*J. Aust. Math. Soc.* **85** (2008), 333–339
doi:10.1017/S1446788708000888

# SEMIFIELDS ARISING FROM IRREDUCIBLE SEMILINEAR TRANSFORMATIONS

WILLIAM M. KANTOR ✉ and ROBERT A. LIEBLER

(Received 14 February 2008; accepted 17 September 2008)

Communicated by Martin W. Liebeck

Dedicated to Cheryl Praeger for her sixtieth birthday

**Abstract**

A construction of finite semifield planes of order $n$ using irreducible semilinear transformations on a finite vector space of size $n$ is shown to produce fewer than $\sqrt{n}\log_2 n$ different nondesarguesian planes.

2000 *Mathematics subject classification*: primary 51E15; secondary 15A04, 17A35.

*Keywords and phrases*: finite projective planes, semifield, semilinear transformation.

## 1. Introduction

Let $V = V_K$ be a $d$-dimensional vector space over a finite field $K$. Suppose that $T \in \Gamma\mathrm{L}(V_K)$ is an *irreducible semilinear transformation*: 0 and $V$ are the only $T$-invariant subspaces of $V$. (The simplest example is $V = K$ and $T \in \mathrm{Aut}(K)$.) Then $\sum_0^{d-1} T^i K$ is a presemifield [5], so that there is a corresponding semifield plane $\pi_T$ (see Section 2 below). While it appears that there might be quite a few projective planes obtained in this manner, the purpose of this paper is to show that this is not the case.

THEOREM 1.1. *Fewer than $\sqrt{n}\log_2 n$ pairwise nonisomorphic nondesarguesian semifield planes $\pi_T$ of order $n$ are obtained from irreducible semilinear transformations $T$ on vector spaces of size $n$.*

A weaker bound announced in [6] highlighted remarks concerning the relatively small number of known semifield planes. Many standard results concerning linear transformations have been generalized to the semilinear case [4, 2], but these do not appear to give the desired information concerning irreducible transformations. In Section 3 we develop enough machinery concerning semilinear transformations to deduce the theorem.

This research was supported in part by NSF grant DMS 0753640.

## 2. Semifield planes

A finite *presemifield* is a finite vector space $V$ together with a product $a * b$ that is left and right distributive and satisfies the condition that $a * b = 0$ implies $a = 0$ or $b = 0$. This produces an affine plane (a *semifield plane* [1, Section 5.3]) with point set $V^2$ and lines $x = c$ and $y = m * x + b$. There is a simple, elegant construction of finite presemifields due to Jha and Johnson [5], using an irreducible semilinear transformation $T$ on a $d$-dimensional vector space $V$ over a finite field $K$. Namely, the set $\mathcal{S}_T := \sum_0^{d-1} T^i K$ consists of $|V|$ additive maps $V \to V$, with all nonzero maps invertible; define $a * b = f(a)(b)$, $a, b \in V$, for an arbitrary additive isomorphism $f \colon V \to \mathcal{S}_T$. This produces a presemifield and hence also an affine plane $\pi_T$. Different choices for $f$ produce isomorphic planes $\pi_T$ [1, p. 135].

We repeat the elementary proof in [6] that, if at least one of the $k_i \in K$ is not zero, then the element $\sum_0^{d-1} T^i k_i$ of $\mathcal{S}_T$ is invertible. If this transformation is not invertible then there is some nonzero vector $v$ such that $\sum_0^{d-1} T^i(k_i v) = 0$. Then there is some $j$ such that $1 \le j \le d$ and $0 \ne T^j(k_j v) = -\sum_0^{j-1} T^i(k_i v)$. Since $TK = KT$, we have $T(KT^{j-1}(v)) = KT(T^{j-1}(k_j v)) \subseteq \sum_0^{j-1} KT^i(v)$, so that the latter is a proper $T$-invariant subspace, whereas $T$ is irreducible.

If $T$ is a linear transformation then this construction produces a field in the standard manner. In general, unlike in the case of fields, if $T$ and $T'$ generate the same cyclic group then the planes $\pi_T$ and $\pi_{T'}$ might not be isomorphic since $\mathcal{S}_T$ is not $T$-invariant.

However, $\Gamma\mathrm{L}(V)$-conjugates of $T$ produce $\Gamma\mathrm{L}(V)$-conjugate sets $\mathcal{S}_T$ and hence isomorphic planes $\pi_T$ (but not conversely, as is easily seen using $\mathrm{GF}(|V|)$). Therefore, in the next section we focus on conjugacy of irreducible semilinear transformations.

