A Note on Semifield Planes Admitting Irreducible Planar Baer Collineations

Ulrich Dempwolff

Abstract

In this note we study finite semifield planes which admit an irreducible planar Baer collineation. This continues previous work of N. Johnson [5].

1 Introduction

In [5] N. Johnson investigates semifield planes of order $q^4, q = p^f, p$ a prime which have rank 2 over the kernel and which admit a planar Baer collineation π of order r, where r is a p-primitive prime divisor of $q+1$. He proves that such planes are obtained from semifield panes of order q^2 and rank 2 by an elegant construction due to Hiramine et. al. [3] (and generalized by Johnson [6]). In this note we remove the restriction on the rank and weaken slightly the assumption on π by assuming that π is an irreducible Baer collineation, that is π acts irreducible on $[X, \pi]$ for any fiber X being fixed by π. In section 2 we show that these planes have usually a structure which is a natural generalization of the rank 2 case. However there is an additional possibility which we call the indecomposable case. In section 3 we discuss a computer enumeration of semifield planes of order 2^8 and 5^4 which admit an irreducible Baer collineation. We find examples which are genuinely of rank 4, i.e. can not be obtained from a rank 2 example by the operations associated with the cubical array of a semifield [8]. In section 4 we present three series of semifield planes genuinely of rank ≥ 4 admitting irreducible Baer collineations. While two series belong to known classes of semifield planes a third series generalizes some examples of section 3 and it seems that this class has not been described in the literature before.

2 Irreducible planar Baer collineations on semifield planes

Set $V = K^n$, $K = \mathrm{GF}(p)$, p a prime and let $\Sigma \subseteq \mathrm{GL}(V) \cap 0$ be a spread set of a (pre–)semifield, i.e. Σ is an additive group. Let $\psi : V \to \Sigma$ be an arbitrary group isomorphism. Then we can associate with Σ a pre–semifield $S = S(\Sigma)$: the additive group is $(V, +)$ and the semifield multiplication is defined by $x * y = x\psi(y)$.

Set $W = V^2$ and define as usual by $\mathcal{S} = \mathcal{S}_\Sigma = \{V(\infty), V(\sigma) \mid \sigma \in \Sigma\}$ the associated spread. Here $V(\infty) = 0 \times V$ and $V(\sigma) = \{(v, v\sigma) \mid v \in V\}$, $\sigma \in \Sigma$ (the notation agrees with [9]). Finally, we denote by $\mathbf{P} = \mathbf{P}(W, \mathcal{S}) = \mathbf{P}_\Sigma$ the translation plane defined by $\mathcal{S}$.

Let $\pi \in \mathrm{GL}(W)$ induce a planar Baer collination, i.e. $n = 2m$, $\dim W_0 = \dim W_1 = n$ where $W_0 = C_W(\pi) = \ker(\pi - 1)$, $W_1 = [W, \pi] = \mathrm{Im}(\pi - 1)$ and π fixes $p^m + 1$ fibers. Let Y be any fiber which is fixed by π. We call π an *irreducible* planar Baer collineation if π as a $\mathrm{GF}(p)$-linear Operator is irreducible on $Y \cap W_1$; i. e. $Y = (Y \cap W_1) \oplus (Y \cap W_0)$. We choose our notation such that $V(\infty)$ and $V(0)$ are fixed by π. Following Johnson [5] we choose bases of these spaces according to the decompositions $V(0) = (V(0) \cap W_1) \oplus (V(0) \cap W_0)$ and $V(\infty) = (V(\infty) \cap W_0) \oplus (V(\infty) \cap W_1)$. Hence:

Lemma 2.1. *With the assumptions from above one has:*

(a) With respect to the decomposition $W = V(0) \oplus V(\infty)$ *the collineation* π *has a matrix* $\mathrm{diag}(\mathcal{X}, \mathcal{Y})$, $\mathcal{X}, \mathcal{Y} \in \mathrm{GL}(n, p)$, *with* $\mathcal{X} = \mathrm{diag}(P, 1)$, $\mathcal{Y} = \mathrm{diag}(1, Q)$, $P, Q \in \mathrm{GL}(m, p)$ *and* $|\pi| = |P| = |Q|$.

(b) The matrix representation $T : \Sigma \to K^{n \times n}$ *has the form*

$$T(\sigma) = \begin{pmatrix} T_{11}(\sigma) & T_{12}(\sigma) \\ T_{21}(\sigma) & T_{22}(\sigma) \end{pmatrix},$$

with quadratic blocks of size m. π *acts on* $T(\Sigma)$ *by* $T(\sigma^\pi) = \mathcal{X}^{-1} T(\sigma) \mathcal{Y}$. *The maps* $T_{ij} : \Sigma \to K^{m \times m}$ *are* π*–morphisms with respect to the actions* $T_{11}(\sigma^\pi) = P^{-1} T_{11}(\sigma)$, $T_{12}(\sigma^\pi) = P^{-1} T_{12}(\sigma) Q$, $T_{21}(\sigma^\pi) = T_{21}(\sigma)$, *and* $T_{22}(\sigma^\pi) = T_{22}(\sigma) Q$.

The following result generalizes section 2 of [5].

Proposition 2.2. *We use the assumptions and the notations of the lemma:*

(a) $m = 2k$ *and* $|\pi|$ *divides* $p^k + 1$.

(b) *Set* $\Sigma_0 = C_\Sigma(\pi)$ *and* $\Sigma_1 = [\Sigma, \pi]$. *Then* $\Sigma = \Sigma_0 \oplus \Sigma_1$ *and* $|\Sigma_0| = |\Sigma_1| = p^m$.

