Adv. Geom. **9** (2009), 31–43
DOI 10.1515/ADVGEOM.2009.003

**Advances in Geometry**


# HMO-planes

William M. Kantor*

(Communicated by T. Penttila)

**Abstract.** Hiramine, Matsumoto and Oyama [9] made the remarkable discovery that every translation plane of order $q^2$ that is 2-dimensional over its kernel produces translation planes of order $q^4$. This construction is studied, with emphasis on isomorphisms among the resulting planes.

2000 Mathematics Subject Classification. Primary 51A40; Secondary 51A35

## 1 Introduction

How many projective planes are there of a given order $n$? Of course, this is a somewhat dubious question in view of the fundamental open question of whether every plane has prime power order; and moreover, since only one plane is known of any given prime order. Nevertheless, the question is meaningful if we only consider suitable sequences of orders. Thus, for example, there are more than $2^{q-1}/q^{16}e$ planes of order $q^2$ whenever $q = p^e$ with $p$ prime (using Bruck's subregular planes [4]; see [1, 2] for more recent similar constructions). Moreover, analogous questions arise concerning the number of planes of special sorts, such as planes over semifields (division algebras) or planes of Lenz–Barlotti Type II.1 [6, §5.4].

By far the most thoroughly studied finite projective planes arise from 4-dimensional vector spaces in the following manner. Let $K = \mathrm{GF}(q)$, $W = K^2$ and $V = W^2$, where we also view $V$ as $K^4$. Let $g, h\colon W \to K$ with $g(0,0) = h(0,0) = 0$. The translates of the subspaces

$$0 \times W, \text{ and } \left\{ \left( w, w \begin{pmatrix} x & y \\ g(x,y) & h(x,y) \end{pmatrix} \right) \;\middle|\; w \in W \right\} \text{ for each } x, y \in K \tag{1.1}$$

of $V$ are the lines of an affine plane $\pi_{g,h}$ of order $q^2$ if, and only if, the following condition holds:

$$\begin{aligned} (x_1 - x_2)(h(x_1,y_1) - h(x_2,y_2)) &\neq (y_1 - y_2)(g(x_1,y_1) - g(x_2,y_2)) \\ &\text{whenever } (x_1,x_2) \neq (y_1,y_2) \end{aligned} \tag{1.2}$$

*This research was supported in part by NSF Grants DMS 9001784 and DMS 0242983.

(cf. [6, p. 220]). These planes have $K$ in their kernels. In this note we will discuss the number of planes of this sort.

We will restrict to a "small" class of such planes, first studied in [9]. Let $q$ be a square, and consider the possibility that $g(x,y) = f(y)$ depends only on $y$, while $h(x,y) = \bar{x} = x^{\sqrt{q}}$; in that case we will abbreviate $\pi_{g,h}$ to $\pi_f$, and call $\pi_f$ an HMO-*plane*. Here the condition (1.2) states that

$$\text{whenever } x, y \in K \text{ are distinct, } (f(x) - f(y))(x - y) \notin \mathrm{GF}(\sqrt{q}). \tag{1.3}$$

Let $\mathrm{HMO}(q)$ denote the set of functions $f\colon \mathrm{GF}(q) \to \mathrm{GF}(q)$ such that $f(0) = 0$ and (1.3) holds. If $f \in \mathrm{HMO}(q)$ then $\pi_f$ is a semifield plane if and only $f$ is additive.

Hiramine, Matsumoto and Oyama [9] made the remarkable discovery that, for $K$, $g$ and $h$ as above, if $L = \mathrm{GF}(q^2)$ and $r \in L - K$ with $r^2 + r \in K$, then the function $f\colon L \to L$, defined by

$$f(x + yr) = h(x,y) - g(x,y) + h(x,y)r \text{ for all } x, y \in K, \tag{1.4}$$

is in $\mathrm{HMO}(q^2)$. This recursive construction of planes $\pi_f$ from planes $\pi_{g,h}$ is the focus of this note. The only other known recursive construction of finite projective planes seems to be in [12, 19, 16, 17], but that is much more unwieldy than the one in [9] and does not apply to odd order planes.

Let $\mathrm{N}_{\mathrm{HMO}}(q^4)$, $\mathrm{N}_{\mathrm{HMO.SEMI}}(q^4)$ and $\mathrm{N}_{\mathrm{II.1}}(q^4)$ denote, respectively, the numbers of isomorphism classes of the following types of planes of order $q^4$: HMO-planes, HMO-planes that are semifield planes, and planes of Lenz–Barlotti Type II.1 [6, §5.4].

**Theorem 1.5.** *If $q = p^e$ with $p$ prime, then*

(a) $\mathrm{N}_{\mathrm{HMO.SEMI}}(q^4) > q^2/4pe^2$,

(b) $\mathrm{N}_{\mathrm{HMO}}(q^4) > 2^{q-1}/4q^{21}e^2$, *and*

(c) $\mathrm{N}_{\mathrm{II.1}}(q^4) > 2^{q-1}/4q^{21}e^2$.

There does not appear to be any published construction of semifield planes of order $q^4$ containing anywhere near the admittedly anemic number of planes in (a). The proof of the preceding theorem uses the HMO-construction, and is rather elementary: only a little group theory (circa 1900) is used – involving the subgroup structure of $\mathrm{PSL}(2,q)$ – and possibly even this is avoidable.