## 3. Proof of Theorem 1.1

We begin with the following result.

PROPOSITION 3.1. *Let $T$ be an irreducible $\sigma$-semilinear transformation on a finite vector space $V$ over a finite field $K$. Then there is a decomposition*

$$V = V_1 \oplus \cdots \oplus V_t \tag{3.2}$$

*of $V$ into subspaces $V_i$ permuted cyclically by $T$ such that $T^t|_{V_1}$ is a 1-dimensional semilinear map over an extension field of $K$. Moreover, $t$ divides the order of $\sigma$, and the map $T^t|_{V_1}$ uniquely determines $T$ up to $\mathrm{GL}(V)$-conjugacy.*

PROOF. We will proceed in several steps. Throughout the proof, $V$ will always denote a vector space over $K$. Whenever a subspace of $V$ is viewed as a vector space over another field, or the field involved needs to be emphasized, we will add that field as a subscript.

STEP 1. Let $s$ be the order of $\sigma$ and $E := C_K(\sigma)$. Clearly $V$ is a vector space over $E$ and $T^s \in \mathrm{GL}(V) \le \mathrm{GL}(V_E)$. Let $\mu(x) \in E[x]$ be the minimal polynomial of $T^s$ on $V_E$. We claim that *$\mu(x)$ is irreducible*. For, if $g(x) \in E[x]$ is a proper nontrivial divisor of $\mu(x)$, then Ker $g(T^s)$ is a proper nontrivial subspace of $V_E$. Since both $K$ and $T$ commute with $g(T^s)$, they leave invariant the $K$-space Ker $g(T^s)$, contrary to the irreducibility of $T$ on $V$.

STEP 2. Let $\mu_1(x) \in K[x]$ be an irreducible factor of $\mu(x)$. Then for some $t \mid s$, $\mu(x) = \prod_{i=1}^{t} \mu_i(x)$ where the polynomials $\mu_i(x) := \mu_1^{\sigma^{i-1}}(x) \in K[x]$ are distinct and irreducible. For $1 \le i \le t$, let $V_i := \mathrm{Ker}(\mu_i(T^s))$. Then (3.2) holds with $T(V_i) = V_{i+1}$ (the subscripts are mod $t$), and $T^s$ has minimal polynomial $\mu_i(x)$ on $(V_i)_K$. Moreover, $m_1 := T^s|_{V_1}$ is $K$-linear with irreducible minimal polynomial $\mu_1(x) \in K[x]$, so that $L := K[m_1]$ is a subfield of $\mathrm{End}(V_1)$ and $V_1$ is a vector space over $L$.

We always let $v_1$ denote an arbitrary nonzero vector of $V_1$. We have

$$T^t(km_1v_1) = k^{\sigma^t} T^t(T^s(v_1)) = k^{\sigma^t} T^s(T^t(v_1)) = k^{\sigma^t} m_1 T^t(v_1)$$

for $k \in K$. It follows that $T^t|_{V_1}$ is $\rho$-semilinear on $V_1$ for an automorphism $\rho$ of $L = K[m_1]$ that coincides with $\sigma^t$ on $K$, fixes $m_1 = T^s$ and hence has the same order $s/t$ as $\sigma^t$.

STEP 3. Most of the proof now focuses on the semilinear transformation $T_1 := T^t|_{V_1}$ of $V_1$, rather than on $T$ and $V$.

The map $T_1$ *acts irreducibly on the $K$-space $V_1$*. For, let $W_1$ be a nonzero $T_1$-invariant subspace of $V_1$. Then $W_i := T^{i-1}(W_1)$ is a subspace of $V_i$ for $1 \le i \le t$, and $T(W_t) = T^t(W_1) = T_1(W_1) = W_1$. By (3.2), $W_1 \oplus \cdots \oplus W_t$ is a nonzero $T$-invariant subspace of $V$, and hence $W_1 = V_1$, as required.

