The autotopism group of p-primitive semifield planes

M. Cordero-Vourtsanis
Department of Mathematics
Texas Tech University
Lubbock, Texas 79409

1 Introduction

Let π denote a semifield plane of order q^2 and kernel $K \simeq \mathrm{GF}(q)$, where $q = p^r$ and p is a prime number. A p-primitive Baer collineation of π is a Baer collineation α whose order is a p-primitive divisor of $q-1$, i.e., $|\alpha| \mid q-1$ but $|\alpha| \not| \, p^i - 1$ for $1 \leq i < r$. A semifield plane of order $p^4, p > 2$, is called a **p-primitive semifield plane** if it admits a p-primitive Baer collineation. In [2] we studied isomorphism of p-primitive semifield planes and gave the exact number of nonisomorphic p-primitive semifield planes. In this article we give the autotopism group of p-primitive semifield planes and show that this group is solvable. In all known situations the autotopism group of a semifield plane is solvable (see e.g. [4]).

Let π be a p-primitive semifield plane. Then π admits a matrix spread set of the form

$$\left\{ \begin{bmatrix} u & v \\ f(v) & u^p \end{bmatrix} : u, v \in \mathrm{GF}(p^2) \right\}$$

where f is an additive function in $\mathrm{GF}(p^2)$. Thus $f(v) = f_0 v + f_1 v^p$ for some $f_0, f_1 \in \mathrm{GF}(p^2)$. We shall denote this plane by $\pi(f)$ or $\pi(f_0, f_1)$.

2 The autotopism group

Let $\pi = \pi(f_0, f_1)$ be a p-primitive semifield plane. Every autotopism of π is an automorphism of π which sends $(X, 0)$ and $(0, X)$ into $(X, 0)$ and $(0, X)$, respectively. From the proof of [2, 3.1] it follows that any element in $\mathcal{A}(\pi)$ is expressed in one of the following forms:

ARS COMBINATORIA 32(1991), pp. 57-64

$$(1) \qquad g = {}_{\sigma}\begin{bmatrix} a_1 & 0 & & \\ 0 & a_4 & & \\ & & b_1 & 0 \\ & & 0 & b_4 \end{bmatrix}$$

with $f_0 = ac^{p-1}f_0^\sigma$ and $f_1 = af_1^\sigma$ where $a = \left[\frac{a_1}{a_4}\right]^{p+1}$, $c = \frac{a_4}{b_1}$, and $\left[\frac{b_1}{a_1}\right]^p = \frac{b_4}{a_4}$

$$(2) \qquad g = {}_{\sigma}\begin{bmatrix} 0 & a_2 & & \\ a_3 & 0 & & \\ & & 0 & b_2 \\ & & b_3 & 0 \end{bmatrix}$$

with $f_0 = ac^{p-1}f_0^\sigma (f_0 \neq 0)$ and $f_1 = af_1^\sigma$ where $a = -\left[\frac{a_3}{a_2}\right]^{p+1} \frac{1}{f_0^{p+1} - f_1^{p+1}}$, $c = \frac{a_2 t f_0}{b_2}$ and $\frac{b_2}{a_2} = \left[\frac{b_3}{a_3}\right]^p$, or $f_0 = 0$ and $f_1 = af_1^\sigma$ where $a = \left[\frac{a_3}{a_2 f_1}\right]^{p+1}$ and $\left[\frac{b_2}{a_2}\right] = \left[\frac{b_3}{a_3}\right]^p$,

$$(3) \qquad g = {}_{\sigma}\begin{bmatrix} a_1 & 0 & & \\ 0 & a_4 & & \\ & & 0 & b_2 \\ & & b_3 & 0 \end{bmatrix}$$

with $f_0 = 0$, $f_1 = a(f_1^p)^\sigma$ where $a = \left(\frac{a_1}{a_4}\right)^{p+1}$ and $\frac{a_4}{b_2} = \left[\frac{a_1}{b_3}\right]^p f_1^\sigma$,

$$(4) \qquad g = {}_{\sigma}\begin{bmatrix} 0 & a_2 & & \\ a_3 & 0 & & \\ & & b_1 & 0 \\ & & 0 & b_4 \end{bmatrix}$$

with $f_0 = 0$, $f_1 = a(f_1^p)^\sigma$ where $a = \left[\frac{b_1}{b_4}\right]^{p+1}$ and $\frac{b_4}{a_2} = \left[\frac{b_1}{a_3}\right]^p f_1^\sigma$,

