Finite semifields

William M. Kantor

Abstract. This note surveys the known finite semifields and discusses the question: *How many finite semifields of a given order are there up to isotopism?*

1. Introduction

A familiar topic in finite geometry is that of finite semifields (division algebras that are not necessarily associative) and their planes. This paper is intended as a survey of some aspects of this subject. See [CW] for a more thorough discussion of additional topics.

2. Wedderburn's Theorem?

Every finite division algebra is commutative. This familiar and now-elementary theorem is attributed to Wedderburn. This is discussed with great care in [Par] (together with the related development of *Veblen-Wedderburn systems*–which we now call "quasifields"–in [VW]). Wedderburn was the first to publish the theorem in 1905, with three proofs in a four-page paper [Wed]. His first proof has a nontrivial hole; this was noticed more than 20 years later by Artin [Art]. The second and third proofs in Wedderburn's short paper used an idea in Dickson's 1905 paper [Di1, p. 379]: primitive prime divisors[1]. If this happened nowadays the theorem would probably be called the "Wedderburn-Dickson Theorem".

2000 Mathematics Subject Classification: Primary 51A40, 17A35; Secondary 05B25, 51A35, 51A50.

[1]Earlier in 1905 Dickson [Di2] rediscovered Zsigmondy's Theorem [Zs] (cf. [Di1, p. 379]).

3. Albert and Knuth

3.1. Isotopy.

A *presemifield* $\mathbf{P} = (F, +, *)$ consists of an additive group $(F, +)$ together with a binary operation $*$ that satisfies both distributive laws together with the requirement that $x * y = 0 \iff x = 0$ or $y = 0$. It is a *semifield* if it has an identity element 1. A translation plane $\mathfrak{A}(\mathbf{P})$ is obtained in the usual way: F^2 is the set of points, and lines are the sets $x = c$ and $y = x * m + b$.

An *isotopism* between two presemifields $\mathbf{P} = (F, +, *)$ and $\mathbf{P}' = (F', +, \circ)$ is a triple (α, β, γ) of additive bijections $F \to F'$ such that

$$(x * y)\gamma = x\alpha \circ y\beta \quad \forall x, y, z \in F. \tag{3.1}$$

Any presemifield $\mathbf{P} = (F, +, *)$ *is isotopic to a semifield*: fix any $0 \neq e \in F$ and define $\circ$ by $(x * e) \circ (e * y) = x * y$ for all $x, y \in F$. Then $(F, +, \circ)$ is a semifield with identity $e * e$, and is obviously isotopic to $\mathbf{P}$. If $(F, +, *)$ is commutative then so is each such semifield $(F, +, \circ)$.

The notion of isotopy was introduced by Albert for purely algebraic reasons [Al1]. However, it enters geometry in view of the following fundamental but elementary result of his:

Theorem 3.1. [Al2] *Two semifields coordinatize isomorphic planes if and only if they are isotopic.*

3.2. Knuth's cubical arrays.

Let $\mathbf{P} = (K^n, +, \circ)$ be a presemifield, with associated translation plane $\mathfrak{A}(\mathbf{P})$; here K is any finite field. 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 multiplication in $\mathbf{P}$ is determined by equations of the form

$$v_i \circ v_j = \sum_k a_{ijk} v_k \tag{3.2}$$

for some $a_{ijk} \in K$. The *cubical array* (a_{ijk}) was introduced and studied by Knuth [Kn1]. He 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. We will describe this from a somewhat different perspective [BB, Ka5] than in [Kn1].

The affine plane $\mathfrak{A} = \mathfrak{A}(\mathbf{P})$ determines a projective plane, whose *dual* is in fact a semifield plane $\mathfrak{A}^*$ defined over the *opposite* presemifield $(K^n, +, \circ^*)$, where $x \circ^* y = y \circ x \quad \forall x, y \in K^n$.

The spread for $\mathfrak{A}$ [De, Section 5.1], consisting of the subspaces of $V = K^n \oplus K^n$ that are the lines of $\mathfrak{A}$ through 0, produces a *dual* spread in the dual space of V,

and hence also another translation plane which is, once again, a semifield plane $\mathfrak{A}^{\mathbf{d}}$.

