Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Algebra 270 (2003) 96–114
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Commutative semifields and symplectic spreads ☆

William M. Kantor

Department of Mathematics, University of Oregon, Eugene, OR 97403 USA

Received 2 August 2002

Communicated by Jan Saxl

Abstract

Commutative semifields are constructed by using their relationship with symplectic spreads. The number of pairwise nonisomorphic commutative semifield planes of even order N obtained in this manner is not bounded above by any polynomial in N. The number previously known for any N was less than $\log N$.

MSC: primary 51A40, 17A35; secondary 05B25, 51A35, 51A50

1. Introduction

Semifields are algebras satisfying all of the axioms for a skew field except (possibly) associativity. Their importance in the theory of projective planes is standard [De, Section 5.3]. Finite ones are not terribly plentiful [CW,KW]; finite commutative ones are painfully lacking.

The study of finite commutative semifields was begun by Dickson almost a century ago; he found the first nonassociative ones [Di1,Di2,Di3]. Since then the only examples found have been some of Albert's *generalized twisted fields* [Al4,Al5] and Knuth's *binary semifields* [Kn2]; then, after about 16 years, Cohen–Ganley semifields [CG] and Ganley semifields [Ga]; then, after another 15 years, Coulter–Matthews semifields [CM]; and, most recently, one sporadic example due to Penttila and Williams [PW]. It is a bit surprising that so few examples are known (up to isotopism).

☆ This research was supported in part by the National Science Foundation.

E-mail address: kantor@math.uoregon.edu.

doi:10.1016/S0021-8693(03)00411-3

In this paper additional finite commutative semifields are defined by means of the awkward formula (4.2). Whereas the number of previously known commutative semifield planes of any given order N is less than $\log N$, the number obtained here is *not bounded above by any polynomial in* N.

Our construction is a simple combination of Knuth's *cubical arrays* [Kn1], their interpretation in [BB], and constructions in [Ka1,KW] for (noncommutative!) semifields arising from *symplectic spreads*. The manner in which these planes were discovered is perhaps as interesting as the planes themselves, since coding theory played a key role in the discovery.[1] The study of symplectic spreads in large-dimensional vector spaces of characteristic 2 was motivated by coding-theory and later also by extremal line-sets in Euclidean spaces [Ka1,CCKS]. In [Ka3] a method was described for obtaining apparently large numbers of symplectic spreads from desarguesian affine planes by natural modifications involving orthogonal geometries and sequences of field changes. The semifield planes among the many types of resulting planes were studied at length in [KW]. This produced the present paper via the following remarkably elementary fact: *Knuth's arrays provide a bijection between commutative semifield planes and symplectic semifield planes* (Proposition 3.8).

In order to state our main result, let $\rho(m)$ denote the number of prime factors of an integer m, counting multiplicities; logarithms are always to the base 2.

Theorem 1.1. *Suppose that $q > 1$ is a power of 2 and $m > 1$ is an odd integer. If m is not a power of 3 or if $q > 2$, then there are more than $q^{m(\rho(m)-1)}/(m \log q)^2$ pairwise nonisomorphic affine planes of order q^m coordinatized by commutative semifields.*

If $m \geqslant 3^3$ is a power of 3 and $q = 2$ then the corresponding number is greater than $2^{m(\rho(m)-2)}/m^2$. See Theorem 4.4 for a more precise statement, and Theorem 4.5 for information concerning the full collineation groups of the planes. We have no idea how to prove these theorems while staying within the framework of the standard theory of translation planes: symplectic and orthogonal spreads provide additional structure for the needed results in [Ka1,KW] concerning different but intimately related symplectic semifield planes.

In Section 5 we briefly survey the small number of known finite commutative semifields and symplectic semifield planes. For some of them slightly more general results are discussed at length in [BB]. Finally, in Section 6 we conclude with a number of remarks concerning commutative semifields and symplectic spreads.

2. Background

We refer to [De] for the standard background concerning translation planes and their kernels and duals, as well as spreads, semifields and isotopisms. Nevertheless, we recall that a presemifield is a semifield if there is an element acting as an identity element. Every

[1] Compare [Kn2, p. 541].

presemifield is isotopic to many different semifields, all of which produce the same affine plane (up to isomorphism), and the kernel of that plane is isomorphic to the kernel (i.e., left nucleus) of any of these semifields. Moreover, two such presemifield planes are isomorphic if and only if their coordinatizing presemifields are isotopic [Al2].

3. Duals and duals

Let $\mathbf{P} = (K^n, +, \circ)$ be a presemifield, with associated translation plane $\mathfrak{A}(\mathbf{P})$. We assume that $x \to x \circ y$ and $x \to y \circ x$ are K-linear maps for each $y \in K^n$. This is certainly the case if K is a prime field.

If $v_1, \ldots, v_n$ is the standard basis of K^n, then

$$v_i \circ v_j = \sum_k a_{ijk} v_k \tag{3.1}$$

for $a_{ijk} \in K$. The *cubical array* (a_{ijk}) was introduced and studied by Knuth [Kn1]. Since it determines $\mathbf{P}$, we will sometimes write $\mathbf{P}(a_{ijk})$ instead of $\mathbf{P}$.

We are interested in two other cubical arrays and presemifields related to the original one. First, the array (a_{jik}) corresponds to the semifield $\mathbf{P}(a_{jik}) = (K^n, +, \circ^*)$, where $x \circ^* y = y \circ x$ coordinatizes the projective plane *dual* to the one determined by $\mathfrak{A}(\mathbf{P})$, and hence also coordinatizes one of the associated affine planes $\mathfrak{A}(\mathbf{P})^*$ of that dual plane. Thus, we write

$$\mathbf{P}(a_{jik}) = \mathbf{P}(a_{ijk})^*, \tag{3.2}$$

with corresponding plane $\mathfrak{A}(a_{jik}) = \mathfrak{A}(a_{ijk})^*$.

More significantly, Knuth [Kn1] observed that, if (a_{ijk}) determines a presemifield, then so does each such array obtained by applying any permutation in S_3 to the subscripts of the array. Thus, each presemifield produces as many as six presemifields.

A simple geometric explanation for this appears first to have been observed only very recently in [BB]. Consider the spread Σ determined by $\mathbf{P}(a_{ijk})$. This consists of the following subspaces of $K^n \oplus K^n$: $K^n \oplus 0$ and

$$\Sigma[s] = \bigl\{(x, x \circ s) \bigm| x \in K^n\bigr\} = \bigl\{(x, xM_s) \bigm| x \in K^n\bigr\}, \quad s \in K^n. \tag{3.3}$$

Here M_s is the matrix of right multiplication by s; the nonsingularity of the matrices $M_s, s \neq 0$, is exactly the condition that $(K^n, +, \circ)$ is a presemifield. In terms of (3.1), if $s = \sum_j s_j v_j$ then $v_i \circ s = \sum_k (\sum_j s_j a_{ijk}) v_k$, so that $M_s = (\sum_j s_j a_{ijk})_{ik}$.