STEP 4. By Step 2, $T_1$ is semilinear on $(V_1)_L$ with associated field automorphism $\rho$ of order $n := s/t$. The 'polynomial algebra' $L[T_1]$ (see [4]) is not commutative if $\rho \ne 1$. This leads us to consider the set $R$ of polynomials $f(x) = \sum_0^d x^j f_j$ with $f_j \in L$, using the *twisted product* $x^j a = a^{\rho^j} x^j$ for $a \in L$. Then $R$ is a (noncommutative) $L$-algebra having $L[T_1]$ as a homomorphic image under the substitution $x \mapsto T_1$. Jacobson [4] viewed $V$ as an $R$-module, but we will not need this point of view. We only need to know that each $f \in R$ has a degree in the usual manner, and that $f(T_1)(v_1) = \sum_0^d T_1^j f_j(v_1)$, where $T_1^j f_j$ is a composition of additive maps on $V_1$. Then $f(T_1)$ is an additive map on $V_1$, but it need not be $K$-semilinear.

STEP 5. Let $0 \ne f(x) = \sum_0^d x^j f_j \in R$, $f_j \in L$, $f_d = 1$, have minimal degree $d$ such that $f(T_1)(V_1) = 0$. Then $d \le n$ since $(T_1^n - m_1 I)(V_1) = (T^s - m_1 I)(V_1) = 0$ (by the definition of $m_1$ in Step 2). We claim that $d = n$; in fact we will show that $f(x) = x^n - m_1$.

Take $a \in L$ lying in no proper subfield, so that $a \ne a^{\rho^j}$ for $0 < j < n$. Consider $g(x) := a^{\rho^d} f(x) - f(x)a \in R$. On the one hand,

$$g(T_1)(v_1) = a^{\rho^d} f(T_1)(v_1) - f(T_1)(av_1) = a^{\rho^d} 0 - 0 = 0.$$

On the other hand, calculating in $R$ we find that

$$g(x) = \sum_0^d (a^{\rho^d} x^j) f_j - \sum_0^d x^j (f_j a) = \sum_0^d x^j (a^{\rho^{d-j}} - a) f_j$$

https://doi.org/10.1017/S1446788708000888 Published online by Cambridge University Press

has degree $< d$ since $a^{\rho^{d-d}} - a = 0$. Now $g(T_1)(V_1) = 0$ and our choice of $f(x)$ imply that $(a^{\rho^{d-j}} - a) f_j = 0$ for $0 \le j < d$. Then $f_j = 0$ for $0 < j < d$ (since $a^{\rho^{d-j}} \ne a$), so that $f(x) = x^d + f_0$. If $d < n$ then $a^{\rho^{d-0}} \ne a$, so that $f_0 = 0$, whereas $T_1^d(V_1) \ne 0$. Thus, $d = n$ and $f(x) = x^n + f_0$. Finally, since $(f_0 + m_1)(V_1) = 0$ we have $f_0 = -m_1$, as claimed.

STEP 6. We next claim that $V_1$ *has dimension one as a vector space over* $L$. Since $T_1$ acts irreducibly on $V_1$ by Step 3, it suffices to exhibit a 1-dimensional subspace of $(V_1)_L$ fixed by $T_1$.

By Step 2, $m_1 \in F := C_L(\rho)$, where $[L\colon F] = |\rho| = s/t = n$. Consequently, if $N_{L/F}\colon L \to F$ is the norm map, then there exists an element $a \in L$ such that $N_{L/F}(a) := \prod_0^{n-1} a^{\rho^j}$ equals $m_1^{-1}$.

Since $h(x) := \sum_0^{n-1} (ax)^j \in R$ has degree less than $n$, by Step 5 we have $h(T_1)(V_1) \ne 0$. Let $v \in V_1$ with $w := \sum_0^{n-1} (aT_1)^j(v) \ne 0$. Then

$$(aT_1)^n(v) = N_{L/F}(a) T_1^n(v) = N_{L/F}(a) m_1 v = v,$$

and hence

$$(aT_1)(w) = \sum_1^{n-1} (aT_1)^j(v) + (aT_1)^n(v) = \sum_1^{n-1} (aT_1)^j(v) + v = w.$$

Thus, $T_1(Lw) = Lw$, so that $Lw$ is the required $T_1$-invariant 1-space over $L$, and hence $\dim(V_1)_L = 1$.