In the past, semifield planes have rarely been constructed in large numbers for a given order; the only exceptions appear to be [17, 13] for even order. While the above theorem produces a number of such planes, it has limitations that somewhat conflict with the impression that the HMO-construction produces "a vast number of new planes" [10]. If $\mathrm{N}_{\mathrm{2SEMI}}(q^2)$ denotes the number of isomorphism classes of semifield planes (1.1) of order $q^2$ with kernel of order at least $q$, then the following is an elementary bound for the number of semifield planes arising as in (1.1) by repeated use of this construction:

**Theorem 1.6.** *Starting with semifield planes* (1.1) *of order $q^2$, repeated use of the* HMO-*construction $k$ times produces at most $(q^{2^{k-1}})^7\,\mathrm{N}_{\mathrm{2SEMI}}(q^2)$ isomorphism classes of semifield planes of order $q^{2^k}$.*

*In particular, semifield planes* (1.1) *of order* $q^2$ *can produce asymptotically more than a polynomial number of semifield planes of order* $q^{2^k}$ *only if there are asymptotically more than a polynomial number of semifield planes* (1.1) *of order* $q^2$.

Note that there is an equally elementary result for non-semifield planes.

After some discussion of HMO-planes in Sections 2 and 3, in Section 4 we prove the above theorems. Finally, in Sections 5 and 6 we discuss a recent different type of construction in [3].

Much of this note was written more than 15 years ago, after Yutaka Hiramine showed me the construction in [9]. I am very grateful to him for instruction in this construction. At the time these results were first obtained I had not understood how few semifield planes were known. Other recent work [17, 13, 14, 15] has now made it clear that a lot more semifield planes of odd order need to be constructed; and Theorems 1.5 and 1.6 are intended to emphasize this point. The fact that there are so many more planes of type II.1 known than semifield planes (including ones of even order) is elementary but a bit disconcerting.

## 2 Isomorphisms among the planes $\pi_f$

Let $K = \mathrm{GF}(q)$ and $f \in \mathrm{HMO}(q)$, where $q$ is a square. In order to study isomorphisms among the planes $\pi_f$ we will need some elementary information concerning their collineation groups.

Let $G(\pi_f)$ be the group of *linear* transformations of $V = K^4$ inducing collineations of $\pi_f$. The treatment in [9] singles out two important subgroups of $G(\pi_f)$. The group

$$P = \left\{ \begin{pmatrix} I & \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix} \\ O & I \end{pmatrix} \;\middle|\; z \in K \right\} \tag{2.1}$$

consists of $q$ elations with axis $0 \oplus W$. All elations (other than the translations) have this axis, so that $G(\pi_f)$ fixes this line [9, Lemma 2.2]. Also, the cyclic group

$$Z = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & z & 0 & 0 \\ 0 & 0 & z & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \;\middle|\; z \in K, z\bar{z} = 1 \right\} \tag{2.2}$$

of order $\sqrt{q}+1$ fixes the Baer subplane $K \oplus 0 \oplus 0 \oplus K$ pointwise. In order to take advantage of $Z$ we will need the following ancient fact:

**Lemma 2.3.** *Let* $R$ *be the subgroup* $\left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & z \end{smallmatrix}\right) \;\middle|\; z \in K, z\bar{z} = 1 \right\}$ *of* $\mathrm{GL}(2,q)$. *Assume that* $S$ *is a subgroup of* $\mathrm{GL}(2,q)$ *conjugate to* $R$. *Then there is an element* $h \in \langle R, S \rangle$ *such that* $S^h = R$ *or* $\left\{ \left(\begin{smallmatrix} z & 0 \\ 0 & 1 \end{smallmatrix}\right) \;\middle|\; z \in K, z\bar{z} = 1 \right\}$.

*Proof.* Project $\langle R, S\rangle$ into $\mathrm{PGL}(2,q)$, obtaining a subgroup $H$ which is, in fact, a subgroup of $\mathrm{PSL}(2,q)$ since every $z \in K$ such that $z\bar{z} = 1$ is a square in $K$. The subgroups $H$ of $\mathrm{PSL}(2,q)$ generated by two different cyclic groups of order $\sqrt{q}+1$ are all known [7, Ch. XII]:

(i) $\mathrm{PSL}(2,q)$,
(ii) $\mathrm{PGL}(2,\sqrt{q})$, and
(iii) a group of order $q(\sqrt{q}+1)$ having a normal subgroup of order $q$.

In each case, any two cyclic subgroups of $H$ of order $\sqrt{q}+1$ are conjugate. Consequently, there is an element $h \in \langle R, S\rangle$ such that $S^h$ and $R$ coincide modulo scalars. Then $S^h$ and $R$ commute, so that $S^h$ consists of diagonal matrices. By hypothesis, $S^h$ fixes a vector. Hence, $S^h$ must be as asserted. □

**Remarks.** The above argument resembles ones in [9, §5] used to study the group $G(\pi_f)$, but it is simpler than what was needed in [9].

The enumeration of subgroups of $\mathrm{PSL}(2,q)$ used above is often attributed to Dickson. However, Dickson [7, p. 260] cites papers by Moore [8] and Wiman [20] for this theorem.

Straightforward calculations produce the following consequence:

**Proposition 2.4.** *Let $K = \mathrm{GF}(q)$ and $f, f' \in \mathrm{HMO}(q)$.*

(i) *If $\pi_f \cong \pi_{f'}$ then there are $u, v \in K^*, k \in K, \tau \in \mathrm{Aut}\, K$ such that one of the following holds:*

$$\begin{aligned}&[f'(z^{\tau^{-1}})]^\tau = uf(vz+k) - uf(k) \text{ for all } z \in K, \text{ or}\\ &[f'(z^{\tau^{-1}})]^\tau = uf^{-1}(vz+k) - uf^{-1}(k) \text{ for all } z \in K.\end{aligned} \tag{2.5}$$

(ii) *If $f(x)/\bar{x}$ is not constant in* (i)*, then $v/u \in \mathrm{GF}(\sqrt{q})$.*
(iii) *If $\tau, u, v$ and $k$ are as in* (2.5) *with $v/u \in \mathrm{GF}(\sqrt{q})$, then $\pi_f \cong \pi_{f'}$.*

*Proof.* Let $\tau$ be any field automorphism of $K$. Then

$$\left\{\left(w, w\begin{pmatrix} x & y\\ f(y) & \bar{x}\end{pmatrix}\right) \;\middle|\; w \in W\right\}^\tau = \left\{\left(w, w\begin{pmatrix} x & y\\ f(y^{\tau^{-1}})^\tau & \bar{x}\end{pmatrix}\right) \;\middle|\; w \in W\right\},$$

so that $\tau$ induces an isomorphism $\pi_f \cong \pi_{\tau f \tau^{-1}}$.