(c) *Choosing the basis of* W *in a suitable way one has* $P = Q$. *Moreover* $L = K[Q]$ *is a subring of* $K^{m\times m}$ *which is isomorphic to* $\mathrm{GF}(p^m)$.

(d) *There exists a semifield spread set* $\overline{\Sigma} \subseteq K^{m\times m}$ *and an additive bijektion* $\alpha : L \to \overline{\Sigma}$ *with:*

$$T(\Sigma_0) = \left\{ \begin{pmatrix} 0 & u \\ \alpha(u) & 0 \end{pmatrix} \mid u \in L \right\}$$

(e) *We have a* π*–morphism* $\beta : T_{11}(\Sigma_1) \to T_{12}(\Sigma_1)$ *such that*

$$T(\Sigma_1) = \left\{ \begin{pmatrix} u & \beta(u) \\ 0 & u^{p^k} \end{pmatrix} \mid u \in L \right\}.$$

Moreover there exists a matrix $B \in K^{m\times m}$ *such that* $\beta(u) = \sum a_i Q^{-i} B Q^i$ *where* u *has the form* $u = f(Q)$, $f \in K[X]$, $f = \sum a_i X^i$.

(f) *Let* $|\pi| = p^k + 1$. *Then* $\beta = 0$ *(i.e.* $B = 0$*) for* $p > 2$. *For* $p = 2$ *let* π *act via conjugation with* Q *on* $K^{m\times m}$. *There exists a* π*–subspace* U *of* $K^{m\times m}$ *of order* 2^{3m} *with* $B \in U$.

Proof. By our assumptions π is a p'-element and $\Sigma = \Sigma_0 \oplus \Sigma_1$ by the theorem of Maschke.

Let $0 \neq \sigma \in \Sigma_0$. Then $T_{11}(\sigma) = P^{-1}T_{11}(\sigma)$, $T_{12}(\sigma) = P^{-1}T_{12}(\sigma)Q$ and $T_{22}(\sigma) = T_{22}(\sigma)Q$. This implies $T_{11}(\sigma) = T_{22}(\sigma) = 0$ and $T_{12}(\sigma), T_{21}(\sigma) \in \mathrm{GL}(m, p)$. Moreover there exist $\lambda, \mu \in \mathrm{GF}(p^m)$ having the order of $|\pi|$, such that $\lambda, \lambda^p, \ldots, \lambda^{p^{m-1}}$ are the eigenvalues of P and $\mu, \mu^p, \ldots, \mu^{p^{m-1}}$ are the eigenvalues of Q. Since both operators are irreducible the eigenvalues in either case are pairwise different. Act with π on $K^{m\times m}$ via $X^\pi = P^{-1}XQ$. Then $T_{12}(\sigma)$ is fixed under this action. As π has on $K^{m\times m}$ the eigenvalues $\lambda^{-p^i}\mu^{p^j}$, $0 \leq i, j \leq m-1$ we must have $\lambda^{p^i} = \mu^{p^j}$ with i, j suitable chosen.

Then P and Q have the same minimal polynomial over K and are therefore conjugate in $\mathrm{GL}(m,p)$. By choosing an appropriate basis of $V(0)\cap W_1$ we can assume $P=Q$. Again as Q is irreducible $L=K[Q]\simeq \mathrm{GF}(p^m)$ and $C_{K^{m\times m}}(Q)=L$. Thus $T_{12}(\sigma)\in L$. (b), (c) and (d) follow.

Assume now $0\neq\sigma\in\Sigma_1$. Since $\Sigma_1=[\Sigma_1,\pi]$ we see $T_{21}(\sigma)=0$. Then there exist $A,C\in \mathrm{GL}(m,p)$ and $B\in K^{m\times m}$ with

$$T(\sigma)=\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}.$$

The transformation $\mathrm{diag}(1,A,C^{-1},1)\in \mathrm{GL}(W)$ commutes with π. Considering the associated basis transformation we may assume $A=C=1$. As $\Sigma_1=\langle\sigma^{\pi^i}\mid i=0,1,2,\ldots\rangle$ we see that β has the form described in (e).

Suppose Q and Q^{-1} have different minimal polynomials over K. Then we have a $f=\sum_i a_iX^i\in K[X]$ with $f(Q^{-1})=0\neq f(Q)$ and

$$T\Big(\sum_i a_i\sigma^{\pi^i}\Big)=\begin{pmatrix} 0 & * \\ 0 & f(Q) \end{pmatrix}\in\Sigma_1,$$

a contradiction. Hence there exists a k with $\lambda^{-1}=\lambda^{p^k}$, i.e. $\lambda^{p^k+1}=1$ respectively. Thus $|\pi|=|Q|$ is a divisor of $(p^{2k}-1,p^m-1)=p^t-1$, where $t=(2k,m)$. Irreducibility implies $m=2k$ and $|\pi|$ divides p^k+1. (a) and (e) follow.

Assume finally $|\pi|=p^k+1$ and consider first the case $p>2$. Pick $0\neq\sigma\in\Sigma_1$ as above. Then $Q_0=Q^{(p^k+1)/2}=-1$ and $-2^{-1}[T(\sigma),\pi^{(p^k+1)/2}]=1\in\Sigma_1$ which implies $B=0$.