The *dual spread* $\Sigma^{\mathbf{d}}$ is a spread of the dual space of $K^n \oplus K^n$. We can identify that dual space with $K^n \oplus K^n$ by using the nondegenerate alternating bilinear form defined by

$$\bigl((x, y), (x', y')\bigr) = x \cdot y' - y \cdot x' \tag{3.4}$$

in terms of the usual dot product. The n-spaces $\{(x, xM_s) \mid x \in K^n\}$ and $\{(x, xM_s^t) \mid x \in K^n\}$ are perpendicular, since $((x, xM_s), (x', x'M_s^t)) = x(x'M_s^t)^t - (xM_s)x'^t = 0$ for all $x, x' \in K^n$. It follows that *we can view* $\Sigma^{\mathbf{d}}$ as consisting of the subspaces $K^n \oplus 0$ and

$$\Sigma^{\mathbf{d}}[s] = \bigl\{\bigl(x, xM_s^t\bigr) \bigm| x \in K^n\bigr\}, \quad s \in K^n.$$

Write $x \circ^{\mathbf{d}} s = xM_s^t$, where $M_s^t = (\sum_j s_j a_{kji})_{ik}$. Then the plane $\mathfrak{A}(\mathbf{P})^{\mathbf{d}}$ corresponding to $\Sigma^{\mathbf{d}}$ is coordinatized by the presemifield

$$\mathbf{P}(a_{kji}) = \mathbf{P}\bigl(K^n, +, \circ^{\mathbf{d}}\bigr) = \mathbf{P}(a_{ijk})^{\mathbf{d}}. \tag{3.5}$$

Note that (3.2) and (3.5) are equalities involving presemifields, with no isotopisms of presemifields or isomorphisms of planes entering at all. These equations arise by applying the transpositions (1,2) or (1,3) to the subscripts of the cubical array (a_{ijk}).

Commutativity. Clearly

$$\mathbf{P}(a_{ijk}) \text{ is commutative} \quad \text{if and only if} \quad \mathbf{P}(a_{ijk})^* = \mathbf{P}(a_{ijk}). \tag{3.6}$$

Symplectic spreads. A spread is called *symplectic* with respect to a nondegenerate alternating bilinear form (,) if $(X, X) = 0$ for each member X of the spread. Using the alternating bilinear form (3.4) we note that

$$\text{The spread } \Sigma \text{ in (3.3) is symplectic} \quad \text{if and only if} \quad \mathbf{P}(a_{ijk})^{\mathbf{d}} = \mathbf{P}(a_{ijk}). \tag{3.7}$$

Namely, $((x, xM_s), (y, yM_s)) = 0$ for all $x, y \iff x(yM_s)^t - xM_s y^t = 0$ for all $x, y \iff x(M_s^t - M_s)y^t = 0$ for all $x, y \iff M_s = (\sum_j s_j a_{ijk})_{ik}$ is symmetric. Now use (3.5).

Symplectic spreads have been studied at length in [Ka1,Ka4,CCKS,KW,Ma]. The following simple way to obtain them led to this paper:

Proposition 3.8. *For a presemifield plane* $\mathfrak{A}$, *some presemifield for* $\mathfrak{A}$ *is commutative if and only if some spread for* $\mathfrak{A}^{\mathbf{d}*}$ *is symplectic.*

Proof. If the presemifield $\mathbf{P}(a_{jik})$ is commutative then $\mathbf{P}(a_{ijk})^* = \mathbf{P}(a_{ijk})$, so that $(\mathbf{P}(a_{ijk})^{\mathbf{d}*})^{\mathbf{d}} = \mathbf{P}(a_{ijk})^{*\mathbf{d}*\mathbf{d}} = \mathbf{P}(a_{ijk})^{\mathbf{d}*}$ since $(1,2)(1,3)(1,2)(1,3) = (1,3)(1,2)$. Now use (3.7).

Conversely, if some spread for $\mathfrak{A}^{\mathbf{d}*}$ is symplectic, then by [Ta, p. 69] we may assume that the alternating form is (3.4). Then $\mathbf{P}(a_{ijk})^{\mathbf{d}*\mathbf{d}} = \mathbf{P}(a_{ijk})^{\mathbf{d}*}$ by (3.7). As above, it follows that $\mathbf{P}(a_{ijk})^* = \mathbf{P}(a_{ijk})^{\mathbf{d}*\mathbf{d}*\mathbf{d}} = \mathbf{P}(a_{ijk})$. □

Remarks.

1. There is a very simple “coincidence” underlying the preceding proposition: (3.3) is symplectic if and only if the matrices M_s are symmetric; and multiplication in a presemifield is commutative if and only if the multiplication constants form symmetric matrices.

2. All of the above discussion involved choices, including a choice of basis and a choice of alternating bilinear form. Even the field was implicitly chosen: everything could have

taken place over the prime field without affecting any of the results. With this in mind we will usually find it convenient to view our vector spaces as being over the prime field, applying the trace map from a more obvious field down to the prime field in order to handle field automorphisms.

3. In [BB], the plane $\mathfrak{A}^{\mathbf{d}}$ is obtained using the *symmetric* bilinear form

$$(x, y) \cdot (x', y') = x \cdot x' + y \cdot y'$$

instead of the alternating one (3.4).

4. Desarguesian scions and a generalization of Knuth's semifields

Assume that we are given fields $F = F_0 \supset F_1 \supset \cdots \supset F_n$ of characteristic 2 with $[F : F_n]$ odd and corresponding trace maps $T_i : F \to F_i$. Choose any elements $\zeta_i \in F^*$, $1 \leqslant i \leqslant n$. Define $\mathbf{D}(F, +, \bullet) = \mathbf{D}((F_i)_0^n, (\zeta_i)_1^n)$ by

$$x \bullet y = xy^2 + \sum_1^n T_i(\zeta_i x)y + \sum_1^n \zeta_i T_i(xy) \tag{4.1}$$

and $\mathbf{B}(F, +, *) = \mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$ by

$$x * y = xy + \left(x \sum_1^n T_i(\zeta_i y) + y \sum_1^n T_i(\zeta_i x)\right)^2. \tag{4.2}$$

The presemifields $\mathbf{D}((F_i)_0^n, (\zeta_i)_1^n)$ were studied in [KW]; there they produced what were called *semifield scions of desarguesian planes* (hence the "**D**"). In Theorem 4.3 will see that $\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$ is a commutative presemifield. This produces a commutative semifield that generalizes Knuth's *binary semifields* [Kn2] (hence the "**B**"); the latter semifields correspond to the presemifields $\mathbf{B}((F_i)_0^1, (1))$.

4.1. *Source of the presemifields* $\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$

Theorem 4.3. $\mathfrak{A}(\mathbf{D}((F_i)_0^n, (\zeta_i)_1^n))^{*\mathbf{d}} \cong \mathfrak{A}(\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n))$.

Proof. We will use the nondegenerate alternating bilinear form $((x, y), (u, v)) = T(xv - yu)$ on F^2, where $T : F \to \mathrm{GF}(2)$ is the trace map. For $m \in F$ we need to find all (u, v) such that

$$0 = \big((x, m \bullet x), (u, v)\big) = T\Big(xv + \Big[mx^2 + \sum T_i(\zeta_i m)x + \sum \zeta_i T_i(mx)\Big]u\Big)$$

for all x. Note that $T(T_i(x)) = T(x)$ for all x, which depends upon the assumption that $[F : F_n]$ is odd; this implies that $T(aT_i(b)) = T(T_i(aT_i(b))) = T(T_i(a)T_i(b)) = T(bT_i(a))$ for all a, b [KW, Lemma 2.14]. Thus,

$$0 = T(xv) + T(x\sqrt{m}\sqrt{u}\,) + \sum T\bigl(xuT_i(\zeta_i m)\bigr) + \sum T\bigl(xmT_i(\zeta_i u)\bigr)$$

for all $x \in F$, so that

$$0 = v + \sqrt{m}\sqrt{u} + \sum uT_i(\zeta_i m) + \sum mT_i(\zeta_i u).$$

It follows that the dual spread consists of $F \oplus 0$ and all

$$\Bigl\{\Bigl(u, \sqrt{u}\sqrt{m} + \sum uT_i(\zeta_i m) + \sum mT_i(\zeta_i u)\Bigr) \Bigm| u \in F\Bigr\}, \quad m \in F,$$

and hence arises from an isotope of the presemifield $\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$. □

Remarks. The above theorem implies that there are at most three planes obtained by repeated use of the operations $*$ and **d**: $\mathfrak{A}(\mathbf{D}((F_i)_0^n, (\zeta_i)_1^n))$, $\mathfrak{A}(\mathbf{D}((F_i)_0^n, (\zeta_i)_1^n))^*$ and $\mathfrak{A}(\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n))$.

