TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 356, Number 3, Pages 895–938
S 0002-9947(03)03401-9
Article electronically published on October 9, 2003

SYMPLECTIC SEMIFIELD PLANES AND $\mathbb{Z}_4$–LINEAR CODES

WILLIAM M. KANTOR AND MICHAEL E. WILLIAMS

In memory of Jaap Seidel

Abstract. There are lovely connections between certain characteristic 2 semifields and their associated translation planes and orthogonal spreads on the one hand, and $\mathbb{Z}_4$–linear Kerdock and Preparata codes on the other. These inter–relationships lead to the construction of large numbers of objects of each type. In the geometric context we construct and study large numbers of nonisomorphic affine planes coordinatized by semifields; or, equivalently, large numbers of non–isotopic semifields: their numbers are not bounded above by any polynomial in the order of the plane. In the coding theory context we construct and study large numbers of $\mathbb{Z}_4$–linear Kerdock and Preparata codes. All of these are obtained using large numbers of orthogonal spreads of orthogonal spaces of maximal Witt index over finite fields of characteristic 2.

We also obtain large numbers of "boring" affine planes in the sense that the full collineation group fixes the line at infinity pointwise, as well as large numbers of Kerdock codes "boring" in the sense that each has as small an automorphism group as possible.

The connection with affine planes is a crucial tool used to prove inequivalence theorems concerning the orthogonal spreads and associated codes, and also to determine their full automorphism groups.

1. Introduction

A surprising advance in coding theory was the discovery that versions of some standard nonlinear binary codes can be viewed as linear codes over $\mathbb{Z}_4$ [HKCSS]. Among these codes were *Kerdock* and *Preparata codes*, well–known examples of nonlinear binary codes containing at least twice as many codewords as any linear code of the same length and minimum distance, which made them combinatorially "better" than linear codes but not as easy to work with. The $\mathbb{Z}_4$–versions combine simpler descriptions and implementations with combinatorial optimality. These codes were further investigated in [CCKS] from the vantage point of projective planes and *semifields* (i.e., either fields or nonassociative division algebras), providing a better understanding of some of their mathematical underpinnings besides

Received by the editors May 29, 2002.

2000 *Mathematics Subject Classification.* Primary 51A40, 94B27; Secondary 05E20, 05B25, 17A35, 51A35, 51A50.

Key words and phrases. Projective planes, semifields, spreads, finite orthogonal geometries, $\mathbb{Z}_4$–codes.

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

producing new connections with other areas of mathematics. The present paper focuses further on the finite geometry aspects of these codes: once we have obtained suitable planes and orthogonal spreads, the machinery developed in [CCKS] has immediate coding–theoretic consequences.

We briefly introduce some of the terminology used throughout this paper. Binary Kerdock codes are constructed using *Kerdock sets*: families of 2^{n-1} skew–symmetric $n \times n$ binary matrices such that the difference of any two is nonsingular. *Orthogonal spreads* (in our setting this means families of $q^m + 1$ totally singular $(m+1)$–spaces of an orthogonal space of type $\mathrm{O}^+(2m+2, q)$ that partition the singular points of the space) arise from analogous sets of $(m+1) \times (m+1)$ matrices over $\mathrm{GF}(q)$ for any q. *Symplectic spreads* (families of $q^m + 1$ totally isotropic m–spaces of a $2m$–dimensional symplectic space over $\mathrm{GF}(q)$ that partition the points of the space) arise in a similar way from symmetric matrices, and produce both *affine planes* and $\mathbb{Z}_4$*–Kerdock codes*. Various aspects of the similarities of the descriptions of these combinatorial objects were thoroughly investigated in [CCKS]; we refer to that paper and [Ka3] for further background. For now we only mention the *Gray map*, an isometry ϕ from $\mathbb{Z}_4^N$ to $\mathbb{Z}_2^{2N}$ that was used so effectively in [HKCSS] for passing between binary and $\mathbb{Z}_4$–codes. We will construct binary Kerdock codes $\mathcal{K}_2$ for which $\mathcal{K}_4 = \phi^{-1}(\mathcal{K}_2)$ is $\mathbb{Z}_4$–linear. The corresponding $\mathbb{Z}_4$*–Preparata code* $\mathcal{P}_4 = \mathcal{K}_4^\perp$ is its dual, and then the corresponding binary 'Preparata' code is $\mathcal{P}_2 = \phi(\mathcal{P}_4)$. It is important to note that *the original Kerdock code* [Ke] *is a special case of these constructions, but the original Preparata code* [Pr] *is not when* $m > 3$.

We work exclusively in characteristic 2, where there is a wonderful connection between orthogonal and symplectic spreads. We use a method that produces large numbers of binary orthogonal spreads and hence also translation planes and Kerdock codes. This method recursively intertwines translation planes, symplectic semifields, symplectic geometries and orthogonal geometries. Assume that m is an odd integer. Begin with a translation plane of even order $(q^n)^m$ whose lines through the origin comprise a symplectic spread $\mathcal{S}$ of an underlying $2m$–dimensional symplectic space W over $\mathrm{GF}(q^n)$. Then $\mathcal{S}$ remains a symplectic spread when viewed as a collection of mn–dimensional subspaces in the $\mathrm{GF}(q)$–space W. Moreover, $\mathcal{S}$ arises from an essentially unique orthogonal spread Σ of an $\mathrm{O}^+(2mn+2, q)$–space (this is where characteristic 2 is crucial); if ν is any nonsingular point of the latter space, then projecting Σ into associated symplectic space $\nu^\perp/\nu$ produces another symplectic spread Σ/ν over $\mathrm{GF}(q)$, producing in turn another translation plane of order q^{mn}. Thus, an orthogonal spread potentially spawns large numbers of nonisomorphic translation planes; moreover, the automorphism group of Σ essentially determines both the automorphism groups of these translation planes and isomorphisms among the planes.

This *up and down process* for constructing orthogonal and symplectic spreads originated in [Ka1]. By starting with a desarguesian plane and going "up and down" just once, it was used there to produce new examples of translation planes, orthogonal spreads and Kerdock codes. Retaining control of isomorphisms and automorphisms during repeated applications of the "up and down process" has been a basic obstacle to its further use. In this paper we preserve some control over this process by using a combination of disgusting calculations with kernels of semifields (Section 3.2), undergraduate group theory, and elementary properties of projective planes (Proposition 4.11). Because of their close relationship, we call all

planes obtained from desarguesian planes via the "up and down process" *scions* of desarguesian planes (cf. [KW]).

Our constructions are based on a strange–looking and awkward binary operation on $F = \mathrm{GF}(q^m)$ for q *even* and m *odd*,

$$x * y = xy^2 + \sum_{i=1}^{n} \Big(T_i\big(\zeta_i x\big) y + \zeta_i T_i\big(xy\big) \Big), \tag{1.1}$$

associated with the following data: a chain $F = F_0 \supset F_1 \supset \cdots \supset F_n \supseteq K = \mathrm{GF}(q)$ of fields with corresponding trace maps $T_i \colon F \to F_i$, together with any sequence $\big(\zeta_1, \ldots, \zeta_n\big)$ of elements $\zeta_i \in F^*$. We will see that this defines a *presemifield* $\mathfrak{P}_*(F, +, *)$. Starting with this presemifield, we will study several objects:

(1) A *symplectic semifield* $\mathfrak{S}_\circ(F, +, \circ)$ (Section 2.3).

(2) A *symplectic spread* $\mathcal{S}_*$ (Section 2.1) of the space F^2 (relative to the alternating bilinear form $((x, y), (x', y')) = T(xy' + x'y)$, using the trace map $T \colon F \to K$):

$$\begin{aligned} \mathcal{S}_* &= \{\mathcal{S}_*[s] \mid s \in F \cup \{\infty\}\}, \text{ where} \\ \mathcal{S}_*[\infty] &= 0 \oplus F \text{ and} \\ \mathcal{S}_*[s] &= \big\{(x, x * s) \mid x \in F\big\}, \ s \in F. \end{aligned} \tag{1.2}$$

(3) An *affine translation plane* $\mathfrak{A}(\mathcal{S}_*) = \mathfrak{A}(\mathfrak{P}_*) = \mathfrak{A}(\mathfrak{S}_\circ)$ of order q^m, whose point set is F^2 and whose lines are the subsets $x = c$ and $y = x * m + b$ for $c, m, b \in F$ (Section 2.1).

For the rest of this list, $F_n \supset K$.

(4) An *orthogonal spread* Σ_* (Section 2.4) of the space

$$\begin{aligned} &V = F \oplus K \oplus F \oplus K \\ &\text{equipped with quadratic form } Q(x, a, y, b) = T(xy) + ab : \end{aligned} \tag{1.3}$$

$$\begin{aligned} \Sigma_* &= \{\Sigma_*[s] \mid s \in F \cup \{\infty\}\}, \text{ where} \\ \Sigma_*[\infty] &= 0 \oplus 0 \oplus F \oplus K \text{ and} \\ \Sigma_*[s] &= \Big\{ \Big(x, a, x * s + s(a + T(xs)), T(xs)\Big) \mid \\ &\qquad x \in F, a \in K \Big\}, s \in F. \end{aligned} \tag{1.4}$$

(5) When $K = \mathrm{GF}(2)$, a *Kerdock set* (Section 5.1)

$$\begin{aligned} \mathcal{M}_* &= \{M_s \mid s \in F\}, \text{ where} \\ (x, a)_B M_s &= (x * s + T(xs)s + as, T(xs))_B, \end{aligned} \tag{1.5}$$

of $(m+1) \times (m+1)$ skew–symmetric matrices written using an orthonormal basis B of $F \oplus K$ (with respect to the K–bilinear form $T(xy)$ on F).

(6) When $K = \mathrm{GF}(2)$, a *Kerdock code* (Section 5.1)

$$\mathcal{K}_2(*) = \{ \, (Q_M(v) + u \cdot v + \varepsilon)_{v \in \mathbb{Z}_2^n} \mid M \in \mathcal{M}_*, u \in \mathbb{Z}_2^n, \varepsilon \in \mathbb{Z}_2 \}, \tag{1.6}$$

where Q_M denotes a quadratic form in $n = m+1$ variables whose associated bilinear form is uMv^t, and $u \cdot v = uv^t$ is the usual dot product.

(7) When $K = \mathrm{GF}(2)$, a $\mathbb{Z}_4$*–linear Kerdock code* $\mathcal{K}_4(*)$; see (5.7).

(8) When $K = \mathrm{GF}(2)$, a $\mathbb{Z}_4$–*linear Preparata code* $\mathcal{P}_4(*) = \mathcal{K}_4(*)^\perp$ whenever $\mathcal{K}_4(*)$ is linear; see (5.9).
(9) When $K = \mathrm{GF}(2)$, a *'Preparata' code* $\mathcal{P}_2(*)$, the image of $\mathcal{P}_4(*)$ under the Gray map; see (5.9).

The following roughly approximates the results of this paper (where $\rho(m)$ denotes the number of prime factors of m, counting multiplicities, and logarithms are always to the base 2):

Theorem 1.7. *Let q be a power of 2 and let m be an odd composite integer. Then there are at least $(q^m-1)^{\rho(m)-3}/(m\log q)^2$ pairwise inequivalent objects of each of the sorts* 1–9 (*where $q = 2$ in* 5–9).

Lumping all of these different types of objects together has produced a noticeably imprecise theorem. For precise statements see Theorems 4.13, 4.15 and 5.11. The above version is intended to provide a flavor of our results: the lower bound clearly is exponential in m, but more significantly it is not bounded above by any polynomial in q^m. We note that the proofs of bounds also deal with more general questions, such as isomorphisms when using different chains $(F_i)_0^n$ of possibly different lengths.

Based on the survey [CW] of semifields, it appears that the number of pairwise nonisomorphic finite semifield planes in print is not very large, and is significantly smaller than the number studied here. In fact the number previously known may not even be as large as the order of the plane for large planes. Undoubtedly there are many many more such planes, but isomorphism questions are, in general, very difficult (cf. Section 6).

This paper is organized as follows. Section 2 contains a construction for some computationally approachable cases of the "up and down process". Section 3 applies this to begin the study of the presemifields in (1.1). A crucial tool, and the starting point for much of this research, was the unexpected observation that, by computing the kernels of semifields, we could then determine equivalences among orthogonal spreads and Kerdock codes. Section 4 contains our results on isomorphisms, automorphisms and numbers of orthogonal spreads, semifields and planes.

Section 5 contains a brief discussion of how our results on semifield symplectic and orthogonal spreads produce coding–theoretic results, essentially as immediate consequences of the results in [CCKS]. However, whereas that paper discussed, for certain lengths, just one $\mathbb{Z}_4$–linear Kerdock and Preparata code other than the codes in [HKCSS], part of the content of Theorem 1.7 is that in this paper we deal with rather large numbers of such codes. In Section 5 we also discuss quasi–automorphism groups. While the latter results are straightforward, they concern aspects of nonlinear codes that do not seem to have been dealt with previously.

We already mentioned that it is difficult to keep track of full automorphism groups during the "up and down process". However, it is possible to preserve some relatively large subgroups of the collineation group of the initial desarguesian plane. In this paper we are concerned with preserving a Sylow 2–subgroup of order q^m of $\mathrm{SL}(2, q^m)$. In [KW] we preserved a subgroup of order $q^m + 1$ acting transitively on orthogonal and symplectic spreads, yielding flag–transitive affine planes. Yet another possibility, explored at length in [Wi], is *nearly flag–transitive planes*, in which a subgroup of order $q^m - 1$ is preserved that fixes two points of the line at infinity and transitively permutes the remaining points of that line. See [Ka5, 3.6] for a summary of those results. Those nearly flag–transitive planes were used to produce $\mathbb{Z}_4$–Kerdock codes that are extended cyclic: each admits a

cyclic automorphism group fixing the 0 coordinate and permuting the remaining coordinates regularly.

In the present paper we construct still further planes and codes in which the full automorphism group is relatively small. In general it is very difficult to determine the automorphism group of a translation plane, especially when the group is not very large. Any translation plane of order q^m arising from a $\mathrm{GF}(q)$–linear spread necessarily has an automorphism group of order at least $q^{2m}(q-1)$. This minimum can occur for the full automorphism group, and a translation plane is called *boring* in this case; thus, its full collineation group fixes every point on the line at infinity. Boring planes are interesting because most of the known finite affine planes have been found by means of relatively large collineation groups. In Section 4.4 we construct boring translation planes, as well as boring semifield planes (whose full collineation groups are generated by perspectivities); we use these later to construct boring binary and $\mathbb{Z}_4$–linear Kerdock codes (Section 5.6). Many boring planes with kernel $\mathrm{GF}(2)$ were obtained in [Ka4]; here our examples have kernels larger than $\mathrm{GF}(2)$. There are very few known examples of this boring phenomenon: two planes of order 17^2 [Ch] and over 300 of order 7^2 [ChD, MR] appear to be the only published examples. Similarly, the only published boring semifield planes appear to be two dual ones of order 32 [Kn1, p. 207].

Each of our translation planes is symplectic. A lovely recent result of Maschietti [Ma] gives a necessary and sufficient condition for a finite translation plane of even order to be symplectic in terms of the existence of line–ovals with special properties.

Most of the results of this paper are essentially in [Wi] (summarized in [Ka3, Ka5]). This paper is dedicated to the memory of Jaap Seidel, who instigated [CCKS] and hence also indirectly the above references as well as this paper.

2. Symplectic and orthogonal spreads and affine planes

Let $K = \mathrm{GF}(q)$.

2.1. **From spreads to projective planes.** Let W be a $2m$–dimensional vector space over K. A *spread* of W is a family $\mathcal{S}$ of $q^m + 1$ subspaces of dimension m whose union is all of W; that is, every nonzero vector is in a unique member of $\mathcal{S}$. Any spread of W determines a *translation plane* $\mathfrak{A}(\mathcal{S})$, an affine plane of order q^m whose points are vectors and whose lines are the cosets $U + w$ with $U \in \mathcal{S}, w \in W$. The spread $\mathcal{S}$ corresponding to a desarguesian plane $\mathfrak{A}(\mathcal{S})$ is called a *desarguesian spread*.

Any isomorphism between two translation planes is induced by a semilinear transformation of the underlying vector spaces. The collineation group of $\mathfrak{A}(\mathcal{S})$ is

$$\mathrm{Aut}\,\mathfrak{A}(\mathcal{S}) = V \rtimes \Gamma\mathrm{L}(V)_{\mathcal{S}}, \tag{2.1}$$

where $\Gamma\mathrm{L}(V)$ is the group of all invertible semilinear transformations of V, while $\Gamma\mathrm{L}(V)_{\mathcal{S}} = \mathrm{Aut}\,\mathfrak{A}(\mathcal{S})_0$, the stabilizer of 0, is the group of those transformations sending $\mathcal{S}$ to itself.

The set of all nonsingular linear transformations fixing every member of $\mathcal{S}$, together with 0, is a field, the *kernel* $\mathfrak{K}(\mathfrak{A}(\mathcal{S}))$ of the translation plane. It is the largest field over which the spread consists of subspaces.

See [De] for the above and for further background concerning translation planes and their associated projective planes.

Symplectic spreads. We refer to [Ta] for background concerning symplectic spaces and groups. Suppose that our K–space W is equipped with a nondegenerate alternating bilinear form $(\ ,\ )$. A spread $\mathcal{S}$ of W is called *symplectic* if each $W \in \mathcal{S}$ is *totally isotropic*: $(W, W) = 0$.

The most obvious example of a symplectic spread $\mathcal{S}$ consists of all 1–spaces of K^2, using the form $((x, y), (x', y')) = xy' - x'y$. Although this only produces the desarguesian plane $\mathfrak{A}(\mathcal{S})$, it is the starting point of this paper: we will "distort" this spread.

The underlying symplectic geometry of the bilinear form has isometry group $\mathrm{Sp}(2n, q)$ and group $\Gamma\mathrm{Sp}(2n, q)$ of semilinear transformations preserving the form projectively and up to field automorphisms.

2.2. **Prequasifields and planes.** A translation plane is usually coordinatized by an algebraic system called a *quasifield* [De, pp. 132-135]. Here it will be convenient to consider a weaker but geometrically equivalent system:

Prequasifields. A *prequasifield* $\mathfrak{P}_* = \mathfrak{P}_*(F, +, *)$ defined on $F = \mathrm{GF}(q^m)$ uses the usual addition on F together with a new binary operation $*$ satisfying (for all $x, y, z \in F$)

$$\begin{aligned} &(x + y) * z = x * z + y * z, \\ &x * y = x * z \Longrightarrow x = 0 \text{ or } y = z, \text{ and} \\ &x * y = 0 \iff x = 0 \text{ or } y = 0. \end{aligned}$$

If it has an identity element, $\mathfrak{P}_*$ is a *quasifield*; in view of (1.1), we must delete this condition even though an identity element is readily introduced (see below). $\mathfrak{P}_*(F, +, *)$ is a *presemifield* if both distributive laws hold, and a *semifield* if, in addition, there is an identity element.

A translation plane $\mathfrak{A}(\mathfrak{P}_*) = \mathfrak{A}(\mathcal{S}_*)$ is obtained using a spread $\mathcal{S}_*$ defined as in (1.2).

Remark 2.2. The *kernel* (or *left nucleus*) $\mathfrak{K}(\mathfrak{P}_*)$ of a quasifield $\mathfrak{P}_*$ is the set of all $k \in F$ satisfying (for all $x, y \in F$)

$$\begin{aligned} k * (x + y) &= k * x + k * y, \\ k * (x * y) &= (k * x) * y. \end{aligned}$$

It is isomorphic to the kernel $\mathfrak{K}(\mathfrak{A}(\mathfrak{P}_*))$ *of the plane* $\mathfrak{A}(\mathfrak{P}_*)$.

Isotopisms. An *isotopism* between two presemifields $\mathfrak{P}_*(F, *, +)$ and $\mathfrak{P}_\circ(F, \circ, +)$ is a triple (α, β, γ) of additive permutations of F such that

$$\gamma(x * y) = \alpha(x) \circ \beta(y) \quad \forall x, y, z \in F. \tag{2.3}$$

We will also regard the equation (2.3) as representing the isotopism. *Any presemifield* $\mathfrak{P}_* = (F, *, +)$ *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 $\mathfrak{P}_*$.

Remark 2.4.

(i) Two semifields coordinatize isomorphic planes if and only if they are isotopic [Al2].

(ii) We will need the following special case of an easy result concerning isotopisms of groups [Al1, Theorem 2]: If $|F|$ is even and $\alpha, \beta\colon F \to F$ are additive permutations such that $\alpha(x)\beta(y)^2 = \beta(xy^2)$ for all $x, y \in F$, then $\alpha(x) = \lambda^{-1}x^\sigma$ and $\beta(x) = \lambda x^\sigma$ for some $\lambda \in F^*$, $\sigma \in \mathrm{Aut}(F)$, and all $x \in F$.

A result corresponding to (i) also holds for ternary rings coordinatizing arbitrary projective planes [Kn1].

2.3. **Symplectic prequasifields. From now on we will always assume that $F = \mathbf{GF}(q^m)$ and $K = \mathbf{GF}(q)$ with q even.**

The trace map $T\colon F \to K$ determines an inner product $T(xy)$ on the K–space F having an orthonormal basis that lets us identify F, equipped with this inner product, with K^m, equipped with its usual dot product.

We assume now that our prequasifield $\mathfrak{P}_*$ is *symplectic*: it satisfies the following two conditions for all $x, y, z \in F$:

$$T(x(x * y)) = T(xy)^2, \tag{2.5}$$

$$T(x(z * y)) = T(z(x * y)). \tag{2.6}$$

One example of a symplectic prequasifield is $x * y = xy^2$; the corresponding plane is desarguesian. In this paper we will study many more examples; even more are studied in [Wi]. Note that, if we had required that our prequasifield has an identity element, then we would have had to use a more complicated version of the inner product. Thus, for example, it is more convenient in the present context to use the preceding inconvenient–looking modification xy^2 of ordinary multiplication in F.

Replacing x in turn by x, z, $x + z$ in (2.5) produces (2.6); but (2.6) is no less restrictive than (2.5) [Ka5, 3.10]. A simple calculation yields the following explanation of the term "symplectic prequasifield":

Proposition 2.7. *Equip the K–space F^2 with the alternating bilinear form*

$$((x_1, y_1), (x_2, y_2)) = T(x_1y_2 - x_2y_1). \tag{2.8}$$

Then the spread $\mathcal{S}_*$ of F^2 associated with a prequasifield $\mathfrak{P}_*$ as in (1.2) *is symplectic if and only if* (2.6) *holds.*

The role of (2.5) will become clear in Theorem 2.18.

2.4. **Orthogonal spreads.** We refer to [Ta, p. 136] for background concerning quadratic forms and their orthogonal groups and geometry. Let $V = K^{2n} = X \oplus Y$ for subspaces X and Y both of which are identified with K^n. Equip V with the quadratic form $Q(x, y) = x \cdot y$ (using the usual dot product on K^n); the associated nondegenerate bilinear form is

$$(u, v) = Q(u + v) - Q(u) - Q(v), \tag{2.9}$$

and determines an underlying symplectic geometry if q is even. The underlying orthogonal geometry of the quadratic form has isometry group $\mathrm{O}^+(V) = \mathrm{O}^+(2n, q)$ and group $\Gamma\mathrm{O}^+(V) = \Gamma\mathrm{O}^+(2n, q)$ of semilinear transformations preserving the form projectively and up to field automorphisms. Moreover, V has $(q^n - 1)(q^{n-1} + 1)$ nonzero singular vectors, and each *totally singular n–space* (i.e., n–space on which Q vanishes, such as X and Y) contains $q^n - 1$ nonzero singular vectors.