Here σ is an automorphism of $GF(p^2)$; thus either $\sigma = 1$ or $\sigma : x \to x^p$. Therefore, if g and h are two semilinear autotopisms (with $\sigma \neq 1$), then $g \cdot h$ is a linear autotopism. Therefore, if there exists a nonlinear autotopism g_0 of π then every autotopism of π is either linear or is the product of a linear autotopism by g_0. Thus, it is enough to determine the linear autotopisms and whether there exists one autotopism which is not linear.

With respect to the four different types of autotopism, notice that if h_1 and h_2 are both linear autotopisms of the same type then $h_1 \cdot h_2$ is a linear autotopism of type 1. Thus, if h_0 is a linear autotopism of type $i, i \in \{2,3,4\}$, then any other linear autotopism of type i is the product of h_0 by a linear autotopism of type 1. Hence, to determine the linear autotopisms it suffices to study the linear autotopisms of type 1 and the existence of a linear autotopism of type i for $i \in \{2,3,4\}$.

Every p-primitive semifield plane $\pi = \pi(f_0, f_1)$ admits linear autotopisms of type 1 as we will show. Notice that if k is a linear autotopism of type 1 then letting $w = b_1/a_1$ we have $b_1 = a_1 w$ and $b_4 = a_4 w^p$ and k is of the form

$$k = \begin{bmatrix} x & 0 & & \\ 0 & y & & \\ & & xw & 0 \\ & & 0 & yw^p \end{bmatrix}$$

with $x, y, w \in \mathrm{GF}(p^2) - \{0\}, (x/y)^{p+1} = a$ and $y/xw = c$. We denote this matrix by $M(x, y, w)$ and by H the following subgroup of $\mathcal{A}(\pi) : H = \langle M(x, y, w) : (x/y)^{p+1} = a$ and $y/xw = c\rangle$ for a given value of $a \in \mathrm{GF}(p)$ and $c \in \mathrm{GF}(p^2)$.

For linear autotopisms of types 3 and 4, we have that a p-primitive semifield plane $\pi = \pi(f_0, f_1)$ admits linear autotopisms of types 3 and 4 if and only if $f_0 = 0$ and $f_1 = af_1^p$ for some $a \in \mathrm{GF}(p) - \{0\}$. Taking the $(p+1)$-st power in each side of this last equality, we get $f_1^{p+1} = a^2 f_1^{p+1}$; hence $a^2 = 1$. Since $f_0 = 0$ then $f_1 \notin \mathrm{GF}(p)$ [2, 2.2]. Hence a cannot be 1, thus $a = -1$ and $f_1^{p-1} = -1$.

Now we describe the autotopism group of any p-primitive semifield plane by considering the following cases:

a) $f_0 = 0$,

b) $f_1 = 0$,

c) $f_0 \neq 0$ and $f_1 \neq 0$.

Case $a : f_0 = 0$.

π admits linear autotopisms $M(x, y, w)$ of type 1 with $(x/y)^{p+1} = a = 1$ and any value of c since $f_0 = 0$. Since there are $p^2 - 1$ possible values for each of x and w, and for every x there are $p + 1$ values of y such that $(x/y)^{p+1} = 1$, we have that $|H| = (p^2 - 1)^2(p + 1)$.

It can be shown by an easy calculation that the transformation

$$g = \begin{bmatrix} 0 & 1 & & \\ f_1 & 0 & & \\ & & 0 & 1 \\ & & f_1 & 0 \end{bmatrix}$$

is a linear autotopism of π of type 2.

By our remarks early, we have that π admits a linear autotopism of types 3 and 4 if and only if $f_1^{p-1} = -1$.