The theorem essentially answers a question in [CW, p. 130] concerning the previously known semifields for which $n = 1$: "It remains an open question: When is a Kantor semifield a Knuth binary semifield?" Interpreting the question as asking whether these semifields are somehow related, the answer is now that they are, in fact, intimately related. On the other hand, by Corollary 4.15(ii) these planes are not isomorphic, at least if $[F : F_1] > 3$.

Source of the presemifields $\mathbf{D}((F_i)_0^n, (\zeta_i)_1^n)$. These were constructed by starting with a desarguesian plane and using an algorithm that produces a sequence of modifications involving orthogonal geometries and field changes. This led precisely to these presemifields and to no others. (There were, however, many other types of planes obtained by the same process, but those are not coordinatizable using semifields.) In this sense these presemifields arose "naturally" from desarguesian planes, and hence the same is true of the presemifields $\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$. This contrasts with the first occurrence of the presemifields $\mathbf{B}((F_i)_0^1, (1))$ in [Kn2], where they had a more magical appearance.

4.2. *Direct proof that (4.2) defines a presemifield*

Write $f(x) = \sum T_i(\zeta_i x)$. Assume that $x \neq 0$ and

$$xy + f(x)^2y^2 + f(y)^2x^2 = 0.$$

Write $a = y/x$. Then $f(x)ax + f(ax)x = \sqrt{xax}$, so that

$$\sqrt{a} = f(x)a + f(ax) = a\sum_1^n T_i(\zeta_i x) + \sum_1^n T_i(\zeta_i ax).$$

We claim that, for $j = 1, \ldots, n$,

$$\sqrt{a} = a\sum_j^n T_i(\zeta_i x) + \sum_j^n T_i(\zeta_i ax).$$

We have seen that this is true for $j = 1$. If it is true for some $j < n$ then it is a quadratic equation satisfied by $\sqrt{a}$ with coefficients in F_j. Since $[F : F_j]$ is odd, $\sqrt{a} \in F_j$. Then

$$\begin{aligned} a\sum_j^n T_i(\zeta_i x) + \sum_j^n T_i(\zeta_i ax) &= aT_j(\zeta_i x) + T_j(\zeta_i ax) + a\sum_{j+1}^n T_i(\zeta_i x) + \sum_{j+1}^n T_i(\zeta_i ax) \\ &= a\sum_{j+1}^n T_i(\zeta_i x) + \sum_{j+1}^n T_i(\zeta_i ax), \end{aligned}$$

as claimed.

Consequently, $\sqrt{a} = T_n(ax) + aT_n(x)$. Once again we have a quadratic equation that shows that $\sqrt{a} \in F_n$. The same equation now yields $\sqrt{a} = 0$, and hence $y = 0$. □

Remarks.

1. The preceding proof was significantly simpler and shorter than the direct proof in [KW] that (4.1) defines a presemifield. In fact, except for an inductive argument, the two proofs have nothing in common. This seems a bit unexpected.

The fact that the presemifields in (4.2) are easier to work with than those in (4.1) will again be apparent in Section 4.4. On the other hand, in Section 4.3 we will see that the presemifields in (4.1) have advantages as well.

2. The field elements ζ_i appear both "inside" and "outside" the trace map T_i in (4.1), but only "inside" in (4.2). In fact, *traces are not needed at all in* (4.2): for each i, the functions $T_i(\zeta_i x)$, $\zeta_i \in F^*$, run through *all* nonzero F_i-linear functionals $F \to F_i$. Nevertheless, we have retained the ζ_i in view of the results, needed later, proved about the presemifields (4.1) in [KW].

Knuth [Kn2] also used an arbitrary nonzero linear functional $F \to F_1$ in his construction. He observed that different linear functionals produce isotopic presemifields, which is not the case when $n > 1$ (cf. Theorem 4.4).

4.3. Isotopisms and autotopisms

There are tolerable but incomplete results concerning both isomorphisms among these semifield planes and their collineation groups:

Theorem 4.4. *Consider the presemifields* $\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$ *and* $\mathbf{B}((F_i')_0^{n'}, (\zeta_i')_1^{n'})$, *where* $n \geqslant 1, n' \geqslant 1$, $F = F_0 = F_0'$, *and either* $[F : F_1] > 3$ *and* $[F : F_1'] > 3$, *or* F_n *and* $F_{n'}'$ *have a common subfield of size* > 2. *Then the following are equivalent*:

(i) $\mathfrak{A}(\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n))$ *and* $\mathfrak{A}(\mathbf{B}((F_i')_0^{n'}, (\zeta_i')_1^{n'}))$ *are isomorphic semifield planes*; *and*

(ii) $n' = n$, $F_i' = F_i$ *and there exist* $\lambda \in F^*$ *and* $\sigma \in \mathrm{Aut}(F)$ *such that* $\zeta_i' = \lambda \zeta_i^\sigma$ *for all* $1 \leqslant i \leqslant n$.

Each of these planes has an obvious group A of collineations arising from the autotopisms obtained from the equation

$$(kx) * \left(k^{-1}y\right) = x * y, \ k \in F_n^*.$$

Theorem 4.5. *Consider a presemifield* $\mathbf{B} = \mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$ *where* $n \geqslant 1$. *Let* $\Lambda \leqslant \mathrm{Aut}(F_0)$ *denote the largest subgroup that fixes each* $\zeta_1^{-1}\zeta_i$, $2 \leqslant i \leqslant n$. *If* $[F_0 : F_1] > 3$ *then* $\mathrm{Aut}\,\mathfrak{A}(\mathbf{B})$ *is the product of* $A\Lambda$ *with the group of order* $|F|^3$ *generated by all elations.*

Proof of Theorems 4.4, 4.5 and 1.1. If the planes are isomorphic then there is a semilinear transformation g of F^2 sending the spread for the first plane to that for the second one. Then g acts on the dual space and sends the first dual spread to the second one. Hence, any isomorphism $\mathfrak{A}(\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)) \to \mathfrak{A}(\mathbf{B}((F_i')_0^{n'}, (\zeta_i')_1^{n'}))$ that fixes 0 induces an isomorphism $\mathfrak{A}(\mathbf{D}((F_i)_0^n, (\zeta_i)_1^n))^* \cong \mathfrak{A}(\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n))^{\mathbf{d}} \to \mathfrak{A}(\mathbf{B}((F_i')_0^{n'}, (\zeta_i')_1^{n'}))^{\mathbf{d}} \cong \mathfrak{A}(\mathbf{D}((F_i')_0^{n'}, (\zeta_i')_1^{n'}))^*$ (Theorem 4.3) and hence also an isomorphism $\mathfrak{A}(\mathbf{D}((F_i)_0^n, (\zeta_i)_1^n)) \to \mathfrak{A}(\mathbf{D}((F_i')_0^{n'}, (\zeta_i')_1^{n'}))$. Consequently, Theorem 4.4 follows from [KW, Theorem 4.12].

For Theorem 4.5, first note that F_n is (isomorphic to) the kernel of $\mathrm{Aut}\,\mathfrak{A}(\mathbf{D})$, since $[F_0 : F_1] > 3$ [KW, Theorem 3.4]. By [KW, Theorem 4.11], $\mathrm{Aut}\,\mathfrak{A}(\mathbf{D})$ is the product of $F_n^*\Lambda$ with the group of order $|F|^3$ generated by all elations. Hence, $|\mathrm{Aut}\,\mathfrak{A}(\mathbf{B})| = |\mathrm{Aut}\,\mathfrak{A}(\mathbf{D})| = |F|^3|F_n^*\Lambda|$, which is exactly the order of the group stated in the theorem.