If $\pi_f \cong \pi_{f'}$ then there is a semilinear transformation $T\colon V \to V$ mapping the subspaces defining $\pi_f$ to those for $\pi_{f'}$. In view of the preceding paragraph, we can compose $T$ with a suitable field automorphism in order to obtain a linear transformation inducing an isomorphism from $\pi_f$ to another HMO-plane. Consequently, we might as well assume that our original $T$ is linear. We will identify $T$ with its matrix with respect to the standard basis of $V$.

By a remark following (2.1), $T$ must send the line $0\times W$ of $\pi_f$ to the line $0\times W$ of $\pi_{f'}$. Moreover, $Z \le G(\pi_f)$, $Z \le G(\pi_{f'})$ and $T^{-1}ZT \le G(\pi_{f'})$. Consider the restrictions of $Z$ and $T^{-1}ZT$ to the 2-space $0 \times W$. By Lemma 2.3, there is an element $U$ of $G(\pi_{f'})$ such that $Z$ and $(TU)^{-1}Z(TU)$ have the same eigenspaces on $0 \times W$. Now replace $T$ by $TU$, so that $Z$ and $T^{-1}ZT$ have the same eigenspaces on $0 \times W$. In particular, $T$

sends the pair $0\times 0\times 0\times K, 0\times 0\times K\times 0$ of eigenspaces of $Z$ on $0\times W$ to the pair $0\times 0\times 0\times K, 0\times 0\times K\times 0$ of eigenspaces of $T^{-1}ZT$.

It follows that $T$ has the form $T=\left(\begin{smallmatrix}A & B\\ O & D\end{smallmatrix}\right)$ with $A=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$, $D=\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$, $B=\left(\begin{smallmatrix}i & j\\ k & \ell\end{smallmatrix}\right)$, and either $\beta=\gamma=0$ or $\alpha=\delta=0$. By multiplying $T$ by a suitable scalar matrix, we may assume that $\delta=1$ or $\gamma=1$, respectively.

Now consider the condition that $T$ is an isomorphism: for any $s,t\in K$ there must be $x,y\in K$ such that

$$\left\{\left(wA, wB+w\begin{pmatrix}s & t\\ f(t) & \bar{s}\end{pmatrix}D\right)\;\middle|\; w\in W\right\}=\left\{\left(w, w\begin{pmatrix}x & y\\ f'(y) & \bar{x}\end{pmatrix}\right)\;\middle|\; w\in W\right\},$$

so that $B+\left(\begin{smallmatrix}s & t\\ f(t) & \bar{s}\end{smallmatrix}\right)D=A\left(\begin{smallmatrix}x & y\\ f'(y) & \bar{x}\end{smallmatrix}\right)$. Consequently,

$$\begin{aligned} i+s\alpha+t\gamma &= ax+bf'(y)\\ j+s\beta+t\delta &= ay+b\bar{x}\\ k+f(t)\alpha+\bar{s}\gamma &= cx+df'(y)\\ \ell+f(t)\beta+\bar{s}\delta &= cy+d\bar{x}. \end{aligned} \tag{2.6}$$

**Case 1.** $\beta=\gamma=0,\delta=1$. For all $x,y\in K$ we have $\alpha f(ay+b\bar{x}-j)=cx+df'(y)-k$, so that $\alpha f(ay-j)=df'(y)-k$ and $\alpha f(b\bar{x}-j)=cx-k$.

If $d\neq 0$ then $f'(y)=(\alpha/d)f(ay-j)+(k/d)$; and $k/d=-(\alpha/d)f(-j)$. Thus, (2.5) holds in this case. Moreover, $f'(y)=(\alpha/d)f(ay-j)+(k/d)$, while $\alpha(\overline{cy+d\bar{x}-\ell})=ax+bf'(y)-i$. Then $f(-j)+k/\alpha=0$, $\alpha\bar{d}=a$ and $a/(\alpha/d)=d\bar{d}\in \mathrm{GF}(\sqrt{q})$, as required in (ii).

Now assume that $d=0$. Since $\alpha f(ay-j)=-k$ for all $y$ we must have $a=0$, so that $b\neq 0$ (as $A$ is invertible) and $\alpha f(b\bar{x}-j)=cx-k$. Then $f(z)=u\bar{z}+u_0$ for all $z\in K$ and some $u,u_0$; and it follows that $f(z)=u\bar{z}$. On the other hand, (2.6) yields that $\bar{s}=cy-\ell$ and hence $\alpha(cy-\ell)=bf'(y)-i$ for all $y$. As above, this implies that $f'(z)=v\bar{z}$ for all $z$ and some $v\in L$. Consequently, $f'(z)=(v/u)f(z)$, and (2.5) holds once again.

**Case 2.** $\alpha=\delta=0,\gamma=1$. This time, for all $x,y\in L$ we have $\beta f(ax+bf'(y)-i)=cy+d\bar{x}-\ell$, so that $\beta f(bf'(y)-i)=cy-\ell$ and $\beta f(ax-i)=d\bar{x}-\ell$.