An *orthogonal spread* of V is a family Σ of $q^{n-1} + 1$ totally singular n–spaces that partitions the set of all nonzero singular vectors. Two orthogonal spreads

are called *equivalent* if there is an element of $\Gamma\mathrm{O}^+(V)$ sending one to the other. The *automorphism group* of Σ is just its set–stabilizer $\Gamma\mathrm{O}^+(V)_\Sigma$ in the (semilinear) orthogonal group (compare (2.1)).

If n is even there is always at least one orthogonal spread [Di, Dy, Ka1]. None exists if n is odd.

2.5. **Orthogonal spreads $\longleftrightarrow$ symplectic spreads.** Let ν denote any nonsingular point (1–space) of the above orthogonal space V: $Q(\nu) \neq 0$. If Σ is any orthogonal spread of V, then n is odd and $\{Z \cap \nu^\perp \mid Z \in \Sigma\}$ is a family of totally singular $(n-1)$–spaces that partitions the set of nonzero singular vectors of $\nu^\perp$. Since the characteristic is 2, ν is contained in the hyperplane $\nu^\perp$. The $(2n-2)$–space $\nu^\perp/\nu$ is turned into a symplectic space using the inherited alternating bilinear form $(u+\nu, v+\nu) := (u,v)$ (for $u, v \in \nu^\perp$). Then

$$\Sigma/\nu := \{\langle Z \cap \nu^\perp, \nu\rangle/\nu \mid Z \in \Sigma\} \tag{2.10}$$

is a symplectic spread of the symplectic space $\nu^\perp/\nu$, obtained by *slicing* the original spread. Note that there is no quadratic form inherited by $\nu^\perp/\nu$.

The preceding construction can be reversed, proceeding from symplectic spreads to orthogonal ones. Namely, let $m = n-1$, and start with a symplectic spread $\mathcal{S}$ in a symplectic K–space W of dimension $2m$. Identify W with the symplectic space $\nu^\perp/\nu$ arising, as above, from the orthogonal space V and one of its nonsingular points ν. Each totally singular $(n-1)$–space of $\nu^\perp$ lies in exactly two totally singular n–spaces of V, one from each family [Ta, 11.61]. Pick a family $\mathbf{M}$ of such n–spaces. Then *the lift*

$$\Sigma^\nu(\mathcal{S}) := \left\{X \,\middle|\, X \in \mathbf{M} \text{ and } \langle X \cap \nu^\perp,\, \nu\rangle/\nu \in \mathcal{S}\right\} \tag{2.11}$$

is an orthogonal spread of V such that

$$\mathcal{S} = \Sigma^\nu(\mathcal{S})/\nu \text{ and } \Sigma = \Sigma^\nu(\Sigma/\nu). \tag{2.12}$$

This passage from symplectic to orthogonal spreads is essentially unique: a different choice of the family $\mathbf{M}$ produces an equivalent orthogonal spread. See [Ka1, I] for more details.

When $\mathcal{S}$ is a desarguesian spread, producing a desarguesian affine plane $\mathfrak{A}(\mathcal{S})$, $\Sigma^\nu(\mathcal{S})$ is called a *desarguesian orthogonal spread.*

Back and forth. Starting with a symplectic spread $\mathcal{S}$ in a $2m$–dimensional symplectic K–space with m odd, we have just produced an orthogonal spread $\Sigma^\nu(\mathcal{S})$ in a $(2m+2)$–dimensional orthogonal K–space, corresponding to a nonsingular point ν, in such a way that $\Sigma^\nu(\mathcal{S})/\nu$ is $\mathcal{S}$. Once we have Σ, we can form a *different* symplectic spread $\Sigma^\nu(\mathcal{S})/\nu'$ using a *different* nonsingular point ν'. In other words, we can use the orthogonal spread to "distort" $\mathfrak{A}(\mathcal{S})$ into a "new" affine plane $\mathfrak{A}(\Sigma^\nu(\mathcal{S})/\nu')$. See Theorem 2.18 for a coordinate version of this.

Isomorphisms.

Theorem 2.13 ([Ka1, 3.6, 3.7])**.** *For $i = 1, 2$, consider an orthogonal spread Σ_i in an $\mathrm{O}^+(2m+2, K)$–space V_i equipped with a quadratic form φ_i. Let ν_i be a nonsingular point of V_i, and write $\mathcal{S}_i = \Sigma_i/\nu_i$.*

(i) *The affine planes $\mathfrak{A}(\mathcal{S}_i)$ are isomorphic if and only if there is a semilinear transformation $\omega\colon V_1 \to V_2$ satisfying*
   (a) $\Sigma_1^\omega = \Sigma_2$,

(b) $\nu_1^\omega = \nu_2$, *and*
(c) $\varphi_2(v^\omega) = \varphi_1(v)^\tau$ *for some* $\tau \in \mathrm{Aut}(F)$ *and all* $v \in V_1$.

(ii) $\mathrm{Aut}\,\mathfrak{A}(\Sigma_1)_0/\mathfrak{K}^*(\mathfrak{A}(\Sigma_1)) \cong \Gamma\mathrm{O}^+(V_1)_{\Sigma_1,\nu_1}/K^*$, *where* $\mathfrak{K}^*(\mathfrak{A}(\Sigma_1)) \geq K^*$.

More precisely, $\mathrm{Aut}\,\mathfrak{A}(\Sigma_1)_0$ *consists of the transformations* $k\bar{g}$, *where* $k \in \mathfrak{K}^*(\mathfrak{A}(\Sigma_1))$ *and* $\bar{g}$ *is the transformation of* $\nu_1^\perp/\nu_1$ *induced by an element* $g \in \Gamma\mathrm{O}^+(V_1)_{\Sigma_1,\nu_1}$.

Part of this is clear: by (2.10), any ω behaving as in (i) produces an isomorphism of planes. It is the converse that is not at all obvious. According to [Ka1, 3.6], any isomorphism $\mathfrak{A}(\mathcal{S}_1) \to \mathfrak{A}(\mathcal{S}_2)$ sending 0 to 0 is essentially symplectic, preserving the symplectic forms on $\nu_i^\perp/\nu_i$ up to scalars and field automorphisms, hence lifting to $\nu_1^\perp \to \nu_2^\perp$ and then also to V. The theorem implies that equivalences among orthogonal spreads completely determine isomorphisms among the affine planes they spawn, while the automorphism group of an orthogonal spread determines, up to the kernels, the collineation groups of the planes it spawns. Consequently, in order to understand an affine plane $\mathfrak{A}(\Sigma/\nu)$ we might focus instead on the orthogonal spread Σ. However, we will also see that knowledge of the kernel $\mathfrak{K}(\mathfrak{A}(\Sigma/\nu))$ of each such plane will greatly aid in our investigation of some orthogonal spreads Σ.

2.6. **Changing fields: up and down.** There is a simple way to use Section 2.5 in order to obtain large numbers of new orthogonal and symplectic spreads.

Start with a symplectic spread $\mathcal{S}$ in a $2m$–dimensional symplectic F'–space $W = F^2$ over a subfield F' of F, with alternating bilinear form $(\ ,\ )$. Let K be any proper subfield of F', and let $T\colon F' \to K$ be the trace map. Then $T(u,v)$ defines a nondegenerate alternating K–bilinear form on the K–space W. Viewed as a family of subspaces of this K–space, $\mathcal{S}$ is still a spread, and each of its members is still totally isotropic with respect to the new form. Thus, $\mathcal{S}$ *is a symplectic spread of the* K*–space* W. Here, $\dim_K W = 2m[F'\colon K]$.

Now Section 2.5 can be applied if $m[F'\colon K]$ is odd, producing an orthogonal spread $\Sigma^\nu(\mathcal{S})$ of a $(2m[F'\colon K]+2)$–dimensional orthogonal K–space, after which we can come down via new nonsingular points ν' and obtain seemingly "new" symplectic spreads $\Sigma^\nu(\mathcal{S})/\nu'$.

Up and down process. This process of repeatedly going from a symplectic spread over some field, changing to a smaller field, going up to an orthogonal spread and then back down to a symplectic spread over the smaller field, is called the *up and down process*. In general it is difficult to keep control over properties of these spreads. However, in Section 1 we mentioned important special cases where control can be maintained.

2.7. **Up and down using coordinates.** Suppose that $F = \mathrm{GF}(q^m) \supseteq F' = \mathrm{GF}(q^{m'}) \supseteq K = \mathrm{GF}(q)$ are fields with mm' odd and with corresponding trace maps $T'\colon F \to F'$ and $T\colon F \to K$. The following observations permeate this paper:

Lemma 2.14. *If* $z \in F$ *and* $u \in F'$, *then*

(i) $TT'(z) = T(z)$,
(ii) $T(uz) = T(uT'(z))$, *and*
(iii) $T'(u) = u$ *and* $T(1) = 1$.

Proof. (i) Let $\mathrm{Aut}(F/K) = \langle\alpha\rangle$, so that $\mathrm{Aut}(F/F') = \langle\alpha^{m/m'}\rangle$. Since $T(z^{\alpha^j}) = T(z)^{\alpha^j} = T(z)$ we have $TT'(z) = T(\sum_{i=1}^{m/m'} z^{\alpha^{m'i}}) = \sum_{i=1}^{m/m'} T(z) = (m/m')T(z) = T(z)$.

(ii) By (i), $T(uz) = TT'(uz) = T(uT'(z))$.

(iii) $T'(u) = \sum_1^{m/m'} u = u$, and $T(1) = 1$ similarly. □

A prequasifield $\mathfrak{P}_*(F, +, *)$ with kernel containing F' defines a spread $\mathcal{S}_*$ in the F'–space $W = F^2$ using (1.2). Consider the following additional properties of $\mathfrak{P}_*$ for some $l \in F$ and all $x, x', y \in F$:

$$T'\big(x(x * y)\big) = T'\big(lxy\big)^2, \tag{2.15}$$

$$T'(x(x' * y)) = T'(x'(x * y)). \tag{2.16}$$

In fact l is not essential here: there is an isotopic prequasifield, defined by $x \circ y = x * (l^{-1}y)$, that satisfies (2.5), (2.6), and hence is symplectic. Moreover, l is not needed for the study of our presemifields. However, including l simplifies a more general result: see Theorem 2.18(ii).

As before, (2.15) *implies* (2.16). Moreover, the members of the spread $\mathcal{S}_*$ (cf. (1.2)) are totally isotropic with respect to the nondegenerate alternating F'–bilinear form $\big((a,b),(c,d)\big)' := T'(ad+bc)$, since $\big((x, x*s), (y, y*s)\big)' = T'(x(y*s)+y(x*s)) = 0$ by (2.16).

A fundamental aspect of our study of orthogonal spreads involves the seemingly simple matter of changing fields (cf. Section 2.6). Thus, we now view W as a K–space and equip it with the nondegenerate alternating K–bilinear form $\big((a,b),(c,d)\big) := T(ad+bc)$. By Lemma 2.14(i), $\mathfrak{P}_*$ satisfies (2.15) and (2.16) with T in place of T', and the members of $\mathcal{S}_*$, when viewed as K–subspaces, remain totally isotropic with respect to this new form (i.e., $T(x(y*s)+y(x*s)) = 0$). This change of perspective does not affect the affine plane $\mathfrak{A}(\mathcal{S}_*)$.

Next, consider the $\mathrm{O}^+(2m+2, q)$–space V in (1.3). The associated alternating bilinear form is given by

$$((x,a,y,b),(x',a',y',b')) = T(xy' + x'y) + ab' + a'b. \tag{2.17}$$

By Section 2.5, for any nonsingular point $\nu \in V$ we can identify W with $\nu^\perp/\nu$ and then lift the symplectic spread $\mathcal{S}_*$ to an orthogonal spread $\Sigma^\nu(\mathcal{S}_*)$ in V. We will need all of this in terms of coordinates:

Theorem 2.18. *Suppose that $\mathfrak{P}_*$ satisfies* (2.15) *for the trace map $T'\colon F \to F'$, and that $k(x * y) = kx * y$ for all $k \in F'$, $x, y \in F$.*

(i) *$\mathfrak{P}_*$ determines the orthogonal spread $\Sigma_* = \{\Sigma_*[s] \mid s \in F \cup \{\infty\}\}$ of the orthogonal K–space V in* (1.3)*, where*

$$\Sigma_*[\infty] = 0 \oplus 0 \oplus F \oplus K,$$

$$\Sigma_*[s] = \Big\{\big(x, a, x * s + ls(a + T(lxs)), T(lxs)\big) \mid x \in F, a \in K\Big\}, s \in F,$$

for the trace map $T\colon F \to K$.

(ii) *For any nonsingular point of the form $\nu = \langle 0, \lambda^2, \zeta, 1\rangle$, $\zeta \in F$, $\lambda \in K^*$, the symplectic spread Σ_*/ν in* (2.10) *arises from the prequasifield $\mathfrak{P}_\circ(F, \circ, +)$ defined, for $x, y \in F$, by*

$$x \circ y = x * y + lyT(lxy) + ly\lambda T(l\lambda xy) + lyT(x\zeta) + \zeta T(lxy).$$

Moreover, $\mathfrak{P}_\circ$ satisfies an analogue of (2.15): $T\big(x(x\circ y)\big) = T(l\lambda xy)^2$ *for all* $x, y \in F$.

(iii) *If* $\nu = \langle 0,1,0,1\rangle$ *then* $\mathcal{S}_\circ = \mathcal{S}_*$.

Proof. (i) By hypothesis, each member of Σ_* is a K–subspace of V of K–dimension $m+1$. We first show each of these subspaces is totally singular. This is obvious for $\Sigma_*[\infty]$. Consider $\Sigma_*[s]$: by (1.3),

$$\begin{aligned} &Q\big((x,a,x*s+ls(a+T(lxs)),T(lxs))\big)\\ &= T\Big(x(x*s)+xlsa+xlsT(lxs)\Big)+aT(lxs)\\ &= T\big(x(x*s)\big)+T\big(lxsT(lxs)\big)=0, \end{aligned}$$

since (2.15) holds with T in place of T' (by Lemma 2.14(i)), as required.

Next we check that the members of Σ_* pairwise intersect trivially. Certainly $\Sigma_*[s]\cap\Sigma_*[\infty]=0$ for each $s\in F$. Hence the members of Σ_* are all maximal totally singular subspaces of the same type $\mathbf{M}$ and any two members of $\mathbf{M}$ intersect in a subspace of even dimension, since $m+1$ is even [Ta, 11.61]. If $s,t\in F$ with $\Sigma_*[s]\cap\Sigma_*[t]\neq 0$, it follows that $\Sigma_*[s]\cap\Sigma_*[t]\cap\langle 0,1,0,1\rangle^\perp\neq 0$. By (2.17), $\langle 0,1,0,1\rangle^\perp = \big\{(x,b,y,b)\mid x,y\in F, b\in K\big\}$. Thus, there exists $x\in F^*$ with $\big(x,T(lxs),x*s,T(lxs)\big)=\big(x,T(lxt),x*t,T(lxt)\big)$. Then $x*s=x*t$, so that $s=t$ as $\mathfrak{P}_*$ is a prequasifield.

(ii) By (2.17), $\langle 0,\lambda^2,\zeta,1\rangle^\perp=\big\{(x,\lambda^2 b+T(x\zeta),y,b)\mid x,y\in F,\ b\in K\big\}$. For each $s\in F$, $\Sigma_*[s]\cap\nu^\perp$ is

$$\Big\{\Big(x,\lambda^2T(lxs)+T(x\zeta),x*s+ls\big[\lambda^2T(lxs)+T(x\zeta)\big]+lsT(lxs),T(lxs)\Big)\mid x\in F\Big\},$$

so that $\big\langle\nu,\Sigma_*[s]\cap\nu^\perp\big\rangle/\nu$ consists of all vectors of the form

$$\begin{aligned} \Big(x,T(x\zeta),x*s+ls\big[\lambda T(l\lambda xs)+T(lxs)+T(x\zeta)\big]+\zeta T(lxs),0\Big)+\langle 0,\lambda^2,\zeta,1\rangle&\\ = (x,T(x\zeta),x\circ s,0)+\nu& \end{aligned}$$

since $\lambda\in K$. Then the isometry $\nu^\perp/\nu\to W$ sending $\big(x,T(x\zeta),y,0\big)+\nu\to(x,y)$ maps the symplectic spread Σ_*/ν to the symplectic spread associated with $\mathfrak{P}_\circ$. Finally, $\mathfrak{P}_\circ$ satisfies the analogue of (2.15):

$$\begin{aligned} T\big(x(x\circ y)\big) &= T\big((x(x*y)+lxyT(lxy)\big)+T\big(l\lambda xyT(l\lambda xy)\big)\\ &\quad+T\big(lxyT(x\zeta)+x\zeta T(lxy)\big)=T(l\lambda xy)^2 \end{aligned}$$

since $\mathfrak{P}_*$ satisfies (2.15) with T in place of T'.

(iii) Here $x\circ y=x*y$. □

Remark. We used λ_i^2 here instead of λ_i in order to simplify the statement of the next proposition.

2.8. **Up and down from desarguesian spreads.** We now iterate Theorem 2.18, starting with the desarguesian spread and using a sequence of subfields of F. We call a symplectic spread $\mathcal{S}$ a *scion* of the desarguesian spread if it is obtained by applying the "up and down process" beginning with the desarguesian spread. Correspondingly, the translation plane $\mathfrak{A}(\mathcal{S})$ is a *scion* of the desarguesian plane. The following result is more general than we need but involves no more effort than the semifield case, which occurs when all λ_i are 1.

Proposition 2.19. *Let $(F_i)_0^n$ be a chain of distinct fields such that $F = F_0$ and $[F\colon F_n]$ is odd, with trace maps $T_i\colon F \to F_i$. Set $\lambda_0 = 1$; let $\lambda_i \in F_i^*$ and $\zeta_i \in F$ be arbitrary for $1 \le i \le n$; and for $0 \le i \le n$ write $c_i = \prod_{j=0}^{i} \lambda_j$. Define $\mathfrak{P}_*(F, +, *)$ by*

$$x * y = xy^2 + \sum_{i=1}^{n} \Big(c_{i-1} y T_i(c_{i-1}xy) + c_i y T_i(c_i xy) \Big) + \sum_{i=1}^{n} \Big(c_{i-1} y T_i(x\zeta_i) + \zeta_i T_i(c_{i-1}xy) \Big).$$

Then $\mathfrak{P}_*(F, *, +)$ is a prequasifield coordinatizing a scion of the desarguesian plane, and $T_n(x(x * y)) = T_n(c_n xy)^2$ for all $x, y \in F$ as in (2.15).

Proof. We use induction on n. If $n = 0$ then $x * y = xy^2$ corresponds to the desarguesian plane, and $T_0(x(x * y)) = T_0(c_0 xy)^2$ for $c_0 = \lambda_0 = 1$.

Suppose that, for some $n \ge 0$, we have the stated semifield $\mathfrak{P}_*$. We now consider an additional field $F_{n+1} \subset F_n$, together with $\lambda_{n+1}, \zeta_{n+1}$ and c_{n+1}. We will use $F' = F_n$ and $K = F_{n+1}$, $T' = F_n$ and $T = T_{n+1}$ in Theorem 2.18(ii). That theorem gives us a coordinate description of the orthogonal spread Σ_* in the K–space $V_{n+1} = F \oplus K \oplus F \oplus K$; moreover, $\Sigma_*/\langle 0, \lambda_{n+1}^2, \zeta_{n+1}, 1\rangle$ is a symplectic spread coordinatized by $\mathfrak{P}_\circ$, where, using $l = c_n$ in the inductive step,

$$\begin{aligned} x \circ y &= x * y + c_n y T_{n+1}(c_n xy) + c_n \lambda_{n+1} y T_{n+1}(c_n \lambda_{n+1} xy) \\ &\quad + \ c_n y T_{n+1}(x\zeta_{n+1}) + \zeta_{n+1} T_{n+1}(c_n xy) \\ &= xy^2 + \sum_{i=1}^{n+1} \Big(c_{i-1} y T_i(c_{i-1}xy) + c_i y T_i(c_i xy) \Big) \\ &\quad + \ \sum_{i=1}^{n+1} \Big(c_{i-1} y T_i(x\zeta_i) + \zeta_i T_i(c_{i-1}xy) \Big). \end{aligned}$$

Also by Theorem 2.18(ii), $T_{n+1}(x(x \circ y)) = T_{n+1}(c_n \lambda_{n+1} xy)^2 = T_{n+1}(c_{n+1} xy)^2$, as required. □

A direct computational proof is given in [Wi] that the multiplication in Proposition 2.19 defines a prequasifield (compare Section 3.1). We already noted above that the prequasifield in the proposition is just the presemifield in (1.1) if all λ_i are 1. In this case any term with $\zeta_i = 0$ can be deleted, as can the corresponding field F_i. This explains the assumption $\zeta_i \in F^*$ in (1.1).

On the other hand, if all ζ_i are 0 then $\mathfrak{A}(\mathfrak{P}_*)$ admits a group of collineations $(x, y) \to (s^{-1}x, sy)$ fixing two points at infinity and cyclically permuting the remaining ones; this situation is studied in detail in [Wi].

Finally, we note that these are far from all scions of the Desarguesian plane. If some λ_i are not 1 and some ζ_i are not 0, then no nontrivial subgroup of $\mathrm{SL}(2, q^m)$ is preserved in the above construction, and presumably the corresponding orthogonal spreads all have tiny automorphism groups. On the other hand, we have only included scions in the theorem whose coordinate versions can be described "easily". There are other noteworthy scions of desarguesian planes, obtained using chains of fields and other choices of $\nu = \langle \alpha, \lambda, \zeta, 1\rangle$ with $\alpha \ne 0$. These include the flag–transitive scions studied in [KW].

2.9. **Elementary abelian groups from presemifields.** We now specialize the situation in Section 2.7 to the case where we start with a *presemifield* $\mathfrak{P}_*(F,+,*)$, $|F| = q^m$, with q even and m odd; we also assume that $l = 1$. Then the associated translation plane $\mathfrak{A}(\mathfrak{P}_*)$ is a symplectic semifield plane. We assume that we are in the situation of Theorem 2.18, so that we have F, F', K, T, T' and Σ_*; (2.5) and (2.6) hold.

The *K–spaces* F^2 and $V = F \oplus K \oplus F \oplus K$ are equipped with the alternating and quadratic forms $\big((x,y),(w,z)\big) = T(xz + yw)$ and $Q(x,a,y,b) = T(xy) + ab$, respectively. For each $e \in F$ define $\psi_e \colon F^2 \to F^2$ and $\eta_e \colon V \to V$ by

$$\begin{aligned}(x,y)\psi_e &= (x, y + x * e),\\ (x,a,y,b)\eta_e &= (x, a + T(xe), y + x * e + (a+b)e, b + T(xe)).\end{aligned} \tag{2.20}$$

By a straightforward calculation, $\psi_e\psi_f = \psi_{e+f}$ and $\eta_e\eta_f = \eta_{e+f}$ for all $e, f \in F$.

If $H \le \Gamma\mathrm{L}(V)$ then $C_V(H)$ denotes the set of vectors fixed by H.

Lemma 2.21.