Now consider the case $p=2$ and assume $B\neq 0$. Then the mappings T_{11},T_{12},T_{22} are all π–monomorphisms into $K^{m\times m}$. Hence $T_{11}(\Sigma_1)\simeq T_{12}(\Sigma_1)\simeq T_{22}(\Sigma_1)$ as π–modules. The lemma shows that $T_{11}(\Sigma_1)$ and $T_{22}(\Sigma_1)$ are isomorphic to K^m where $D:\langle\pi\rangle\to \mathrm{GL}(K^m)$ is the natural action on this space via multiplication with Q. On the other hand $T_{12}(\Sigma_1)$ is a π–submodule of $\Delta=K^{m\times m}$ with the action $X^\pi=Q^{-1}XQ$. Choose $\Phi\in \mathrm{GL}(m,2)$ such that $Q^\Phi=Q^2$ (see [4], Kap. II, 7.3 Satz, p. 187). Then

$$\Delta=\bigoplus_{j=0}^{m-1}\Phi^jL,$$

is a decomposition into π–modules. Obviously, the module $\Phi^j L$ induces the representation $D^{1-2^j} \sim D^{2^j-1}$ and π has on this module the eigenvalues $\lambda^{2^j-1}, (\lambda^{2^j-1})^2, \dots, (\lambda^{2^j-1})^{2^{m-1}}$. Assume that B projects nontrivially into $\Phi^j L$. Then $\lambda^{2^j-1} \in \{\lambda, \lambda^2, \dots, \lambda^{2^{m-1}}\}$, i.e. $\lambda^{2^\ell - 2^j + 1} = 1$ with a suitably chosen ℓ. We conclude

$$2^\ell - 2^j + 1 \equiv 0 \,(\mathrm{mod}\, 2^k + 1).$$

We claim that solutions only occur for $(\ell, j) = (0,1), (k-1, 2k-1), (k+1, k)$ in that case. Then assertion (f) will follow.

In order to prove the claim we distinguish 4 cases according as to whether or not $j(\ell) \le k$ or $j(\ell) > k$. Assume first $j, \ell \le k$. Then $|2^\ell - 2^j + 1| \le 2^k$ and thus $2^\ell - 2^j + 1 = 0$. This forces $j = 1$, $\ell = 0$. Assume next $j, \ell > k$. As $2^k \equiv -1 \,(\mathrm{mod}\, 2^k + 1)$ we have $-2^{\ell-k} + 2^{j-k} + 1 \equiv 0 \,(\mathrm{mod}\, 2^k + 1)$ and hence $j = k$, $\ell = k + 1$ by the previous case. But this contradicts $j > k$. The case $\ell \le k < j$ leads to $j = 2k - 1$, $\ell = k - 1$ in a similar manner. The case $j \le k < \ell$ implies $j = k$, $\ell = k + 1$. □

Remarks. (a) Use the notation of the proposition. If $\beta = 0$ then the group $\langle \pi \rangle$ can be extended in $\mathrm{Aut}(\mathbf{P}_\Sigma)$ to a cyclic group $\langle \pi^* \rangle$ of order $p^k + 1$ of planar collineations ($\pi^* = diag(Q^*, 1, 1, Q^*)$ with $Q^* \in L$ of order $p^k + 1$).

(b) If $\mathbf{P}_\Sigma$ has the kernel $F \simeq \mathrm{GF}(q)$, $q = p^m$, and if π is a F-linear map we see that $T_{12}(\sigma^\pi) = T_{12}(\sigma)$ for $\sigma \in \Sigma$. Hence $\beta = 0$. These assumptions are satisfied in the situation of Johnson [5] and thus the results of section 2 of [5] are a consequence of proposition 2.2.

Definition. Use the notation of the proposition. We call Σ *decomposable* if $T_{12}(\Sigma_1) = 0$ (i.e. $\beta = 0$) and *indecomposable* if $T_{12}(\Sigma_1) \ne 0$ (i.e. $\beta \ne 0$). Let $\mathrm{MinRk}\,(\Sigma)$ be the minimum of the dimensions of the associated pre–semifield over the seminuclei (left, right, and middle nucleus).

Remark. Consider the cubical array associated with Σ (see Knuth [8]). Clearly, any member Σ' of the cubical array admits a planar irreducible Baer-collineation too. On the other hand the kernel of Σ and of Σ' can be different (see [1]); indeed the operations associated with a cubical array permute the roles of the left, right, and middle nuclei by the natural action of the group $\mathrm{Sym}(3)$ (recall that the left nucleus is isomorphic to the kernel of $\mathbf{P}_\Sigma$ as we are using the conventions of [9], p. 24). In order to obtain examples which are *genuinely* different from the examples provided by [5] we are interested in the following questions.

- Are there indecomposable examples?
- Are there examples Σ with $\mathrm{MinRk}\,(\Sigma) > 2$?

The next result concerns the computation of the seminuclei.

Denote by K_ℓ, K_m, K_r the left, middle and right nucleus of the pre–semifield $S = S(\Sigma)$. The multiplicative groups K_ℓ^*, K_m^*, K_r^* are isomorphic to the groups of $((0,0), L_\infty)$-homologies, $((0), V(\infty))$-homologies, and of $((\infty), V(0))$-homologies, [9], p. 24. Using coordinates we therefore obtain:

$$\begin{array}{rcl} K_\ell \simeq k_\ell & = & \{(X,Y) \in (\mathrm{GL}(n,p) \cup 0)^2 \,|\, XA = AY, A \in T(\Sigma)\} \\ K_m \simeq k_m & = & \{X \in \mathrm{GL}(n,p) \cup 0 \,|\, XT(\Sigma) \subseteq T(\Sigma)\} \\ K_r \simeq k_r & = & \{X \in \mathrm{GL}(n,p) \cup 0 \,|\, T(\Sigma)X \subseteq T(\Sigma)\} \end{array}$$

The planar collineation acts on k_m by conjugation with $\mathcal{X}$ (notation of (2.1)), on k_r by conjugation with $\mathcal{Y}$, and on k_ℓ by conjugation with $(\mathcal{X}, \mathcal{Y})$. Finally, for $u = f(Q) \in L$, $f \in K[X]$, we denote the elements of Σ_0 and Σ_1 corresponding to u by

$$s_0(u) = \begin{pmatrix} 0 & u \\ \alpha(u) & 0 \end{pmatrix}, \quad s_1(u) = \begin{pmatrix} u & \beta(u) \\ 0 & \overline{u} \end{pmatrix}$$

where $\overline{u} = u^{p^k}$.