The involutory maps $\mathfrak{A} \to \mathfrak{A}^*$ and $\mathfrak{A} \to \mathfrak{A}^{\mathbf{d}}$ generate Knuth's S_3 [BB, Ka5].

Knuth had already noticed by 1965 that there is a nice interpretation for his map $\mathfrak{A} \to \mathfrak{A}^{\mathbf{d}}$ that extends to quasifields other than semifields: use the transposes of the right multiplications $x \to x * m$. This is just another way to describe the dual spread indicated above.

Symplectic spreads. A spread Σ of V is called *symplectic* if there is a non-degenerate alternating bilinear form $(\ ,\ )$ on V such that $(X, X) = 0$ for each $X \in \Sigma$. Symplectic spreads have been studied in [Dil, Dy, Ka1, Ka3, Ka4, Ka5, BKL, CCKS, BB, KW1, KW2, Ma, BBP]. There are surprisingly few different *types* of constructions of symplectic spreads presently known in odd characteristic [BKL, Ka5, BBP]. The most interesting and original research presently being done with symplectic spreads in characteristic 2 is that of Maschietti [Ma], who relates such spreads to very special types of line ovals in the corresponding affine planes.

The relevance of this notion to semifields is the following elementary observation:

Proposition 3.2. [Ka5, Proposition 3.8] *For a semifield plane* $\mathfrak{A}$, *some presemifield for* $\mathfrak{A}$ *is commutative if and only if some spread for* $\mathfrak{A}^{\mathbf{d}*}$ *is symplectic.*

We will call a presemifield or a semifield plane *symplectic* if the corresponding spread is symplectic.

3.3. Albert's twisted fields.

Albert [Al4, Al5] defined a (generalized) *twisted field* as a semifield associated to the presemifield $(F, +, *)$, where F is a finite field and

$$x * y = xy - jx^{\alpha}y^{\beta} \tag{3.3}$$

for some nontrivial $\alpha, \beta \in \mathrm{Aut}(F)$. He obtained the precise conditions for two twisted fields to be isotopic (cf. [BJJ]).

The twisted field planes with $\beta = \alpha^2$ and $j = -1$, where q is odd and α has 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.

3.4. Dickson and Knuth semifields.

Assume that q is odd, let k be a nonsquare in $K = \mathrm{GF}(q)$, and let $1 \neq \sigma \in \mathrm{Aut}(K)$. The commutative Dickson semifield $(K^2, +, *)$ [Di1] has

$$(a, b) * (c, d) = (ac + kb^{\sigma}d^{\sigma}, ad + bc). \tag{3.4}$$

Different choices k produce isotopic semifields and hence isomorphic planes.

In his 1963 Ph. D. research under Marshall Hall, Jr., Knuth introduced the cubical arrays mentioned earlier, together with two very different families of semifields [Kn1]. The first of these generalized Dickson's construction as follows. Let α, β, τ be automorphisms of K, at least one of which is nontrivial; let $1 \neq \sigma \in \mathrm{Aut}(K)$; let $k \in K - (K^{\alpha+1}K^{\tau+1}K^{\beta-1})$ if possible; and let the polynomial $t^{\sigma+1} + gt - f$ have no root in K, where $f, g \in K$. Then each of the following rules for $(a,b) * (c,d)$ produces a semifield $(K^2, +, *)$:

1. $(ac + kb^\alpha d^\beta, a^\tau d + bc)$
2. $(ac + fb^\sigma d^{\sigma^{-2}}, bc + a^\sigma d + gb^\sigma d^{\sigma^{-1}})$
3. $(ac + fb^\sigma d, bc + a^\sigma d + gb^\sigma d)$
4. $(ac + fb^{\sigma^{-1}} d^{\sigma^{-2}}, bc + a^\sigma d + gbd^{\sigma^{-1}})$
5. $(ac + fb^{\sigma^{-1}} d, bc + a^\sigma d + gbd)$.

The planes determined by the semifields 1, with $\alpha = \tau$ of order 2 and $\beta = 1$, were studied in [HuK]. They have the following in common with the specific twisted field planes mentioned at the end of Section 3.3: they have exactly one "image" under the action of Knuth's S_3. 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.)