(i) $E(\mathcal{S}_*) := \big\{\psi_e \mid e \in F\big\}$ *is an elementary abelian group of symplectic isometries of the K–space F^2 that stabilizes $\mathcal{S}_*[\infty]$ and permutes the remaining members of $\mathcal{S}_*$ regularly. It induces all elations of the semifield plane $\mathfrak{A}(\mathcal{S}_*)$ with axis $\mathcal{S}_*[\infty]$.*

(ii) $E(\Sigma_*) := \big\{\eta_e \mid e \in F\big\}$ *is an elementary abelian group of orthogonal isometries of the K–space V that stabilizes $\Sigma_*[\infty] = 0 \oplus 0 \oplus F \oplus K$ and permutes the remaining members of Σ_* regularly.*

(iii) $C_V\big(E(\Sigma_*)\big) = \big\{(0,a,y,a) \mid a \in K,\ y \in F\big\}$, *and $E(\Sigma_*)$ permutes the set $\{\langle 0,0,y,1\rangle \mid y \in F\}$ of points of $\Sigma_*[\infty]$ not in $C_V\big(E(\Sigma_*)\big)$ regularly.*

(iv) *The set of nonsingular points of $C_V\big(E(\Sigma_*)\big)$ is $\big\{\langle 0,1,y,1\rangle \mid y \in F\big\}$, and has size q^m.*

Proof. These all involve simple calculations. □

3. The semifields

We now begin our study of the presemifields (1.1). **We always let m be an odd integer such that $q^m > 8$.**

The presemifields in (1.1) involve a relatively unwieldy formula. To complicate matters, we will need to introduce isotopic semifields (cf. Section 2.2). These will involve even more awkward formulas (3.7)(iii) and calculations.

This section contains many of the computations needed later: we will determine the kernels of many of the semifields and hence of the associated affine planes (Theorem 3.4), prove that the semifields are not commutative if the chain of fields contains more than one field (Theorem 3.24), and determine exactly when two of the presemifield operations are equal (Proposition 3.38). Each of these is crucial for later results concerning planes or codes.

3.1. **The presemifields in** (1.1)**.** When we specialize Theorem 2.19 to the case $\lambda_i = 1$ and $\zeta_i \ne 0$ for all i, then all $c_i = 1$ and *we obtain the binary operation defined in* (1.1). Thus, writing $F_0 = F$,

$$\mathfrak{P}\big((F_i)_0^n, (\zeta_i)_1^n\big) = \mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big) := \mathfrak{P}_*(F,+,*) \tag{3.1}$$

is a symplectic presemifield (i.e., satisfying (2.5) and (2.6)), and $\mathfrak{A}(\mathfrak{P}_*)$ is a symplectic semifield scion of the desarguesian plane (by Proposition 2.19). The case $n = 0$ corresponds to the desarguesian plane we started with.

For completeness we provide a *direct computational proof that* (1.1) *does, indeed, define a presemifield.* This will allow some of the remarkable features of (1.1) to become evident, features that will figure prominently in the rest of this paper.

Since $*$ clearly is 2–sided distributive, we only need to prove that $x, y \in F$ *and* $x * y = 0 \Rightarrow z := xy$ *is* 0. Multiply (1.1) by x:

$$z^2 + \sum_{i=1}^{n} \Big(zT_i(\zeta_i x) + \zeta_i x T_i(z) \Big) = 0. \tag{3.2}$$

Let $T_0 = 1\colon F_0 \to F_0$. Using backwards induction, we will prove that $T_j(z) = 0$ for each $0 \le j \le n$. For $j = n$, apply T_n to (3.2). By Lemma 2.14(i),

$$\begin{aligned} 0 &= T_n(z^2) + \sum_{i=1}^{n} T_n T_i\Big(zT_i(\zeta_i x) + \zeta_i x T_i(z) \Big) \\ &= T_n(z)^2 + \sum_{i=1}^{n} T_n\Big(T_i(z)T_i(\zeta_i x) + T_i(\zeta_i x)T_i(z) \Big) \\ &= T_n(z)^2. \end{aligned}$$

If $T_{j+1}(z) = \cdots = T_n(z) = 0$ for some $0 \le j \le n-1$, then (3.2) becomes

$$z^2 + \sum_{i=1}^{j} \Big(zT_i(\zeta_i x) + \zeta_i x T_i(z) \Big) + \sum_{i=j+1}^{n} zT_i\big(\zeta_i x\big) = 0.$$

Apply T_j:

$$T_j(z^2) + \sum_{i=1}^{j} \Big(T_j(zT_i(\zeta_i x)) + T_j(\zeta_i x T_i(z)) \Big) + T_j(z) \sum_{i=j+1}^{n} T_i(\zeta_i x) = 0,$$

so by Lemma 2.14(ii)

$$T_j(z^2) + \sum_{i=1}^{j} \Big(T_j(T_i(z)T_i(\zeta_i x)) + T_j(T_i(\zeta_i x)T_i(z)) \Big) + T_j(z) \sum_{i=j+1}^{n} T_i(\zeta_i x) = 0,$$

and hence

$$T_j(z)^2 + T_j(z) \sum_{i=j+1}^{n} T_i(\zeta_i x) = 0.$$

Thus, if $T_j(z) \ne 0$, then $T_j(z) = \sum_{i=j+1}^{n} T_i(\zeta_i x)$, and hence, by Lemma 2.14(i),

$$T_j(z) = \sum_{i=j+1}^{n} T_i(\zeta_i x) = T_{j+1}\big(\sum_{i=j+1}^{n} T_i(\zeta_i x) \big) = T_{j+1}(T_j(z)) = T_{j+1}(z) = 0,$$

a contradiction. Thus, $T_j(z) = 0$, as claimed.

Hence, by backwards induction, $z = T_0(z) = 0$. Consequently, $\mathfrak{P}_*$ is a semifield.

3.2. **Kernels.** In order to compute the kernel of a semifield plane, it suffices to compute the kernel

$$\mathfrak{K}(\mathfrak{S}_\circ) = \big\{k \in F \mid (k \circ x) \circ y = k \circ (x \circ y) \text{ for all } x, y \in F\big\} \tag{3.3}$$

of *any* coordinatizing semifield $\mathfrak{S}_\circ(F, +, \circ)$. The goal of this section is the following

Theorem 3.4. *If $n \geq 1$ and $[F\colon F_1] > 3$, then the kernel of any semifield isotopic to $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ is isomorphic to F_n.*

Note that some numerical restriction is needed here, since the plane is desarguesian if $q^m = 8$. Nevertheless, the restriction on F_1 is unfortunate.

In order to try to minimize notation, for the remainder of this section all summations will be from 1 to n unless otherwise indicated. We will need the reduction contained in part (ii) of the next observation:

Lemma 3.5.

(i) *If $\lambda \in F^*$ and $\sigma \in \mathrm{Aut}(F)$, then $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ and $\mathfrak{P}_\circ\big((F_i)_0^n, (\lambda\zeta_i^\sigma)_1^n\big)$ are isotopic: $\lambda(x * y)^\sigma = (\lambda^{-1}x^\sigma) \circ (\lambda y^\sigma)$ for all $x, y \in F$.*

(ii) *$\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ is isotopic to a presemifield $\mathfrak{P}_\circ\big((F_i)_0^n, (\zeta_i')_1^n\big)$ with $\sum T_i(\zeta_i') = 0$.*

Proof. (i) This is an easy calculation using (1.1).

(ii) Define an additive map $\Phi\colon F \to F_1$ by $\lambda \to \sum T_i(\lambda\zeta_i)$. Since $F\Phi \subseteq F_1 \subset F$, the kernel of Φ contains some $\lambda \in F^*$. Now use (i) with $\sigma = 1$. □

Remark 3.6. The semifields (1.1) arising when $n = 1$ were studied in [Ka1], where the corresponding plane was called a second cousin of the desarguesian plane. The preceding lemma explains why there was only one semifield other than a field arising there for a chain of fields $F = F_0 \supset F_1\colon$ each presemifield $\mathfrak{P}((F_i)_0^1, (\zeta_1))$ is isotopic to $\mathfrak{P}((F_i)_0^1, (1))$.

Since $x * y = xy^2 + T(x)y + T(xy)$, we have $\mathrm{Aut}(F) \leq \mathrm{Aut}(\mathfrak{P}_*)$. For later reference we note that, by [Ka1, I 4.1] and Corollary 3.23, if $q^m > 8$ then this plane is nondesarguesian, its kernel is isomorphic to F_1, and

$$\mathrm{Aut}\,\mathfrak{A}(\mathfrak{P}_*)_0 = (E(\mathcal{S}_*) \times K^*) \rtimes \mathrm{Aut}(F)$$

(cf. Lemma 2.21(i)), where $K^* \rtimes \mathrm{Aut}(F)$ acts on F^2 via $(x, y) \to (kx^\sigma, ky^\sigma)$ for $k \in K^*$, $\sigma \in \mathrm{Aut}(F)$.

We now obtain semifields from our presemifields as in Section 2.2:

Definition 3.7.

(i) $x \to \overline{x}$ is the inverse of $x \to 1 * x$, so that $\overline{x}^2 + \sum T_i(\zeta_i)\overline{x} + \sum \zeta_i T_i(\overline{x}) = x$, i.e., $1 * \overline{x} = x$.

(ii) $x \to \hat{x}$ is the inverse of $x \to x * 1$, so that $\hat{x} + \sum \Big(T_i(\zeta_i\hat{x}) + \zeta_i T_i(\hat{x})\Big) = x$, i.e., $\hat{x} * 1 = x$.

(iii) $\mathfrak{S}_\circ := \mathfrak{S}_\circ(F, \circ, +)$ is the semifield isotopic to $\mathfrak{P}_*$ defined by

$$x \circ y = \hat{x} * \overline{y}\,,$$

with multiplicative identity $1 * 1$.

We will also use further abbreviations: for all $u \in F$,

$$\begin{aligned} \hat{u} * y &= \hat{u}y^2 + c_u y + \sum \zeta_i T_i(\hat{u}y) \text{ with} \\ c_u &= \sum T_i(\zeta_i \hat{u}) \in F_1. \end{aligned} \tag{3.8}$$

Proof of Theorem 3.4. By Lemma 3.5(ii), we can change the ζ_i so as to have

$$\sum T_i(\zeta_i) = 0. \tag{3.9}$$

It suffices to consider the semifield (3.7)(iii) determined by the new elements ζ_i. We will make frequent use of the fact that (3.9) simplifies (3.7)(i).

Lemma 3.10.

(i) *The map $x \to \overline{x}$ is additive.*
(ii) *The map $x \to \hat{x}$ is F_n–linear.*
(iii) *If $\sum T_i(\zeta_i \hat{x}) = 0$ and $T_1(\hat{x}) = 0$, then $\hat{x} = x$, $\sum T_i(\zeta_i x) = 0$ and $T_i(x) = 0$ for all i.*
(iv) *If $T_1(\overline{y}) = 0$ then $\overline{y}^2 = y$.*
(v) *$\widehat{x * 1} = x$ and $\overline{1 * x} = x$ for all $x \in F$.*

Proof. (i) and (ii) are clear.

(iii) $T_i(\hat{x}) = 0$ for all i by Lemma 2.14(i), so that (3.7)(ii) reduces to $\hat{x} = x$, and hence $\sum T_i(\zeta_i x) = 0$ and $T_i(x) = 0$ for all i.

(iv) $T_i(\overline{y}) = 0$ for all i by Lemma 2.14(i), so that (3.7)(i) reduces to $\overline{y}^2 = y$ by (3.9).

(v) By definition, $\widehat{x * 1}$ is the unique z such that $z * 1 = x * 1$, so that $\widehat{x * 1} = x$. Similarly, $\overline{1 * x}$ is the unique z such that $1 * z = 1 * x$, so that $\overline{1 * x} = x$. □

Lemma 3.11. *If $\sum T_i(\zeta_i \hat{y}) = 0$ and $T_1(\hat{y}) = 0$, then $\overline{y}^2 = y$.*

Proof. By Lemma 3.10(iii), $\hat{y} = y$ and $T_j(y) = 0$ for all j. We will prove that $T_j(\overline{y}) = 0$ using backwards induction on $j = n, \dots, 1$. First consider the case $j = n$. By (3.7)(i),

$$\overline{y}^2 + \sum \Big(T_i(\zeta_i)\overline{y} + \zeta_i T_i(\overline{y}) \Big) = y\,. \tag{3.12}$$

Apply T_n:

$$T_n(\overline{y}^2) + \sum \Big(T_n(T_i(\zeta_i)\overline{y}) + T_n(\zeta_i T_i(\overline{y})) \Big) = T_n(y) = 0.$$

By Lemma 2.14(ii),

$$T_n(\overline{y}^2) + \sum \Big(T_n(T_i(\zeta_i)T_i(\overline{y})) + T_n(T_i(\zeta_i)T_i(\overline{y})) \Big) = 0,$$

and hence $T_n(\overline{y}) = 0$.

If $T_{j+1}(\overline{y}) = \cdots = T_n(\overline{y}) = 0$ for some $j \geq 1$, then (3.12) becomes

$$\overline{y}^2 + \sum_{i=1}^{j} \Big(T_i(\zeta_i)\overline{y} + \zeta_i T_i(\overline{y}) \Big) + \sum_{i=j+1}^{n} T_i(\zeta_i)\overline{y} = y.$$

Applying T_j and again using Lemma 2.14 yields

$$0 = T_j(y) = T_j(\overline{y}^2) + \sum_{i=1}^{j} T_j\Big(T_i(\zeta_i)T_i(\overline{y}) + T_i(\zeta_i)T_i(\overline{y})\Big) + T_j\Big(\sum_{i=j+1}^{n} T_i(\zeta_i)\overline{y}\Big)$$
$$= T_j(\overline{y})^2 + \sum_{i=j+1}^{n} T_i(\zeta_i)T_j(\overline{y}),$$

since $\sum_{i=j+1}^{n} T_i(\zeta_i) \in F_{j+1}$. If $T_j(\overline{y}) \neq 0$ then

$$T_j(\overline{y}) = \sum_{i=j+1}^{n} T_i(\zeta_i) = T_{j+1}\big(\sum_{i=j+1}^{n} T_i(\zeta_i)\big) = T_{j+1}(T_j(\overline{y})) = T_{j+1}(\overline{y}) = 0$$

by Lemma 2.14(i), a contradiction. Thus, $T_j(\overline{y}) = 0$.

Induction now gives $T_j(\overline{y}) = 0$ for all $j \geq 1$. By (3.9), (3.12) now reduces to $\overline{y}^2 = y$. □

We need to prove that the kernel $\mathfrak{K}$ of our semifield $\mathfrak{S}_\circ$ equals $\kappa := \{f * 1 \mid f \in F_n\}$, and hence is a field of size $|F_n|$. (N.B.—The fact that κ is a field can be seen directly: if $k, l \in F_n$ then $(k * 1) \circ (l * 1) = (kl) * 1$ using (1.1) and (3.7)(iii).)

First of all, $\mathfrak{K} \supseteq \kappa$: if $k \in F_n$ then $k * 1 \in \mathfrak{K}$. For, let $x, y \in F$ and calculate using (3.7)(iii):

$$(k * 1) \circ (x \circ y) = \widehat{k * 1} * \overline{(x \circ y)} = k * \overline{(x \circ y)} = k(1 * \overline{(x \circ y)}),$$

since $\widehat{k * 1} = k$ by Lemma 3.10(v) and $*$ is left F_n–linear. By (3.7)(i), the left F_n–linearity of $*$ and Lemma 3.10(v),

$$k(1 * \overline{(x \circ y)}) = k(x \circ y) = k(\hat{x} * \overline{y}) = (k\hat{x}) * \overline{y} = \widehat{kx} * \overline{y} = (kx) \circ y.$$

Again since $*$ is left F_n–linear, Lemma 3.10(i,v) and (3.7)(iii) imply that

$$(kx) \circ y = (k(1 * \overline{x})) \circ y = (k * \overline{x}) \circ y = \big((\widehat{k * 1}) * \overline{x}\big) \circ y = \big((k * 1) \circ x\big) \circ y.$$

Then $k * 1 \in \mathfrak{K}$ by (3.3).

It remains to prove that $\mathfrak{K} \subseteq \kappa$. Let k behave as in (3.3).

We restrict the elements x in (3.3) in the following ways:

(A1) Assume that $c_x = 0$ and $T_1(\hat{x}) = 0$. Then $\hat{x} = x$, $T_1(x) = 0$ and $\overline{x}^2 = x$ by Lemmas 3.10(iii) and 3.11.

(A2) Assume that $c_{k\circ x} = 0$ and $T_1(\widehat{k \circ x}) = 0$. Then $\widehat{k \circ x} = k \circ x$ and $\overline{k \circ x}^2 = k \circ x$, again by Lemmas 3.10(iii) and 3.11.

(A3) $x \neq 0$. Note that $x \neq 1$ by (A1), since $T_1(1) = 1 \neq T_1(x)$ by Lemma 2.14(iii).

Thus, x lies in the kernel of four additive maps $F \to F_1$. By hypothesis, $[F\colon F_1] > 3$, so that $|F|/|F_1|^4 \geq |F_1| \geq 2$ and there is an element x meeting all of these conditions. *We now fix x subject to these conditions.*

Lemma 3.13. *We may assume that some $k \in \mathfrak{K}$ satisfies $\hat{k} \notin F_n$, $c_k = 0$ and $k \circ x = \hat{k}x$.*

Proof. The first assertion is obvious. We use it to deal separately with the case $|F| = 2^5$. Since each line of $\mathfrak{A}(\mathcal{S}_\circ)$ is a vector space over $\mathfrak{K}$, we must have $\mathfrak{K} = F$ (i.e., $\mathcal{S}_\circ$ is a field). Then there are at least $|F|/|F_1|^2 = 8$ choices for k such that

$c_k = 0$ and $T_1(\hat{k}\overline{x}) = 0$; by (3.8), (3.7)(iii) and (A1), $k \circ x = \hat{k}x$ for at least 6 such elements $k \notin F_1$.

Now assume that $|F| > 2^5$; we will show that $c_k = 0$ and $k \circ x = \hat{k}x$. Consider all $y \neq 0$ satisfying the following four conditions (dependent upon our choice of x):

(B1) Assume that $T_1((k \circ x)\overline{y}) = 0$. Then $T_i((k \circ x)\overline{y}) = 0$ for all i by Lemma 2.14(i).

(B2) Assume that $T_1(x\overline{y}) = 0$. Then $T_i(x\overline{y}) = 0$ for all i by Lemma 2.14(i).

(B3) Assume that $T_1(\hat{k}\,\overline{x\overline{y}^2}) = 0$. Then $T_i(\hat{k}\,\overline{x\overline{y}^2}) = 0$ for all i by Lemma 2.14(i).

(B4) Assume that $T_1(\overline{x\overline{y}^2}) = 0$. Then $\overline{x\overline{y}^2}^2 = x\overline{y}^2$ by Lemma 3.10(iv).

By (A1), (3.7)(ii,iii), (3.8) and (B2), $\hat{x} = x$ and $x \circ y = \hat{x} * \overline{y} = \hat{x}\overline{y}^2 + c_x\overline{y} + \sum \zeta_i T_i(\hat{x}\overline{y}) = x\overline{y}^2$. Then, by (3.7)(ii), (3.8) and (B3),

$$\begin{aligned} k \circ (x \circ y) = \hat{k} * \overline{x\overline{y}^2} &= \hat{k}\,\overline{x\overline{y}^2}^2 + c_k\,\overline{x\overline{y}^2} + \sum \zeta_i T_i(\hat{k}\,\overline{x\overline{y}^2}) \\ &= \hat{k}\,\overline{x\overline{y}^2}^2 + c_k\,\overline{x\overline{y}^2}. \end{aligned} \tag{3.14}$$

By (A1) and (A2), $\widehat{k \circ x} = k \circ x$ and $\overline{x} = \sqrt{x}$. By (3.7)(iii) and (3.8),

$$k \circ x = \hat{k} * \overline{x} = \hat{k}x + c_k\sqrt{x} + \Lambda_{k,x} \tag{3.15}$$

for $\Lambda_{k,x} := \sum \zeta_i T_i(\hat{k}\overline{x})$. Moreover, by (3.7)(iii), (3.8), (A2) and (B1),

$$\begin{aligned} (k \circ x) \circ y = \widehat{k \circ x} * \overline{y} &= (k \circ x) * \overline{y} \\ &= (k \circ x)\overline{y}^2 + c_{k\circ x}\overline{y} + \sum \zeta_i T_i((k \circ x)\overline{y}) \\ &= (k \circ x)\overline{y}^2. \end{aligned}$$

Write $z = \overline{y}^2$, so that $\overline{xz}^2 = xz$ by (B4). By (3.3), (3.14) and (3.15),

$$\hat{k}\,\overline{xz}^2 + c_k\,\overline{xz} = (\hat{k}x + c_k\sqrt{x} + \Lambda_{k,x})z,$$

so that $c_k\sqrt{xz} = c_k\sqrt{x}\,z + \Lambda_{k,x}z$. Since $z = \overline{y}^2 \neq 0$,

$$c_k\sqrt{x/z} \;=\; c_k\sqrt{x} + \Lambda_{k,x}\,,$$

where the right side depends only on our chosen x satisfying (A1)–(A3).

Since $|F| > 2^5$ there are at least $|F|/|F_1|^4 \geq 4$ choices for y satisfying (B1)–(B4) (i.e., at least $|F_1| > 4$ choices if $n = 1$ and at least $|F_1| \geq |F_2|^3 \geq 8$ choices if there are $n + 1 \geq 3$ fields in our chain $(F_i)_0^n$). Then $c_k = \Lambda_{k,x} = 0$, and $k \circ x = \hat{k}x$ by (3.15). □

Lemma 3.16. $\hat{k} \in F_n$.

Proof. Again we are dealing with (3.3). We still have a fixed x satisfying (A1)–(A3), but this time we let y remain arbitrary. We have $\widehat{k \circ x} = k \circ x = \hat{k}x$ by (A2) and Lemma 3.13. By (3.7)(ii,iii), (3.8) and (A2),

$$\begin{aligned} (k \circ x) \circ y = \widehat{(k \circ x)} * \overline{y} &= \hat{k}x\overline{y}^2 + c_{k\circ x}\overline{y} + \sum \zeta_i T_i(\hat{k}x\overline{y}) \\ &= \hat{k}x\overline{y}^2 + \sum \zeta_i T_i(\hat{k}x\overline{y}). \end{aligned} \tag{3.17}$$

On the other hand, by (A1), (3.7)(iii) and (3.8), we have $\hat{x} = x$ and

$$x \circ y = \hat{x}\overline{y}^2 + c_x\overline{y} + \sum \zeta_i T_i(\hat{x}\overline{y}) = x\overline{y}^2 + \sum \zeta_i T_i(x\overline{y}).$$

By (3.7)(iii), (3.8) and Lemma 3.13,

$$k \circ (x \circ y) = \hat{k}\{\overline{x\overline{y}^2 + \sum \zeta_i T_i(x\overline{y})}\}^2 + \sum \zeta_i T_i(\hat{k}\{\overline{x\overline{y}^2 + \sum \zeta_i T_i(x\overline{y})}\}). \tag{3.18}$$

Write $z = \overline{y}$. By (3.3), (3.17) and (3.18),

$$\begin{aligned} &\hat{k}xz^2 + \sum \zeta_i T_i(\hat{k}xz) \\ &\quad = \hat{k}\{\overline{xz^2 + \sum \zeta_i T_i(xz)}\}^2 + \sum \zeta_i T_i(\hat{k}\{\overline{xz^2 + \sum \zeta_i T_i(xz)}\}). \end{aligned} \tag{3.19}$$

By (3.7)(i) and (3.9),

$$\overline{xz^2 + \sum \zeta_i T_i(xz)}^2 = \sum \zeta_i T_i\Big(\overline{xz^2 + \sum \zeta_i T_i(xz)}\Big) + xz^2 + \sum \zeta_i T_i(xz). \tag{3.20}$$

Substituting this into (3.19) and rearranging gives

$$\begin{aligned} &\sum \zeta_i T_i\Big(\hat{k}\{xz + \overline{xz^2 + \sum \zeta_i T_i(xz)}\}\Big) \\ &= \hat{k} \sum \zeta_i T_i\Big(xz + \overline{xz^2 + \sum \zeta_i T_i(xz)}\Big) \end{aligned} \tag{3.21}$$

for our choice of x and all $z \in F$.