Finally, Theorem 1.1 and the remark after it follow from Theorem 4.4 as in [KW, Theorem 4.15(iii′)]; alternatively, in [KW, Theorem 4.15(iii′)] use $q = 2$ if $[F : F_1] > 3$ and $\mathrm{GF}(q) = F_n \cap F_{n'}'$ otherwise. □

Remark. Despite the first remark in Section 4.2, the presemifields (4.1) are superior to those in (4.2) for the study of isotopisms and autotopisms: as indicated in the introduction, we have no idea how to prove the preceding theorems while staying entirely within the theory of projective planes and their spreads. This is, in fact, possibly the most interesting aspect of this paper. On the other hand, a proof that does not wander off into orthogonal geometries would be desirable, since it might provide a route to the removal of the unfortunate numerical assumptions in the preceding theorems.

Corollary 4.6. *If* $[F_0 : F_1] > 3$ *then the kernel of* $\mathfrak{A}(\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n))$ *is* $\mathrm{GF}(2)$.

Proof. If K is the kernel then K^* can be viewed as a group of collineations. It must be conjugate to a subgroup of $A\Lambda$. In view of the actions of $A\Lambda$ and K^* on the plane, this is only possible if $|K^*| = 1$. □

4.4. Kernel

We next compute the kernel of essentially *all* of the semifields and their planes. The computation is somewhat messy, though not as disgusting as for the corresponding result in [KW, Theorem 3.4] (which was crucial for the proof of the above Theorem 4.5 and its corollary).

Theorem 4.7. *If $n \geqslant 1$ and $|F| > 8$, then the kernel of the plane $\mathfrak{A}(\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n))$ is* GF(2).

Note that the hypothesis $|F| > 8$ is essential here since any semifield of order 8 is a field.

Proof. As in the proof of [KW, Theorem 3.4], we begin with a slight modification of $\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$: *we may assume that*

$$\sum T_i(\zeta_i) = 0. \tag{4.8}$$

For, if $\lambda \in F^*$ then $\mathbf{B}_*((F_i)_0^n, (\zeta_i)_1^n)$ and $\mathbf{B}_\circ((F_i)_0^n, (\lambda\zeta_i)_1^n)$ are isotopic: by (4.2), $\lambda^2(x * y) = (\lambda x) \circ (\lambda y)$ for all $x, y \in F$. Now choose $\lambda \neq 0$ in the kernel of the additive map $\lambda \to \sum T_i(\lambda\zeta_i)$ from F to F_1, and replace $\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n)$ by $\mathbf{B}((F_i)_0^n, (\lambda\zeta_i)_1^n)$ in order to have (4.8).

We now have the presemifield we need. The kernel of the plane $\mathfrak{A}(\mathbf{B}((F_i)_0^n, (\zeta_i)_1^n))$ is isomorphic to the kernel of any associated semifield. The semifield $(F, +, \circ)$ we will use is defined as follows (for all $x, y \in F$):

$$x = \bar{x} + \sum T_i(\zeta_i \bar{x})^2 \tag{4.9}$$

$$f_x = \sum T_i(\zeta_i \bar{x})^2 \tag{4.10}$$

$$x \circ y = \bar{x} * \bar{y} = \bar{x}\,\bar{y} + \bar{x}^2 f_y + \bar{y}^2 f_x. \tag{4.11}$$

By (4.2) and (4.8), $x \to \bar{x}$ is the inverse of the map $x \to x * 1$, so that $(F, +, \circ)$ is a semifield $\mathbf{S}$ with identity element 1.

The kernel (or left nucleus) of $\mathbf{S}$ is $\{k \in F \mid (k \circ x) \circ y = k \circ (x \circ y) \text{ for all } x, y \in F\}$. We will assume that there is some k in this kernel such that $\bar{k} \neq 0, 1$, and eventually deduce a contradiction.

Lemma 4.12. *If $f_{k\circ x} = f_{x\circ y} = 0$, then*

$$\begin{aligned}
&\bar{k}\big(\bar{x}\bar{y} + \bar{x}^2 f_y + \bar{y}^2 f_x\big) + \big(\bar{x}\,\bar{y} + \bar{x}^2 f_y + \bar{y}^2 f_x\big)^2 f_k \\
&\quad = \bar{y}\big(\bar{k}\bar{x} + \bar{k}^2 f_x + \bar{x}^2 f_k\big) + \big(\bar{k}\bar{x} + \bar{k}^2 f_x + \bar{x}^2 f_k\big)^2 f_y.
\end{aligned}$$

Proof. By (4.9), $\overline{k \circ x} = k \circ x$ and $\overline{x \circ y} = x \circ y$. By (4.11),

$$k \circ (x \circ y) = k \circ (\bar{x} * \bar{y}) = \bar{k}(\bar{x} * \bar{y}) + (\bar{x} * \bar{y})^2 f_k,$$
$$(k \circ x) \circ y = (k \circ x) * \bar{y} = (\bar{k} * \bar{x})\bar{y} + (\bar{k} * \bar{x})^2 f_y.$$

Now use (4.11) two more times. □

Lemma 4.13. $f_k = 0$.

Proof. First choose x satisfying $f_{x \circ k} = f_x = 0$; there are at least $|F|/|F_1|^2 > 1$ choices, since $[F\colon F_1] \geqslant 3$ and $x \to f_x$ is an additive map from F to F_1. Thus, we may assume also that $x \neq 0$. Now choose y so that both hypotheses of Lemma 4.12 hold, together with $f_y = 0$. For these x, y, Lemma 4.12 reduces to $\bar{x}^2\bar{y}^2 f_k = \bar{y}\bar{x}^2 f_k$.

If $f_k \neq 0$ then $\bar{y} \in \{0, 1\}$. However, there are at least $|F|/|F_1|^2$ choices for y, so that $|F_1| \leqslant |F|/|F_1|^2 \leqslant 2$, whereas we have assumed that $|F| > 8$. □

Lemma 4.14. *If* $f_{k \circ x} = 0$ *then* $f_x = 0$.

Proof. Suppose that $f_{k \circ x} = 0$ but $f_x \neq 0$. Choose any y as in Lemma 4.12. By Lemmas 4.12 and 4.13,

$$\bar{k}\big(\bar{x}^2 f_y + \bar{y}^2 f_x\big) = \bar{y}\big(\bar{k}^2 f_x\big) + \big(\bar{k}\bar{x} + \bar{k}^2 f_x\big)^2 f_y,$$

or

$$f_x(\bar{y}^2 + \bar{y}\bar{k}) = f_y\big\{\bar{x}^2 + \bar{k}\bar{x}^2 + \bar{k}^3 f_x^2\big\}.$$

Thus, for each y chosen in Lemma 4.12, $\bar{y}^2 + \bar{y}\bar{k} \in F_1\{\bar{x}^2 + \bar{k}\bar{x}^2 + \bar{k}^3 f_x^2\}$. Consequently, the number of y is at most $2|F_1|$, while there are at least $|F|/|F_1|$ choices for y satisfying the hypotheses of Lemma 4.12. Thus, $|F|/|F_1|^2 \leqslant 2$, which is a contradiction as in the preceding lemma. □

Conclusion of the proof. This time choose any y, and choose any x such that $f_{k \circ x} = 0$. By Lemmas 4.13 and 4.14 together with (4.9) and (4.11),

$$\begin{aligned}
\bar{k}\big(\bar{x}\bar{y} + \bar{x}^2 f_y + f_{x \circ y}\big) + \bar{k}^2 f_{x \circ y} &= \bar{k}(x \circ y + f_{x \circ y}) + \bar{k}^2 f_{x \circ y} \\
&= \bar{k}\overline{(x \circ y)} + \bar{k}^2 f_{x \circ y} \\
&= \bar{k} * \overline{(x \circ y)} = k \circ (x \circ y) \\
&= (k \circ x) \circ y = (k \circ x) * \bar{y} \\
&= (k \circ x)\bar{y} + (k \circ x)^2 f_y \\
&= (\bar{k} * \bar{x})\bar{y} + (\bar{k} * \bar{x})^2 f_y \\
&= (\bar{k}\bar{x})\bar{y} + (\bar{k}\bar{x})^2 f_y.
\end{aligned}$$

Thus, $(\bar{k}+\bar{k}^2)\bar{x}^2 f_y = (\bar{k}\bar{x}^2+(\bar{k}\bar{x})^2)f_y = (\bar{k}+\bar{k}^2)f_{x\circ y}$, where $f_y, f_{x\circ y}\in F_1$. We are assuming that $\bar{k}+\bar{k}^2\neq 0$. Consequently, if we can choose y such that $f_y\neq 0$ then there are at most $|F_1|$ choices for $\bar{x}$ such that $f_{k\circ x}=0$, which is not the case.