Lemma 2.3. *Use the notation from above.*

(a) k_ℓ *is the field of pairs* $(diag(u,u), diag(u,u))$, $u \in L$ *with* $\alpha(v)u = u\alpha(v)$ *and* $\beta(v)u = u\beta(v)$ *for all* $v \in L$.

(b) k_m *is the field of matrices* $diag(u, \overline{u})$, $u \in L$ *with* $\alpha(uv) = \overline{u}\alpha(v)$ *and* $\beta(uv) = u\beta(v)$ *for all* $v \in L$.

(c) k_r *is the field of matrices* $diag(u, \overline{u})$, $u \in L$ *with* $\alpha(vu) = \alpha(v)\overline{u}$ *and* $\beta(vu) = \beta(v)\overline{u}$ *for all* $v \in L$.

Proof. (b) Suppose $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \in k_m - C_{k_m}(\pi)$. Then $0 \neq B = A^{\mathcal{X}} - A \in k_m$ and $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & 0 \end{pmatrix}$ with $\det B_{12} \neq 0 \neq \det B_{21}$. Let M be the additive group generated by $B, B^{\mathcal{X}}, B^{\mathcal{X}^2}, \ldots$. Then $|M| \geq p^m$: The row space (column space) K^m is under the natural action $Q : v \mapsto vQ$ ($Q : v^t \mapsto Qv^t$) an irreducible $\mathrm{GF}(p)\langle Q\rangle$-module. Hence $B_{12}, B_{12}Q, B_{12}Q^2, \ldots$ generate (as an additive group) a group of order $\geq p^m$. As $B^2 \in k_m - M$ we see that even $|k_m| \geq p^{m+1}$ holds. On the other hand Σ is a vectorspace over k_m. This implies $|k_m| = p^n$. Hence Σ is desarguesian. However a desarguesian spread does not admit an irreducible, planar Baer collineation, a contradiction. Hence π centralizes k_m. This shows that $0 \neq A \in k_m$ has the form $A = diag(A_1, A_2)$ with $A_i \in \mathrm{GL}(m,p)$ and $A\Sigma_i = \Sigma_i,\ i = 0, 1$. Form $As_1(1) \in \Sigma_1$ we deduce $A_1 = u \in L$ and $A_2 = \overline{u}$. Finally $As_1(v) = s_1(uv)$ implies $u\beta(v) = \beta(uv)$ for all $v \in L$. Similarly one obtains $\overline{u}\alpha(v) = \alpha(uv)$ for all $v \in L$.

(c) follows by symmetry.

(a) By considering the action of π on k_ℓ one observes as before that π centralizes k_ℓ. This shows that the elements in k_ℓ have the form $(diag(A_1, A_2), diag(B_1, B_2))$. From $diag(A_1, A_2)s_1(1) = s_1(1)diag(B_1, B_2)$ we deduce $A_i = B_i \in L$ and as $diag(A_1, A_2)s_0(1) = s_0(1)diag(A_1, A_2)$ we see $A_1 = A_2 = u \in L$. Finally we get $u\alpha(v) = \alpha(v)u$ and $u\beta(v) = \beta(v)u$ from $diag(u, u)s_i(v) = s_i(v)diag(u, u),\ i = 0, 1$. □

3 Small orders

Semifields of order 2^4 and 3^4 are known [2]. For order 2^4 the example with an irreducible planar Baer collineation has dimension 2 over the kernel. For order 3^4 all 8 examples with such collineations have $\mathrm{MinRk}\,(\Sigma) = 2$. By a straightforward computer enumeration we determined the semifield planes of order 2^8 and 5^4 with this property. We summarize the results; more details are displayed on my home page:

`www.mathematik.uni-kl.de/~dempw/dempw_IrrCol.semi.html`

Order 2^8**.** There are 14 semifield planes which admit an irreducible planar Baer collineation. They are all decomposable and for 13 of them we have $\mathrm{MinRk}\,(\Sigma) = 2$. For the remaining spread set Σ we have $\mathrm{MinRk}\,(\Sigma) = 4$. A multiplication of an associated semifield $S(\Sigma)$ (which is identified as a GF(2)–space with with $\mathrm{GF}(16)^2$) is given by:

$$(u, v) * (x, y) = (ux + v(z^{12}x + z^8\overline{x}) + \overline{v}(x + z^3\overline{x}), uy + v\overline{x})$$

Here z is a generator of $\mathrm{GF}(16)^*$ with $z^4 + z + 1 = 0$ and $\overline{x} = x^4$.

Order 5^4**.** There are 36 semifield planes which admit an irreducible planar Baer collineation. For 21 spread sets we have $\mathrm{MinRk}\,(\Sigma) = 2$. For remaining the 15 semifield planes $\mathrm{MinRk}\,(\Sigma) = 4$ holds. Moreover 9 of these semifield planes are decomposable and 6 indecomposable. We now describe the multiplication rules of the associated semifields in the case $\mathrm{MinRk}\,(\Sigma) = 4$. For this purpose we identify $S(\Sigma)$ with $\mathrm{GF}(25)^2$ and denote by z generator of $\mathrm{GF}(25)^*$ with $z^2 - z + 2 = 0$. The 9 decomposable spread sets are partitioned in 3 cubical arrays each of them having 3 members. We present the multiplication rule for representatives from each cubical array. It has the form