The map $z \to xz + \overline{xz^2 + \sum \zeta_i T_i(xz)}$ is additive. We claim that it is invertible. For suppose that $xz = \overline{xz^2 + \sum \zeta_i T_i(xz)}$ for some z. Then we can replace $\overline{xz^2 + \sum \zeta_i T_i(xz)}$ by xz in (3.20) and obtain

$$(xz)^2 = \sum \zeta_i T_i(xz) + xz^2 + \sum \zeta_i T_i(xz),$$

so that $x^2z^2 = xz^2$. Then $z = 0$ by (A3). Thus, our map is invertible.

Let $w \in F$ be arbitrary and let z satisfy $w = xz + \overline{xz^2 + \sum \zeta_i T_i(xz)}$ in (3.21):

$$\sum \zeta_i T_i(\hat{k}w) \;=\; \hat{k} \sum \zeta_i T_i(w) \quad \forall w \in F. \tag{3.22}$$

Temporarily let $w = 1$: $\sum \zeta_i T_i(\hat{k}) = \hat{k} \sum \zeta_i$ by Lemma 2.14(iii). Thus,

$$w \sum_{i=1}^{n} \zeta_i T_i(\hat{k}) \;=\; w\hat{k} \sum_{i=1}^{n} \zeta_i$$

for all $w \in F$. Now temporarily let $w \in F_{n-1} - F_n$. Then (3.22) becomes

$$\sum_{i=1}^{n-1} \zeta_i w T_i(\hat{k}) + \zeta_n T_n(\hat{k}w) \;=\; \hat{k}\Big(\sum_{i=1}^{n-1} \zeta_i w + \zeta_n T_n(w)\Big)$$

by Lemma 2.14(iii). Adding the preceding equations yields

$$w\zeta_n T_n(\hat{k}) + \zeta_n T_n(\hat{k}w) \;=\; \hat{k}w\zeta_n + \hat{k}\zeta_n T_n(w).$$

Since $w \in F_{n-1} - F_n$ we have $w + T_n(w) \neq 0$, and hence

$$\hat{k} = (wT_n(\hat{k}) + T_n(\hat{k}w))/(w + T_n(w)) \in F_{n-1}.$$

Consequently, (3.22) reduces to $\hat{k}\zeta_n T_n(w) = \zeta_n T_n(\hat{k}w)$ for all $w \in F$. Set $w = 1$ and use Lemma 2.14(iii) in order to obtain $\hat{k} = \hat{k}T_n(1) = T_n(\hat{k}1) \in F_n$. This proves the lemma, contradicts Lemma 3.13, and hence completes the proof of Theorem 3.4. □

Corollary 3.23. *If $q^m > 8$ then the kernel of $\mathfrak{A}_*((F_i)_0^1, (1))$ is isomorphic to F_1.*

Proof. This was proved in [Ka3, 5.3] when $|F_1| > 2$. If $|F_1| = 2$ then $[F\colon F_1] \geq 5$, and Theorem 3.4 completes that proof.

If $|F_1| > 2$ we will give a shorter version of [Ka3, 5.3]. Define a semifield $\mathfrak{S}_\circ$ as in (3.7)(iii) using $\mathfrak{P}_*((F_i)_0^1, (1))$. Let $a \in F_1$. By (3.7)(i,ii), $\hat{a} = a$ and $\overline{a}^2 = a$ since $T_1(\zeta_1 a) = T_1(a) = a$. By (3.7), if $z \in F$ then $\hat{z} = z$, $z \circ a = z\overline{a}^2 = za$ and $a \circ z = a\overline{z}^2 + T_1(a)\overline{z} + T_1(a\overline{z}) = a(\overline{z}^2 + \overline{z} + T_1(\overline{z})) = az$. Then $F_1 \subseteq \mathfrak{K}$: if $x, y \in F$ then $(a \circ x) \circ y = (ax) \circ y = a(x \circ y) = a \circ (x \circ y)$ since $x \to x \circ y$ is F_1–linear, so that $a \in \mathfrak{K}$ by (3.3).

Suppose that $|\mathfrak{K}| > |F_1|$. Then each line of F^2 is a vector space over $\mathfrak{K}$, hence of odd dimension, so that $[\mathfrak{K}\colon F_1]$ is odd. Fix $a \in F_1 - \{0, 1\}$. By (3.3), $x \circ (y \circ a) = (x \circ y) \circ a$ for all $x, y \in \mathfrak{K}$. By the preceding paragraph, it follows that $x \circ (ya) = (x \circ y)a$, and hence

$$x\overline{ya}^2 + T_1(x)\overline{ya} + T_1(x\,\overline{ya}) = \{x\overline{y}^2 + T_1(x)\overline{y} + T_1(x\overline{y})\}a.$$

Thus,

$$x\{\overline{ya}^2 + \overline{y}^2 a\} = T_1(x)(\overline{ya} + \overline{y}a) + T_1(x\,\overline{ya}) + T_1(x\overline{y})a.$$

If $\overline{ya}^2 + \overline{y}^2 a \neq 0$ for some $y \in \mathfrak{K}$, then $\mathfrak{K}$ is contained in a 2–dimensional F_1–subspace of F (recall that $a \in F_1$), whereas $[\mathfrak{K}\colon F_1] \geq 3$. Thus, $\overline{ya}^2 + \overline{y}^2 a = 0$ for all $y \in \mathfrak{K}$, so that

$$T_1(x)(\overline{y}\sqrt{a} + \overline{y}a) = T_1(x\overline{y}\sqrt{a}) + T_1(x\overline{y})a \in F$$

for all $x, y \in \mathfrak{K}$. Since $\sqrt{a} + a \neq 0$ and $T_1(1) = 1$, this produces the contradiction $\overline{\mathfrak{K}} \subseteq F_1$. □

3.3. **Noncommutativity and dual kernel.** Theorem 3.4 and Corollary 3.23 do not handle all of the presemifields $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$; this remains an open question. However, those results and the next one show that most of them coordinatize nondesarguesian planes.

Proposition 3.24. *$\mathcal{S}_\circ\big((F_i)_0^n, (\zeta_i)_1^n\big)$ is not commutative if $n \geq 1$ and $|F_n| > 2$.*

Proof. Assume that $\mathcal{S}_\circ$ is commutative. Let $a \in F_n - \mathrm{GF}(2)$. The right side of $x \circ y = y \circ x$ is F_n–linear in y (by (3.7)), and hence the same must be true of the left side, so that

$$\hat{x}\,\overline{a\overline{y}}^2 + \sum \big[T_i(\zeta_i\hat{x})\overline{a\overline{y}} + \zeta_i T_i(\hat{x}\,\overline{a\overline{y}})\big] \;=\; a\big\{\hat{x}\overline{\overline{y}}^2 + \sum \big[T_i(\zeta_i\hat{x})\overline{\overline{y}} + \zeta_i T_i(\hat{x}\overline{\overline{y}})\big]\big\}$$

for all $x, y \in F$, by (1.1). Write x in place of $\hat{x}$ and rearrange, using the fact that $a \in F_n$: for all $x, y \in F$,

$$x(\overline{a\overline{y}}^2 + a\overline{\overline{y}}^2) \;=\; \sum T_i(\zeta_i x)[\overline{a\overline{y}} + a\overline{\overline{y}}] + \sum \zeta_i T_i(x[\overline{a\overline{y}} + a\overline{\overline{y}}]). \tag{3.25}$$

We claim that $\overline{a\overline{y}}^2 + a\overline{\overline{y}}^2 = 0$ for all $y \in F$. For, temporarily choose $x \neq 0$ such that $\sum T_i(\zeta_i x) = 0$ and $T_1(x[\overline{a\overline{y}} + a\overline{\overline{y}}]) = 0$, and then $T_i(x[\overline{a\overline{y}} + a\overline{\overline{y}}]) = 0$ for all i by Lemma 2.14(i); since $[F\colon F_1] \geq 3$ there exists such a nonzero x. Then (3.25) implies our claim.

Since $a \in F_n$, (3.25) now states that

$$(a + \sqrt{a})\Big(\sum T_i(\zeta_i x)\overline{\overline{y}} + \sum \zeta_i T_i(x\overline{\overline{y}})\Big) = 0,$$

for all $x, y \in F$. Since $a + \sqrt{a} \neq 0$,

$$\sum T_i(\zeta_i x)\overline{\overline{y}} + \sum \zeta_i T_i(x\overline{\overline{y}}) = 0 \quad \forall x, \overline{\overline{y}} \in F. \tag{3.26}$$

We now show that (3.26) *is impossible.* Fix x, choose $y \neq 0$ such that $T_1(x\overline{y}) = 0$ and hence $T_i(x\overline{y}) = 0$ for all i (Lemma 2.14(i)), and obtain $\sum T_i(\zeta_i x)\overline{y} = 0$ for at least $|F|/|F_1| \geq 2$ choices for y. It follows that, for all $x \in F$, $T_1(\zeta_1 x)$ is 0 if $n = 1$ and is $\sum_2^n T_i(\zeta_i x) \in F_2$ if $n > 1$. Since x is arbitrary, this contradicts the fact that $T_1(\zeta_1 F) = F_1$. □

Proposition 3.27. *If $n \geq 1$ and $[F\colon F_1] > 5$, then the kernel of the dual of the plane $\mathfrak{A}\big((F_i)_0^n, (\zeta_i)_1^n\big)$ is* GF(2).

Proof. We will use the same semifield $\mathcal{S}_\circ(F, +, \circ)$ as in the proof of Theorem 3.4; this is defined in (3.7)(iii). The dual plane is coordinatized by $\mathcal{S}_{\circ'}(F, +, \circ')$, where $x \circ' y = y \circ x$ [De, 3.1.36]. Therefore, in view of (3.3), assume that $k \in F$ and

$$(x \circ y) \circ k = x \circ (y \circ k) \tag{3.28}$$

for all $x, y \in F$. We must prove that there are only two possibilities for k.

We first show that

$$\overline{y}\overline{k} = \overline{y \circ k} \tag{3.29}$$

for all y. For, fix y and choose x satisfying various additional conditions:

(1) $c_{x\circ y} = T_1(\widehat{x \circ y}) = 0$, so that $\widehat{x \circ y} = x \circ y$ by Lemma 3.10(iii).
(2) $c_x = T_1(\hat{x}\bar{y}) = 0$, so that $x \circ y = \hat{x} * \overline{y} = \hat{x}\overline{y}^2$ by (3.8) and Lemma 2.14(i).
(3) $T_1((x \circ y)\bar{k}) = 0$, so that $(x \circ y) * \overline{k} = (x \circ y)\overline{k}^2 = \hat{x}\overline{y}^2\overline{k}^2$ by (3.8), (1), (2) and Lemma 2.14(i).
(4) $T_1(\hat{x}\,\overline{y \circ k}) = 0$, so that $\hat{x} * \overline{y \circ k} = \hat{x}\,\overline{y \circ k}^2$ by (3.8), (2) and Lemma 2.14(i).

Since $[F\colon F_1] \geq 7$, some $x \neq 0$ satisfies these six additive conditions. By (3.7)(iii), (3.28) now becomes $\hat{x}\,\overline{y}^2\bar{k}^2 = (x \circ y) * \overline{k} = \hat{x} * \overline{y \circ k} = \hat{x}\,\overline{y \circ k}^2$, so that (3.29) holds.

Next we fix x and choose y satisfying additional conditions:

(1′) $c_{x\circ y} = T_1(\widehat{x \circ y}) = 0$, so that $\widehat{x \circ y} = x \circ y$ by Lemma 3.10(iii).
(2′) $T_1(\hat{x}\overline{y}) = 0$, so that $x \circ y = \hat{x} * \overline{y} = \hat{x}\overline{y}^2 + c_x\overline{y}$ by (3.8) and Lemma 2.14(i).
(3′) $c_{x\circ y} = T_1((x \circ y)\bar{k}) = 0$, so that $(x \circ y) * \bar{k} = (x \circ y)\bar{k}^2 = (\hat{x}\overline{y}^2 + c_x\overline{y})\bar{k}^2$ by (3.8), Lemma 2.14(i) and (2′).
(4′) $T_1(\hat{x}(\overline{y}\overline{k})) = 0$, so that $\hat{x} * (\overline{y}\overline{k}) = \hat{x}(\overline{y}\overline{k})^2 + c_x(\overline{y}\overline{k})$ by (3.8) and Lemma 2.14(i).

Once again some $y \neq 0$ satisfies these six requirements. By (3.7)(iii), (3.28) and (3.29),

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

Here $\overline{y} \neq 0$, and we can choose x so that $c_x \neq 0$ (since $T_1(\zeta_1 F) = F_1$). It follows that $\overline{k}^2 = \overline{k}$. □

3.4. **Duality.** It seems likely that all of our semifield planes are not self–dual, except for the desarguesian ones; this would contain Proposition 3.24 as a very special case. However, we have not been able to prove this without additional hypotheses (Theorem 3.31).

If $\mathfrak{S}_\circ$ is a semifield, then $\mathfrak{A}(\mathfrak{S}_\circ)$ is self–dual if and only if $\mathfrak{S}_\circ$ has an *antiautotopism*: a triple (α, β, γ) of additive permutations of $\mathfrak{S}_\circ$ such that $\gamma(y \circ x) =$

$\alpha(x)\circ\beta(y)$ for all $x,y\in\mathfrak{S}_\circ$. Clearly, the autotopisms and antiautotopisms form a group. We begin with a simple observation:

Theorem 3.30. *Assume that $\mathfrak{S}_\circ$ is a semifield whose group of autotopisms has odd order. If $\mathfrak{A}(\mathfrak{S}_\circ)$ is self–dual, then*

(i) *$\mathfrak{A}(\mathfrak{S}_\circ)$ admits a polarity, and*

(ii) *if $|\mathfrak{S}_\circ|$ is not a square, then there is some $k\neq 0$ in $\mathfrak{S}_\circ$ such that $(k\circ x)\circ y=(k\circ y)\circ x$ for all $x,y\in\mathfrak{S}_\circ$.*

Proof. (i) A group whose order is twice an odd number contains involutions.

(ii) Since the plane has nonsquare order n, a polarity has exactly $n+1$ absolute points by a classical result of Baer [Ba, Theorems 5 and 6]. Then $\mathfrak{A}(\mathfrak{S}_\circ)$ can be coordinatized by a commutative semifield by [Ga, Theorem 3], and hence the desired k exists by [Ga, Theorem 4]. □

Theorem 3.31. *The plane $\mathfrak{A}_*((F_i)_0^n,(\zeta_i)_1^n)$, $n\geq 1$, is not self–dual if either*

(i) *$[F\colon F_1]>5$ and $|F_n|>2$, or*

(ii) *$[F\colon F_1]>3$ and $|F|$ is not a square.*

Proof. (i) By Theorem 3.4 and Proposition 3.27, $\mathfrak{A}_*\big((F_i)_0^n,(\zeta_i)_1^n\big)$ and its dual have different kernels.

(ii) We will prove later in Theorem 4.12 that the autotopism group of $\mathfrak{A}_*$ is isomorphic to a subgroup of $\mathrm{Aut}(F)$, so that the hypotheses of Theorem 3.30 hold.

Thus, we will consider the semifield $\mathfrak{S}_\circ$ in (3.7), assume that there is some $k\in F^*$ such that

$$(k\circ x)\circ y=(k\circ y)\circ x\quad\forall x,y\in F, \tag{3.32}$$

and deduce a contradiction. By [Kn1, p. 207], we may assume that $|F|>2^5$.

As in the proof of Theorem 3.4, we begin by making restrictions on x and y:

(1x) Assume that $c_{k\circ x}=0$ and $T_1(\widehat{k\circ x})=0$. Then $\widehat{k\circ x}=k\circ x=\hat{k}*\overline{x}$ by Lemma 3.10(iii).

(1y) Assume that $c_{k\circ y}=0$ and $T_1(\widehat{k\circ y})=0$. Then $\widehat{k\circ y}=k\circ y=\hat{k}*\overline{y}$.

By (1x), (3.7) and (3.8),

$$\begin{aligned}(k\circ x)\circ y&=(k\circ x)*\overline{y}\\&=(k\circ x)\overline{y}^2+\sum\zeta_iT_i((k\circ x)\overline{y})\\&=\{\hat{k}\overline{x}^2+c_k\overline{x}+\sum\zeta_jT_j(\hat{k}\overline{x})\}\overline{y}^2\\&\quad+\sum\zeta_iT_i\big(\{\hat{k}\overline{x}^2+c_k\overline{x}+\sum\zeta_jT_j(\hat{k}\overline{x})\}\overline{y}\big),\end{aligned} \tag{3.33}$$

with a similar formula for $(k\circ y)\circ x$.

We claim that $c_k=0$. For this purpose we further restrict x and y as follows:

(2x) Assume that $T_1(\hat{k}\overline{x})=0$, so that $T_i(\hat{k}\overline{x})=0$ for all i by Lemma 2.14(i).

(2y) Assume that $T_1(\hat{k}\overline{y})=0$, so that $T_i(\hat{k}\overline{y})=0$ for all i.

(3) Assume that,

$$T_1\Big(\{\hat{k}\overline{x}^2+c_k\overline{x}+\sum\zeta_jT_j(\hat{k}\overline{x})\}\overline{y}+\{\hat{k}\overline{y}^2+c_k\overline{y}+\sum\zeta_jT_j(\hat{k}\overline{y})\}\overline{x}\Big)=0,$$

so that, for all i,

$$T_i\Big(\{\hat{k}\overline{x}^2+c_k\overline{x}+\sum\zeta_jT_j(\hat{k}\overline{x})\}\overline{y}+\{\hat{k}\overline{y}^2+c_k\overline{y}+\sum\zeta_jT_j(\hat{k}\overline{y})\}\overline{x}\Big)=0.$$

Then (3.32), together with (3.33) and its version for $(k \circ y) \circ x$, implies that

$$(\hat{k}\overline{x}^2 + c_k\overline{x})\overline{y}^2 = (\hat{k}\overline{y}^2 + c_k\overline{y})\overline{x}^2. \tag{3.34}$$

There are at least $|F|/|F_1|^3 \geq 4$ choices for x satisfying (1x) and (2x), and then $|F|/|F_1|^4 \geq 4$ choices for y satisfying (1y), (2y) and (3), since $|F| > 2^5$. Thus, we can choose x and y such that $\overline{x} \neq 0$ and $\overline{y} \neq 0, \overline{x}$. Then $c_k = 0$ by (3.34).

Now fix x such that $c_{k\circ x} = \sum T_i(\zeta_i \widehat{k \circ x}) \neq 0$ (cf. (3.8)); such a choice is possible since $T_1(\zeta_1 F) = F_1$. Choose y such that (1y) holds, as well as $T_1(\hat{k}\overline{y}) = 0$ and $T_1(\hat{k}\overline{y}^2\overline{x}) + T_1(\widehat{k \circ x}\,\bar{y}) = 0$. Then

$$T_i(\hat{k}\overline{y}) = T_i(\hat{k}\overline{y}^2\overline{x} + \widehat{k \circ x}\,\overline{y}) = 0 \tag{3.35}$$

for all i, by Lemma 2.14(i), and the version of (3.33) for $(k \circ y) \circ x$ reduces to

$$(k \circ y) \circ x = \hat{k}\overline{y}^2\overline{x}^2 + \sum \zeta_i T_i(\hat{k}\overline{y}^2\overline{x}). \tag{3.36}$$

On the other hand, for any x we have, by (3.7) and (3.8),

$$\begin{aligned}(k \circ x) \circ y &= \widehat{k \circ x} * \overline{y} \\ &= \widehat{k \circ x}\,\overline{y}^2 + c_{k\circ x}\overline{y} + \sum \zeta_i T_i(\widehat{k \circ x}\,\overline{y}),\end{aligned} \tag{3.37}$$

while $\widehat{k \circ x} + c_{k\circ x} + \sum \zeta_i T_i(\widehat{k \circ x}) = k \circ x = \hat{k} * \overline{x} = \hat{k}\overline{x}^2 + \sum \zeta_i T_i(\hat{k}\overline{x})$. Thus, by (3.35)–(3.37),

$$\Big\{\hat{k}\overline{x}^2 + \sum \zeta_i T_i(\hat{k}\overline{x}) + c_{k\circ x} + \sum \zeta_i T_i(\widehat{k \circ x})\Big\}\overline{y}^2 + c_{k\circ x}\overline{y} = \hat{k}\overline{y}^2\overline{x}^2,$$

so that

$$\Big\{\sum \zeta_j T_i(\hat{k}\overline{x}) + c_{k\circ x} + \sum \zeta_i T_i(\widehat{k \circ x})\Big\}\overline{y}^2 = c_{k\circ x}\overline{y}.$$

Here $c_{k\circ x} \neq 0$, so that there is just one possible $\overline{y} \neq 0$ satisfying this equation. However, for our chosen x we made four additive restrictions on y, so that the number of chosen y is at least $|F|/|F_1|^4 \geq 4$ since $|F| > 2^5$, a contradiction. □

3.5. **Equality.** It appears to be not entirely trivial to determine when two of our presemifields are *equal*, although the result holds no surprises:

Proposition 3.38. *For presemifields* $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ *and* $\mathfrak{P}_\circ\big((F_i')_0^{n'}, (\zeta_i')_1^{n'}\big)$ *with* $F = F_0 = F_0'$, *if* $x * y = x \circ y$ *for all* $x, y \in F$, *then* $n = n', F_i = F_i'$ *and* $\zeta_i = \zeta_i'$ *for* $1 \leq i \leq n$.

Proof. Set

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

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

Lemma 3.39.

(i) *If* $n \geq 1$, *then* $f(x,y) \neq 0$ *for some* $x, y \in F$.
(ii) *If* $f(kx,y) = kf(x,y)$ *for all* $x, y \in F$, *then* $k \in F_n$.

Proof. (i) We have already proved that (3.26) is impossible.

(ii) Let $x \in F^*$. Since $[F\colon F_1] \geq 3$, some $y \in F^*$ satisfies $T_1\big(kxy\big) = 0 = T_1(xy)$. By Lemma 2.14(i), $T_i\big(kxy\big) = 0$ and $T_i(xy) = 0$ for all i, and the equation $f(kx, y) = kf(x, y)$ reduces to $\sum T_i\big(\zeta_i kx\big)y = k\sum T_i(\zeta_i x)y$. Hence, for all $x \in F$,

$$\sum_{i=1}^{n} T_i\big(\zeta_i kx\big) = k\sum_{i=1}^{n} T_i(\zeta_i x).$$

Let $0 \leq j \leq n$ be maximal such that $k \in F_j$. Suppose that $j < n$. Then $T_i(\zeta_i kx) = kT_i(\zeta x)$ for all $i \leq j$, so that

$$\sum_{i=j+1}^{n} T_i\big(\zeta_i kx\big) = k\sum_{i=j+1}^{n} T_i(\zeta_i x) \tag{3.40}$$

for all $x \in F$. Choose x such that $T_{j+1}(\zeta_{j+1}x) \neq 0$. Then $T_{j+1}(\zeta_{j+1}F_{j+1}x) = F_{j+1}$ properly contains the image of F_{j+1} under the map $l \to \sum_{j+2}^{n} T_i(\zeta_i lx)$ (we interpret this sum to be 0 if $j + 1 = n$). Then there is some $l \in F_{j+1}$ such that $\sum_{j+1}^{n} T_i(\zeta_i lx) \neq 0$. Now (3.40) yields the contradiction $k \in F_{j+1}$.