3.5. Knuth's "binary" semifields [Kn2].

Knuth's second [Kn2], very different type of presemifield $(F, +, *)$ uses $F = \mathrm{GF}(q^n)$ with q even and $n > 1$ odd, together with the trace map $T\colon F \to \mathrm{GF}(q)$:

$$x * y = xy + (T(x)y + T(y)x)^2. \tag{3.5}$$

We will generalize these in Section 5.3. For now we comment on *how* Knuth discovered these semifields. In the early 1960's, Walker [Wa] and Knuth (cf. [HaK]) independently enumerated all isotopism types of semifields of order 32 using computer calculations. (Note that the computers used were extraordinarily weak by present-day standards–and not simple to program.) Knuth examined the results and managed to see that one of the semifields could be constructed in the manner just indicated.

4. More commutative or symplectic semifields

4.1. Cohen–Ganley commutative semifields [CG].

These are defined as $(K^2, +, *)$ where

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

with $q \geq 9$ a power of 3 and $j \in K = \mathrm{GF}(q)$ a nonsquare. Different choices j produce isotopic semifields.

4.2. Thas–Payne semifields [TP].

These symplectic semifields $(K^2, +, *)$ are obtained from the preceding ones using Proposition 3.2, where

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

with $q \geq 9$ a power of 3 and $j \in K = \mathrm{GF}(q)$ a nonsquare.

4.3. Ganley semifields [Ga].

These are defined as $(K^2, +, *)$ using

$$(a, b) * (c, d) = (ac - b^9d - bd^9, ad + bc + b^3d^3), \tag{4.1}$$

with $K = \mathrm{GF}(q)$, $q = 3^r$, and $r \geq 3$ odd. This time Proposition 3.2 produces a symplectic semifield with multiplication

$$(a, b) * (c, d) = (ac + bc^{1/3} - b^{1/9}d^{1/9} - b^9d, ad + bc). \tag{4.2}$$

4.4. Coulter-Matthews semifields [CoM].

These are defined using a commutative presemifield $(F, +, *)$ with

$$x * y = x^9y + xy^9 + x^3y^3 - xy, \tag{4.3}$$

where $F = \mathrm{GF}(3^e)$ and $e > 3$ is odd; these are not isotopic to any previously known commutative semifields [CoH]. Proposition 3.2 produces the related symplectic presemifield with multiplication

$$x * y = x^9y + (xy)^{1/9} + xy^{1/3} - xy.$$

A few weeks after the Pingree Conference, Coulter informed me that Ding and Yuan [DiY] have observed a variation $(F, +, *)$ on (4.3), using

$$x * y = x^9y + xy^9 - x^3y^3 - xy$$

and F as before. Coulter and Henderson have determined that these commutative presemifields are not isotopic to any other known ones [CoH].

4.5. Johnson-Jha presemifields [JJ].

These are a beautifully simple generalization of previously known examples of semifields (cf. [Sa]). Consider a (right) d–dimensional vector space V over a finite field F, and let T be an irreducible *semilinear* transformation of V (that is, T leaves invariant no proper subspace of V; in particular, T is invertible).

Theorem 4.1. *$S = \sum_0^{d-1} FT^i$ consists of $|S| = |V|$ elements, with all nonzero ones invertible, and hence S determines a presemifield $(V, +, *)$ via $u * v = u(vf)$ for any additive isomorphism $f: V \to S$.*

Proof. If at least one of the scalars a_i is not 0, we need to show that $\sum_0^{d-1} a_i T^i$ is invertible. If some such transformation is not invertible then there is some nonzero vector v such that $\sum_0^{d-1} va_iT^i = 0$. Then there is some k such that $1 \le k \le d$ and $0 \ne va_kT^k = -\sum_0^{k-1} va_iT^i$. Since all powers of T are semilinear, $(vT^{k-1}F)T = va_kT^kF \subseteq \sum_0^{k-1} va_iT^iF \subseteq \langle vT^i \mid 0 \le i \le k-1\rangle$, so the latter is a proper T-invariant subspace, which is a contradiction. □

Different choices for f produce isotopic presemifields. For more about isotopy of these presemifields, see Section 6.2.

Note that the transpose of S has the same form, so that the map $\mathfrak{A} \to \mathfrak{A}^d$ in Section 3.2 preserves this class of semifield planes.

If T is a *linear* transformation then this construction produces a field.