$$(u, v) * (x, y) = (ux + v(ay + b\overline{y}) + \overline{v}(cy + d\overline{y}), uy + v\overline{x})$$

with $(a, b, c, d) = (z^{a'}, z^{b'}, z^{c'}, z^{d'})$ and (a', b', c', d') is one of the following quadruples

$$(13, 14, 14, 22), (14, 15, 5, 6), (20, 20, 12, 19),$$

and $\overline{x} = x^5$. The 6 indecomposable spread sets represent 6 cubical arrays with one member. The multiplication has the form

$$(u, v) * (x, y) = (ux + bv\overline{y}, uy + a\overline{u}x + v\overline{x})$$

with $(a, b) \in \{(z^5, z^7), (z^{13}, z^9), (z, 1), (z^9, z^8), (z, z), (z^5, z)\}$.
In the indecomposable case it is not difficult to see that a semifield with the opposite multiplication (i.e. $(x, y) \circ (u, v) = (u, v) * (x, y)$) is isotopic to a semifield of type II in the notation of Knuth [8], p. 215.

4 Series with $\mathrm{MinRk}(\Sigma) \geq 4$

We present three series of semifield planes $\mathbf{P}_\Sigma$ admitting irreducible, planar Baer collineations and with $\mathrm{MinRk}\,(\Sigma) \geq 4$. Two of these series are described for instance by Knuth in [8] while the third series generalizes examples of the previous section.

In this section we will use Oyamas [10] description of vectors and matrices which for convenience we sketch briefly. Let $F = \mathrm{GF}(q)$ and $E = \mathrm{GF}(q^m)$. The vectorspace F^m is identified with the F-space ${}^0F^m$ of vectors of the form $((a)) = (a, a^q, \ldots, a^{q^{m-1}}) \in E^m$, $a \in E$. The F-endomorphisms of ${}^0F^m$ form the F-space ${}^0F^{m\times m}$ of matrices $(a_{ij}) \in E^{m\times m}$ with the property $a_{i+1,j+1} = a_{ij}^q$, $0 \le i, j < m$ (indices are read modulo m). Such a matrix is determined by it's first column and thus we define $[a_0, \ldots, a_{m-1}]^t := (a_{ij})$ if $(a_0, \ldots, a_{m-1}) = (a_{00}, \ldots, a_{m-1,0})$. Set

$$T_k(a) = \sum_{i=0}^{m-1} a^{q^i} E_{k+i,i}.$$

Then $[a_0, \ldots, a_{m-1}]^t = \sum_{i=0}^{m-1} T_i(a_i)$. We have the multiplication rules

$$T_j(u)T_k(v) = T_{j+k}(u^{q^k} v), \quad T_k(a)^{-1} = T_{m-k}(a^{-q^{m-k}}),\ a \neq 0.$$

The main advantage of Oyamas notation is that the cyclic Singer group $\{T_0(u) \mid u \in E - \{0\}\}$ of order $q^m - 1$ is a group of diagonal matrices.

We apply these notations to the notions of section 2. We have $W = V \times V$ with $V = {}^0F^N \times {}^0F^N$ where $m = N \cdot r$ and $q = p^r$, p a prime. We write (u, v) for a typical element in V instead of $(((u)), ((v)))$. The matrices of a spread set will have the form

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad A, B, C, D \in {}^0\mathrm{GL}(N, F) \cup 0$$

where ${}^0\mathrm{GL}(N, F)$ is the group of invertible elements in ${}^0F^{N\times N}$. The matrices $T_0(u)$, $u \in E$, form a field L of matrices isomorphic to E (see proposition 2.2). The planar collineation π has the form $diag(T_0(u), 1, 1, T_0(u))$ where $u \in E^*$ has order $p^k + 1$ in the decomposable case (has an order dividing $p^k + 1$ in the indecomposable case).

Example 4.1. Set $K = F = \mathrm{GF}(p)$, p a prime and $E = \mathrm{GF}(p^m)$, $m = 2k$. Choose $a, b \in \{0, \ldots, m-1\}$ such that $E \neq E^{p^b+1} E^{p^{|a-b|}+1} E^{p^{b+k}-1}$ and pick $g \in E - E^{p^b+1}E^{p^{|a-b|}+1}E^{p^{b+k}-1}$. The exponents of p are always read modulo $m = 2k$ in this example. Then

$$(u, v) * (x, y) = (ux + gv^{p^a}y^{p^b}, uy + vx^{p^k})$$

defines a semifield multiplication on V. It can easily be seen that no zero divisors occur. In fact it is also not hard to see that this semifield is isotopic to a semifield defined in [8] on p. 215 by (7.16). Let Σ be the spread set associated with this semifield and $T(\Sigma)$ it's coordinatization. It has the form $T(\Sigma) = \{s(x, y) \mid x, y \in E\}$ where

$$s(x, y) = \begin{pmatrix} T_0(x) & T_0(y) \\ T_a(gy^{p^b}) & T_0(x^{p^k}) \end{pmatrix}.$$

Then Σ is invariant under π and the mappings α, β of proposition 2.2 have the form $\alpha(T_0(y)) = T_a(gy^{p^b})$ and $\beta(T_0(x)) = 0$. In particular Σ is decomposable. We have:

(1) $k_\ell \simeq \mathrm{GF}(p^{(a,m)})$, $\quad k_m \simeq \mathrm{GF}(p^{(a+k-b,m)})$, $\quad k_r \simeq \mathrm{GF}(p^{(k-b,m)})$:

By lemma 2.3 the element $s(u, 0)$ lies in k_m iff for all y

$$T_a(g(uy)^{p^b}) = \alpha(T_0(uy)) = T_0(\overline{u})\alpha(T_0(y)) = T_0(u^{p^k})T_a(gy^{p^b}) = T_a(gu^{p^{a+k}}y^{p^b}).$$

This shows $u^{p^b} = u^{p^{a+k}}$ and thus $k_m \simeq \mathrm{GF}(p^{(a+k-b,m)})$. The other assertions follow similarly.