STEP 7. Finally, we need to show that the action of $T_1$ on $V_1$ determines $T$ up to $\mathrm{GL}(V)$-conjugacy. For, if $\mathbf{B} := \{v_{i1} \mid i = 1, \ldots, d\}$ is a $K$-basis of $V_1$ and $v_{ij} := T^{j-1}(v_{i1})$, then $\{v_{ij} \mid i = 1, \ldots, d\}$ is a $K$-basis of $V_j$ for $1 \le j \le t$. If $A$ is the matrix of $T_1 = T^t|_{V_1}$ with respect to $\mathbf{B}$ then

$$v_{1i} \mapsto v_{2i} \mapsto \cdots \mapsto v_{ti} \mapsto Av_{1i}, \quad 1 \le i \le d,$$

uniquely describes $T$ up to $\mathrm{GL}(V)$-conjugacy. □

Observe that, in the notation of Steps 1 and 2, $|K| = |C_K(\sigma)|^s = |E|^{nt}$, so $|V| = |L|^t = (|K|^{\deg \mu_1})^t = |E|^{nt^2 \deg \mu_1}$.

PROOF OF THEOREM 1.1. We are given a vector space $V$ of size $n = p^r$ over the prime field $\mathrm{GF}(p)$. We will imitate the preceding proposition in order to construct semilinear transformations over subfields of $\mathrm{End}(V)$ that include all irreducible ones but also include many others. Thus, we will need a decomposition (3.2), a subfield $L$ of $\mathrm{End}(V_1)$ implicit in the statement of Proposition 3.1, a field $K$, automorphisms of $K$ and $L$ (see Step 2 of the proposition), and a semilinear transformation $T_1 = T^t|_{V_1}$ on $V_1$.

https://doi.org/10.1017/S1446788708000888 Published online by Cambridge University Press

Choose a factorization $r = te$ with $e > 1$ and $t|e$; the number of these factorizations is the number $\tau(r) - 1$ of positive divisors of $r$ other than 1. Fix a decomposition (3.2) of $V$ into subspaces $V_i$ of size $p^e$. Fix a subfield $L \cong \mathrm{GF}(p^e)$ of $\mathrm{End}(V_1)$, so that $V_1$ is an $L$-vector space. Given $e$, all such decompositions and fields are $\mathrm{GL}(r, p)$-conjugate.

Choose a subfield $K \neq \mathrm{GF}(p)$ of $L$.

Choose $1 \neq \sigma' \in \mathrm{Aut}(L)$ such that $\sigma'|_K \neq 1$ has order divisible by $t$. Let $\rho := \sigma'^t$. (Thus, $\sigma := \sigma'|_K \in \mathrm{Aut}(K)$ and $\rho \in \mathrm{Aut}(L)$ satisfy $\sigma^t = \rho|_K$, as required in Step 2 of the proof of Proposition 3.1. According to that step we should also require that $|\sigma^t| = |\rho|$, but we will ignore this restriction in our estimates.)

Extend the action of $K$ from $V_1$ in order to make $V$ and all $V_i$ vector spaces over $K$. All such extensions are $\mathrm{GL}(r, p)$-conjugate.

Choose $\ell \in L^*$, and let $T_1 \in \mathrm{End}(V_1)$ be $v \mapsto \ell v^\rho$, $v \in V_1$ (see Proposition 3.1). We can restrict the choice of $\ell$ as follows. If $M_a : v \mapsto av$, $a \in L^*$, then $M_a^{-1} T_1 M_a : v \mapsto \ell a^{\rho-1} v^\rho$. Since we require different conjugacy classes of transformations $T_1$, we can restrict $\ell$ to a set $\Lambda(e, \rho)$ of

$$|L^*/(L^*)^{\rho-1}| = |C_{L^*}(\rho)| = p^{e/|\rho|} - 1$$

coset representatives of $(L^*)^{\rho-1}$ in $L^*$.

Up to conjugacy in $\mathrm{GL}(r, p)$, the choices made above uniquely determine $T_1 = T^t|_{V_1}$, and hence also $T$ by the last part of Proposition 3.1. (However, we emphasize that a $\sigma$-semilinear map obtained in this manner need not be irreducible on $V_K$.) Thus, the number of $\mathrm{GL}(r, p)$-conjugacy classes of pairs $K, T$, with $T$ an irreducible $K$-semilinear transformation that is not linear is at most

$$\sum_{e|r, e\neq 1} \sum_{\sigma' \neq 1} |\Lambda(e, \sigma'^t)| (\# K \subseteq L, \sigma'|_K \neq 1). \tag{3.3}$$