4.6. The HMO construction [HMO].

Hiramine, Matsumoto and Oyama magically produce planes of order q^4 from ones of order q^2: Suppose that

$$(a,b) * (x,y) = (a,b)\begin{pmatrix} x & y \\ g(x,y) & h(x,y)\end{pmatrix}$$

defines a semifield on $K^2 = \mathrm{GF}(q)^2$ for some $g, h: K^2 \to K$. If $L = \mathrm{GF}(q^2)$ and $\lambda \in L - K$ with $\lambda^2 + \lambda \in K$, then the equations

$$f(x + y\lambda) = h(x,y) - g(x,y) + h(x,y)\lambda \quad (x, y \in K)$$

$$(s,t) \bullet (u,v) = (s,t)\begin{pmatrix} u & v \\ f(v) & \overline{u}\end{pmatrix}$$

define a semifield on L^2. (This process is not just about semifields: it also transforms quasifields of order q^2 to quasifields of order q^4. Also see [Jo].)

Note that isotopic semifields of order q^2 will, in general, produce non-isotopic ones of order q^4.

5. Recent semifields

5.1. Penttila–Williams sporadic symplectic semifield of order 3^5 [PW].

This arose in the discovery of a sporadic ovoid of $Q(4,3^5)$. The corresponding spread (under the Klein correspondence) is symplectic, determined by the semifield $(K^2,+,*)$ with

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

where $K=\mathrm{GF}(3^5)$. Proposition 3.2 then produces a commutative semifield $(K^2,+,*)$ (cf. [BLP, p. 60]) given by

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

5.2. Kantor–Williams symplectic presemifields [KW2].

Let $F=\mathrm{GF}(q^m)$ for q *even* and $m>1$ *odd*. Then $(F,+,*)$ is a symplectic presemifield, where

$$x*y=xy^2+\sum_{i=1}^{n}\Big(T_i\big(\zeta_i x\big)y+\zeta_i T_i\big(xy\big)\Big),$$

associated with the following data:

fields $F=F_0\supset F_1\supset\cdots\supset F_n\supseteq K=\mathrm{GF}(q)$, $n\geq 1$

trace maps $T_i\colon F\to F_i$

any sequence $(\zeta_1,\ldots,\zeta_n)$ of elements $\zeta_i\in F^*$.

All of these presemifields were obtained by starting with a desarguesian plane and applying an algorithm that produces precisely these examples. The algorithm involves the use of high-dimensional orthogonal spreads, with coding theory as one of the motivations. The presemifields with $F_1=K$ were first observed in [Ka1].

5.3. Associated commutative presemifields [Ka5].

Applying Proposition 3.2 to the preceding examples produces a lot of commutative presemifields in characteristic 2 associated with the same data as above:

$$x*y=xy+\Big(x\sum_{1}^{n}T_i(\zeta_i y)+y\sum_{1}^{n}T_i(\zeta_i x)\Big)^2,$$

generalizing Knuth's examples in Section 3.5 (where $n=1$ and $F_n=K$).

5.4. That's all.

We have now surveyed almost all of the *known* finite semifields, up to isotopism. Up to Knuth's S_3, the only further semifield planes in the literature are among six of order 64 constructed in [HuJ].

It is perhaps worth noting that there are other semifields that have appeared in the literature. For example, the ones in [Ze, Co, Pr] all describe isotopes of Dickson semifields (3.4); while the ones in [Ka2, Theorem 7.1] turn out to be (up to $\circ^*$ in Section 3.2) examples of some of Knuth's semifields 3. in Section 3.4 (with $\sigma = 2$).

Excluding fields, there are 2 isotopy classes of semifields of order 16 [Kl] and 5 of order 32 [Wa, HaK]. These computer-assisted results used very weak computers by modern standards; it is surprising that there has not yet been an enumeration of all semifields of order at most 256 since the resulting data might be useful for finding new general constructions. All semifields of order p^3 are twisted fields (for p an odd prime), and their number is known [Me1, Me2].

6. How many?

Conjecture: *The number of pairwise non-isomorphic semifield planes of order N is not bounded above by a polynomial in N.*

Equivalently: The number of pairwise non-isotopic presemifields of order N is not bounded above by a polynomial in N.