(2) For any choice of a, b, g we have $\mathrm{MinRk}(\Sigma) < n = 2m$. If $p > 2$ or if $p = 2$ and k is odd one can choose a, b, g such that $\mathrm{MinRk}(\Sigma) = m$:

$\mathrm{MinRk}(\Sigma) = n$ and $m = 2k$ implies $(a+k-b, 2k) = (k-b, 2k) = (a, 2k) = 1$. But then $a, k-b$ are odd and 2 divides $(a+k-b, 2k)$, a contradiction.

Assume first $p > 2$ and let g be a nonsquare in E. Then $a = 2$, $b = 1$, imply $\mathrm{MinRk}(\Sigma) = m$.

Assume now $p = 2$. The condition for the existence of a semifield multiplication of the desired type is equivalent to $(2^{2k}-1, 2^{b+k}-1, 2^{|a-b|}+1, 2^b+1) > 1$. This in turn is equivalent to

$$a_2 > b_2 = k_2$$

where x_2 denotes the 2-part of a positive integer x:
Recall that $(2^x+1, 2^y-1) = 2^{(x,y)}+1$ iff $x/(x,y) \equiv 1$, $y/(x,y) \equiv 0 \,(\mathrm{mod}\, 2)$ (and $= 1$ otherwise) and $(2^x+1, 2^y+1) = 2^{(x,y)}+1$ iff $x/(x,y) \equiv y/(x,y) \equiv 1 \,(\mathrm{mod}\, 2)$ (and $= 1$ otherwise). Then $(2^{2k}-1, 2^b+1) > 1$ and $(2^{b+k}-1, 2^b+1) > 1$ imply $b_2 = k_2$ and $(2^{|a-b|}+1, 2^b+1) > 1$ implies $a_2 > b_2$. On the other hand if $a_2 > b_2 = k_2$ we observe $(2^{2k}-1, 2^{b+k}-1, 2^{|a-b|}+1, 2^b+1) = 2^{(a,b,k)}+1 > 1$. If k is odd we can take $a = 2$, $b = 1$ as before. Now (2) follows.

Conclusion. The preceding examples show that in any characteristic there exist decomposable semifield planes $\mathbf{P}_\Sigma$ with arbitrary large MinRk(Σ) and which admit irreducible planar Baer collineations.

For the next two examples we have $F = \mathrm{GF}(q)$, $E = \mathrm{GF}(q^2)$, with $q = p^k$, p a prime. We write $\overline{x}$ for x^q.

Example 4.2. First we generalize the indecomposable examples of order 5^4 from section 3. Let q be an odd prime power. Choose $a, b \in E$ such that $y^{q+1} + ay - b \neq 0$ for $y \in E$. Then the multiplication

$$(u, v) * (x, y) = (ux + bv\overline{y}, uy + a\overline{u}x + v\overline{x})$$

is a semifield multiplication of a semifield which is isotopic to an opposite semifield of Knuth type II (see [8], (7.17.II)). The semifield spread set Σ has the coordinatization $T(\Sigma) = S(a,b) = \{s(x,y) | x, y \in E\} \subseteq {}^0F^{4\times 4}$ where $s(x,y)$ is given by

$$s(x,y) = \begin{pmatrix} T_0(x) & T_0(y) + T_1(ax) \\ T_0(b\overline{y}) & T_0(\overline{x}) \end{pmatrix}.$$

The mappings α, β of proposition 2.2 have the form $\alpha(T_0(y)) = T_0(b\overline{y})$ and $\beta(T_0(x)) = T_1(ax)$. In particular we are in the indecomposable case. Assume $\pi = diag(T_0(\delta), 1, 1, T_0(\delta))$, is a planar Baer collineation.

(1) π has order 3 and divides $q+1$. The collineation is irreducible iff $q = p$ is a prime $\equiv -1 \,(\mathrm{mod}\, 3)$:

A computation shows that we must have $\delta^{q-2} = 1$, i.e. $|\pi| = 3$ as $|\pi|$ divides $p^k + 1 = q + 1$. In order to be an irreducible Baer collineation $T_0(\delta)$ must be irreducible as a K-linear operator on ${}^0F^2$ (note that this is a stronger requirement than assuming merely the irreducibility as a F-linear operator). This forces $k = 1$ and $p \equiv -1 \pmod 3$.

(2) $\mathrm{MinRk}\,(\Sigma) = 4$:

By 2.3 an element in k_m has the form $diag(T_0(w), T_0(\overline{w}))$, $w \in E$. To compute k_m we must determine these $w \in E$ with

$$T_1(a\overline{w}x) = T_0(w)T_1(ax) = T_0(w)\beta(T_0(x)) = \beta(T_0(wx)) = T_1(awx)$$

for all $x \in E$. This shows $w \in F$ and thus $k_m \simeq F$. A similar computation shows $k_r \simeq F$. To determine k_ℓ we inspect the equation

$$T_1(a\overline{w}x) = T_0(w)\beta(T_0(x)) = \beta(T_0(x))T_0(w) = T_1(awx)$$

which again forces $w \in F$. Hence $k_\ell \simeq F$ and $\mathrm{MinRk}\,(\Sigma) = 4$ follows.

Conclusion. For any odd prime $p \equiv -1 \pmod 3$ there exist indecomposable semifield planes $\mathbf{P}_\Sigma$ of order p^4 with $\mathrm{MinRk}(\Sigma) = 4$ which admit irreducible planar Baer collineations of order 3 .