If $b\neq 0$ then $f'(y)=(i/b)+f^{-1}([c/\beta]y-[\ell/\beta])/b$; and $i/b=-f^{-1}(-[\ell/\beta])/b$. Once again, (2.5) holds. Moreover, $f'(y)=(i/b)+f^{-1}([c/\beta]y-[\ell/\beta])/b$, while $\beta(\overline{cx+df'(y)-k})=ay+b\bar{x}-j$. Then $\beta\bar{c}=b$ and $[c/\beta]b=1/c\bar{c}\in\mathrm{GF}(\sqrt{q})$, as required in (ii).

Now suppose that $b=0$. Then $a\neq 0$, $t=ax-i$ and hence $\beta f(ax-i)=cy+d\bar{x}-\ell$ for all $x,y$. As before, this implies that $c=0$ and $f(z)=u\bar{z}$ for some $u$. Then also $\bar{s}=df'(y)-k$ and $\beta s=ay-j$. Once again we find that $f'(z)/f(z)$ is independent of $z\in L$, as required.

Finally, in Cases 1 and 2 it is straightforward to reverse the preceding calculations in order to obtain (iii). □

**Remark.** If $f(x)/\bar{x}$ is not constant, then $b = c = 0$ in Case 1 and $a = d = 0$ in Case 2.

**Corollary 2.7.** *Given $f \in \mathrm{HMO}(q)$, where $q = p^e$ with $p$ a prime and $f(x)/\bar{x}$ is not constant, there are fewer than $2eq(q-1)(\sqrt{q}-1)$ functions $f' \in \mathrm{HMO}(q)$ such that $\pi_f \cong \pi_{f'}$.*

*Proof.* In (2.5) there are at most $e$ possibilities for $\tau$, $q$ for $k$, $q-1$ for $u$, and $\sqrt{q}-1$ for $v$. □

It should be possible to prove Proposition 2.4 by a direct calculation, without any assistance from groups as in Lemma 2.3. A similar argument is used in [9, Proposition 6.4] to study $\mathrm{Aut}\,\pi_f$.

## 3 The HMO-construction

In (1.4) we have already indicated the construction of a new plane $\pi_f$ of order $q^4$ from the plane $\pi_{g,h}$ of order $q^2$ in (1.1):

**Theorem 3.1** ([9]). (i) *$f \in \mathrm{HMO}(q^2)$. Hence, $f$ determines an* HMO*-plane $\pi_f$ of order $q^4$.*
(ii) *$\pi_f$ is nondesarguesian.*
(iii) *$\pi_f$ is a semifield plane if and only if $g$ and $h$ are additive.*

Clearly, $g$ and $h$ determine $f$, and the reverse is also true (cf. [10]).

Note that $\pi_{g,h}$ can be a semifield plane even when $g$ and $h$ are not additive, if the "wrong" coordinate axes are chosen. Also note that, when $q$ is odd, a simpler construction is used in [9]: let $r \in L - K$ with $r^2 \in K$, write

$$f(x + yr) = g(x, y) + h(x, y)r \tag{3.2}$$

for all $x, y \in K$, and then the preceding theorem again holds. All of this is easy to check, as is the following observation:

**Lemma 3.3.** *In* (1.4)*, $f(z)/\bar{z}$ is not constant.*

*Proof.* If $f(x+yr) = c(x+y\bar{r}) = c(x+y[-1-r])$ for some constant $c$ and all $x, y \in K$, then $h(x, y) = -cy$ by (1.4), which contradicts (1.2) when $y_1 = y_2$ but $x_1 \neq x_2$. □

## 4 Proofs of the theorems

Each of the planes in the theorems has $K$ in its kernel, and is 4-dimensional over $K$, so that every isomorphism (or automorphism) is induced by an element of the group of invertible affine semilinear transformations of $K^4$. We will focus on the stabilizer $(\mathrm{Aut}\,\pi)_0$ of the point 0.

**Proposition 4.1.** *Let $\pi$ be a translation plane of order $q^2$ that can be presented as in* (1.1)*. Then*
(a) *The number of different pairs $g, h$ of functions arising from such presentations of $\pi$ is between $(q^2+1)q^2(q^2-1)^2(q^2-q)^2/|(\mathrm{Aut}\,\pi)_0|$ and $(q^2+1)q^2(q^2-1)^2(q^2-q)^2/(q-1)$; and*
(b) *If $\pi$ is a nondesarguesian semifield plane, then the number of such pairs $g, h$ of additive functions is between $q^2(q^2-1)^2(q^2-q)^2/|(\mathrm{Aut}\,\pi)_0|$ and $(q^2-1)^2(q^2-q)^2/(q-1)$.*

*Proof.* In (1.1) we chose two lines $K \times K \times 0 \times 0$ and $0 \times 0 \times K \times K$ through 0, and two pairs of $K$-linearly independent points (vectors) of those lines: $(1,0,0,0), (0,1,0,0)$ and $(0,0,1,0), (0,0,0,1)$. There are $(q^2+1)q^2\{(q^2-1)(q^2-q)\}^2$ such ordered 4-tuples of points, and each produces a pair $g, h$. If two such ordered pairs of functions coincide then there is an element of $(\mathrm{Aut}\,\pi)_0$ sending one such ordered 4-tuple to another. Hence, there are at least as many distinct pairs $g, h$ of these functions as there are orbits of $\mathrm{Aut}\,\pi$ on the set of all such 4-tuples. Since the same pair is produced by two 4-tuples in the same orbit of the group of homologies with center 0, this proves (a).

