. Wene, Private Communication.

Mathematics Dept., University of Iowa,
Iowa City, Iowa 52242