Example 4.3. Now we generalize the decomposable rank 4 examples of orders 4^4 and 5^4. We consider the additive group $S(a,b,c,d) = \{s(x,y) | x, y \in E\} \subseteq {}^0F^{4\times 4}$ where $s(x,y)$ is defined by

$$s(x,y) = \begin{pmatrix} T_0(x) & T_0(y) \\ T_0(ay + b\overline{y}) + T_1(cy + d\overline{y}) & T_0(\overline{x}) \end{pmatrix}.$$

Denote by $n : E \to F$ the norm and by $tr : E \to F$ the trace. A computation shows:

$$\begin{aligned} \det s(x,y) &= n(x)^2 + n(y)^2(n(a) + n(b) - n(c) - n(d)) - n(x)n(y)tr(b) \\ &\quad -n(x)tr(ay^2) + n(y)tr((a\overline{b} - c\overline{d})y^2) \end{aligned}$$

Suppose that we have chosen the parameters a, b, c, d such that $T(\Sigma) = S(a,b,c,d)$ is the coordinatization of a (decomposable) spread set Σ. Then we deduce from proposition 2.2 that $\mathbf{P}_\Sigma$ admits an irreducible planar Baer collineation of order $q + 1$. Clearly, every seminucleus has a subfield isomorphic to F. Similar computations as in 4.1 and 4.2 show $k_\ell \simeq E$ iff $c = d = 0$,

$k_m \simeq E$ iff $a = d = 0$, and $k_r \simeq E$ iff $a = c = 0$. Therefore we have $\mathrm{MinRk}\,(\Sigma) = 4$ if at least two of the parameters a, c, d are nontrivial. The semifield multiplication has the form

$$(u, v) * (x, y) = (ux + v(ay + b\overline{y}) + \overline{v}(cy + d\overline{y}), uy + v\overline{x}).$$

The following lemma (and for $q = 5$ by section 3) shows that the parameters a, b, c, d always can be chosen such that $a, c, d \neq 0$ and that $S(a, b, c, d)$ is a spread set.

Lemma 4.4. *Use the notation of example 4.3 and assume $q > 3$ and $q \neq 5$. There exist $a, b, c, d \in E$ such that $S(a, b, c, d)$ is a spread set. In addition one can choose a, c, d to be not 0.*

Proof. We first show that one can choose $0 \neq u, v \in E$ such that the mapping $d_{u,v} : E \times E \to E$ defined by

$$d_{u,v}(x, y) = n(x) + un(y) + vy^2$$

has only the zero $(x, y) = (0, 0)$. Then we choose $a, b, c, d \in E$ such that $\det s(x, y) = n(d_{u,v}(x, y))$ for $(x, y) \in E \times E$ and that in addition $a, c, d \neq 0$. Then the assertions of the lemma follow.

Let $E = F[\alpha]$. If q is odd we can assume $\alpha^2 = t \in F - F^2$ and if q is even we can assume $\alpha^2 = t\alpha + 1$, $t \in F$, chosen suitably.

Step 1. Write elements $z \in E$ as $z = z_1 + \alpha z_2$, $z_1, z_2 \in F$. Choose $0 \neq u \in E$, $0 \neq v_2 \in F$ such that $v_2 \pm u_2 \neq 0$ and if $\mathrm{char}\, F = 2$ in addition $u_2 \neq 0$ (but otherwise arbitrary).

Assume first that q is odd. Then $n(x) = x_1^2 - tx_2^2$, $y^2 = y_1^2 + ty_2^2 + 2\alpha y_1 y_2$. This shows

$$\begin{aligned} d_{u,v}(x, y) &= n(x) + u_1 n(y) + v_1(y_1^2 + ty_2^2) + 2tv_2 y_1 y_2 \\ &\quad +\alpha((u_2 + v_2)y_1^2 + (v_2 - u_2)ty_2^2 + 2v_1 y_1 y_2). \end{aligned}$$

We now choose v_1 such that

$$Q(X, Y) = (u_2 + v_2)X^2 + 2v_1 XY + (v_2 - u_2)tY^2$$

is a anisotropic quadratic form, i.e. the discriminant $D = 4(v_1^2 - (v_2^2 - u_2^2)t)$ is a nonsquare. This shows $d_{u,v}(x, y) \in E - F$ for $(x, y) \in E \times E^*$. Hence

$d_{u,v}(x,y) \neq 0$ for $(x,y) \neq (0,0)$.

Assume now that q is even. Then $tr(\alpha) = t$, $\overline{\alpha} = \alpha^{-1}$ and $n(x) = x_1^2 + x_2^2 + tx_1x_2$, $y^2 = y_1^2 + y_2^2 + \alpha t y_2^2$. Hence

$$vy^2 = v_1(y_1^2 + y_2^2) + tv_2y_2^2 + \alpha(v_1ty_2^2 + v_2y_1^2 + v_2y_2^2 + t^2v_2y_2^2).$$

This implies

$$d_{u,v}(x,y) = R + \alpha((u_2 + tv_1 + v_2 + t^2v_2)y_2^2 + (u_2 + v_2)y_1^2 + tu_2y_1y_2)$$

with $R \in F$. Choose $v_1 \in F$ such that

$$Q(X,Y) = (u_2 + v_1t + v_2 + t^2v_2)Y^2 + (v_2 + u_2)X^2 + tu_2XY$$

is a anisotropic quadratic form. As before $d_{u,v}(x,y) \neq 0$ for $(x,y) \neq (0,0)$.