Thus, $f_y=0$ for all $y\in F$. However, by (4.10) this is impossible since $T_1(\zeta_1 F)=F_1$ while, if $n\geqslant 2$, then $\sum_2^n T_i(\zeta_i)\in F_2$. This is a final contradiction. □

Remark. A similar proof shows that the middle nucleus $\{k\in F \mid (x\circ k)\circ y = x\circ (k\circ y)$ for all $x,y\in F\}$ is also GF(2).

Corollary 4.15.

(i) *If $n\geqslant 1$ and $|F|>8$, then the kernel of* $\mathfrak{A}(\mathbf{D}((F_i)_0^n,(\zeta_i)_1^n))^*$ *is* GF(2).

(ii) *If $[F\colon F_1]>3$ then $\mathfrak{A}(\mathbf{D}((F_i)_0^n,(\zeta_i)_1^n))$ is not self-dual. Hence, $\mathfrak{A}(\mathbf{D}((F_i)_0^n,(\zeta_i)_1^n)) \ncong \mathfrak{A}(\mathbf{B}((F_i)_0^n,(\zeta_i)_1^n))$.*

Proof.

(i) The kernel of $\mathfrak{A}(\mathbf{B}((F_i)_0^n,(\zeta_i)_1^n))$ is isomorphic to the field of linear transformations of F^2 that fix each member of the spread. This field of linear transformations is the same for the dual space of F^2, and hence is isomorphic to the kernel of $\mathfrak{A}(\mathbf{B}((F_i)_0^n,(\zeta_i)_1^n))^{\mathbf{d}} \cong \mathfrak{A}(\mathbf{D}((F_i)_0^n,(\zeta_i)_1^n))^*$ (Theorem 4.3).

(ii) Since $[F:F_1]>3$, the kernel of $\mathfrak{A}(\mathbf{D}((F_i)_0^n,(\zeta_i)_1^n))$ is F_n by [KW, Theorem 3.4]. By (i), this handles the case $|F_n|>2$. If $|F_n|=2$ see [KW, Theorem 3.31(ii)]. □

Presumably (ii) is true without any hypotheses other than $n\geqslant 1$ and $|F|>8$. The above special case is somewhat stronger than a previous one in [KW, Theorem 3.31] when $|F_n|>2$; (i) is stronger than [KW, Proposition 3.27].

Theorem 1.1 gives a lower bound that is useful only when m has several prime factors. We can now provide a small amount of information in the opposite situation:

Corollary 4.16. *There are at least three pairwise nonisomorphic semifield planes of order 2^p for any prime $p>3$: $\mathfrak{A}(\mathbf{D}((F,\mathrm{GF}(2)),(1))$, $\mathfrak{A}(\mathbf{D}((F,\mathrm{GF}(2)),(1))^*$ and Knuth's plane $\mathfrak{A}(\mathbf{D}((F,\mathrm{GF}(2)),(1))^{*\mathbf{d}} = \mathfrak{A}(\mathbf{B}((F,\mathrm{GF}(2)),(1))$.*

Proof. By the preceding corollary, $\mathfrak{A}(\mathbf{D}((F,\mathrm{GF}(2)),(1))$ and $\mathfrak{A}(\mathbf{D}((F,\mathrm{GF}(2)),(1))^*$ are not isomorphic, whereas $\mathfrak{A}(\mathbf{B}((F,\mathrm{GF}(2)),(1))$ is self-dual. □

4.5. Boring planes

A semifield plane of order q^m is called *boring* if its full collineation group is as small as possible: order $q^{3m}|K^*|$, where K is the kernel of the plane. By Theorem 4.7, in the present setting this means that the order is q^{3m}, which is as small as possible for any semifield plane of order q^m.

Proposition 4.17. *If m is composite and not a power of 3 then there are at least $(2^m-1)^{\rho(m)-2}2^m/2m$ pairwise nonisomorphic boring commutative semifield planes of order 2^m. If $m\geqslant 3^4$ is a power of 3, then this number is at least $(2^m-3)^{\rho(m)-3}2^m/2m$.*

Proof. By Theorem 4.5, we merely need to guarantee that $A\Lambda = 1$. Use $|F_n| = 2$ so that $A = 1$. In order to deal with Λ and the count, we will assume that m is not a power of 3, leaving the excluded case to the reader.

Consider a chain $(F_i)_0^{\rho(m)}$ of subfields of F in which each has prime degree over the next and $[F : F_1] > 3$. Let $(\zeta_i)_1^{\rho(m)}$ be a sequence of elements of F^* such that $\zeta_1 = 1$ and ζ_2 is any generator of F over $\mathrm{GF}(2)$; there are at least $(2^m - 1)^{\rho(m)-2}|F|/2$ such sequences. Since the stabilizer of $\zeta_1^{-1}\zeta_2$ in $\mathrm{Aut}(F)$ is trivial, Theorem 4.5 implies that the number of planes obtained is at least $(2^m - 1)^{\rho(m)-2}|F|/2|\,\mathrm{Aut}(F)|$. □

5. Other commutative semifields

In this section we survey the previously known finite commutative semifields in light of Proposition 3.8. In each case we will have planes of order p^n for an odd prime p. The numbers of pairwise nonisomorphic commutative semifield planes of that order in the various sections is as follows:

$[(n-1)/2]$	in Section 5.1:	Albert's generalized twisted fields
1	in Section 5.2:	Coulter–Matthews semifield
$[n/4]$	in Section 5.3:	Dickson semifields
1	in Section 5.4:	Cohen–Ganley semifield
1	in Section 5.5:	Ganley semifield
1	in Section 5.6:	Penttila–Williams semifield

Thus, the total number *known* of order p^n is less than $\log p^n$. Each member of the last four families has square order, which is the case for some members of the first family but none in the second one.

5.1. *Twisted fields*

Albert [Al4,Al5] defined *generalized twisted fields* as follows: Let $F = \mathrm{GF}(q)$, where q can be odd or even. Let $\alpha, \beta \in \mathrm{Aut}(F)$ and $j \in F^*$ be such that the equation $j = x^{\alpha-1}y^{\beta-1}$ has no solutions. Then

$$x * y = xy - jx^{\alpha}y^{\beta} \tag{5.1}$$

defines a presemifield $(F, +, *)$; a corresponding semifield is called a *generalized twisted field* $\mathbf{T}(q, \alpha, \beta, j)$ if $\alpha \neq \beta$, $\alpha \neq 1$, $\beta \neq 1$, with corresponding affine plane $\mathfrak{A}(q, \alpha, \beta, j)$.

Proposition 5.2.