For (b), observe that one of the above lines is the axis of $q^2$ elations, and hence is uniquely determined since we want additive functions. Since these elations preserve the pair $g, h$, we obtain the desired estimates. □

**Proof of Theorem 1.5.** Let $q = p^e$, $K$, $L$ and $r$ be as in (1.4).

(a) Start with one of Knuth's semifield planes $\pi$ of order $q^2$ [18] for which $|(\mathrm{Aut}\,\pi)_0| \le q^2(q-1)(p-1)e$. By Proposition 4.1(b), the plane $\pi$ can be obtained using at least $q^2(q^2-1)^2(q^2-q)^2/q^2(q-1)(p-1)e$ different pairs $g, h$ of additive functions on $\mathrm{GF}(q)^2$. Each of these pairs produces a function $f \in \mathrm{HMO}(q^2)$, and hence a semifield plane $\pi_f$ of order $q^4$, by Theorem 3.1; and $\pi_f$ arises from at most $4eq^2(q^2-1)(q-1)$ functions in $\mathrm{HMO}(q^2)$ by Corollary 2.7. Thus, we obtain at least

$$q^2(q^2-1)^2(q^2-q)^2/\{q^2(q-1)(p-1)e \cdot 4eq^2(q^2-1)(q-1)\} > q^2/4pe^2$$

pairwise nonisomorphic semifield planes of order $q^4$, as required.

(b) A construction due to Bruck [4] produces $2^{q-1}$ different spreads in $\mathrm{PG}(3,q)$ whenever $q = p^e$ with $p$ prime, corresponding to some of his subregular planes of order $q^2$. Since any isomorphism of planes arises from a collineation of $\mathrm{PG}(3,q)$, we obtain the very crude lower bound $2^{q-1}/q^{16}e$ for the number of nondesarguesian planes obtained in this manner. (A better bound is $2^{q-1}/4q^2e$, but the difference is minuscule compared to the exponential term $2^{q-1}$.)

Each such plane produces many pairs $g, h$ in (1.1), and hence more than $2^{q-1}/q^{16}e$ functions $f \in \mathrm{HMO}(q^2)$ via (1.4). As above, each of the resulting planes $\pi_f$ of order $q^4$ arises from at most $4eq^2(q^2-1)(q-1)$ functions in $\mathrm{HMO}(q^2)$. Hence, we obtain more than $2^{q-1}/\{q^{16}e \cdot 4eq^2(q^2-1)(q-1)\} > 2^{q-1}/4q^{21}e^2$ pairwise nonisomorphic HMO-planes of order $q^4$, as required.

(c) The obvious approach for $\mathrm{N}_{\mathrm{II}.1}$ is to derive the duals of the planes $\pi_f$ that are not semifield planes (so that the duals are not translation planes). This produces planes of type II.1. The isomorphism problem is settled by an argument already in [11, Theorem 4.3]: the dual planes are isomorphic if and only if their derived planes are. □

**Proof of Theorem 1.6.** By Proposition 4.1(b) there exist at most $(q^2-1)^2(q^2-q)^2/(q-1) < q^7$ different pairs of additive functions $g, h$ in (1.1) for each of the $\mathrm{N}_{2\mathrm{SEMI}}(q^2)$ semifield planes of order $q^2$. Thus, $\mathrm{N}_{\mathrm{SEMI.HMO}}(q^4) < q^7\,\mathrm{N}_{2\mathrm{SEMI}}(q^2)$. Now iterate. □

## 5 An operation on HMO-planes

In [3] there is a construction of a semifield plane starting with a semifield 2-dimensional over its kernel. We apply our results to some of these and at the same time consider the more general setting in [3].

Since we are considering semifields, the functions $g$ and $h$ in Section 1 can be written $g(x,y) = g_1(x) + g_2(y)$ and $h(x,y) = h_1(x) + h_2(y)$ for additive functions $g_1, g_2, h_1$, $h_2\colon K \to K$; (1.2) still holds in the following simplified form:

$$x[h_1(x) + h_2(y)] \neq y[g_1(x) + g_2(y)] \text{ whenever } xy \neq 0. \tag{5.1}$$

The associated presemifield operation on $W = K^2$ is given by

$$(a,b) * (x,y) = (ax + bh_1(x) + bh_2(y), ay + bg_1(x) + bg_2(y)). \tag{5.2}$$

Equip $K$ with the nondegenerate symmetric bilinear form $(x,y) := T(xy)$, where $T$ denotes the trace map from $K$ to the prime field. We will often use the fact that $(xa,y) = (x,ay)$ for all $a,x,y \in K$. For any additive map $f\colon K \to K$, define $f^t\colon K \to K$ by $(f(x),y) = (x, f^t(y))$ for all $x,y \in K$. For example, if $\sigma \in \mathrm{Aut}\, K$ then $\sigma^t = \sigma^{-1}$ since $T(x^\sigma y) = T(x^\sigma y)^{\sigma^{-1}}$.

By [3, Table in Section 6], the operation

$$(a,b) \circ (x,y) = (ax + bh_1^t(x) + bg_1^t(y), ay + bh_2^t(x) + bg_2^t(y)) \tag{5.3}$$

defines a presemifield. This construction can also be described as follows:

**Lemma 5.4.** *If the ordered* 4*-tuple* $(g_1, g_2, h_1, h_2)$ *determines a presemifield via* (5.2) *then so do the* 4*-tuples* $(h_2^t, g_2^t, h_1^t, g_1^t)$, $(h_2, h_1, g_2, g_1)$ *and* $(g_1^t, h_1^t, g_2^t, h_2^t)$.