Thus, $j = n$ and $k \in F_n$, as claimed. □

Proof of Proposition 3.38. Suppose that $n' = 0$. Then $g(x, y)$ is identically 0. If $n > 0$, then $f(x, y)$ is nonzero for some $x, y \in F$, by Lemma 3.39(i). Thus, the proposition holds if n or n' is 0.

Now suppose, inductively, that $n, n' > 0$, and that the conclusion holds for $\big((F_i)_0^{n-1}, (\zeta_i)_1^{n-1}\big)$ and $\big((F'_i)_0^{n'-1}, (\zeta'_i)_1^{n'-1}\big)$.

Lemma 3.39(ii) implies that F_n is the largest subfield of F over which $f(x, y)$ is linear in x. Likewise $F'_{n'}$ is the largest subfield of F over which $g(x, y)$ is linear in x. Hence $F_n = F'_{n'} := K$.

Most of the proof consists of showing that $\zeta_n = \zeta'_{n'}$. We write ζ for ζ_n and ζ' for $\zeta'_{n'}$. We may assume that $[F_{n-1}\colon K] \geq [F'_{n'-1}\colon K]$.

Fix $l \in F'_{n'-1} - K$. By hypothesis,

$$f(lx, y) + lf(x, y) = g(lx, y) + lg(x, y)$$

for all $x, y \in F$. If k is such that $l \in F_{k-1} - F_k$, then this simplifies to

$$\begin{aligned}\sum_{i=k}^{n} \Big(\zeta_i T_i(lxy) + T_i(\zeta_i lx)y\Big) + l\sum_{i=k}^{n} \Big(\zeta_i T_i(xy) + T_i(\zeta_i x)y\Big)\\ = \ \zeta' T'_{n'}(lxy) + T'_{n'}(\zeta' lx)y + l\Big(\zeta' T'_{n'}(xy) + T'_{n'}(\zeta' x)y\Big).\end{aligned}$$

Since $T_n = T'_{n'}$, it follows that

$$\begin{aligned}\sum_{i=k}^{n-1} \Big(\zeta_i T_i(lxy) + T_i(\zeta_i lx)y\Big) + l\sum_{i=k}^{n-1} \Big(\zeta_i T_i(xy) + T_i(\zeta_i x)y\Big)\\ = \ T_n\big((\zeta + \zeta')lx\big)y + (\zeta + \zeta')T_n(lxy)\\ + \ l\Big(T_n((\zeta + \zeta')x)y + (\zeta + \zeta')T_n(xy)\Big)\end{aligned} \tag{3.41}$$

for all $x, y \in F$.

If possible, choose $x, y \in F$ such that the left hand side of (3.41) is not zero. Then $l \notin F_{n-1}$, so that $F_{n-1} \neq F'_{n'-1}$. As $[F_{n-1}\colon K] \geq [F_{n'-1}\colon K]$ was assumed,

we must have $[F_{n-1}\colon K] > [F'_{n'-1}\colon K] \geq 3$. Moreover, the map $F_{n-1} \to F$ given by

$$\begin{aligned} t \;\to\; & \sum_{i=k}^{n-1}\Big(\zeta_i T_i(l(tx)y) + T_i(\zeta_i l(tx))y\Big) + l\sum_{i=k}^{n-1}\Big(\zeta_i T_i((tx)y) + T_i(\zeta_i(tx)y\Big) \\ = \; & t\Big(\sum_{i=k}^{n-1}\Big(\zeta_i T_i(lxy) + T_i(\zeta_i lx)y\Big) + l\sum_{i=k}^{n-1}\Big(\zeta_i T_i(xy) + T_i(\zeta_i x)y\Big)\Big) \end{aligned}$$

is injective, and hence its image spans a K–subspace of F having K–dimension exactly $[F_{n-1}\colon K] \geq 5$. However, using the right hand side of (3.41), we see that our map is also

$$\begin{aligned} t \;\to\; & T_n\Big((\zeta+\zeta')l(tx)\Big)y + (\zeta+\zeta')T_n\Big(l(tx)y\Big) \\ & + lT_n\Big((\zeta+\zeta')(tx)\Big)y + l(\zeta+\zeta')T_n\Big((tx)y\Big). \end{aligned}$$

Since y, $\zeta+\zeta'$, ly and $y(\zeta+\zeta')$ are fixed, the image of this map spans at most a 4–dimensional K–subspace, which is a contradiction.

Hence, no such x, y exist, and for all $x, y \in F$ both sides of (3.41) are 0:

$$T_n\big((\zeta+\zeta')lx\big)y + (\zeta+\zeta')T_n(lxy) = lT_n\big((\zeta+\zeta')x\big)y + l(\zeta+\zeta')T_n(xy).$$

Then

$$\Big(lT_n\big((\zeta+\zeta')x\big) + T_n\big((\zeta+\zeta')lx\big)\Big)y = l(\zeta+\zeta')T_n(xy) + l(\zeta+\zeta')T_n(lxy) \tag{3.42}$$

for all $x, y \in F$.

Suppose that $\zeta \neq \zeta'$. Choose $x \in F$ such that $T_n(l(\zeta+\zeta')x) \neq 0$. Then $lT_n((\zeta+\zeta')x) + T_n(l(\zeta+\zeta')x) \neq 0$ (as otherwise $lT_n((\zeta+\zeta')x) = T_n(l(\zeta+\zeta')x) \in K^*$ and hence $l \in F_n = K$, which is not the case). Consequently, as y varies over F the left side of (3.42) spans F and the right side spans at most a 2–dimensional K–subspace of F, whereas $[F\colon K] \geq 3$.

Thus, $\zeta = \zeta'$, so that $f(x,y) + \zeta T_n(xy) + T_n(\zeta x)y = g(x,y) + \zeta T_n(xy) + T_n(\zeta x)y$ states that

$$\sum_{i=1}^{n-1}\Big(\zeta_i T_i(xy) + T_i(\zeta_i x)y\Big) = \sum_{i=1}^{n'-1}\Big(\zeta'_i T'_i(xy) + T'_i(\zeta'_i x)y\Big)$$

for all $x, y \in F$. Induction now completes the proof of the proposition. □

4. The semifield orthogonal spreads and semifield planes

This is the main section of this paper. Its goals are the determination, under mild arithmetical assumptions, of the automorphism groups of our semifield orthogonal spreads and planes (Theorem 4.12), as well as equivalences between pairs of these semifield orthogonal spreads or planes (Theorem 4.13). For example, under mild arithmetical assumptions two presemifields $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ and $\mathfrak{P}_\circ\big((F'_i)_0^{n'}, (\zeta'_i)_1^{n'}\big)$ determine equivalent orthogonal spreads if and only if $n' = n$, $F'_i = F_i$ and $\zeta'_i = \lambda\zeta_i^\sigma$ for all $1 \leq i \leq n$ and some $\lambda \in F^*$ and $\sigma \in \mathrm{Aut}(F)$.

When $[F\colon F_1] > 3$, the crucial idea is to use kernels of semifields to detect the equivalence of orthogonal spreads: we will see that there is a unique nonsingular point ν of V fixed by $E(\Sigma_*)$ (cf. Lemma 2.21(ii)) such that the kernel of the plane $\mathfrak{A}(\Sigma_*/\nu)$ is largest. It follows that $\mathrm{O}(V)_{\Sigma_*}$ must fix ν and hence is determined by $\mathrm{Aut}\,\mathfrak{A}(\Sigma_*/\nu)$. At this point induction can be used. This outline is the pleasant

part of the argument. The difficult part is the implementation: in Theorem 3.4 we had to calculate the kernels of planes defined using the ridiculous formula (1.1).

Always m will be an arbitrary odd integer > 1, and we will use the fields $F = \mathrm{GF}(q^m)$ and $K = \mathrm{GF}(q)$, $q^m > 8$, with corresponding trace map $T\colon F \to K$. In this section we study the following objects:

- a presemifield $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$, where we always assume that $F_0 = F$;
- a symplectic spread (1.2), denoted $\mathcal{S}_* = \mathcal{S}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$, of the F_n–space F^2;
- a corresponding affine plane (cf. Section 2.1), denoted $\mathfrak{A}(\mathcal{S}_*) = \mathfrak{A}(\mathfrak{P}_*) = \mathfrak{A}_*\big((F_i)_0^n, (\zeta_i)_1^n\big) = \mathfrak{A}\big((F_i)_0^n, (\zeta_i)_1^n\big)$; and
- an orthogonal spread $\Sigma_* = \Sigma_*((F_i)_0^{n+1}, (\zeta_i)_1^n) = \Sigma((F_i)_0^{n+1}, (\zeta_i)_1^n)$, defined in (1.4), of the K–space V given in (1.3), where $K = F_{n+1}$. Note that

$$\begin{aligned} \mathcal{S}((F_i)_0^n, (\zeta_i)_1^n) &= \Sigma((F_i)_0^{n+1}, (\zeta_i)_1^n)/\langle 0,1,0,1\rangle, \\ \mathcal{S}((F_i)_0^{n+1}, (\zeta_i)_1^{n+1}) &= \Sigma((F_i)_0^{n+1}, (\zeta_i)_1^n)/\langle 0,1,\zeta_{n+1},1\rangle, \end{aligned} \tag{4.1}$$

  for any $\zeta_{n+1} \in F^*$, by Theorem 2.18(ii,iii) and Propositon 2.19.

Recall that an orthogonal spread Σ is called *desarguesian* if it is the lift $\Sigma^\nu(\mathcal{S})$ of a desarguesian spread $\mathcal{S}$, so that $\mathfrak{A}(\Sigma/\langle 0,1,0,1\rangle)$ is a desarguesian plane $\mathfrak{A}(\mathcal{S})$ (cf. (2.12)). In the above notation, $n = 0$ and $\Sigma = \Sigma((F_i)_0^1, (\zeta_1))$ if the orthogonal space is an F_1–space; each nondesarguesian plane corresponding to a slice $\Sigma/\langle 0,1,\zeta,1\rangle$ is a second cousin whose kernel is F_1 (cf. Remark 3.6 and Corollary 3.23).

4.1. **Nondesarguesian orthogonal spreads.** At crucial points in the proofs of Proposition 4.11 and Theorem 4.13 we will need to know that we are not dealing with desarguesian spreads:

Proposition 4.2. *Assume that $n \geq 1$.*

(i) *The affine plane $\mathfrak{A}(\mathcal{S}_*\big((F_i)_0^n, (\zeta_i)_1^n\big))$ is nondesarguesian if either $[F\colon F_1] > 3$ or $|F_n| > 2$.*
(ii) *The orthogonal spread $\Sigma_*((F_i)_0^{n+1}, (\zeta_i)_1^n)$ is nondesarguesian.*

Proof. (i) If $[F\colon F_1] > 3$ use Theorem 3.4, while if $|F_n| > 2$ use Proposition 3.24.

(ii) By (4.1), $\mathfrak{A}(\mathcal{S}_*) \cong \mathfrak{A}(\Sigma_*/\langle 0,1,0,1\rangle) = \mathfrak{A}\big((F_i)_0^n, (\zeta_i)_1^n\big)$, so the kernel of this plane contains $F_n \supset F_{n+1}$. This plane is nondesarguesian by (i).

Assume that Σ_* is a desarguesian spread of an orthogonal F_{n+1}–space. Then, as noted in Remark 3.6, every semifield spread slice (2.10) of Σ_* produces either a desarguesian plane or a second cousin of a desarguesian plane, where this second cousin has kernel F_{n+1}. Since $F_n \supset F_{n+1}$, this is not the case for $\mathfrak{A}(\mathcal{S}_*)$. □

4.2. **Automorphism groups of semifield orthogonal spreads.** Given a semifield orthogonal spread $\Sigma_* = \Sigma_*((F_i)_0^{n+1}, (\zeta_i)_1^n)$, under mild arithmetical assumptions we will show in Theorem 4.12 that $\Gamma\mathrm{O}^+(2m+2, K)_{\Sigma_*} \cong (K^* \times E(\Sigma_*)) \rtimes \Lambda$, where $K = F_{n+1}$, $E(\Sigma_*)$ is the elementary abelian group of order q^m in Lemma 2.21(ii) and $\Lambda \leq \mathrm{QAut}(F)$. Critical to this will be the fact that $\Gamma\mathrm{O}^+(2m+2, K)_{\Sigma_*}$ fixes the nonsingular point $\langle 0,1,0,1\rangle$ (Proposition 4.4).

We note that only the cases of the results in this and the next section involving the hypothesis $[F\colon F_1] > 3$ are needed for our coding–theoretic applications in Sections 5.5 and 5.6.

For the orthogonal space V in (1.3), let

$$X = F \oplus K \oplus 0 \oplus 0 \quad \text{and} \quad Y = 0 \oplus 0 \oplus F \oplus K. \tag{4.3}$$

These play the roles of the x– and y–axes.

Proposition 4.4. *Let $\Sigma_*((F_i)_0^{n+1}, (\zeta_i)_1^n)$ and $\Sigma_\circ((F'_{i'})_0^{n'+1}, (\zeta'_i)_1^{n'})$ be semifield orthogonal spreads in the K–space V in* (1.3)*, where $n \geq 1, n' \geq 1$, $F = F_0 = F'_0$ and $K = F_{n+1} = F'_{n'+1}$. Suppose that either $[F\colon F_1] > 3$ and $[F\colon F'_1] > 3$, or $|K| > 2$. If $\omega \in \Gamma\mathrm{O}^+(V)$ satisfies*

$$\Sigma_*^\omega = \Sigma_\circ \quad \text{and} \quad E(\Sigma_*)^\omega = E(\Sigma_\circ),$$

then ω fixes the nonsingular point $\langle 0,1,0,1\rangle$.

Proof. Since ω sends $C_V(E(\Sigma_*))$ to $C_V(E(\Sigma_\circ))$, it permutes the set $\{\langle 0,1,\zeta,1\rangle \mid \zeta \in F\}$ of all nonsingular points in $C_V(E(\Sigma_*)) = C_V(E(\Sigma_\circ))$ (cf. Lemma 2.21(iv)). Thus, $\langle 0,1,0,1\rangle^\omega = \langle 0,1,\zeta,1\rangle$ for some $\zeta \in F$. *We must show that* $\zeta = 0$.

By Lemma 2.21(iii), $C_V(E(\Sigma_*))$ has nonzero intersection with a unique member $\Sigma_*[\infty] = Y$ of Σ_* and a unique member $\Sigma_\circ[\infty] = Y$ of $\Sigma_\circ$, so that $Y^\omega = Y$. Since $E(\Sigma_\circ)$ fixes $\langle 0,1,0,1\rangle$ and is transitive on $\Sigma_\circ - \{Y\}$, we may assume that $X^\omega = X$.

We now consider separately the cases $[F\colon F_1] > 3$ and $[F\colon F'_1] > 3$, or $|K| > 2$.

Case 1. $[F\colon F_1] > 3$ *and* $[F\colon F'_1] > 3$. By (2.10), ω induces an isomorphism between the affine planes $\mathfrak{A} = \mathfrak{A}(\Sigma_*/\langle 0,1,0,1\rangle)$ and $\mathfrak{A}' = \mathfrak{A}(\Sigma_\circ/\langle 0,1,\zeta,1\rangle)$. By (4.1), $\mathfrak{A} = \mathfrak{A}\big((F_i)_0^n, (\zeta_i)_1^n\big)$.

Assume that $\zeta \neq 0$, and write $\zeta'_{n'+1} = \zeta$. Then $\mathfrak{A}' = \mathfrak{A}((F'_i)_0^{n'+1}, (\zeta'_i)_1^{n'+1})$ by (4.1). By Theorem 3.4, $\mathfrak{A}'$ has kernel isomorphic to F_{n+1}, while $\mathfrak{A}_*$ has kernel isomorphic to F_n, hence of size greater than $|F_{n+1}|$.

This contradiction implies that $\zeta = 0$ and $\langle 0,1,0,1\rangle^\omega = \langle 0,1,0,1\rangle$.

Remark. The above use of kernels was the starting point for much of this paper. The case $|K| = 2$ is the one required in Sections 5.5 and 5.6.

Case 2. $|K| > 2$. We begin with a slight reduction. We first assume that the result holds when ω is restricted to belonging to $\mathrm{O}^+(V)$ and deduce the general statement from this special case. By [Ta, p. 136] we can write $\omega = k\omega'\tau$ with $k \in K^*$, $\omega' \in \mathrm{O}^+(V)$, and $\tau \in \mathrm{Aut}(K)$. The scalar transformation

$$k\colon (x,a,y,b) \to k(x,a,y,b)$$

fixes X, Y, $\langle 0,1,0,1\rangle$ and Σ_*, while the field automorphism

$$\tau\colon (x,a,y,b) \to (x^\tau, a^\tau, y^\tau, b^\tau)$$

fixes X, Y and $\langle 0,1,0,1\rangle$. We have $\Sigma_*^{\omega'} = \Sigma_*^{\omega\tau^{-1}} = \Sigma_\circ^{\tau^{-1}}$. By (1.1) and (1.4), $\Sigma_\circ^{\tau^{-1}} = \Sigma_\sharp$ for the presemifield $\mathfrak{P}_\sharp\big((F'_i)_0^{n'}, (\zeta_i'^{\tau^{-1}})_0^{n'}\big)$, while $E(\Sigma_\circ)^{\tau^{-1}} = E(\Sigma_\sharp)$ by (2.20) and Lemma 2.21(ii). Thus, $\Sigma_*^{\omega'} = \Sigma_\sharp$ and $E(\Sigma_*)^{\omega'} = E(\Sigma_\circ)^{\tau^{-1}} = E(\Sigma_\sharp)$, where $\omega' \in \mathrm{O}^+(V)$. Now our assumption concerning elements of $\mathrm{O}^+(V)$ implies that ω' fixes $\langle 0,1,0,1\rangle$, and hence so does ω.

Hence, we may now assume that $\omega \in \mathrm{O}^+(V)$.

Lemma 4.5. *For some invertible K–linear maps γ and δ on F and some $\zeta \in F$,*

$$(x,a,y,b)^\omega = \big(\gamma(x), T\big(\zeta\gamma(x)\big) + a, \delta(y) + \zeta b, b\big),$$
$$T(xy) = T\big(\gamma(x)\delta(y)\big),$$

for all $x, y \in F$ and $a, b \in K$.

Proof. We already have $X^\omega = X$ and $Y^\omega = Y$. Since ω conjugates $E(\Sigma_*)$ to $E(\Sigma_\circ)$, it stabilizes $C_V(E(\Sigma_*)) = C_V(E(\Sigma_\circ)) = \big\{(0,a,y,a) \mid a \in K, y \in F\big\}$, $C_V(E(\Sigma_*)) \cap Y = 0 \oplus 0 \oplus F \oplus 0$ and hence also $(C_V(E(\Sigma_*)) \cap Y)^\perp \cap X = \langle 0,1,0,0\rangle$ (using (2.17)). Then there are invertible K–linear maps $\gamma, \delta\colon F \to F$, a K–linear map $f\colon F \to K$, and $c, c' \in K$, $u \in F$, such that ω sends

$$\begin{aligned}(0,1,0,0) &\to (0,c,0,0)\\ (x,0,0,0) &\to (\gamma(x), f(x), 0, 0)\\ (0,0,y,0) &\to (0,0,\delta(y),0)\\ (0,0,0,1) &\to (0,0,u,c'),\end{aligned}$$

for all $x, y \in F$. Since ω must preserve the quadratic form on V as well as the associated bilinear form (2.17), we have $1 = \big((0,1,0,0,), (0,0,0,1)\big) = cc'$, $T(xy) = \big((x,0,0,0),(0,0,y,0)\big) = T(\gamma(x)\delta(y))$, and $0 = \big((x,0,0,0),(0,0,0,1)\big) = T(\gamma(x)u) + f(x)c'$. Since $(0,c,u,c') = (0,1,0,1)^\omega \in \big\langle 0,1,\zeta,1\big\rangle$, we have $c = c'$. Since $cc' = 1$, $c = 1$. Consequently, $u = \zeta$, and hence ω behaves as required. □

Lemma 4.6. $\delta(x*y) = \gamma(x)\circ\delta(y) + T\Big(\zeta\gamma(x)\Big)\delta(y) + \zeta T\Big(\gamma(x)\delta(y)\Big)$ *for all* $x, y \in F$.

Proof. We study how ω conjugates $E(\Sigma_*)$ to $E(\Sigma_\circ)$. Using (2.20), we associate to each $e \in F$ *unique* elements $\eta_e^* \in E(\Sigma_*)$ and $\eta_e^\circ \in E(\Sigma_\circ)$ such that

$$(0,1,0,0)\eta_e^* = (0,1,e,0) = (0,1,0,0)\eta_e^\circ.$$

By Lemma 4.5,

$$(0,1,0,0)\omega^{-1}\eta_e^*\omega = (0,1,e,0)\omega = (0,1,\delta(e),0) = (0,1,0,0)\eta_{\delta(e)}^\circ,$$

so that $\omega^{-1}\eta_e^*\omega = \eta_{\delta(e)}^\circ$. For all $x \in F$, $a \in K$, by (2.20) we have

$$\begin{aligned}(x,a,0,0)\eta_e^*\omega &= \big(x, a + T(xe), x*e + ae, T(xe)\big)\omega\\ &= \big(\gamma(x), T(\zeta\gamma(x)) + a + T(xe),\\ &\qquad \delta(x*e) + \delta(ae) + \zeta T(xe), T(xe)\big),\\ (x,a,0,0)\omega\eta_{\delta(e)}^\circ &= \big(\gamma(x), T(\zeta\gamma(x)) + a, 0, 0\big)\eta_{\delta(e)}^\circ\\ &= \big(\gamma(x), T(\zeta\gamma(x)) + a + T(\gamma(x)\delta(e)),\\ &\qquad \gamma(x)\circ\delta(e) + T(\zeta\gamma(x))\delta(e) + a\delta(e), T(\gamma(x)\delta(e))\big).\end{aligned}$$

Equating third coordinates yields

$$\delta(x*e) + \delta(ae) + \zeta T(xe) = \gamma(x)\circ\delta(e) + T(\zeta\gamma(x))\delta(e) + a\delta(e),$$

where $T(xe) = T\big(\gamma(x)\delta(e)\big)$ by Lemma 4.5 and $\delta(ae) = a\delta(e)$ since δ is K–linear. □

We now come to the place in our argument where we use the assumption $|K| > 2$ in order to take advantage of the square appearing in (1.1):

Lemma 4.7. $\delta(xy^2) + \gamma(x)\delta(y)^2 = 0$ *for all* $x, y \in F$.