(i) $\mathfrak{A}(q, \alpha, \beta, j)^* \cong \mathfrak{A}(q, \beta, \alpha, j)$.
(ii) $\mathfrak{A}(q, \alpha, \beta, j)^{*\mathbf{d}} \cong \mathfrak{A}(q, \beta^{-1}, \alpha\beta^{-1}, j^{-\beta^{-1}})$.

Proof.
(i) This is obvious.

(ii) The spread corresponding to $\mathfrak{A}(q,\alpha,\beta,j)^*$ has members $x=0$ and $\{(x,m*x) \mid x\in F\}$, $m\in F$. We will use the alternating bilinear form $((x,y),(u,v))=T(xv-yv)$ on $F\oplus F$, where T is the trace map to the prime field.

For each $m\in F$ we need to find all (u,v) such that $0=((x,m*x),(u,v))=T(xv-[mx-jm^\alpha x^\beta]u)$ for all $x\in F$. Since $0=T(xv-xum)+T(xj^{-\beta^{-1}}m^{-\alpha\beta^{-1}}u^{\beta^{-1}})$ we have $v-um+j^{-\beta^{-1}}m^{-\alpha\beta^{-1}}u^{\beta^{-1}}=0$. Consequently, we obtain the subspace $\{(u,um-j^{-\beta^{-1}}v^{\beta^{-1}}m^{-\alpha\beta^{-1}}) \mid u\in F\}$, which proves (ii). □

In [BKL] the generalized twisted field planes $\mathfrak{A}(q,\alpha^2,\alpha,-1)$ were shown to be symplectic. In view of Propositions 3.8 and 5.2, we should look at $\mathbf{T}(q,\alpha,\alpha^{-1},-1)$. Here multiplication is given by $x\circ y=xy+x^\alpha y^{\alpha^{-1}}$, and is clearly not commutative; but the isotope $x\circ' y:=x\circ y^\alpha=xy^\alpha+x^\alpha y$ is commutative. The result in [BKL] can now be slightly strengthened:

Proposition 5.3.

(i) *A generalized twisted field plane is coordinatized by a commutative semifield if and only if it has the form $\mathfrak{A}(q,\alpha^{-1},\alpha,-1)$ with q odd.*
(ii) *A generalized twisted field plane has a symplectic spread if and only if it has the form $\mathfrak{A}(q,\alpha^2,\alpha,-1)$ with q odd.*
(iii) *The generalized twisted field planes $\mathfrak{A}(q,\alpha^{-1},\alpha,-1)$ with q odd and α of order 3 are precisely the ones for which all planes obtained using the six permutations of Knuth's cubical array are isomorphic.*

Proof.

(i) Albert [Al4,Al5] proved that every semifield coordinatizing a generalized twisted field plane is a generalized twisted field, and that the only commutative ones among these are as stated.

(ii) This follows from (i) and Propositions 3.8 and 5.2.

(iii) This is clear from (i) and (ii). □

Remark. There are self-dual planes $\mathfrak{A}(q,\alpha,\beta,j)$ that do not arise from commutative semifields [BJJ, pp. 120, 121]. Correspondingly, there are planes $\mathfrak{A}(q,\alpha,\beta,j)$ whose spreads Σ are equivalent to their duals $\Sigma^{\mathbf{d}}$ but are not symplectic.

Corollary 5.4. *No generalized twisted field plane is isomorphic to any of the planes $\mathfrak{A}(\mathbf{B}((F_i)_0^n,(\zeta_i)_1^n))$, $\mathfrak{A}(\mathbf{B}((F_i)_0^n,(\zeta_i)_1^n))^*$ or $\mathfrak{A}(\mathbf{B}((F_i)_0^n,(\zeta_i)_1^n))^{*\mathbf{d}}$.*

Proof. There are no commutative generalized twisted fields in characteristic 2, and if $\mathfrak{A}$ is a generalized twisted field plane then, by Proposition 5.2, so are $\mathfrak{A}^*$ and $\mathfrak{A}^{\mathbf{d}}$. □

The number of generalized twisted field planes. By [Al5] (cf. [BJJ, Theorem 6.1]), $\mathfrak{A}(q,\alpha,\beta,j)\cong\mathfrak{A}(q,\alpha',\beta',j')$ if and only if $\alpha'=\alpha^{\pm1}$, $\beta'=\beta^{\pm1}$ and $j'=(ja^{\alpha-1}b^{\beta-1})^{\pm\theta}$ for some $a,b\in F^*,\theta\in\mathrm{Aut}(F)$ and sign ±. Let $q=p^n$ with p prime. Then it follows that *the number of pairwise nonisomorphic nondesarguesian generalized twisted field planes of order* $q = p^n$ *is less than* $(n-1)(n-2)\{(p^n-1)/(p^{n/2}-1)\}/n < np^{n/2} \leqslant \sqrt{q}\log q$.

However, we are especially concerned with *commutative* semifield planes. As noted above, by [Al5] any semifield coordinatizing a generalized twisted field plane is a generalized twisted field. The commutative ones are $\mathfrak{A}(q,\alpha^{-1},\alpha,-1) \cong \mathfrak{A}(q,\alpha,\alpha^{-1},-1)$ with $\alpha \neq \alpha^{-1}$, so that the number of nonisomorphic nondesarguesian ones is $[(n-1)/2]$.

5.2. Coulter–Matthews presemifields

Coulter and Matthews [CM] introduced presemifields $\mathbf{CM}(3^e) = (F,+,*)$, where $F = \mathrm{GF}(3^e)$ with $e > 1$ odd, somewhat resembling those of the preceding section:

$$x * y = x^9y + xy^9 + x^3y^3 - xy \tag{5.5}$$

(cf. Remark 4 in Section 6). R. Coulter has informed me that, if $e \geqslant 3$, then these planes are nondesarguesian, and moreover they are not twisted field planes (concerning the latter he notes "that is more of a sketch than a proof at this stage"). Since the order is not a square, these are the only possibilities for known commutative semifield planes to which any $\mathbf{CM}(3^e)$ plane might be isomorphic.

As in Section 5.1, using the alternating bilinear form $((x,y),(u,v)) = T(xv - yv)$ on $F \oplus F$ produces the presemifield $(F,+,\bullet)$ given by

$$x \bullet y = x^9y + (xy)^{1/9} + xy^{1/3} - xy. \tag{5.6}$$

The corresponding spread is symplectic with respect to that form.

5.3. Dickson semifields

Assume that q is odd, let j be a nonsquare in $K = \mathrm{GF}(q)$, and let $1 \neq \sigma \in \mathrm{Aut}(K)$. Following [De, p. 241] define the commutative Dickson semifield $\mathbf{D}(q,\sigma) = (K^2,+,*)$ [Di3] by

$$(a,b) * (c,d) = \bigl(ac + jb^\sigma d^\sigma, ad + bc\bigr), \tag{5.7}$$

and the Knuth semifield $\mathbf{K}(q,\sigma) = (K^2,+,\bullet)$ [Kn1] by

$$(a,b) \bullet (c,d) = \bigl(ac + j^{-1}bd^\sigma, ad + bc\bigr). \tag{5.8}$$

In both cases, different choices for j produce isotopic semifields and hence isomorphic planes.

Theorem 5.9. $\mathfrak{A}(\mathbf{D}(q,\sigma))^{\mathbf{d}*} \cong \mathfrak{A}(\mathbf{K}(q,\sigma^{-1}))$.

Proof. This time we use the alternating bilinear form

$$\big((a,b,c,d),(s,t,u,v)\big)=T(av+bu-ct-ds) \tag{5.10}$$

on K^4, where T denotes the trace from K to the prime field.