*Proof.* By (5.1), for the 4-tuple $(h_2^t, g_2^t, h_1^t, g_1^t)$ we need to show that

$$[h_1^t(x) + g_1^t(y)]x = [h_2^t(x) + g_2^t(y)]y \text{ implies that } x = y = 0;$$

or, equivalently, that

$$T([h_1^t(x) + g_1^t(y)]xu) = T([(h_2^t(x) + g_2^t(y))]yu) \text{ for all } u \in K^*$$

implies that $x = y = 0$. If we write $X = xu$, $Y = -yu$ and $v = 1/u$, then the above condition can be rewritten successively as

$$T(h_1(xu)xu \cdot v + g_1(xu)yu \cdot v) = T(h_2(yu)xu \cdot v + g_2(yu)yu \cdot v)$$

and

$$T([h_1(X) + h_2(Y)]Xv) = T([g_1(X) + g_2(Y)]Yv)$$

for all $v \in K^*$. Hence, $[h_1(X) + h_2(Y)]X = [g_1(X) + g_2(Y)]Y$, so that $X = Y = 0$ by (5.1), as required.

For the 4-tuples $(h_2, g_2, h_1, g_1)$ and $(g_1^t, h_1^t, g_2^t, h_2^t)$ just interchange the roles of $x$ and $y$ in (5.1). □

See [3] for motivation and other proofs for the case $(h_2^t, g_2^t, h_1^t, g_1^t)$.

In particular, if the initial plane arises from an additive function $f \in \mathrm{HMO}(q)$, and if "bar" denotes the involutory field automorphism of $K$, then the HMO-construction uses $h_1 = g_2 = 0$, $h_2 = f$, $g_1 = \mathrm{bar}$, and we obtain the HMO-presemifield operation

$$(a, b) * (x, y) = (ax + bf(y), ay + b\bar{x}). \tag{5.5}$$

Since $\mathrm{bar}^t = \mathrm{bar}$, the lemma implies that $f^t \in \mathrm{HMO}(q)$. Direct verification is, of course, even easier in this special case.

**Proposition 5.6.** *If $f, f' \in \mathrm{HMO}(q)$ and $\pi_f \cong \pi_{f'}$, then $\pi_{f^t} \cong \pi_{f'^t}$.*

*Proof.* Note that $(\tau f \tau^{-1})^t = \tau f^t \tau^{-1}$ since we have $T(xf^t(y^{\tau^{-1}})^\tau) = T(f(x^{\tau^{-1}})^\tau y) = T(x(\tau f \tau^{-1})^t(y))$. Thus, we may assume that $\tau = 1$ in Proposition 2.4. If $f'(x) = uf(vx)$ for all $x \in K$, then $f'^t(x) = vf^t(ux)$ since, for all $y \in K$, $T(f'^t(x)y) = T(xuf(vy)) = T(f^t(xu)vy)$. Thus, Proposition 2.4 applies. The possibility $f'(x) = uf^{-1}(vx)$ is handled in the same way. □

Thus, the HMO-plane $\pi_{f^t}$ is determined by the original HMO-plane $\pi_f$ rather than by the specific function $f$ used. We will generalize this in Theorem 6.1.

Our next goal is to discuss the (lack of) relationship between the BEL-construction [3] and the Knuth transformations on presemifields [18]. For this we need the following simple

**Lemma 5.7.** *If an* HMO*-presemifield and its image under a Knuth transformation have the same kernel, then they determine isomorphic planes.*

*Proof.* By [3, Table in Section 6], in view of the stated kernel condition the only presemifield we need to consider is defined by

$$(a, b)(x, y) = (ax + by, a\bar{y} + bf(x)).$$

Let $a' = b, b' = a, x' = y, y' = f(x)$, and obtain the new operation

$$(a', b') \cdot (x', y') = (a'x' + b'f^{-1}(y'), a'y' + b'\overline{x'})$$

producing the same plane. Now note that $f$ and $f^{-1}$ determine isomorphic planes by Proposition 2.4. □

In [3] it was evidently hoped, but not proved, that the BEL-construction produces new planes, that is, planes not obtainable from the original one by a Knuth transformation. We now give examples of this fact; there are undoubtedly simpler examples than the ones we describe.

**Example 5.8.** Start with one of Knuth's semifields [18] of odd order $q^2$, with multiplication given by

$$(a,b)(x,y) = (ax + eby^\alpha, ay + bx) \text{ for all } x, y \in K = \mathrm{GF}(q),$$

using $q = p^k$ for an odd $k \geq 3$ and a prime $p \equiv 1 \pmod 4$, $1 \neq \alpha \in \mathrm{Aut}\, K$, and a generator $e$ of $K^*$. We view each field automorphism $\tau$ as a power of $p$, and then $(\tau + 1, p^k - 1) = 2$ since $k$ is odd.

Let $L = \mathrm{GF}(q^2)$, and define $f\colon L \to L$ using (3.2). We will prove the following

**Claim.** *$\pi_{f^t}$ is not isomorphic to any plane produced from $\pi_f$ by a Knuth transformation.* In view of Lemma 5.7, we only need to show that $\pi_{f^t}$ and $\pi_f$ are not isomorphic.

We digress briefly: we will need the fact that $K^\perp = rK$ with respect to the nondegenerate symmetric bilinear form $T(XY)$ on $L$ (here $X, Y \in L$; recall that $r \in L - K$ and $r^2 \in K$). For, since $r^{2q} = r^2 \in K$ but $r \notin K$ we have $r^q = -r$. Then $k_1 r k_2 + (k_1 r k_2)^q = 0$ whenever $k_1, k_2 \in K$, so that $rK \subseteq K^\perp$. Since $\dim_{\mathrm{GF}(p)} rK + \dim_{\mathrm{GF}(p)} K^\perp = \dim_{\mathrm{GF}(p)} L = 2 \dim_{\mathrm{GF}(p)} K$, it follows that $K^\perp = rK$.