Better but not quite as "likely": *there is an exponential number of pairwise non-isotopic presemifields of order N.*

6.1. General results.

Several of the older constructions give the appearance of producing many planes. However, Albert's twisted fields produce fewer than N planes of order N [Al4, Al5, BJJ], while Knuth and similar constructions using $\mathrm{GF}(q)^2$ (Sections 3.4, 4.1, 4.2, 4.3, 4.4, 5.1) yield much fewer than $N = q^2$ planes of order N. Moreover:

- *For N odd the number* known *is less than N^3.*

- *For N even the conjecture is true*: the semifields defined in Section 5.2 do the job. The isomorphism problem for the corresponding planes is settled in [KW2] when restricted to the case $[F\colon F_1] > 3$. While further cases are also dealt with in [KW2, Ka5], the general case remains open. These isotopism questions are difficult, involving disgusting calculations together with properties of orthogonal geometries and affine planes as well as elementary group theory. The isomorphism problem for the planes arising in Section 5.3 is settled under the same restrictions [Ka5].

More precisely: if $S(N)$ denotes the number of *presently known* semifield planes of order at most N, and $S_2(N)$ denotes the corresponding number for planes of even order, then $\lim_{N\to\infty} S_2(N)/S(N) = 1$.

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

A similar conjecture can be made concerning symplectic translation planes in odd characteristic (cf. Section 3.2). In fact, almost all known odd characteristic symplectic spreads were already seen earlier in this paper (possibly after an application of Proposition 3.2). The only exceptions are some very new ones in [BBP].

6.2. Two upper bounds.

The HMO construction in Section 4.6 appears to provide quite a lot of semifields. However:

Theorem 6.1. (Kantor, unpublished) *The number of pairwise nonisomorphic planes of order q^4 obtained via the HMO construction from a plane of order q^2 is less than q^{10}.*

Consequently, the number of planes of order q^{2^k} obtained by iterated use of the HMO construction is not bounded above by polynomial in q^{2^k} only if the number of planes of order q^2 is not bounded above by polynomial in q^2.

There also appear to be a lot of semifields obtained using the Jha-Johnson construction (Section 4.5). Recall that $S = \sum_0^{d-1} FT^i$ determines a presemifield if T is an irreducible *semilinear* transformation on a vector space V. Clearly, *conjugates of T in $\Gamma\mathrm{L}(V)$ produce isomorphic presemifields* (but not conversely, as is easily seen using $\mathrm{GF}(q^d)$). Therefore, we need an upper bound on the number of $\Gamma\mathrm{L}(V)$-conjugacy classes of irreducible semilinear transformations on V:

Theorem 6.2. (Kantor-Liebler, unpublished) *The number of conjugacy classes is less than d^2q^d.*

This number probably is less than q^d. In any event, the number of these semifields of order $N = q^d$ is much less than N^3.

Examples of irreducible T:

1. Suitable $T \in N_{\Gamma L(V)}$(Singer cycle). Versions of these are provided in [JJ].
2. Let $F = \mathrm{GF}(q)$, $1 \neq \alpha \in \mathrm{Aut}(F)$, and $t \notin F^{\alpha+1}$. Then $T\colon F^2 \to F^2$, defined by

$$(x, y)T = (ty^\alpha, x^\alpha),$$

is a semilinear transformation that fixes no 1-space, so $F + FT$ determines a presemifield (it produces one of Knuth's semifields; cf. Section 3.4).

3. In general $\langle T\rangle$ transitively permutes the summands in a decomposition $V = V_1 \oplus \cdots \oplus V_r$, where T^r is irreducible and linear on each V_i.

References

[Al1] A. A. Albert, On nonassociative division algebras. TAMS 72 (1952) 296–309.

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

[Al3] A. A. Albert, On the collineation groups associated with twisted fields. 1958/1959 Calcutta Math. Soc. Golden Jubilee Commemoration Part II, 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. Ci. 33 (1961) 265–275.

[Art] E. Artin, Über einen Satz von Herrn J. H. Maclagan Wedderburn. Abh. Math. Sem. Hamb. 5 (1927) 245–250.

[BB] S. Ball and M. R. Brown, The six semifield planes associated with a semifield flock (to appear).

[BBP] S. Ball, J. Bamberg and T. Penttila, Symplectic spreads. Des. Codes Cryptography 32 (2004) 9–14.