Consider the member $\{(a,b,an+bm,bn+ja^\sigma m^\sigma)\mid a,b\in K\}$ of the spread for $\mathbf{D}(q,\sigma)$. We need to find all $(s,t,u,v)\in K^4$ such that

$$0=T\big(av+bu-\big[am+jb^\sigma n^\sigma\big]t+[an+bm]s\big)\quad \text{for all } a,b\in K.$$

When $a=0$ this says that $T(b[u-j^{\sigma^{-1}}nt^{\sigma^{-1}}-ms])=0$ for all b, so that $u=j^{\sigma^{-1}}nt^{\sigma^{-1}}+ms$. When $b=0$ we have $T(a[v-mt-ns])=0$, so that $v=mt+ns$. Thus, we obtain the 2-space $\{(s,t,ms+j^{\sigma^{-1}}nt^{\sigma^{-1}},mt+ns)\mid s,t\in K\}$. This is a member of the spread obtained using $(K^2,+,\bullet^*)$. □

It is straightforward to check directly that the spread for $\mathbf{D}(q,\sigma)$ is symplectic with respect to the form (5.10). See [Bu,Sa] for complete solutions to the isotopism and autotopism questions for Dickson semifields. In particular, if $q=p^e$ for a prime p, then these semifields produce $[e/2]$ pairwise nonisomorphic nondesarguesian planes of order q^2. Note that these planes are not isomorphic to twisted field planes because their collineation groups behave differently [Al4,Bu].

The above argument also shows that, for the semifield $\mathbf{S}(q,\alpha,\beta,\theta,j)=(K^2,+,\circ)$ defined by

$$(a,b)\circ(c,d)=\big(ac+jb^\alpha d^\beta,ad+bc^\theta\big)$$

where $\alpha,\beta,\theta\in\operatorname{Aut}(K)$ and $j\in K^*$ (cf. [Kn1, pp. 213–214], [De, p. 241]),

$$\mathfrak{A}\big(\mathbf{S}(q,\alpha,\beta,\theta,j)\big)^{\mathbf{d}}\cong\mathfrak{A}\big(\mathbf{S}\big(q,\alpha^{-1},\beta\alpha^{-1},\theta^{-1},-j^{\alpha^{-1}}\big)\big). \tag{5.11}$$

We note that the semifields discovered by Prince [Pr] are isotopic to the Dickson ones, according to [BB,BL].

5.4. Cohen–Ganley semifields

Let $q\geqslant 9$ be a power of 3 and let $j\in K=GF(q)$ be a nonsquare. The Cohen–Ganley[2] commutative semifield $\mathbf{CG}(q)=(K^2,+,*)$ [CG] is defined by

$$(a,b)*(c,d)=\big(ac+jbd+j^3(bd)^9,ad+bc+j(bd)^3\big),$$

and the Thas–Payne semifield $\mathbf{TP}(q)=(K^2,+,\bullet)$ is defined by

$$(a,b)\bullet(c,d)=\big(ac+jbd+j^{1/3}bc^{1/9}+j^{1/3}bd^{1/3},ad+bc\big).$$

[2] This is sometimes called a “Ganley semifield”, but Ganley [Ga] is clear about its origin.

In [TP] the focus is on ovoids of the generalized quadrangle $Q(4,q)$; those ovoids are equivalent to the required symplectic spreads by the Klein correspondence. Up to isomorphism there is exactly one of each of these planes for each possible q. As above, the following is straightforward using (5.10):

Theorem 5.12. $\mathfrak{A}(\mathbf{CG}(q))^{\mathbf{d}*} \cong \mathfrak{A}(\mathbf{TP}(q))$.

5.5. *Ganley semifields*

Let $K = \mathrm{GF}(q)$, $q = 3^r$, with $r \geqslant 3$ odd. Ganley [Ga] constructed another commutative semifield $\mathbf{G}(q) = (K^2, +, *)$, defined by

$$(a,b) * (c,d) = \bigl(ac - b^9 d - bd^9, ad + bc + b^3 d^3\bigr). \tag{5.13}$$

In fact, he defined a number of semifields of size q^2 each of which is isotopic to a commutative semifield, but it is easy to check that they are all isotopic to (5.13).

This time another straightforward calculation shows that $\mathbf{G}(q)^{\mathbf{d}} = (K^2, +, \bullet^*)$, where

$$(a,b) \bullet (c,d) = \bigl(ac + bc^{1/3} - b^{1/9} d^{1/9} - b^9 d, ad + bc\bigr) \tag{5.14}$$

determines a spread that is symplectic with respect to the form (5.10). Note that this is *not* a spread of K^4, since the kernel of $(K^2, +, \bullet)$ is GF(3); it is symplectic only as a spread of $\mathrm{GF}(3)^{4r}$. These, and the spreads arising from Proposition 5.3(ii) or (5.6), are *the only symplectic spreads presently known in vector spaces of odd characteristic and having dimension greater than* 4 *over their kernels.*

5.6. *The Penttila–Williams semifield*

Let $K = \mathrm{GF}(3^5)$. Penttila and Williams [PW] discovered an ovoid of $Q(4, 3^5)$. The corresponding spread (under the Klein correspondence), determined by the semifield $(K^2, +, \bullet)$ given by

$$(a,b) \bullet (c,d) = \bigl(ad + bd^9 + bc^{27}, ac + bd\bigr),$$

is symplectic with respect to the form (5.10). This time Proposition 3.8 produces a commutative semifield $(K^2, +, *)$ (cf. [BLP, p. 60]) given by

$$(a,b) * (c,d) = \bigl(ac + (bd)^9, ad + bc + (bd)^{27}\bigr).$$

Remark. Each of the Dickson, Cohen–Ganley and Penttila–Williams semifields differs from the other commutative semifields discussed in this paper by having rank 2 over its middle nucleus.

6. Concluding remarks

1. The main problem concerning commutative semifields is that there are too few of them known. In particular, more of them in characteristic 2 having odd dimension over GF(2) would immediately feed into the coding-theoretic machinery in [CCKS] and produce extremal $\mathbb{Z}_4$-linear codes and extremal line-sets in Euclidean spaces.

Albert [Al1, p. 309] observed back in 1952 that "No central finite commutative division algebras of characteristic two are known and the question of their existence is a major problem of our theory." Of course, Knuth [Kn2] settled this problem in 1965. However, the results of the present paper now indicate a major problem in the opposite direction, since now there are many different semifield planes known in characteristic 2 but not so many in odd characteristic. To be more precise, if $S(x)$ denotes the number of *known* commutative semifield planes of order at most equal to the real number x, and $S_2(x)$ denotes the corresponding number for planes of even order, then $\lim_{x\to\infty} S_2(x)/S(x) = 1$.

On the other hand, there are more *types* of constructions of commutative semifields known in odd characteristic than in characteristic 2. Constructions are needed that produce significantly larger numbers of planes than appear in Section 5: the above (time-dependent!) limit should be 0.

2. By Proposition 5.3(i), (ii), the twisted field planes $\mathfrak{A}(q, \alpha^2, \alpha, -1)$ with q odd and α of order 3 have a property in common with desarguesian planes: they are *simultaneously commutative semifield planes and symplectic planes*. No other known planes share both of these properties.

Both of the nondesarguesian semifield planes of order 16 have the following in common with the preceding planes: they have exactly one "image" under the action of Knuth's S_3 [Kn1, p. 209]. However, these planes do not arise from commutative semifields, and hence also not from symplectic semifields. (There is a subtle difference between a plane being self-dual and being coordinatized by a commutative semifield.)

There are many more examples of this phenomenon. For example, all semifields $(K^2, +, *)$ with

$$(a, b) * (c, d) = \bigl(ac + bd^\sigma j, ad + bc^\sigma\bigr),$$

for an involutory automorphism σ of K and $j \notin K^{\sigma+1}$ (cf. [HK]), behave in this manner.

3. *All* known symplectic spreads in odd characteristic, having dimension greater than 4 over their kernels, are semifield spreads. This is not, however, the case in characteristic 2 [Ka1,KW].