In order to prove the claim, note that

$$f(x + ry) = ex^\alpha + ry \text{ for } x, y \in K \tag{5.9}$$

in (3.2). By Proposition 2.4, the planes $\pi_{f^t}$ and $\pi_f$ are isomorphic if and only if

$$uf(vX) = [f^{\pm 1}]^t (X^{\tau^{-1}})^\tau \text{ for all } X \in L$$

for some $u, v \in L^*$ with $u/v \in K$, some $\tau \in \mathrm{Aut}\, L$ and some choice of sign. Thus,

$$T(uf(vX)Y) = T(\{[f^{\pm 1}]^t (X^{\tau^{-1}})\}^\tau Y) = T(X\{f^{\pm 1}(Y^{\tau^{-1}})\}^\tau) \tag{5.10}$$

for all $X, Y \in L$ (recall that $T$ maps to the prime field). We specialize this identity several times in order to obtain information concerning the elements $u, v, e$, ultimately leading to a contradiction. We will mostly consider the case $[f^{-1}]^t$ of (5.10). We always let $x$ and $y$ denote arbitrary elements of $K^*$.

When $vX = rx$ and $Y = y$, (5.9) and (5.10) imply that

$$\begin{aligned} T(urxy) &= T\big([rx/v] f^{-1}(y^{\tau^{-1}})^\tau\big) \\ &= T([rx/v][y^{\tau^{-1}}/e]^{\alpha^{-1}\tau}) = T([rx/v]^\alpha [y^{\tau^{-1}}/e]^\tau), \end{aligned}$$

so that $urx - (rx/v)^\alpha / e^\tau \in K^\perp = rK$. Then $urx^{1-\alpha} - (r/v)^\alpha / e^\tau \in rK$ for all $x \in K^*$, so that $ur(x^{1-\alpha} - 1) = [urx^{1-\alpha} - [r/v]^\alpha / e^\tau] - [ur - [r/v]^\alpha / e^\tau] \in rK$. Since $\alpha \neq 1$ we have $x^{1-\alpha} \neq 1$ for some $x$. Then

$$u \in K \text{ and hence } v = (u/v)^{-1} u \in K.$$

Similarly, when $vX = x$ and $Y = y$, (5.9) and (5.10) yield

$$T(uex^\alpha y) = T([x/v][y^{\tau^{-1}}/e]^{\alpha^{-1}\tau}) = T([x/v]^\alpha [y^{\tau^{-1}}/e]^\tau),$$

so that $uex^\alpha - [x/v]^\alpha/e^\tau \in rK$. Then $ue - [1/v^\alpha e^\tau] \in rK$. Since we already know that $u, v, e \in K$, it follows that

$$uv^\alpha e^{\tau+1} = 1.$$

Finally, when $vX = rx$ and $Y = ry$, (5.9) and (5.10) imply that

$$T(urxry) = T\big([rx/v]\{f^{-1}([ry]^{\tau^{-1}})\}^\tau\big) = T([rx/v]\{[ry]^{\tau^{-1}}\}^\tau)$$

since $[ry]^{\tau^{-1}} = r \cdot r^{\tau^{-1}-1} y^{\tau^{-1}} \in rK$, so that $urxr - [rx/v]r \in rK$. Then $uvr^2 = r^2$ since $u, v, r^2 \in K$.

Consequently, $v^{\alpha-1}e^{\tau+1} = uv^\alpha e^{\tau+1} = 1$. Here $v^{\alpha-1} \in K^{*4}$ since $p \equiv 1 \pmod 4$. However, $e^{\tau+1}$ generates $K^{*2}$ since $(\tau + 1, p^k - 1) = 2$ and $e$ generates $K^*$. This is the desired contradiction.

The case $f^t$ of (5.10) is similar but simpler. The two specializations $vX = x, Y = y$ and $vX = x, Y = ry$ lead to the relations

$$uex^{\alpha-\alpha^{-1}} - [e^{\alpha^{-1}\tau}/v^{\alpha^{-1}}] \in rK \text{ and } uex^{\alpha-1} - [1/v] \in K$$

for all $u \in K^*$. These imply that $u \in rK$ and $u \in K$ both hold, which is again a contradiction. □

## 6 An operation on planes: general case

We conclude by digressing for a brief consideration of the general case of Proposition 5.6, answering another open question in [3]:

**Theorem 6.1.** *If the* 4*-tuples* $(g_1, g_2, h_1, h_2)$ *and* $(g_1', g_2', h_1', h_2')$ *determine isomorphic semifield planes via* (5.2)*, then so do the* 4*-tuples* $(h_2^t, g_2^t, h_1^t, g_1^t)$ *and* $(h_2'^t, g_2'^t, h_1'^t, g_1'^t)$.

*Proof.* We may assume that an isomorphism of semifield planes fixes both axes. As in the proof of Proposition 5.6, we only need to consider linear transformations.

In view of these reductions, by (1.1) we are given

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} m & n \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} m' & n' \\ g' & h' \end{pmatrix} \tag{6.2}$$

for some invertible $2 \times 2$ matrices $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, where

$$\begin{aligned} g &= g_1(m) + g_2(n) \qquad & h &= h_1(m) + h_2(n) \\ g' &= g_1'(m') + g_2'(n') \qquad & h' &= h_1'(m') + h_2'(n'). \end{aligned}$$

By a tedious calculation,

$$\begin{aligned} \begin{pmatrix} -\delta & \beta \\ \gamma & -\alpha \end{pmatrix} \begin{pmatrix} x' & y' \\ g_1'^t(x') + h_1'^t(y') & g_2'^t(x') + h_2'^t(y') \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \\ = \begin{pmatrix} x & y \\ g_1^t(x) + h_1^t(y) & g_2^t(x) + h_2^t(y) \end{pmatrix}, \end{aligned} \tag{6.3}$$

which implies the theorem. We will not provide all of the manipulations required to verify (6.3), but will only discuss one of the four formulas implicit in (6.3).