There are $\tau(r) - 1$ choices for $e$ and $L$, and then at most $e - 1$ choices for $\sigma'$, at most $\tau(e) - 1$ subfields $K$, and $p^{e/|\rho|} - 1$ elements in $\Lambda(e, \rho)$, where again $\rho = \sigma'^t$. Clearly, $p^{e/|\rho|} - 1$ dominates the corresponding term in (3.3). This is at most $p^{r/3} - 1$ unless $\sigma'$ has order 2 and either

(i) $|L| = p^r$, $t = 1$, $\rho = \sigma'$ has order 2 and $|\Lambda(e, \rho)| = p^{r/2} - 1$; or
(ii) $|L| = p^{r/2}$, $t = 2$, $\rho = 1$, $|\sigma'| = 2$ and $|\Lambda(e, \rho)| = p^{r/2} - 1$.

Possibilities (i) and (ii) together contribute at most $2(p^{r/2} - 1)(\tau(r) - \tau(r/2))$ to (3.3). Then (3.3) is easily bounded as required in the theorem if $r$ is not too small, leaving a few cases to be handled by a slightly more detailed and tedious examination of (3.3). □

## 4. Concluding remarks

We conclude with some elementary observations concerning the semifields $\mathcal{S}_T$ and our arguments.

https://doi.org/10.1017/S1446788708000888 Published online by Cambridge University Press

REMARK 4.1. Note that $\pi_{kT} \cong \pi_T$, $\pi_{T+kI} \cong \pi_T$ and $\pi_{T^{-1}} \cong \pi_T$ for all $k \in K^*$, since $\mathcal{S}_{kT} = \mathcal{S}_T$, $\mathcal{S}_{T+kI} = \mathcal{S}_T$ and $\mathcal{S}_{T^{-1}} T^{d-1} = \mathcal{S}_T$. Thus, as in the desarguesian case, there are isomorphisms among the planes $\pi_T$ that do not arise from conjugate semilinear transformations.

REMARK 4.2. As in Section 2, if we fix $0 \neq e \in V$ then we obtain a presemifield operation on $V$ from $\mathcal{S}_T$ via $a * b = g(a)(b)$, $a, b \in V$, using the additive isomorphism $g\colon V \to \mathcal{S}_T$ defined by $g(A(e)) = A$ for $A \in \mathcal{S}_T$. Then

$$A(e) * v = A(v) \quad \text{for all } A \in \mathcal{S}_T, v \in V,$$

gives a simple description of our operation. In fact, this turns $V$ into a semifield with identity element $e$, since $e * v = I(e) * v = I(v)$ and $A(e) * e = A(e)$ for all $v$ and $A$.

REMARK 4.3. It is straightforward to extend the action of $L$ in Proposition 3.1 from $V_1$ to all of $V$ so as to make all $V_i$ into 1-dimensional $L$-spaces. However, as has been pointed out to us by Dempwolff via an example [3], there can be irreducible semilinear transformations over $K$ that are not semilinear over any such extension field $L$.

Nevertheless, a simple way to obtain a candidate for an irreducible $\sigma$-semilinear map on a vector space $V$ over a field $K$ is to use $\sigma$-semilinearity together with the requirement

$$T\colon v_1 \mapsto v_2 \mapsto \cdots \mapsto v_t \mapsto m v_1 \tag{4.1}$$

for some basis $\{v_1, \ldots, v_t\}$ of $V$ and some $m \in K$. If $t > 1$ in (4.1), it is easy to check that the corresponding semilinear map has no invariant 1-space if and only if $m \notin K^{1+\sigma+\cdots+\sigma^{t-1}}$. In this case, if $t = 2$ then the corresponding semifield was discovered by Knuth [7].

REMARK 4.4. Similarly, we can obtain many irreducible semilinear transformations by assuming $\sigma$-semilinearity in (4.1).