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

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

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

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

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

[Co] V. Corbas, Su di una classe di quasicorpi commutativi finiti e su di una congettura del Dickson. Rend. Mat. e Appl. 21 (1962) 245–265.

[CoH] R. S. Coulter and M Henderson, Commutative semifields of odd order (in preparation).

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

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

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

[Di1] L. E. Dickson, On finite algebras. Nachrichten der Gesellschaften der Wissenschaften zu Göttingen (1905) 358–393.

[Di2] L. E. Dickson, On the cyclotomic function. Amer. Math. Monthly 12 (1905) 86–89.

[Dil] J. F. Dillon, Elementary Hadamard difference sets. Ph. D. thesis, U. of Maryland 1974.

[DiY] C. Ding and J. Yuan, A new family of skew Paley-Hadamard difference sets (preprint).

[Dy] R. H. Dye, Partitions and their stabilizers for line complexes and quadrics. Ann. Mat. Pura Appl. 114 (1977) 173–194.

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

[HaK] M. Hall, Jr. and D. E. Knuth, Combinatorial analysis and computers. Amer. Math. Monthly 72 (1965) 21–28.

[HMO] Y. Hiramine, M. Matsumoto and T. Oyama, On some extension of 1-spread sets. Osaka Math. J. 24 (1987) 123-137.

[HuJ] H. Huang and N. L. Johnson, 8 semifield planes of order 8^2. Discrete Math. 80 (1990) 69–79.

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

[JJ] V. Jha and 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 and Geometries 6 (1989) 1-35.

[Jo] N. L. Johnson, Sequences of derivable translation planes. Osaka J. Math. 25 (1988) 519-530.

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

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

[Ka3] W. M. Kantor, Codes, quadratic forms and finite geometries, pp. 153–177 in: Different aspects of coding theory (Ed. A. R. Calderbank), Proc. AMS Symp. Applied Math. 50 (1995).

[Ka4] W. M. Kantor, Projective planes of order q whose collineation groups have order q^2. J. Alg. Combin. 3 (1994) 405–425.

[Ka5] W. M. Kantor, Commutative semifields and symplectic spreads. J. Algebra 270 (2003) 96–114.

[KW1] W. M. Kantor and M. E. Williams, New flag–transitive affine planes of even order. JCT(A) 74 (1996) 1–13.

[KW2] W. M. Kantor and M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$–linear codes. TAMS 356 (2004) 895–938.

[Kl] E. Kleinfeld, Techniques for enumerating Veblen-Wedderburn systems. J. AACM 7 (1960) 330–337.

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

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

[Ma] A. Maschietti, Symplectic translation planes and line ovals. Adv. Geom. 3 (2003) 123–143.

[Me1] G. Menichetti, Algebre Tridimensionali su un campo di Galois. Ann. Mat. Pura Appl. 97 (1973) 293-302.

[Me2] G. Menichetti, n-Dimensional algebras over a field with a cyclic extension of degree n. Geom. Ded. 63 (1996) 69-94.

[Par] K. H. Parshall, In pursuit of the finite division algebra theorem and beyond: Joseph H. M. Wedderburn, Leonard E. Dickson, and Oswald Veblen. Arch. Internat. Hist. Sci. 33 (1984) 274–299.

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

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

[Sa] R. Sandler, Autotopism groups of some finite non-associative algebras. Amer. J. Math. 84 (1962) 239-264.

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

[VW] O. Veblen and J. H. Maclagan-Wedderburn, Non-desarguesian and non-pascalian geometries. TAMS 8 (1907) 379–388.

[Wa] R. J. Walker, Determination of division algebras with 32 elements, pp. 83–85 in: Proc. AMS Symp. Applied Math. 15 (1962).

[Wed] J. H. M. Wedderburn, A theorem on finite algebras. TAMS 6 (1905) 349–352.

[Ze] J. L. Zemmer, Jr., On the subalgebras of finite division algebras, Canad. J. Math. 4 (1952) 491-503.

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste. Monatsh. Math. Phys. 3 (1892) 265–284.

William M. Kantor, Department of Mathematics, University of Oregon, Eugene, OR 97403, USA

Email: kantor@math.uoregon.edu