Step 2. First we observe that

$$\begin{aligned} n(d_{u,v}(x,y)) &= n(x)^2 + n(x)n(y)tr(u) + n(y)^2(n(u) + n(v)) \\ &\quad + n(x)tr(vy^2) + n(y)tr(\overline{u}vy^2). \end{aligned}$$

This shows that the parameters $a, \ldots, d$ must satisfy the equations:

$$n(u) + n(v) = n(a) + n(b) - n(c) - n(d) \tag{1.1}$$
$$tr(u) = -tr(b) \tag{1.2}$$
$$v = -a \tag{1.3}$$
$$\overline{u}v = a\overline{b} - c\overline{d} \tag{1.4}$$

Eliminating a we have:

$$n(u) = n(b) - n(c) - n(d) \tag{2.1}$$
$$tr(u) = -tr(b) \tag{2.2}$$
$$c\overline{d} = -v(\overline{b} + \overline{u}) \tag{2.3}$$

Assume first that q is odd. Then $b_1 = -u_1$ by (2.2) and by (2.3) $c = v\overline{d}^{-1}(b_2 + u_2)\alpha$ and therefore $n(c) = n(v)n(d)^{-1}(-t)(b_2 + u_2)^2$. Thus $n(d)$ must be a solution of the equation

$$X^2 + t(b_2^2 - u_2^2)X - t(b_2 + u_2)^2 n(v) = 0$$

whose discriminant is $D = (b_2+u_2)^2(t^2(b_2-u_2)^2+4tn(v))$. We claim that one can choose b_2 such that D is a square and that $b_2+u_2 \neq 0$, i.e. $a, c, d \neq 0$. This is implied by the following observation (where we choose $A = t^2$, $B = 4tn(v)$, $X = b_2 - u_2$, and $Y = 1$):

Claim: Let $Q(X, Y) = AX^2 + BY^2$ be a nondegenerate quadratic form over F. Then there exist at least 2 elements $w_1, w_2 \in F^*$ such that the value of Q at $(X, Y) = (w_i, 1)$, $i = 1, 2$, is a nontrivial square.

One knows that Q has every element in F^* precisely $q+1$ times as a value if Q is elliptic and $q-1$ times as a value if Q is hyperbolic. Consider pairs in $\mathcal{L} = F^* \times F^*$ which has the partition

$$\mathcal{L} = \bigcup_{f \in F^*} F^*(f, 1).$$

The values of Q on the elements of a class $F^*(f, 1)$ differ only by squares. The set $F^* \times \{0\} \cup \{0\} \times F^*$ produces at most $2(q-1)$ nontrivial squares. Thus Q has on $\mathcal{L}$ at least $(q-1)^2/2 - 2(q-1) = (q-1)(q-5)/2$ times as a value a nontrivial square. As $q > 5$ there are at least two classes whose values are nontrivial squares. The claim follows.

We now assume that q is even. Equations (2.1)-(2.3) lead to $u_2 = b_2$ and:

$$(b_1 + u_1)^2 + tu_2(b_1 + u_1) = n(c) + n(d) \tag{3.1}$$
$$c\overline{d} = v(\overline{b} + \overline{u}) \tag{3.2}$$

Then $c = v\overline{d}^{-1}(b_1+u_1)$ and therefore $n(d)$ must be a solution of the equation

$$X^2 + ((b_1 + u_1)^2 + tu_2(b_1 + u_1))X + (b_1 + u_1)^2 n(v) = 0.$$

Choose $b_1 = u_1 + tu_2$ and d such that $n(d) = tu_2\sqrt{n(v)}$. Then the equation holds and step 2 is done and $a, c, d \neq 0$ if we take $u_2 \neq 0$ in step 1. $\square$

Conclusion. For any prime power $q \geq 4$ there exist decomposable semifield planes $\mathbf{P}_\Sigma$ which admit irreducible planar Baer collineations of order $q+1$ and with $\mathrm{MinRk}(\Sigma) = 4$.

Remarks. We keep the notation of this section.

(a) To verify the existence the examples of 4.3 we use a particular construction in 4.4; there may be more ways to obtain such examples. However by a rough estimate we see that this special method already produces at least $q(q-1)(q^2-1)$ examples of order q^4.

(b) Our investigations rise more questions than they answer. The following problems deserve further attention:

- Find decomposable examples of order p^{4n}, p a prime, with $\mathrm{MinRk}\,(\Sigma) = 4n$. So far only for p^4, $p \geq 5$, and $\mathrm{MinRk}\,(\Sigma) = 4$ the series of 4.3 provide such examples.
- Find more indecomposable examples, in particular examples in characteristic 2 and/or examples with a large order of π.

Acknowledgment. We take the opportunity to thank Norman Johnson who pointed out to us [7] that the examples of 4.1 admit irreducible planar Baer collineations.

References

[1] S. Ball, M. Brown: *The six semifield planes associated with a semifield flock*, Adv. Math. **189** (2004), 68-87.

[2] U. Dempwolff: *Semifield planes of order 81*, to appear in J. Geom.

[3] Y. Hiramine, M. Matsumoto, T. Oyama: *On some extensions of 1–spread sets*, Osaka J. Math. **24** (1987) 123-137.

[4] B. Huppert: Endliche Gruppen I, Springer, 1973.

[5] N. Johnson: *Semifield planes of characteristic p admitting p–primitive Baer collinations*, Osaka J. Math. **26** (1989) 281-285.

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

[7] N. Johnson: private communication.

[8] D. Knuth: *Finite semifields and projective planes*, J. Algebra **2** (1965) 182-217.

[9] H. Lüneburg: Translation planes, Springer, 1980.

[10] T. Oyama: *On quasifields*, Osaka J. Math. **22** (1985) 35-54.

Adress:
Ulrich Dempwolff
FB Mathematik
Universität
67653 Kaiserslautern
GERMANY

email: dempwolff@mathematik.uni-kl.de