Proof. Let $f(x,y) = x*y + xy^2$ and $g(x,y) = x\circ y + xy^2$ for all $x, y \in F$. By Lemma 4.6, for all $x, y \in F$,

$$\begin{aligned}\delta(xy^2) + \gamma(x)\delta(y)^2 &= \delta(f(x,y)) + g(\gamma(x),\delta(y))\\ &\qquad + T\big(\zeta\gamma(x))\delta(y) + \zeta T(\gamma(x)\delta(y))\big).\end{aligned} \tag{4.8}$$

By (1.1) and the K–linearity of δ, the right side is K–linear in y. Let $k \in K - \{0,1\}$. Replace y by ky in (4.8) and add the result to (4.8) multiplied by k in order to obtain $(k^2+k)\Big(\delta(xy^2) + \gamma(x)\delta(y)^2\Big) = 0$ for all $x, y \in F$, where $k^2 + k \neq 0$. □

Completion of the proof of Proposition 4.4. In view of the preceding lemma we can apply Remark 2.4(ii). Then Lemma 4.6 becomes: for some $\lambda \in F^*$ and $\sigma \in \mathrm{Aut}(F)$,

$$\lambda(x * y)^\sigma = (\lambda^{-1}x^\sigma) \circ (\lambda y^\sigma) + T(\zeta(\lambda^{-1}x^\sigma))(\lambda y^\sigma) + \zeta T\big((\lambda^{-1}x^\sigma)(\lambda y^\sigma)\big) \tag{4.9}$$

for all $x, y \in F$.

Assume that $\zeta \neq 0$. Consider the presemifield $\mathfrak{P}_\sharp\big((F_i')_0^{n'+1}, (\lambda^{-\sigma^{-1}}\zeta_i'^{\sigma^{-1}})_1^{n'+1}\big)$, where $\zeta_{n'+1}' = \zeta$. In view of (1.1), (4.9) states that $x * y = x\sharp y$ for all $x, y \in F$. The last field in the chain $(F_i'')_0^{n'+1}$ is $K = F_{n+1}$, and this is smaller than F_n, the last field in $\big((F_i)_0^n, (\zeta_i)_1^n\big)$. Thus, Proposition 3.38 produces a contradiction.

Hence, $\zeta = 0$, as required. □

For future use we will need a slight variation on part of the proof of Proposition 4.4:

Lemma 4.10. *Let $\mathcal{S}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ and $\mathcal{S}_\circ\big((F_i')_0^{n'}, (\zeta_i')_1^{n'}\big)$ be semifield symplectic spreads in the K–space F^2, where $F = F_0 = F_0' = \mathrm{GF}(q^m)$, $F_n, F_{n'}' \supseteq K = \mathrm{GF}(q)$ and $q > 2$. Suppose that $g \in \Gamma\mathrm{L}(2m, q)$ satisfies*

$$\mathcal{S}_*^g = \mathcal{S}_\circ,\ (0 \oplus F)^g = 0 \oplus F \quad \textit{and} \quad (F \oplus 0)^g = F \oplus 0.$$

Then

(i) *g has the form $(x, y) \to k(\lambda^{-1}x^\sigma, \lambda y^\sigma)$ for some $k \in K^*$, $\lambda \in F^*$, $\sigma \in \mathrm{Aut}(F)$;*

(ii) *g induces the isotopism $\lambda(x * y)^\sigma = \lambda^{-1}x^\sigma \circ \lambda y^\sigma$ from $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ to $\mathfrak{P}_\circ\big((F_i')_0^{n'}, (\zeta_i')_1^{n'}\big)$; and*

(iii) *$n' = n$, $F_i' = F_i$ and $\zeta_i' = \lambda\zeta_i^\sigma$ for $1 \leq i \leq n$.*

Proof. (i) Both spreads are symplectic over K (this is why K is needed). Then $g \in \Gamma\mathrm{Sp}(2m, q)$ by [Ka1, 3.6] (this is really just Theorem 2.13(ii)): we can write $g = kg'\tau$ with $k \in K$, $g \in \mathrm{Sp}(2m, q)$, $\tau \in \mathrm{Aut}(F)$, and reduce to the case $g \in \mathrm{Sp}(2m, q)$ exactly as in Case 2 of the proof of Proposition 4.4.

This time g has the form $(x, y) \to (\gamma(x), \delta(y))$ for invertible K–linear maps $\gamma, \delta\colon F \to F$. Since g is symplectic, once again it is straightforward to obtain $T(xy) = T\big(\gamma(x)\delta(y)\big)$ and $\delta(x * y) = \gamma(x) \circ \delta(y)$. As in (4.8), for all $x, y \in F$ this states that $\delta(xy^2) + \gamma(x)\delta(y)^2 = \delta(f(x, y)) + g(\gamma(x), \delta(y))$. Exactly as in the proof of Lemma 4.7, we can use $|K| > 2$ in order to deduce that $\delta(xy^2) + \gamma(x)\delta(y)^2 = 0$ for all $x, y \in F$. Then Remark 2.4(ii) implies (i) and (ii).

(iii) By Lemma 3.5(i), $\lambda(x * y)^\sigma = (\lambda^{-1}x^\sigma) \circ (\lambda y^\sigma)$ states that $x * y = x\sharp y$ for all $x, y \in F$, using the presemifield $\mathfrak{P}_\sharp\big((F_i')_0^{n'}, (\lambda^{-\sigma^{-1}}\zeta_i'^{\sigma^{-1}})_1^{n'}\big)$. Now Proposition 3.38 yields (iii). □

Next we use an entirely different approach in order to study the group $\Gamma\mathrm{O}^+(V)_{\Sigma_*}$:

Proposition 4.11. *Let $\Sigma_*((F_i)_0^{n+1}, (\zeta_i)_1^n)$ be a semifield orthogonal spread in the F_{n+1}–space* (1.3) *(using $K = F_{n+1}$), where either $[F\colon F_1] > 3$ or $|F_{n+1}| > 2$. Then $E(\Sigma_*)$ is the unique Sylow 2–subgroup of $\mathrm{O}^+(V)_{\Sigma_*}$.*

Proof. We proceed in two steps.

Step 1: $E(\Sigma_*)$ *is a Sylow* 2*–subgroup of* $\mathrm{O}^+(V)_{\Sigma_*}$. For otherwise, there is a 2–subgroup $E_0 > E(\Sigma_*)$ of $\mathrm{O}^+(V)_{\Sigma_*}$ with $[E_0\colon E(\Sigma_*)] = 2$. Then E_0 normalizes $E(\Sigma_*)$ and hence fixes the unique member $\Sigma_*[\infty]$ of Σ_* fixed by $E(\Sigma_*)$. Let $\omega \in E_0 - E(\Sigma_*)$. Since $E(\Sigma_*)$ is transitive on $\Sigma_* - \{\Sigma_*[\infty]\}$, we may assume that $\Sigma_*[0]^\omega = \Sigma_*[0]$. By Proposition 4.4, $\langle 0,1,0,1\rangle^\omega = \langle 0,1,0,1\rangle$. Then $\omega^2 = 1$ since ω^2 is an element of $E(\Sigma_*)$ fixing $\Sigma_*[0]$.

By (2.10) and Theorem 2.13(ii), ω induces a nontrivial collineation of the affine plane $\mathfrak{A} = \mathfrak{A}(\Sigma_*/\langle 0,1,0,1\rangle)$. Since $\mathfrak{A}$ has even order and ω fixes both $\mathcal{S}_*[0]$ and $\mathcal{S}_*[\infty]$, ω induces a Baer involution on $\mathfrak{A}$ [De, p. 172]. Then ω fixes $|F_{n+1}|^{m/2}$ points of each line stabilized by ω. Since ω is F_{n+1}–linear and m is odd, this is impossible.

Step 2: $E(\Sigma_*) \trianglelefteq \mathrm{O}^+(V)_{\Sigma_*}$. First note that $\mathrm{O}^+(V)_{\Sigma_*}$ stabilizes $\Sigma_*[\infty]$. For otherwise, since $E(\Sigma_*)$ is transitive on $\Sigma_* - \{\Sigma_*[\infty]\}$, $\mathrm{O}^+(V)_{\Sigma_*}$ would be 2–transitive on Σ_*. Since Σ_* is nondesarguesian by Proposition 4.2, this contradicts [Ka1, II3.3].

By Lemma 2.21(iii), $E(\Sigma_*)$ acts on $\Sigma_*[\infty]$ as all transvections with axis H: it induces the identity on the hyperplane $H := \big\{(0,0,t,0) \mid t \in F\big\}$ and is transitive on the points of $\Sigma_*[\infty] - H$.

Let $\omega \in \mathrm{O}^+(V)_{\Sigma_*}$, so that $\Sigma_*[\infty]^\omega = \Sigma_*[\infty]$. Consider H^ω and $E(\Sigma_*)^\omega$.

If $H^\omega \neq H$, then $G := \langle E(\Sigma_*), E(\Sigma_*)^\omega\rangle$ is transitive on the points of $\Sigma_*[\infty] - (H \cap H^\omega)$. There are $q^{m-1}(q+1)$ such points. The stabilizer in G of a point in $H - (H \cap H^\omega)$ contains $E(\Sigma_*)$ and hence has order divisible by q^m. Thus, G has order divisible by $q^{m+(m-1)}$, which contradicts Step 1.

Thus, $H = H^\omega$. Hence both $E(\Sigma_*)$ and $E(\Sigma_*)^\omega$ induce all transvections of $\Sigma_*[\infty]$ with axis H. Consequently, if $E(\Sigma_*) \neq E(\Sigma_*)^\omega$, then there exists $1 \neq \eta \in \langle E(\Sigma_*), E(\Sigma_*)^\omega\rangle$ inducing the identity on $\Sigma_*[\infty]$. With respect to a suitable hyperbolic basis of V (containing bases of X and Y), one easily checks that the matrix of η has the form $\left(\begin{smallmatrix} I & M \\ O & I \end{smallmatrix}\right)$ and so has order 2. Thus, η lies in a Sylow 2–subgroup of $\mathrm{O}^+(V)_{\Sigma_*}$, and hence lies in some conjugate of $E(\Sigma_*)$. However, no element of $E(\Sigma_*)$ is 1 on a member of Σ_*.

Thus, $E(\Sigma_*) = E(\Sigma_*)^\omega$ for any $\omega \in \mathrm{O}^+(V)_{\Sigma_*}$, and hence $E(\Sigma_*)$ is the unique Sylow 2–subgroup of $\mathrm{O}^+(V)_{\Sigma_*}$. □

Theorem 4.12. *Consider a presemifield* $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$, *where* $F = F_0 \supset F_n$. *Let* Λ *denote the largest subgroup of* $\mathrm{Aut}(F)$ *that fixes each* $\zeta_1^{-1}\zeta_i, 2 \le i \le n$. *Then*

(i) $\mathrm{Aut}\,\mathfrak{A}(\mathcal{S}_*)_0/\mathfrak{K}^*(\mathfrak{A}(\mathcal{S}_*)) \cong E(\mathcal{S}_*)\rtimes\Lambda$ *if either* $[F\colon F_1] > 3$ *or* $|F_n| > 2$, *and*

(ii) $\Gamma\mathrm{O}^+(V)_{\Sigma_*}/F_{n+1}^* \cong E(\Sigma_*)\rtimes\Lambda$ *for* $\Sigma_* = \Sigma_*((F_i)_0^{n+1}, (\zeta_i)_1^n)$ *if either* $[F\colon F_1] > 3$ *or* $|F_{n+1}| > 2$.

Proof. By Lemma 3.5(i), $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ and $\mathfrak{P}_\circ\big((F_i)_0^n, (\zeta_1^{-1}\zeta_i)_1^n\big)$ are isotopic, so we may assume that $\zeta_1 = 1$. We use induction on n to prove the following two slightly more precise versions of (i) and (ii), where we view Λ as consisting of maps $(x,y) \to (x^\sigma, y^\sigma)$ in (i′) or $(x,a,y,b) \to (x^\sigma, a^\sigma, y^\sigma, b^\sigma)$ in (ii′), for $\sigma \in \mathrm{Aut}(F)$:

(i′) $\mathrm{Aut}\,\mathfrak{A}(\mathcal{S}_*)_0 = (\mathfrak{K}^*(\mathfrak{A}(\mathcal{S}_*)) \times E(\mathcal{S}_*))\rtimes\Lambda$ if either $[F\colon F_1] > 3$ or $|F_n| > 2$, and

(ii′) $\Gamma\mathrm{O}^+(V)_{\Sigma_*} = (F_{n+1}^* \times E(\Sigma_*))\rtimes\Lambda$ for $\Sigma_* = \Sigma_*((F_i)_0^{n+1}, (\zeta_i)_1^n)$ if either $[F\colon F_1] > 3$ or $|F_{n+1}| > 2$.

(N.B.—These are not correct without the restriction $\zeta_1 = 1$: in general, in place of Λ we would need the conjugate of Λ by $(x,y) \to (\zeta_1 x, \zeta_1^{-1} y)$ in (i) or $(x,a,y,b) \to (\zeta_1 x, a, \zeta_1^{-1} y, b)$ in (ii).)

If $n = 1$ then $\operatorname{Aut}\mathfrak{A}(\mathcal{S}_*)_0 = (\mathfrak{K}^*(\mathfrak{A}(\mathcal{S}_*)) \times E(\mathcal{S}_*)) \rtimes \operatorname{Aut}(F)$ by Remark 3.6. Thus, (i′) holds when $n = 1$ (without the assumption $[F\colon F_1] > 3$ or $|F_1| > 2$).

We now assume, inductively, that (i′) is true for some n, then deduce that (ii′) is true for the same n, and finally prove that (i′) holds when n is replaced by $n+1$.

Assume that (i′) holds and that we are in the situation of (ii′). Then $\Gamma\mathrm{O}^+(V)_{\Sigma_*}$ fixes $\langle 0, 1, 0, 1\rangle$ by Propositions 4.4 and 4.11. Moreover, $|F_n| > |F_{n+1}| \geq 2$, so that (i′) can be applied. Then (ii′) holds by Theorem 2.13(ii).

Now assume that (ii′) holds, and consider $\mathcal{S}\big((F_i)_0^{n+1}, (\zeta_i)_1^{n+1}\big)$ for some $\zeta_{n+1} \in F^*$. By (4.1), $\mathcal{S}\big((F_i)_0^{n+1}, (\zeta_i)_1^{n+1}\big) = \Sigma_*/\nu$ for the nonsingular point $\nu = \langle 0, 1, \zeta_{n+1}, 1\rangle$ of V. The hypotheses for this case of (i′) are exactly what are needed for (ii′). Thus, by (ii′) and Theorem 2.13(ii), $\operatorname{Aut}\mathfrak{A}(\Sigma_*/\nu)_0$ is generated by $\mathfrak{K}^*(\mathfrak{A}(\Sigma_*/\nu))$ and the group induced on $\nu^\perp/\nu$ by

$$\Gamma\mathrm{O}^+(V)_{\Sigma_*,\nu} = [(F_{n+1}^* \times E(\Sigma_*)) \rtimes \Lambda]_\nu = (F_{n+1}^* \times (E(\Sigma_*)) \rtimes \Lambda_{\zeta_{n+1}},$$

since F_{n+1}^* and $E(\Sigma_*)$ both fix ν. Thus, (i′) holds for the new value of n. □

Remark. For suitably chosen ζ_1 and ζ_2 the group Λ can be any subgroup of $\operatorname{Aut}(F)$. In particular, Λ can have even order if q is a square, in which case $\operatorname{Aut}\mathfrak{A}(\mathcal{S}_*)$ contains Baer involutions. The smallest examples occur when $|K| = 4$ and $m = 3$, producing several semifield planes of order 64 for which the kernel is GF(4) and $|\operatorname{Aut}\mathfrak{A}(\mathcal{S}_*)_0| = 64 \cdot 2$.

4.3. **Equivalences of semifield planes and orthogonal spreads.** We now deal with equivalence questions for our semifield planes and semifields. We also establish lower bounds on the number of pairwise nonisomorphic semifield planes and inequivalent semifield orthogonal spreads produced in (1.1)–(1.4). Recall that these are nondesarguesian under mild arithmetical assumptions (Proposition 4.2). The following is the main result of this paper:

Theorem 4.13. *Consider the presemifields* $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$, $\mathfrak{P}_\circ\big((F_i')_0^{n'}, (\zeta_i')_1^{n'}\big)$, *where* $n \geq 1$, $n' \geq 1$, $F = F_0 = F_0'$, $F_n, F_{n'}' \supseteq K$, *and either* $[F\colon F_1] > 3$ *and* $[F\colon F_1'] > 3$, *or* $|K| > 2$. *Then the following are equivalent*:

(i) $\mathfrak{A}(\mathfrak{P}_*)$ *and* $\mathfrak{A}(\mathfrak{P}_\circ)$ *are isomorphic semifield planes*; *and*
(ii) $n' = n$, $F_i' = F_i$, *and there exist* $\lambda \in F^*$ *and* $\sigma \in \operatorname{Aut}(F)$ *such that* $\zeta_i' = \lambda\zeta_i^\sigma$ *for all* $1 \leq i \leq n$.

If, in addition, $F_n, F_{n'}' \supset K = F_{n+1} = F_{n'+1}'$, *then* (i) *and* (ii) *are both equivalent to*

(iii) $\Sigma_*((F_i)_0^{n+1},(\zeta_i)_1^n)$ *and* $\Sigma_\circ((F_i')_0^{n'+1},(\zeta_i')_1^{n'})$ *are equivalent orthogonal spreads of the orthogonal* K*–space* (1.3).

Proof. (i)⇒(ii): By Lemma 2.21(i), $E(\mathcal{S}_*)$ is a group of elations of $\mathfrak{A}(\mathcal{S}_*)$ having axis $\mathcal{S}_*[\infty]$ and transitive on $\mathcal{S}_* - \{\mathcal{S}_*[\infty]\}$. Then $\operatorname{Aut}\mathfrak{A}(\mathcal{S}_*)_0$ fixes this line (as otherwise $\mathfrak{A}(\mathcal{S}_*)$ would be desarguesian by a standard result concerning projective planes [De, p. 130], contradicting Proposition 4.2).

As in the proof of Proposition 4.4, we can use the transitivity of $E(\mathcal{S}_*)$ in order to assume that an isomorphism sends $0 \oplus F$ and $F \oplus 0$ to themselves. Now apply Lemma 4.10 if $q > 2$.

It remains to consider the case $[F\colon F_1] > 3$ and $[F\colon F_1'] > 3$. By Theorem 3.4, the kernels of these planes are F_n and $F_{n'}'$, respectively, so that $F_n = F_{n'}'$. Once

again we can use Lemma 4.10 if $|F_n| > 2$. Thus, we must now deal with the case $F_n = F'_{n'} = \mathrm{GF}(2)$. We may assume that $n \geq n'$.

If $n = 1$ then $\mathfrak{A}(\mathcal{S}_*)$ is a second cousin of a desarguesian plane, and $\mathfrak{A}(\mathcal{S}_\circ)$ is either desarguesian or also a second cousin of a desarguesian plane, and hence (ii) holds by Remark 3.6.

Now assume that $n \geq 2$. We will use the orthogonal spreads $\widetilde{\Sigma}_* = \Sigma((F_i)_0^n, (\zeta_i)_1^{n-1})$ and $\widetilde{\Sigma}_\circ = \Sigma((F'_i)_0^{n'}, (\zeta'_i)_1^{n'-1})$ in the usual F_n–space $V = F \oplus F_n \oplus F \oplus F_n$. (N.B.—The subscripts $*$ and $\circ$ are included only for bookkeeping purposes: these binary operations are *not* the ones involved in the definitions of these orthogonal spreads.)

By (4.1), $\mathcal{S}_* = \widetilde{\Sigma}_*/\nu_*$ and $\mathcal{S}_\circ = \widetilde{\Sigma}_\circ/\nu_\circ$ for the nonsingular points $\nu_* = \langle 0, 1, \zeta_n, 1\rangle$ and $\nu_\circ = \langle 0, 1, \zeta'_{n'}, 1\rangle$ of V. By Theorem 2.13(i), $\nu_*^g = \nu_\circ$ and $\widetilde{\Sigma}_*^g = \widetilde{\Sigma}_\circ$ for some $g \in \Gamma\mathrm{O}^+(V)$. As in the proof of Proposition 4.4, we can use the transitivity of $E(\Sigma_*)$ in order to assume that g fixes the subspaces (4.3). By Propositions 4.4 and 4.11, g normalizes $E(\Sigma_*)$ and hence fixes $\nu = \langle 0, 1, 0, 1\rangle$. Consequently, g induces an element $\bar{g} \in \Gamma\mathrm{Sp}(\nu^\perp/\nu)$ such that $(\widetilde{\Sigma}_*/\nu)^{\bar{g}} = \widetilde{\Sigma}_\circ/\nu$.

By (4.1), $\widetilde{\Sigma}_*/\nu = \mathcal{S}((F_i)_0^{n-1}, (\zeta_i)_1^{n-1})$ and $\widetilde{\Sigma}_\circ/\nu = \mathcal{S}((F'_i)_0^{n'-1}, (\zeta'_i)_1^{n'-1})$. By Theorem 3.4, these planes have kernels F_{n-1} and $F'_{n'-1}$, respectively. We have $F_{n-1} = F'_{n'-1} \supset F_n$, so that Lemma 4.10 applies: $n' - 1 = n - 1$, $F'_i = F_i$ for all $1 \leq i < n$, and there exist $k \in F_n^*$, $\lambda \in F^*$ and $\sigma \in \mathrm{Aut}(F)$ such that $\overline{g}$ has the form $(x, y) \to k(\lambda^{-1}x^\sigma, \lambda y^\sigma)$; moreover, $\zeta'_i = \lambda\zeta_i^\sigma$ for all $1 \leq i < n$.

Since g fixes ν and the subspaces (4.3), it easily follows that $(x, a, y, b)^g = (\lambda^{-1}x^\sigma, a^\sigma, \lambda y^\sigma, b^\sigma)$ for all $(x, a, y, b) \in V$. In particular, $\nu_*^g = \nu_\circ$ states that $\zeta'_{n'} = \lambda\zeta_n^\sigma$, so that (ii) holds.

(ii)⇒(i): The semifields are isotopic by Lemma 3.5(i), so that Remark 2.4(i) applies.

Now we will assume that $F_n, F'_{n'} \supset K = F_{n+1} = F'_{n'+1}$. In view of (4.1) we will consider

$$\mathcal{S}_* = \Sigma_*((F_i)_0^{n+1}, (\zeta_i)_1^n)/\nu = \mathcal{S}_*((F_i)_0^n, (\zeta_i)_1^n)$$

and

$$\mathcal{S}_\circ = \Sigma_\circ((F'_i)_0^{n'+1}, (\zeta'_i)_1^{n'})/\nu = \mathcal{S}_\circ((F'_i)_0^{n'}, (\zeta'_i)_1^{n'}),$$

where $\nu = \langle 0, 1, 0, 1\rangle$.

(i)⇒(iii): Since we are assuming (i), $\mathcal{S}_*$ and $\mathcal{S}_\circ$ are equivalent symplectic spreads. Consequently, Theorem 2.13(i) implies (iii).

(iii)⇒(i): As before, Propositions 4.4 and 4.11 imply that any $g \in \Gamma\mathrm{O}^+(V)$ sending Σ_* to $\Sigma_\circ$ fixes the nonsingular point ν and hence, by (2.10), induces an isomorphism between the semifield planes $\mathfrak{A}(\mathcal{S}_*)$ and $\mathfrak{A}(\mathcal{S}_\circ)$. □

We now give lower bounds on the number of pairwise inequivalent orthogonal spreads or translation planes we have constructed.