4. Commutative semifields in odd characteristic arose in research of Dembowski and Ostrom [DO] (compare [De, p. 245]). In that paper these authors were concerned with *planar functions*, which they invented in order to try to construct new finite affine planes admitting groups that are point-regular but do not consist of translations. The function they used that arises from a commutative presemifield was just $f(x) = x * x$; the associated plane is the one coordinatized by the presemifield. Conversely, each planar function f corresponding to a commutative presemifield of odd characteristic determines that presemifield via $x * y = [f(x + y) - f(x) - f(y)]/2$.

Dembowski and Ostrom then discussed examples arising from fields, commutative twisted fields or Dickson semifields. At that time the examples in Sections 5.2, 5.4, 5.5 and 5.6 were not known.

5. The presemifield (4.2) has exactly the same appearance as in Knuth's paper [Kn2]: $x * y = xy + (xf(y) + yf(x))^2$. The fundamental difference is that $f : F \to F_1$ was F_1-linear in [Kn2], whereas we have used more general additive maps $F \to F_1$. Are there still more additive maps $f : F \to F_1$ for which this formula produces presemifields? In view of Proposition 3.8 and [KW] it seems unlikely that there are other possibilities.

6. Menichetti [Me] proved a striking result concerning presemifields $\mathbf{S} = (F, +, *)$, $F = \mathrm{GF}(q^n)$, for which $*$ is both left and right $\mathrm{GF}(q)$-linear: *for a given prime n*, if q is sufficiently large then **S** is isotopic to a field or a generalized twisted field. This should be compared with Corollary 4.16.

7. In the course of the research in [Ka2] I came across symplectic semifields (5.8) that turned out to have been dealt with earlier by Knuth [Kn1]. The work on semifields in [Ka1, KW] now turns out also to be related to other semifields studied by Knuth [Kn2] by using the ideas in [Kn1]. This suggests that [Kn1] has been neglected for many years. The results in [BB] further emphasize this point.

8. In 1965, at the end of my first year as a graduate student, R.H. Bruck arranged for me to spend the summer studying at the University of Chicago. A.A. Albert took off about an hour each week from his duties as Dean in order to guide me through his papers [Al3, Al4,Al5], among others. It is quite a pleasant surprise that the results studied so long ago arose in the present paper.

Acknowledgment

I am grateful to the referee for pointing out the semifields in [CM]. His comments also led to Remark 4.

References

[Al1] A.A. Albert, On nonassociative division algebras, Trans. Amer. Math. Soc. 72 (1952) 296–309.

[Al2] A.A. Albert, Finite division algebras and finite planes, in: Proc. Sympos. Appl. Math., Vol. 10, 1960, pp. 53–70.

[Al3] A.A. Albert, On the collineation groups associated with twisted fields, in: Calcutta Math. Soc. Golden Jubilee Commemoration, 1958/1959, Part II, 1963, pp. 485–497.

[Al4] A.A. Albert, Generalized twisted fields, Pacific J. Math. 11 (1961) 1–8.

[Al5] A.A. Albert, Isotopy for generalized twisted fields, An. Acad. Brasil. Ciênc. 33 (1961) 265–275.

[BB] S. Ball, M.R. Brown, The six semifield planes associated with a semifield flock, Preprint.

[BJJ] M. Biliotti, V. Jha, N. Johnson, The collineation groups of generalized twisted field planes, Geom. Dedicata 76 (1999) 97–126.

[BKL] L. Bader, W.M. Kantor, G. Lunardon, Symplectic spreads from twisted fields, Boll. Un. Mat. Ital. 8-A (1994) 383–389.

[BL] S. Ball, M. Lavrauw, Commutative semifields of rank 2 over their middle nucleus, in: G.L. Mullen et al. (Eds.), Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer, Berlin, 2002, pp. 1–21.

[BLP] L. Bader, G. Lunardon, J. Pinneri, A new semifield flock, J. Combin. Theory Ser. (A) 86 (1999) 49–62.

[Bu] M.V.D. Burmester, On the commutative non-associative division algebras of even order of L.E. Dickson, Rend. Mat. Appl. 21 (1962) 143–166.

[CCKS] A.R. Calderbank, P.J. Cameron, W.M. Kantor, J.J. Seidel, $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, Proc. London Math. Soc. 75 (1997) 436–480.

[CG] S.D. Cohen, M.J. Ganley, Commutative semifields, two-dimensional over their middle nuclei, J. Algebra 75 (1982) 373–385.

[CW] M. Cordero, G.P. Wene, A survey of finite semifields, Discrete Math. 208/209 (1999) 125–137.

[CM] R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz–Barlotti class II, Des. Codes Cryptogr. 10 (1997) 167–184.

[De] P. Dembowski, Finite Geometries, Springer, Berlin, 1968.

[DO] P. Dembowski, T.G. Ostrom, Planes of order n with a collineation group of order n^2, Math. Z. 103 (1968) 239–258.

[Di1] L.E. Dickson, On finite algebras, Göttingen Nachrichtung (1905) 358–393.

[Di2] L.E. Dickson, Linear algebras in which division is always uniquely possible, Trans. Amer. Math. Soc. 7 (1906) 370–390.

[Di3] L.E. Dickson, On commutative linear algebras in which division is always uniquely possible, Trans. Amer. Math. Soc. 7 (1906) 514–522.

[Ga] M.J. Ganley, Central weak nucleus semifields, European J. Combin. 2 (1981) 339–347.

[HK] D.R. Hughes, E. Kleinfeld, Seminuclear extensions of Galois fields, Amer. J. Math. 82 (1960) 389–392.

[Ka1] W.M. Kantor, Spreads, translation planes and Kerdock sets I, II, SIAM J. Alg. Discr. Meth. 3 (1982) 151–165; SIAM J. Alg. Discr. Meth. 3 (1982) 308–318.

[Ka2] W.M. Kantor, Ovoids and translation planes, Canad. J. Math. 34 (1982) 1195–1207.

[Ka3] W.M. Kantor, Expanded, sliced and spread spreads, in: N.L. Johnson et al. (Eds.), Finite Geometries. Proc. Conf. in Honor of T.G. Ostrom, Dekker, New York, 1983, pp. 251–261.

[Ka4] W.M. Kantor, Codes, quadratic forms and finite geometries, in: A.R. Calderbank (Ed.), Different Aspects of Coding Theory, in: Proc. Amer. Math. Soc. Sympos. Appl. Math., Vol. 50, 1995, pp. 153–177.

[Kn1] D.E. Knuth, Finite semifields and projective planes, J. Algebra 2 (1965) 182–217.

[Kn2] D.E. Knuth, A class of projective planes, Trans. Amer. Math. Soc. 115 (1965) 541–549.

[KW] W.M. Kantor, M.E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes, Trans. Amer. Math. Soc., in press. http://darkwing.uoregon.edu/~kantor/PAPERS/semifieldZ4Codes2.pdf.

[Ma] A. Maschietti, Symplectic translation planes and line ovals, Adv. Geom., in press.

[Me] G. Menichetti, n-dimensional algebras over a field with a cyclic extension of degree n, Geom. Dedicata 63 (1996) 69–94.

[Pr] A.R. Prince, Two new families of commutative semifields, Bull. London Math. Soc. 32 (2000) 547–550.

[PW] T. Penttila, B. Williams, Ovoids of parabolic spaces, Geom. Dedicata 82 (2000) 1–19.

[Sa] R. Sandler, The collineation groups of some finite projective planes, Portugal. Math. 21 (1962) 189–199.

[Ta] D.E. Taylor, The Geometry of the Classical Groups, Heldermann, Berlin, 1992.

[TP] J.A. Thas, S.E. Payne, Spreads and ovoids in finite generalized quadrangles, Geom. Dedicata 52 (1994) 227–253.