PROPOSITION 4.2. *Let $V$ be a vector space over $K$ with basis $v_1, \ldots, v_t$, and let $\sigma \in \mathrm{Aut}(K)$ and $\rho = \sigma^t$. If $m \in K$ with $m^{\sigma^j - 1} \notin K^{\rho - 1}$ for $1 \le j < t$, then (4.1) defines an irreducible $\sigma$-semilinear transformation on $V$ with associated field automorphism $\sigma$.*

PROOF. Suppose that $W$ is a nonzero $T$-invariant subspace of $V$. Let $0 \neq \sum_1^t k_i v_i \in W$, $k_i \in K$, with the minimum number of $k_i \neq 0$. Using $T$ we may assume that $k_1 = 1$. By (4.1) and the fact that $W$ is $T^t$-invariant,

$$T^t\left(\sum_1^t k_i v_i\right) - m \sum_1^t k_i v_i = \sum_2^t (k_i^\rho m^{\sigma^{i-1}} v_i - k_i m v_i)$$

lies in $W$ and has smaller support, and hence is zero. Then $k_i^\rho m^{\sigma^{i-1}} = k_i m$ for $2 \le i \le t$. If some such $k_i \neq 0$ then $m^{\sigma^{i-1}-1} = 1/(k_i^{\rho-1})$, contradicting our condition on $m$.

https://doi.org/10.1017/S1446788708000888 Published online by Cambridge University Press

Thus, $v_1 \in W$. Applying $T$ shows that all $v_i \in W$, so that $W = V$. □

REMARK 4.5. We conclude with a very elementary but weaker version of Theorem 1.1 (compare to [6, Theorem 6.2]) having a less informative proof.

PROPOSITION 4.3. *Given a vector space $V$ of size $n$ over a prime field* $\mathrm{GF}(p)$, *there are fewer than $n \log_p^2 n$ conjugacy classes of pairs $(K, T)$ consisting of a field $K \subseteq \mathrm{End}(V)$ over which $V$ is a vector space and an irreducible semilinear transformation $T$ on $V_K$.*

PROOF. Let $d = \dim_K V$. Let $T$ be an irreducible $\sigma$-semilinear transformation of $V_K$. Fix a nonzero vector $v$. Then $\{T^i(v) \mid 0 \le i < d\}$ is a basis of $V$ (in Section 2 we saw that $\sum_0^{d-1} k_i T^i(v) = 0$, $k_i \in K$, implies that all $k_i = 0$).

Write $T^d(v) = \sum_0^{d-1} k_i T^i(v)$ with $k_i \in K$. Since $T^i(kv) = k^{\sigma^i} T^i(v)$ for each $i$ and each $k \in K$, the $k_i$ completely determine $T$.

Thus, $T$ is determined by the following choices: a field $K = \mathrm{GF}(p^e)$ over which $V$ is a vector space, an automorphism $\sigma$ of $K$, and a choice of $d = r/e$ elements $k_i \in K$, where $|V| = p^r$. There are at most $r$ divisors $e$ of $r$, at most $e$ choices for $\sigma$, and then $|V|$ choices for the $k_i$. Choosing a $K$-basis of $V$ amounts to conjugating in $\mathrm{GL}(V_K)$ and hence in $\mathrm{GL}(r, p)$. Consequently, the number of $\mathrm{GF}(p)$-conjugacy classes of pairs $(K, T)$ is less than $rr|V| = |V| \log_p^2 |V|$, as required. □

Unlike in the proof of Proposition 3.1, this argument used all $|K|^d = p^r$ possible $d$-tuples $(k_1, \ldots, k_d)$, which is independent of the choice of $K$ and $\sigma$.

## Acknowledgement

We are grateful to U. Dempwolff for very helpful comments.

## References

[1] P. Dembowski, *Finite Geometries* (Springer, Berlin, 1968).
[2] U. Dempwolff, 'Normalformen semilinearer operatoren', *Math. Semesterber.* **46** (1999), 205–214.
[3] ———, Private communication, 2008.
[4] N. Jacobson, 'Pseudo-linear transformations', *Ann. Math.* **38** (1943), 484–507.
[5] V. Jha and N. L. Johnson, 'An analog of the Albert–Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem', *Algebras Groups Geom.* **6** (1989), 1–35.
[6] W. M. Kantor, 'Finite semifields', in: *Finite Geometries, Groups, and Computation*, Proc. Conf., Pingree Park, CO, September 2005 (eds. A. Hulpke *et al.*) (de Gruyter, Berlin, 2006), pp. 103–114.
[7] D. E. Knuth, 'Finite semifields and projective planes', *J. Algebra* **2** (1965), 182–217.

WILLIAM M. KANTOR, Department of Mathematics, University of Oregon, Eugene, OR 97403, USA
e-mail: kantor@math.uoregon.edu

ROBERT A. LIEBLER, Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA
e-mail: liebler@math.colostate.edu