From (6.2) we obtain

$$g'((\alpha m+\beta g)a+(\alpha n+\beta h)c,(\alpha m+\beta g)b+(\alpha n+\beta h)d)=(\gamma m+\delta g)a+(\gamma n+\delta h)c.$$

Set $n=0$:

$$\begin{aligned}T([(\alpha m+\beta g_1(m))a+\beta h_1(m)c]{g'_1}^t(x)+[(\alpha m+\beta g_1(m))b+\beta h_1(m)d]{g'_2}^t(x))\\ =T([(\gamma m+\delta g_1(m))a+\delta h_1(m)c]x)\end{aligned}$$

for all $m,x\in K$, so that

$$\begin{aligned}g_1^t(-\delta ax+\beta M{g'_1}^t(x)+\beta b{g'_2}^t(x))+h_1^t(-\delta cx+\beta c{g'_1}^t(x)+\beta d{g'_2}^t(x)\\ =-\alpha H{g'_1}^t(x)-\alpha b{g'_2}^t(x)+\gamma ax\end{aligned}$$

for all $x\in K$, as required in (6.3). Similar calculations with $m=0$, and using $h'$ in place of $g'$, produce the desired equality (6.3). □

Now that the above theorem is known to be true, it would be very desirable to have a conceptual proof rather than the above disgustingly computational one. Based on remarks in [3, end of Section 4], a geometric description of the new planes is needed that is different from the original one given in [3].

**Acknowledgement.** I am grateful to M. Cordero and the referees for their helpful comments.

## References

[1] R. D. Baker, J. M. Dover, G. L. Ebert, K. L. Wantz, Hyperbolic fibrations of $\mathrm{PG}(3,q)$. *European J. Combin.* **20** (1999), 1–16. MR1669584 (2000d:51017) Zbl 0923.51005

[2] R. D. Baker, G. L. Ebert, T. Penttila, Hyperbolic fibrations and $q$-clans. *Des. Codes Cryptogr.* **34** (2005), 295–305. MR2128337 (2005m:51009) Zbl 1079.51504

[3] S. Ball, G. Ebert, M. Lavrauw, A geometric construction of finite semifields. *J. Algebra* **311** (2007), 117–129. MR2309880 (2008d:51001) Zbl 1125.12002

[4] R. H. Bruck, Construction problems of finite projective planes. In: *Combinatorial Mathematics and its Applications* (*Proc. Conf., Univ. North Carolina, Chapel Hill, N.C.,* 1967), 426–514, Univ. North Carolina Press, Chapel Hill, N.C. 1969. MR0250182 (40 #3422) Zbl 0206.23402

[5] M. Cordero, G. P. Wene, A survey of finite semifields. *Discrete Math.* **208/209** (1999), 125–137. MR1725526 (2001f:12015) Zbl 1031.12009

[6] P. Dembowski, *Finite geometries*. Springer 1968. MR0233275 (38 #1597) Zbl 0159.50001

[7] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*. Dover Publications Inc., New York 1958. MR0104735 (21 #3488) Zbl 0082.24901

[8] E. H. Moore, *The subgroups of the generalized modular group*. Decennial Publ., Chicago 1903. Zbl 34.0172.02

[9] Y. Hiramine, M. Matsumoto, T. Oyama, On some extension of 1-spread sets. *Osaka J. Math.* **24** (1987), 123–137. MR881751 (88b:51008) Zbl 0646.51006

[10] N. L. Johnson, Sequences of derivable translation planes. *Osaka J. Math.* **25** (1988), 519–530. MR969015 (90c:51007) Zbl 0707.51002

[11] W. M. Kantor, On point-transitive affine planes. *Israel J. Math.* **42** (1982), 227–234. MR687128 (84f:51026) Zbl 0511.51011

[12] W. M. Kantor, Spreads, translation planes and Kerdock sets. I. *SIAM J. Algebraic Discrete Methods* **3** (1982), 151–165. MR655556 (83m:51013a) Zbl 0493.51008

[13] W. M. Kantor, Commutative semifields and symplectic spreads. *J. Algebra* **270** (2003), 96–114. MR2015931 (2004k:51003) Zbl 1041.51002

[14] W. M. Kantor, Finite semifields. In: *Finite geometries, groups, and computation*, 103–114, de Gruyter 2006. MR2258004 (2007i:51003) Zbl 1102.51001

[15] W. M. Kantor, R. A. Liebler, Semifields arising from irreducible semilinear transformations. Submitted.

[16] W. M. Kantor, M. E. Williams, New flag-transitive affine planes of even order. *J. Combin. Theory Ser. A* **74** (1996), 1–13. MR1383501 (97e:51012) Zbl 0852.51005

[17] W. M. Kantor, M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. *Trans. Amer. Math. Soc.* **356** (2004), 895–938. MR1984461 (2005e:51011) Zbl 1038.51003

[18] D. E. Knuth, Finite semifields and projective planes. *J. Algebra* **2** (1965), 182–217. MR0175942 (31 #218) Zbl 0128.25604

[19] M. E. Williams, $\mathbb{Z}_4$-linear Kerdock codes, orthogonal geometries, and non-associative division algebras. Ph.D. thesis, University of Oregon, 1995.

[20] A. Wiman, Bestimmung alle Untergruppen einer doppelt unendlichen Reihe von einfachen Gruppen. *Stock. Akad. Bihang* **25** (1900), 1–47. Zbl 31.0147.01,

Received 13 March, 2007

K. W. Kantor, Department of Mathematics, University of Oregon, Eugene, OR 97403, USA
Email: kantor@uoregon.edu