Definition 4.14. Let $m = m_0$ be an odd composite integer. Let $\xi = (m_i)_0^{l(\xi)}$ denote any sequence of $l(\xi) + 1 \geq 2$ distinct integers such that $m_i \mid m_{i-1}$ for $1 \leq i \leq l(\xi)$. Then ξ determines a chain $(F_i)_0^{l(\xi)}$ of fields with $F_i = \mathrm{GF}(q^{m_i})$, $1 \leq i \leq l(\xi)$, all of which contain $\mathrm{GF}(q)$.

We defined $\rho(m)$ in Section 1. Write

$$\rho^\bullet(m) = \begin{cases} \rho(m) & \text{if } m \text{ is not a power of 3,} \\ \rho(m) - 1 & \text{if } m = 3^{\rho(m)}. \end{cases}$$

Theorem 4.15. *Let q be a power of 2 and let m be an odd integer such that $\rho^\bullet(m) \geq 3$.*

(i) *There are more than $q^{m(\rho^\bullet(m)-2)}/m\log q$ pairwise inequivalent semifield orthogonal spreads of an $\mathrm{O}^+(2m+2,q)$–space.*

(ii) *There are more than $\sum_\xi (q^m-1)^{l(\xi)-2}/m\log q$ pairwise inequivalent semifield orthogonal spreads of an $\mathrm{O}^+(2m+2,q)$–space. This sum runs over all sequences ξ such that $m_{l(\xi)}=1$, with the additional restriction $m>3m_1$ if $q=2$.*

(iii) *If m is not a power of 3 or if $q>2$, then there are more than $q^{m(\rho^\bullet(m)-1)}/(m\log q)^2$ pairwise nonisotopic symplectic semifields of order q^m having kernel isomorphic to $\mathrm{GF}(q)$.*

(iii′) *If m is not a power of 3 or if $q>2$, then there are more than $q^{m(\rho^\bullet(m)-1)}/(m\log q)^2$ pairwise nonisomorphic symplectic semifield planes of order q^m having kernel isomorphic to $\mathrm{GF}(q)$.*

(iv) *There are more than $\sum_\xi (q^m-1)^{l(\xi)}/\big(m\log q\big)^2$ pairwise nonisomorphic symplectic semifield planes of order q^m. This sum runs over all sequences ξ such that $m_{l(\xi)}>1$, with the additional restriction $m>3m_1$ if $q=2$.*

Proof. (i) Let $\xi = (\prod_{j=i+1}^{\rho(m)} p_j)_0^{\rho^\bullet(m)}$, where $m=\prod_1^{\rho(m)} p_i$ for primes p_i such that $p_1>3$ if m is not a power of 3; if m is a power of 3 then merge two 3's so that $m_1 = m/9$. There is a corresponding chain $(F_i)_0^{\rho^\bullet(m)}$ of fields. Note that $F_{\rho^\bullet(m)} = \mathrm{GF}(q)$.

Consider the orthogonal spreads $\Sigma((F_i)_0^{\rho^\bullet(m)}, (\zeta_i)_1^{\rho^\bullet(m)-1})$, where the ζ_i vary, but now no longer make the usual restriction on the ζ_i: allow any of them to be 0. This has the effect of deleting some of the fields F_i from the chain $(F_i)_0^{\rho^\bullet(m)}$, leaving a formula looking exactly like (1.1) but having fewer fields involved. This does not influence our assumptions concerning m.

There are $q^{m(\rho^\bullet(m)-1)}$ sequences $(\zeta_i)_1^{\rho^\bullet(m)-1}$, and hence there are at least

$$q^{m(\rho^\bullet(m)-1)}/(q^m-1)m\log q > q^{m(\rho^\bullet(m)-2)}/m\log q$$

pairwise inequivalent orthogonal spreads, where we divided by $(q^m-1)m\log q$ in order to account for the pairs λ,σ in Theorem 4.13, where we use $K=\mathrm{GF}(q)$. (N.B.—One of these orthogonal spreads is desarguesian, where all $\zeta_i=0$.)

(ii) This is again immediate from Theorem 4.13, using the orthogonal spreads $\Sigma((F_i)_0^{l(\xi)}, (\zeta_i)_1^{l(\xi)-1})$ for all sequences ξ subject to the stated restrictions and all sequences $(\zeta_i)_1^{l(\xi)-1}$ of nonzero elements; we need $m_{l(\xi)}=1$ in order to have $F_{l(\xi)} = \mathrm{GF}(q)$.

(iii), (iii′), (iv) By Theorem 2.13, counting either the number of pairwise nonisomorphic semifield planes or the number of nonisotopic semifields requires lower bounds for both the number of pairwise inequivalent orthogonal spreads and the number of pairwise nonisomorphic semifield planes produced by each such orthogonal spread.

For the sequence ξ defined in (i) the number of orthogonal spreads in (i) is greater than $q^{m(\rho^\bullet(m)-2)}/(q^m-1)m\log q$. By Lemma 2.21(ii) and Theorems 4.12 and 2.13(i), each orthogonal spread produces at least $(q^m-1)/m\log q$ pairwise nonisomorphic semifield planes. Multiplying our lower bounds proves (iii) and (iii′)

(which trivially say the same thing). The kernel statements follow from Theorem 3.4, since $[F\colon F_1] > 3$.

For (iv), proceed in the same manner using all sequences ξ; this time the restriction $m_{l(\xi)} > 1$ allows us to construct the required orthogonal spread

$$\Sigma((F_i)_0^{l(\xi)+1}, (\zeta_i)_1^{l(\xi)})$$

over $F_{l(\xi)+1} = \mathrm{GF}(q)$. □

4.4. **Boring planes.** We now turn to boring planes. We call a geometric object *boring* provided its automorphism group is minimal subject to suitable conditions. For example, a semifield plane $\mathfrak{A}(\mathcal{S})$ or a semifield orthogonal spread Σ is *boring* if $\mathrm{Aut}\,\mathfrak{A}(\mathcal{S})_0/\mathfrak{K}^* \cong E(\mathcal{S})$ or $\Gamma\mathrm{O}^+(V,K)_\Sigma/K^* \cong E(\Sigma)$, respectively (cf. Lemma 2.21). Hence, in the case of planes, $\mathrm{Aut}\,\mathfrak{A}(\mathcal{S})$ is generated by the elations and homologies fixing the line at infinity pointwise together with all elations having axis $\mathcal{S}[\infty]$. Thus, if $\mathfrak{A}(\mathcal{S})$ is a boring semifield plane of order q^m whose kernel has size q, then $|\mathrm{Aut}\,\mathfrak{A}(\mathcal{S})| = (q-1)q^{3m}$.

Many of the spreads in the preceding theorem are boring:

Theorem 4.16. *Let q be a power of 2 and let m be an odd integer such that $\rho^\bullet(m) \geq 3$.*

(i) *There are at least $(q^m-1)^{\rho^\bullet(m)-2}q^m/2m\log q$ pairwise inequivalent boring semifield orthogonal spreads of an $\mathrm{O}^+(2m+2,q)$–space.*

(ii) *There are at least $(q^m-1)^{\rho^\bullet(m)-1}q^m/2m\log q$ pairwise nonisomorphic boring semifield planes of order q^m having kernel of size q.*

Proof. (i) Consider a chain $(F_i)_0^{\rho^\bullet(m)}$ of subfields defined as in the proof of Theorem 4.15(i). Let $(\zeta_i)_1^{\rho^\bullet(m)-1}$ be a sequence of elements of F^* such that $\zeta_1 = 1$ and ζ_2 is a primitive element of F; there are at least $(q^m-1)^{\rho^\bullet(m)-3}|F|/2$ such sequences. Since the stabilizer of ζ_2 in $\mathrm{Aut}(F)$ is trivial, Theorem 4.12 implies that $\Gamma\mathrm{O}^+(V)_\Sigma = K^* \times E(\Sigma)$ for the corresponding presemifield orthogonal spread $\Sigma((F_i)_0^{\rho^\bullet(m)}, (\zeta_i)_1^{\rho^\bullet(m)-1})$. By Theorem 4.13 we must divide by $m\log q$, since $\mathrm{Aut}(F)$ sends ζ_2 to that many other primitive elements.

(ii) As before, two affine planes arising from inequivalent orthogonal spreads are never isomorphic. Consider an orthogonal spread Σ in (i). By Lemma 2.21(iii) each nonsingular point $\langle 0,1,\zeta,1\rangle$, $\zeta \in F^*$, is fixed by $\Gamma\mathrm{O}^+(V)_{\Sigma_*} = K^* \times E(\Sigma)$. By Theorem 2.13(i), the q^m-1 planes $\mathfrak{A}(\Sigma/\langle 0,1,\zeta,1\rangle)$, $\zeta \in F^*$, are pairwise nonisomorphic and satisfy $|\mathrm{Aut}\,\mathfrak{A}(\Sigma/\langle 0,1,\zeta,1\rangle)_0/\mathfrak{K}^*| = q^m$.

In view of the construction of $(F_i)_0^{\rho^\bullet(m)}$ we have $[F\colon F_1] > 3$. By Theorem 3.4, each of these planes has kernel of order q and hence has full automorphism group of order $(q-1)q^{3m}$. □

Lastly we construct large numbers of *boring translation planes*, meaning that the full collineation group fixes the line at infinity pointwise. If $\mathfrak{A}$ is such a plane of order q^m, and if $\mathfrak{K}(\mathfrak{A}) \cong \mathrm{GF}(q)$, then $|\mathrm{Aut}\,\mathfrak{A}| = (q-1)q^{2m}$. In [Ka4] the "up and down process" was used in order to construct large numbers of boring planes with $\mathfrak{K}(\mathfrak{A}) \cong \mathrm{GF}(2)$; those planes have order 2^m and full collineation groups of order 2^{2m}. However, the argument there is very different from the one given below; neither extends to the situation in the other.

Theorem 4.17. *Let q be a power of 2 and let m be an odd integer with $\rho^\bullet(m) \geq 3$. Then there are more than $(q-1)(q^m-1)^{\rho^\bullet(m)-2}q^m/2m\log q$ pairwise nonisomorphic boring translation planes of order q^m with kernel of size at least q.*

Proof. By Theorem 4.16(i), there are at least $(q^m-1)^{\rho^\bullet(m)-2}q^m/2m\log q$ inequivalent boring orthogonal spreads Σ of our $\mathrm{O}^+(2m+2,q)$–space V over $K=\mathrm{GF}(q)$ each having full automorphism group $\Gamma\mathrm{O}^+(V)_\Sigma = K^* \times E(\Sigma)$. For each such spread, the nonsingular points $\langle 0,\lambda,0,1\rangle, \lambda \in K^* - \{1\}$, are all in different $E(\Sigma)$–orbits and have trivial stabilizers in $E(\Sigma)$ (cf. Lemma 2.21). Hence, for any such nonsingular point, Theorem 2.13(ii) implies that

$$\mathrm{Aut}\,\mathfrak{A}(\Sigma/\langle 0,\lambda,0,1\rangle)_0/\mathfrak{K}^*(\mathfrak{A}(\Sigma/\langle 0,\lambda,0,1\rangle) = 1.$$

Each of these planes arises from a symplectic spread of a K–space and hence has kernel containing K. □

Remark. We do not know the kernels of the preceding planes, but we expect that a calculation similar to that in Theorem 3.4 will suffice in order to obtain them. This might provide a different approach to the type of result in [Ka4].

5. Binary and $\mathbb{Z}_4$–linear Kerdock and Preparata codes

Using orthogonal geometries and semifield planes, we now construct large numbers of $\mathbb{Z}_4$–linear Kerdock codes, and then by dualizing we obtain large numbers of $\mathbb{Z}_4$–linear Preparata codes. The images of these $\mathbb{Z}_4$–linear codes under the Gray map are binary codes with the same weight distribution as Kerdock's or Preparata's original codes.

For background concerning this section we refer to [HKCSS], [CCKS] and [Ka3]. We will only very briefly survey parts of those papers.

5.1. **Binary Kerdock codes.** In this section we will index vectors over $v \in \mathbb{Z}_2^n$, for a fixed ordering of $\mathbb{Z}_2^n$. The *first* and *second order Reed–Muller codes* are the subspaces

$$R(1,n) = \left\{(u\cdot v+\epsilon)_v \mid u\in\mathbb{Z}_2^n, \epsilon\in\mathbb{Z}_2\right\} \text{ and}$$
$$R(2,n) = \left\{(Q(v)+u\cdot v+\epsilon)_v \mid Q\in\mathcal{Q}, u\in Z_2^n, \epsilon\in\mathbb{Z}_2\right\}$$

of $\mathbb{Z}_2^{2^n}$, where $\mathcal{Q}$ denotes the set of all quadratic forms on $\mathbb{Z}_2^n$ and we are using the usual dot product on $\mathbb{Z}_2^n$. A *Kerdock code* is a certain union of cosets

$$Q + R(1,n) := \left\{(Q(v)+u\cdot v+\epsilon)_v \mid u\in\mathbb{Z}_2^n, \epsilon\in\mathbb{Z}_2\right\}$$

of $R(1,n)$ in $R(2,n)$, where n is even. These quadratic forms Q are chosen so that the minimum distance between any of two of the cosets $Q+R(1,n)$ and $Q'+R(1,n)$ is as large as possible, namely $2^{n-1}-2^{(n-2)/2}$, which occurs if and only if $Q+Q'$ is nonsingular.

Each quadratic form Q on $\mathbb{Z}_2^n$ can be written $Q(v)=vUv^t$ for a strictly upper triangular $n\times n$ matrix U (hence with 0 diagonal); the corresponding bilinear form (cf. (2.9)) is given by $(u,v)=uMv^t$, where $M=U+U^t$ is a skew–symmetric matrix (again the diagonal is 0). Conversely, each skew–symmetric matrix M can be written $M=U_M+U_M^t$ for a unique strictly upper triangular matrix U_M.

Kerdock sets. This leads to the definition of a (binary) *Kerdock set* of $n \times n$ skew–symmetric matrices: a set $\mathcal{M}$ of 2^{n-1} such matrices, containing 0, such that the difference of any two of them is nonsingular. Such a set exists if and only if n is even. The following proposition establishes their existence and relates them to the previous sections:

Proposition 5.1 ([Ka3, 3.3])**.** *Let $X \cong Y \cong \mathbb{Z}_2^n$ and equip $V = X \oplus Y$ with the quadratic form $Q(x, y) = x \cdot y$. Let $x_1, \dots, x_n, y_1, \dots, y_n$ be a basis of V with $x_i \in X$, $y_i \in Y$, and $x_i \cdot x_j = y_i \cdot y_j = 0$ and $x_i \cdot y_j = \delta_{ij}$ for $1 \le i, j \le n$. Then, with respect to this basis,*

(i) *every orthogonal spread Σ of V containing X and Y can be written as*

$$\Sigma = \{Y\} \cup \left\{ X \begin{pmatrix} I & M_i \\ O & I \end{pmatrix} \mid 1 \le i \le 2^{n-1} \right\}$$

for a Kerdock set $\mathcal{M} = \{M_i \mid 1 \le i \le 2^{n-1}\}$; and

(ii) *every binary Kerdock set arises in this way.*

Note that a choice for Y is made when defining Σ in Proposition 5.1, so that this proposition *does not* guarantee a bijection between binary orthogonal spreads and Kerdock sets. (See Theorem 5.3(iii). In view of that theorem, the choice of X does not affect matters in any significant way.)

Kerdock codes. Each Kerdock set $\mathcal{M}$ produces a family of upper triangular matrices U_M, $M \in \mathcal{M}$, and hence also a family of quadratic forms Q_M as well as the binary *Kerdock code*

$$\mathcal{K}_2(\mathcal{M}) = \left\{ (Q_M(v) + u \cdot v + \epsilon)_v \mid M \in \mathcal{M}, u \in \mathbb{Z}_2^n, \epsilon \in \mathbb{Z}_2 \right\} \subset \mathbb{Z}_2^{2^n}.$$

Here $\mathcal{K}_2(\mathcal{M})$ is a code of length 2^n having $2^{n-1} \cdot 2^n \cdot 2 = 2^{2n}$ codewords and minimum distance $2^{n-1} - 2^{(n-2)/2}$. Also, as an approximation to linearity, $\mathcal{K}_2(\mathcal{M})$ is *distance–invariant*: any $c \in \mathcal{K}_2(\mathcal{M})$ partitions the codewords of $\mathcal{K}_2(\mathcal{M})$ according to their distance from c:

(5.2)

distance from c	# of words at that distance
0	1
$2^{n-1} - 2^{(n-2)/2}$	$2^n(2^{n-1} - 1)$
2^{n-1}	$2^{n+1} - 2$
$2^{n-1} + 2^{(n-2)/2}$	$2^n(2^{n-1} - 1)$
2^n	1

Equivalence and quasi–equivalence of binary codes. Two binary codes of length N are *equivalent* if there is a permutation of the coordinates of $\mathbb{Z}_2^N$ that maps one code to the other. An *automorphism* of a code C is a permutation of coordinates that stabilizes the code, and $\mathrm{Aut}\, C$ denotes its group of automorphisms.

Two codes are *quasi–equivalent* if one is equivalent to a translate of the other by an element of $\mathbb{Z}_2^N$. In Section 5.6 we will study the quasi–automorphism group $\mathrm{QAut}\, C$ of a Kerdock code C. We will reduce this study and questions of equivalence to equivalence among the corresponding binary orthogonal spreads (cf. Theorem 5.3 and Proposition 5.13).

Note that two codes are quasi–equivalent if and only each is the image of the other by means of an isometry of the underlying metric space ($\mathbb{Z}_2^N$, Hamming metric). In the case of linear codes, quasi–equivalence is almost the same as equivalence. For a nonlinear code C, even one containing 0, it is noticeably weaker: if $w \in C$, then

C and $C + w$ are quasi–equivalent but, in general, not equivalent; yet clearly they are not "significantly" different.

Equivalence of Kerdock sets. Two Kerdock sets $\mathcal{M}_1$ and $\mathcal{M}_2$ of $n \times n$ binary matrices are called *equivalent* if and only if there are an invertible matrix A and a skew–symmetric matrix M such that $A^t \mathcal{M}_1 A + M = \mathcal{M}_2$. Note that here, and in the rest of this section, matrices and vector spaces are over $\mathbb{Z}_2$, so that field automorphisms are not needed.

Theorem 5.3 ([Ka3, 3.4])**.** *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be Kerdock sets of $n \times n$ binary matrices, with corresponding orthogonal spreads $\Sigma_{\mathcal{M}_1}$ and $\Sigma_{\mathcal{M}_2}$ of $V = X \oplus Y$ arising as in Proposition* 5.1(i)*. Then the following are equivalent*:

(i) *$\mathcal{M}_1$ and $\mathcal{M}_2$ are equivalent.*
(ii) *The Kerdock codes $\mathcal{K}_2(\mathcal{M}_1)$ and $\mathcal{K}_2(\mathcal{M}_2)$ are quasi-equivalent.*
(iii) *The orthogonal spreads $\Sigma_{\mathcal{M}_1}$ and $\Sigma_{\mathcal{M}_2}$ are equivalent by an isometry of V that stabilizes Y.*

More is proved in [Ka3, 3.4]: *The quasi–equivalences $g\colon \mathcal{K}_2(\mathcal{M}_1) \to \mathcal{K}_2(\mathcal{M}_2)$ are precisely the maps*

$$g\colon (c_v)_v \to (c_{vA+w})_v + (Q_M(vA + w) + u \cdot (vA + w) + \epsilon)_v \tag{5.4}$$

for some $u, w \in \mathbb{Z}_2^n, \epsilon \in \mathbb{Z}_2$, $M \in \mathcal{M}_2$ and $A \in \mathrm{GL}(n, 2)$ satisfying $A\mathcal{M}_1 A^t = \mathcal{M}_2 + M$. In particular, (i) $\Rightarrow$ (ii).

5.2. **Kerdock codes from prequasifields.** Let $F = \mathrm{GF}(2^m)$ with $m > 1$ odd, and let $T\colon F \to \mathbb{Z}_2$ be the trace map. Define an inner product on the $\mathbb{Z}_2$–space $F \oplus \mathbb{Z}_2$ by $\big((x, a), (y, b)\big) = T(xy) + ab$. We use an orthonormal basis B to write matrices, and we write $(x, a)_B$ for the coordinate vector of (x, a). We now index vectors over $v \in \mathbb{Z}_2^m \oplus \mathbb{Z}_2$, for a fixed ordering of $\mathbb{Z}_2^m \oplus \mathbb{Z}_2$. Then it is easy to check the following

Lemma 5.5 ([Ka3, 2.2])**.** *Consider a symplectic prequasifield $\mathfrak{P}_*(F, *, +)$ (so it satisfies* (2.5) *and* (2.6)*. For each $s \in F$ let M_s be the matrix defined by*

$$(x, a)_B M_s = (x * s + T(xs)s + as, T(xs))_B.$$

Then $\mathcal{M}_* = \{M_s \mid s \in F\}$ is a Kerdock set with corresponding Kerdock code

$$\mathcal{K}_2(*) = \big\{(Q_{M_s}(v) + u \cdot v + \epsilon)_v \mid s \in F, u \in \mathbb{Z}_2^n, \epsilon \in \mathbb{Z}_2\big\} \subset \mathbb{Z}_2^{2^{m+1}}. \tag{5.6}$$

For example, the operation $x * s = xs^2$ coordinatizes the desarguesian plane and the desarguesian orthogonal spread, and determines via the above lemma the classical Kerdock code $\mathcal{K}_2(*)$ discovered by Kerdock [Ke] in 1972. His construction technique was, however, rather different.

More generally, all of the prequasifields in Proposition 2.19 determine Kerdock codes. We will study those of the form $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ given in (1.1). Since these are semifields, the corresponding codes have additional structure: they produce $\mathbb{Z}_4$–linear Kerdock and Preparata codes as well as elementary abelian groups of quasi–automorphisms acting transitively on the set of codewords (cf. Sections 5.5 and 5.6).

On the other hand, those prequasifields arising in Proposition 2.19 with all $\zeta_i = 0$ have the additional property $z(x * y) = (z^{-1}x) * (zy)$ for all $x, y \in F$, $z \in F^*$. The resulting *nearly extended cyclic* binary or $\mathbb{Z}_4$–Kerdock codes were studied in [Wi]. Their properties are briefly surveyed in [Ka3].

5.3. **$\mathbb{Z}_4$–codes and the Gray map.** The breakthrough paper [HKCSS] introduced the *Gray map*, an isometry $\phi\colon \mathbb{Z}_4^N \to \mathbb{Z}_2^{2N}$. (The metric on $\mathbb{Z}_2^{2N}$ is the usual Hamming metric. The metric on $\mathbb{Z}_4^N$ is the *Lee metric*, defined by $d_L((a_i),(b_i)) = \sum |a_i - b_i|$, where $|a_i - b_i| \in \{0,1,2,3\}$ has been reduced mod 4 and the sum is taken in $\mathbb{Z}$.) It was shown in [HKCSS] that, if $\mathcal{K}_2$ is the classical Kerdock code of length $N = 2^{m+1}$ with m odd, then $\mathcal{K}_4 = \phi^{-1}(\mathcal{K}_2)$ is a $\mathbb{Z}_4$–linear code. This led to the *definition* of the $\mathbb{Z}_4$–linear Preparata code $\mathcal{P}_4 = \mathcal{K}_2^\perp$ and the binary 'Preparata' code $\mathcal{P}_2 = \phi(\mathcal{P}_4)$, having the exact same weight distribution as the original code discovered by Preparata [Pr] in 1968. It is a code of length N, minimum distance 6 (a double error–correcting code), and has as many codewords as possible subject to these conditions: $2^{N-2(m+1)}$. If $m > 3$ then no binary 'Preparata' code is equivalent to any of Preparata's original codes [CCKS, 10.2]. Nevertheless, these ideas provide a partial explanation for the remarkable formal duality between the distance distributions of the Kerdock and Preparata codes given by the MacWilliams transform [HKCSS]. (We use quotation marks when discussing binary 'Preparata' codes in order to emphasize the fact that the class of codes we discuss does not include Preparata's original codes.)

Note that it is customary to talk about *the* Gray map, although this depends on a particular arrangement of the coordinates of binary and $\mathbb{Z}_4$–vectors.

Equivalence of $\mathbb{Z}_4$–codes. Two $\mathbb{Z}_4^N$–codes are *equivalent* if there is a monomial transformation of $\mathbb{Z}_4^N$ mapping one code to the other.

5.4. **Prequasifields and $\mathbb{Z}_4$–Kerdock codes.** Consider a symplectic prequasifield $\mathfrak{P}_*(F,*,+)$ (cf. (2.5) and (2.6)). We temporarily identify $\mathbb{Z}_2^m$ with $F = \mathrm{GF}(2^m)$ and the dot product with the bilinear form $T(xy)$. We fix an orthonormal basis, and write matrices using it. Then (2.6) can be interpreted as saying that the linear operator $x \to x * s$ is *self–adjoint relative to this form*; in other words, when written with respect to our orthonormal basis it arises from a *symmetric* matrix P_s. Then $\{P_s \mid s \in F\}$ is a set of symmetric matrices such that the difference of any two is nonsingular [CCKS, 5.1].

The $\mathbb{Z}_4$–valued quadratic form F_{P_s}. Identify the entries of P_s with elements of $\mathbb{Z}_4$. Define $F_{P_s}\colon \mathbb{Z}_2^m \to \mathbb{Z}_4$, a *$\mathbb{Z}_4$–valued quadratic form* [Br], by $F_{P_s}(v) = vPv^t$, where, for $v \in \mathbb{Z}_2^m$, we first identify the entries of v with elements of $\mathbb{Z}_4$ and then perform the matrix multiplication in the ring $\mathbb{Z}_4$. This function has a property analogous to (2.9):

$$F_{P_s}(u+v) = F_{P_s}(u) + F_{P_s}(v) + 2uP_sv^t$$

for all $u, v \in \mathbb{Z}_2^m$ viewed as lying in $\mathbb{Z}_4^m$. We also consider the expression $2u \cdot v \pmod 4$ when $u, v \in \mathbb{Z}_2^m$, using the same convention.

This time we index vectors in $\mathbb{Z}_4^{2^m}$ over $v \in \mathbb{Z}_2^m$, for a fixed ordering of $\mathbb{Z}_2^m$. As in [CCKS], define the *$\mathbb{Z}_4$–Kerdock code* corresponding to $\mathfrak{P}_*(F,*,+)$ by

$$\mathcal{K}_4(*) = \{(F_{P_s}(v) + 2u\cdot v + \epsilon)_v \mid s \in F, u \in \mathbb{Z}_2^n, \epsilon \in \mathbb{Z}_4\} \subset \mathbb{Z}_4^{2^m} \tag{5.7}$$

(compare (5.6)).

Proposition 5.8 ([CCKS, 8.3, 8.9])**.**

(i) *$\mathcal{K}_2(*)$ is the image of $\mathcal{K}_4(*)$ under the Gray map.*

(ii) *$\mathcal{K}_4(*)$ is $\mathbb{Z}_4$–linear if and only if $\mathfrak{P}_*$ is closed under addition; that is, if and only if $\mathfrak{P}_*$ is a presemifield.*

The presemifield for the original $\mathbb{Z}_4$–linear Kerdock code [HKCSS] is $F = \mathrm{GF}(2^m)$ but with the operation $x * y = xy^2$ (compare (1.1)), so that every corresponding semifield is isomorphic to $\mathrm{GF}(2^m)$.

5.5. **Equivalences among equivalences.** Consider a presemifield $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ in (1.1). The corresponding binary and $\mathbb{Z}_4$–Kerdock codes $\mathcal{K}_2(*)$ and $\mathcal{K}_4(*)$ were defined in (5.6) and (5.7). By Proposition 5.8, $\mathcal{K}_4(*)$ is $\mathbb{Z}_4$–linear, so we can also consider the corresponding $\mathbb{Z}_4$–linear and binary 'Preparata' codes

$$\mathcal{P}_4(*) = \mathcal{K}_4(*)^\perp \text{ and } \mathcal{P}_2(*) = \phi(\mathcal{P}_4(*)) \tag{5.9}$$

using the Gray map ϕ.

Theorem 5.10. *The following are equivalent for two presemifields* $\mathfrak{P}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ *and* $\mathfrak{P}_\circ\big((F_i')_0^{n'}, (\zeta_i')_1^{n'}\big)$ *in* (1.1), *where* $n \geq 1$, $|F_n| > 2$, $|F_{n'}'| > 2$, $[F\colon F_1] > 3$ *and* $[F\colon F_1'] > 3$:

(i) $\mathcal{K}_4(*)$ *and* $\mathcal{K}_4(\circ)$ *are equivalent* $\mathbb{Z}_4$*–linear Kerdock codes of length* 2^m.
(ii) $\mathcal{P}_4(*)$ *and* $\mathcal{P}_4(\circ)$ *are equivalent* $\mathbb{Z}_4$*–linear Preparata codes of length* 2^m.
(iii) $\mathcal{K}_2(*)$ *and* $\mathcal{K}_2(\circ)$ *are quasi–equivalent binary Kerdock codes of length* 2^{m+1}.
(iv) $\mathcal{P}_2(*)$ *and* $\mathcal{P}_2(\circ)$ *are quasi–equivalent binary 'Preparata' codes of length* 2^{m+1}.
(v) $\Sigma_*\big((F_i)_0^{n+1}, (\zeta_i)_1^n\big)$ *and* $\Sigma_\circ\big((F_i')_0^{n'+1}, (\zeta_i')_1^{n'}\big)$ *are equivalent binary orthogonal spreads of an* $\mathrm{O}^+(2m+2, 2)$*–space, where* $F_{n+1} = F_{n'+1}' = \mathbb{Z}_2$.
(vi) $\mathfrak{A}_*\big((F_i)_0^n, (\zeta_i)_1^n\big)$ *and* $\mathfrak{A}_\circ\big((F_i')_0^{n'}, (\zeta_i')_1^{n'}\big)$ *are isomorphic semifield planes of order* 2^m.
(vii) $n' = n$ *and* $m_i' = m_i$, $\zeta_i' = \lambda\zeta_i^\sigma$ *whenever* $1 \leq i \leq n$, *for some* $\lambda \in F^*$, $\sigma \in \mathrm{Aut}(F)$.

Proof. By [CCKS, 10.3], (i)–(iv) are equivalent.

By Theorem 4.13, (v)–(vii) are equivalent.

(i)⇒(v): [CCKS, 10.5].

(vii)⇒(iii): By Theorem 4.13, (vii) produces an equivalence in (v) that fixes Y, and hence (iii) holds by Theorem 5.3. □

Remark. We needed to have $F_n, F_{n'}' \supset F_{n+1} = F_{n'+1}' = \mathbb{Z}_2$ here in order to be able to define the codes and orthogonal spreads. The fact that (v) implies (iii) amounts to verifying the hypotheses in [CCKS, 10.5(iii)] (see Propositions 4.4 and 4.11).

Theorem 5.11. *If* m *is not a power of* 3 *and* $\rho(m) \geq 3$, *then there are more than* $2^{m(\rho(m)-2)m}/m$

(i) *pairwise inequivalent* $\mathbb{Z}_4$*–linear Kerdock and Preparata codes of length* 2^m, *and*
(ii) *pairwise quasi–inequivalent binary Kerdock and 'Preparata' codes of length* 2^{m+1}.

If $m \geq 3^4$ *is a power of* 3, *then this lower bound is* $2^{m(\rho(m)-3)m}/m$.

Proof. See Theorems 4.15(i) and 5.10. □

5.6. **Quasi–automorphisms of binary Kerdock codes.** Recall that an *extraspecial* 2*–group* has center of order 2, modulo which the group is elementary abelian and nontrivial. Extraspecial 2–groups played a crucial role in the applications of Kerdock codes to Euclidean line–sets [CCKS]. Here they arise in a rather different manner (where once again we index vectors over $v \in \mathbb{Z}_2^n$).

Lemma 5.12. *Every Kerdock code $\mathcal{K}_2(\mathcal{M})$ of length 2^n has an extraspecial group $\langle \mathcal{T}, \mathcal{T}^* \rangle = \mathcal{T}\mathcal{T}^*$ of 2^{2n+1} quasi–automorphisms stabilizing each coset of $R(1,n)$ in $\mathcal{K}_2(\mathcal{M})$. Here*

$$\mathcal{T} = \{\mathcal{T}_w \mid w \in \mathbb{Z}_2^n\} \quad \textit{and} \quad \mathcal{T}^* = \{\mathcal{T}^*_{(t,\delta)} \mid t \in \mathbb{Z}_2^n, \delta \in \mathbb{Z}_2\},$$

where

$$(c_v)_v \mathcal{T}_w = (c_{v+w})_v \quad \textit{and} \quad (c_v)_v \mathcal{T}^*_{(t,\delta)} = (c_v + t \cdot v + \delta)_v.$$

Moreover, $\mathcal{T}^*$ acts transitively on each such coset.

Proof. This is a straightforward calculation. The center of $\mathcal{T}\mathcal{T}^*$ is generated by $\mathcal{T}^*_{(0,1)}$. □

Note that the elements of $\mathcal{T}^*$ correspond to ordinary addition of codewords taken from the subcode $R(1,n)$ of $\mathcal{K}_2(\mathcal{M})$.

Proposition 5.13. *Let $\mathcal{M}$ be a Kerdock set, and $\mathcal{K}_2(\mathcal{M})$ and $\Sigma_{\mathcal{M}}$ the corresponding Kerdock code and orthogonal spread (cf. Proposition 5.1). Then*

$$\mathrm{QAut}\,\mathcal{K}_2(\mathcal{M})/\langle \mathcal{T}, T^* \rangle \cong \Gamma\mathrm{O}^+(2m+2,2)_{\Sigma_{\mathcal{M}},Y}.$$

Proof. Map g in (5.4) to $\begin{pmatrix} A^{-1} & O \\ O & A^t \end{pmatrix} \begin{pmatrix} I & M \\ O & I \end{pmatrix}$, which represents an orthogonal transformation of the space V in Proposition 5.1. This map is a homomorphism, and is onto $\Gamma\mathrm{O}^+(2m+2,2)_{\Sigma_{\mathcal{M}},Y}$ by the proof of Theorem 5.3 given in [Ka3, 3.4]. □

Remark. Each semifield orthogonal spread Σ_* in an $\mathrm{O}^+(2m+2,2)$–space is preserved by the elementary abelian group $E(\Sigma_*)$ in Lemma 2.21. By the preceding proposition (cf. Theorem 5.3(iii) or (5.4)), this in turn produces an elementary abelian group $\mathcal{E}$ of automorphisms of the associated code $\mathcal{K}_2(*)$ that acts transitively on the cosets of $R(1,m+1)$ in $\mathcal{K}_2(*)$; $\mathcal{E}$ also acts on $\mathcal{K}_4(*)$, and this corresponds exactly to $\mathbb{Z}_4$–linearity. It is easy to check that *the group $\mathcal{T}^*\mathcal{E}$ generated by $\mathcal{T}^*$ and $\mathcal{E}$ is an elementary abelian group acting regularly on the set of codewords of $\mathcal{K}_2(*)$*. For, $\mathcal{E}$ is transitive on the cosets or $R(1,m+1)$ in $\mathcal{K}_2(*)$, while $\mathcal{T}^*$ acts transitively on each such coset. Thus, distance–invariance (5.2) has a simple explanation for the codes $\mathcal{K}_2(*)$ arising from presemifields.

Boring codes. Every Kerdock code $\mathcal{K}_2(\mathcal{M})$ of length 2^{m+1} admits the extraspecial 2–group of order $2^{2(m+1)+1}$ in Lemma 5.12 that stabilizes every coset of $R(1,m+1)$. If this is the *full* quasi–automorphism group of the code, then we say that the Kerdock code is *boring*. Similarly, a $\mathbb{Z}_4$–linear Kerdock or Preparata code is *boring* if its full automorphism group consists of the translations corresponding to $\mathbb{Z}_4$–linearity.

Theorem 5.14. *If m is odd, not a power of 3, and $\rho(m) \geq 3$, then there are more than $(2^m-1)^{\rho(m)-3}2^{m-1}$ pairwise quasi–inequivalent boring binary Kerdock codes of length 2^{m+1}, and the same number of inequivalent $\mathbb{Z}_4$–linear Kerdock codes.*

Proof. For the second part use any one of the orthogonal spreads Σ_* in Theorem 4.16(i) together with Proposition 5.1 and (5.4). Also use the same Σ_* for the first part: there is a distinguished member $Y \in \Sigma_*$ fixed by $\mathrm{O}^+(V)_{\Sigma_*} = E(\Sigma_*)$, so choose any $Y' \neq Y$ in Σ_* and use it in place of Y in the preceding proposition. □

Of course, there is an analogous result when $m = 3^{\rho(m)} \geq 3^4$.

6. Summary; open problems

We have constructed large numbers of semifields, semifield orthogonal spreads, and $\mathbb{Z}_4$–linear Kerdock and Preparata codes. We were able to retain some reasonable amount of control over the "up and down process", whereas previous work on orthogonal spreads or Kerdock codes had to settle for chains of at most two or three fields [Ka1, Ka2].

We have not discussed the relationship between these objects and extremal line–sets in Euclidean and complex spaces [CCKS].

While most of our results assert the existence of many more examples of various types of geometries and codes than were previously known, the proofs and the ideas behind them leave various open problems.

1. All of our semifield planes and $\mathbb{Z}_4$–linear Kerdock and Preparata codes start with a desarguesian spread and then use the "up and down process". There must be many other "starter" planes that could be used for this purpose, but it is not clear where to look for them.

2. The scions of desarguesian planes, obtained by the "up and down process", need to be studied further. We have focused on the semifield planes among those planes, [KW] handles the flag–transitive ones, and [Wi] deals with those admitting a cyclic group of order $q^m - 1$ on the line at infinity. The boring planes in Theorem 4.17 are also among these scions. Are there others of these planes with interesting properties? Is there any way to find the full automorphism groups of the planes or the orthogonal spreads without using a "large" group as a crutch, as was done in all of the preceding instances?

3. G. Wene has asked how the second cousin $\mathfrak{C}$ of the desarguesian plane of order 32 [Ka1] is related to the plane determined by Knuth's commutative semifield of the same order [Kn2]. In view of the classification of semifield planes of order 32 [Wa, Kn1], and the determination of their automorphism groups [Kn1, p. 207], $\mathfrak{C}$ must be isomorphic to one of three planes in those references: Knuth's plane $\mathfrak{A}$, the plane $\mathfrak{A}^T$ obtained from it by "transposing" and the plane $\mathfrak{A}^{TD}$ obtained from $\mathfrak{A}^T$ by dualizing. On the other hand, the plane arising from the dual spread of a semifield plane $\mathfrak{A}'$ is $\mathfrak{A}'^{DTD}$ [BB], and hence $\mathfrak{C}^{DTD} \cong \mathfrak{C}$ (this is an essential part of the construction here and in [Ka1]). Consequently, *the second cousin is* $\mathfrak{A}^T$, the only one of the aforementioned three planes $\mathfrak{A}'$ in [Kn1, p. 207] that is isomorphic to $\mathfrak{A}'^{DTD}$.

However, this is an unsatisfactory proof: it depends on 40 year old computer computations (made independently by Walker [Wa] and Knuth [HK, p. 27]) and provides no real explanation. An explanation will be given in [Ka6].

4. Constructions are needed for boring translation planes of order q^m when m is even or q is odd. Undoubtedly there are very large numbers of these.

5. Constructions are needed for boring orthogonal spreads; none is known. In characteristic 2 such an orthogonal spread would produce many boring translation planes and many boring Kerdock codes. We suspect that most of the prequasifields in Proposition 2.19 give rise to boring orthogonal spreads, but this appears to be difficult to prove.

6. Various field restrictions in our results, concerning either field-size > 2 or $[F\colon F_1] > 3$, need to be removed. Of course, best of all in this regard would be a less computational approach to the main theorems of this paper.

7. Are there special properties of the line ovals in our symplectic semifield planes (cf. [Ma])?

In order to define one of these line ovals, fix an orthonormal basis of F with respect to the bilinear form $T_n(xy)$, and for each $s \in F$ let P_s be the matrix of $x \to x * s$ with respect to this basis. Write elements of F using this basis, and let $d(P_s) \in F$ be the vector whose entries are the square roots of those of the diagonal of P_s in the natural order. Then the lines $x = 0$ and $y = xP_s + d(P_s)$, $s \in F$, comprise a line oval. This is invariant under the group of translations

$$(x, y) \to (x, xP_r + d(P_r)), \qquad r \in F.$$

We refer to [Ma] for the much more important regularity property of this line oval.

Note also that the vectors $d(P_s)$ played a significant role in [CCKS]. Namely, the matrices $P = P_s$ and $M = M_s \in \mathcal{M}$ are related by the formula

$$M = \begin{pmatrix} P + d(P)^T d(P) & d(P)^T \\ d(P) & 0 \end{pmatrix}$$

[CCKS, 7.4], which defines a nonlinear bijection $P \to M$ from symmetric $m \times m$ matrices P to skew-symmetric $(m+1)\times(m+1)$ matrices M. It is not clear whether there is a relationship between the roles in these two very different settings.

8. Finally, we come to the most important problem: *much larger numbers of semifield planes are needed in all characteristics.* The difficulty is the nonisomorphism question for planes, which is harder than that for the semifields themselves. Isotopies are notoriously difficult to deal with. A classical question concerning semifields and their planes is the solvability of their autotopism groups, a difficult question discussed in [De, pp. 242–243] (compare [Al2]) and for which little has been done since the 1960's. This question, usually dealt with by detailed computations using (2.3), seems to be less difficult than that of determining whether two semifields are not isotopic. One of the few families of semifields for which there is presently a complete solution to the isotopy question is dealt with in [Al3]. The semifields studied there have a feature in common with those studied here: multiplication is defined using elements of an underlying field F, rather than in terms of a basis of the semifield over some field.

In this paper we calculated, but we also had more additional structure than is usually available in the study of semifields. What is needed is a better and more general approach to proving nonisotopy. A simple way is to compare the kernels of two semifields, or to compare various nuclei [De, p. 237]. However, these are very weak invariants, and by themselves appear to be unable to produce as many as m nonisomorphic planes of order q^m for prime q and large m.

References

[Al1] A. A. Albert, Quasigroups I. Trans. AMS 54 (1943) 507–519. MR **5:**229c

[Al2] A. A. Albert, Finite division algebras and finite planes, pp. 53–70 in: AMS Proc. Symp. Appl. Math. 10, 1960. MR **22:**6831

[Al3] A. A. Albert, Isotopy for generalized twisted fields. An. Acad. Brasil. Ci. 33 (1961) 265–275. MR **25:**3070

[Ba] R. Baer, Polarities in finite projective planes. Bull. AMS 52 (1946) 77–93. MR **7:**387d

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

[Br] E. H. Brown, Generalizations of Kervaire's invariant. Annals of Math. 95 (1972) 368–383. MR **45:**2719

[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. MR **98i:**94039

[Ch] C. Charnes, A non–symmetric translation plane of order 17^2. J. Geometry 37 (1990) 77–83. MR **91g:**51009

[ChD] C. Charnes and U. Dempwolff, The translation planes of order 49 and their automorphism groups. Math. Comp. 67 (1998) 1207–1224. MR **98j:**51007

[CW] M. Cordero and G. P. Wene, A survey of finite semifields. Discrete Math. 208/209 (1999) 125–137. MR **2001f:**12015

[De] P. Dembowski, Finite geometries. Springer, Berlin–Heidelberg–NY 1968. MR **38:**1597

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

[Dy] R. H. Dye, Partitions and their stabilizers for line complexes and quadrics. Ann. Mat. Pura Appl. 114 (1977) 173–194. MR **58:**12698

[Ga] M. J. Ganley, Polarities in translation planes. Geom. Dedicata 1 (1972) 103–116. MR **46:**6157

[HK] M. Hall, Jr. and D. E. Knuth, Combinatorial analysis and computers. Amer. Math. Monthly 72 (1965) 21–28. MR **30:**3030

[HKCSS] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $\mathbb{Z}_4$–linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inform. Theory 40 (1994) 301–319. MR **95k:**94030

[Ka1] W. M. Kantor, Spreads, translation planes and Kerdock sets. I, II. SIAM J. Alg. Discr. Meth. 3 (1982) 151–165 and 308–318. MR **83m:**51013b

[Ka2] W. M. Kantor, An exponential number of generalized Kerdock codes. Inform. Control 53 (1982) 74–80. MR **85i:**94022

[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. MR **96m:**94010

[Ka4] W. M. Kantor, Projective planes of order q whose collineation groups have order q^2. J. Alg. Combin. 3 (1994) 405–425. MR **96a:**51003

[Ka5] W. M. Kantor, Orthogonal spreads and translation planes, pp. 227–242 in: Progress in Algebraic Combinatorics (Eds. E. Bannai and A. Munemasa), Advanced Studies in Pure Mathematics 24, Mathematical Society of Japan 1996. MR **97i:**51017

[Ka6] W. M. Kantor, Commutative semifields and symplectic spreads (to appear in J. Algebra).

[Ke] A. M. Kerdock, A class of low–rate nonlinear binary codes. Inform. Control 20 (1972) 182–187. MR **49:**10438

[Kn1] D. E. Knuth, Finite semifields and projective planes. J. Algebra 2 (1965) 182–217. MR **31:**218

[Kn2] D. E. Knuth, A class of projective planes. Trans. AMS 115 (1965) 541–549. MR **34:**1916

[KW] W. M. Kantor and M. E. Williams, New flag–transitive affine planes of even order. J. Comb. Theory (A) 74 (1996) 1–13. MR **97e:**51012

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

[MR] R. Mathon and G. Royle, The translation planes of order 49. Des. Codes Crypt. 5 (1995) 57–72. MR **95j:**51016

[Pr] F. P. Preparata, A class of optimum nonlinear double–error correcting codes. Inform. Control 13 (1968) 378–400. MR **39:**3894

[Ta] D. E. Taylor, The geometry of the classical groups. Heldermann, Berlin 1992. MR **94d:**20028

[Wa] R. J. Walker, Determination of division algebras with 32 elements, pp. 83–85 in: Proc. AMS Symp. Applied Math. 15, 1962. MR **28:**1219

[Wi] M. E. Williams, $\mathbb{Z}_4$–Linear Kerdock codes, orthogonal geometries, and non–associative division algebras. Ph.D. thesis, U. of Oregon 1995.

Department of Mathematics, University of Oregon, Eugene, Oregon 97403
E-mail address: kantor@math.uoregon.edu

Raytheon, Dallas, Texas 75042
E-mail address: Michael_E1_Williams@raytheon.com