If $f_1^{p-1} = -1$ then it follows by straightforward computation that the following transformations h and k are linear autotopisms of π of type 3 and 4, respectively:

$$h = \begin{bmatrix} -1 & 0 & & \\ 0 & e & & \\ & & 0 & e \\ & & f_1 & 0 \end{bmatrix}$$

where e is an element of $\mathrm{GF}(p^2)$ of order $2(p+1)$.

$$k = g \cdot h = \begin{bmatrix} 0 & e & & \\ -f_1 & 0 & & \\ & & f_1 & 0 \\ & & 0 & ef_1 \end{bmatrix}$$

Also, by direct computation, we obtain that the semilinear transformation

$$\ell = {}_{\sigma}\begin{bmatrix} 1 & 0 & & \\ 0 & e & & \\ & & 1 & 0 \\ & & 0 & e \end{bmatrix}$$

where e is an element in $\mathrm{GF}(p^2)$ of order $2(p+1)$ and $\sigma \neq 1$ is an autotopism of π. Therefore, by our remarks above,

$$\mathcal{A}(\pi) = \langle g, h, \ell \rangle \cdot H, H \triangleleft \mathcal{A}(\pi) \text{ and } \mathcal{A}(\pi)/H \simeq \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Hence $|\mathcal{A}(\pi)| = 8(p^2-1)^2(p+1)$.

If $f_1^{p-1} \neq -1$ then the semilinear transformation

$$\ell = {}_{\sigma}\begin{bmatrix} 0 & 1 & & \\ f_1^p & 0 & & \\ & & 1 & 0 \\ & & 0 & 1 \end{bmatrix}$$

with $\sigma \neq 1$ is an autotopism of π which is not linear. In this case $\mathcal{A}(\pi) = \langle g, \ell \rangle \cdot H$ and it has order $4(p^2-1)^2(p+1)$.

Case b: $f_1 = 0$

π admits linear autotopisms $M(x, y, w)$ of type 1 with $ac^{p-1} = 1$ and therefore $a^2 = 1$. Given a, for each of the $p^2 - 1$ values of x, there are $p+1$ vales of y such that $(x/y)^{p+1} = a$ and for every pair (x, y) there are $p-1$

values of w such that $a \cdot (y/xw)^{p-1} = 1$. Therefore $|H| = 2(p+1)(p-1)(p^2-1) = 2(p^2-1)^2$. The linear transformation

$$g = \begin{bmatrix} 0 & 1 & & \\ f_0 & 0 & & \\ & & 0 & f_0 \\ & & f_0^{p+1} & 0 \end{bmatrix}$$

is a linear autotopism of π of type 2, and since $f_0 \neq 0$, π admits no linear autotopism of types 3 and 4.

The semilinear transformation

$$\ell = \sigma\begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & f_0 & 0 \\ & & 0 & f_0^p \end{bmatrix}$$

with $\sigma \neq 1$ is an autotopism of π.

Therefore $\mathcal{A}(\pi) = \langle g, \ell \rangle \cdot H$ and it has order $8(p^2-1)^2$.

Case c: $f_0 \neq 0$ and $f_1 \neq 0$

π admits linear autotopisms $M(x,y,w)$ of type 1 with $(x/y)^{p+1} = a = 1$ and $(y/xw)^{p-1} = c^{p-1} = 1$. For each of the p^2-1 possible values of x, there are $p+1$ values of y such that $(x/y)^{p+1} = 1$ and $p-1$ values of w such that $(y/xw)^{p-1} = 1$. Thus $|H| = (p^2-1)^2$. The linear transformation

$$g = \begin{bmatrix} 0 & 1 & & \\ s & 0 & & \\ & & 0 & u \\ & & u^p s & 0 \end{bmatrix}$$

where $u = tf_0$ ($t^{p-1} = -1$) and s is an element in GF(p^2) with the property that $s^{p+1} = f_1^{p+1} - f_0^{p+1}$ (by [2, 2.2], $s \neq 0$) is an autotopism of π of type 2. Since $f_0 \neq 0$, there is no linear autotopism of π of types 3 and 4.

π admits a nonlinear autotopism if and only if $f_1 = af_1^p$ for some $a \in$ GF(p)$-\{0\}$. Taking the ($p+1$)-st power in both sides, we get $f_1^{p+1} = a^2 f_1^{p+1}$ and thus $a^2 = 1$. Hence, the condition is now $f_1^{2(p-1)} = 1$.

Therefore, if $f_1^{2(p-1)} \neq 1$, π does not admit a nonlinear autotopism, and the autotopism group is given by

$$\mathcal{A}(\pi) = \langle g \rangle \cdot H$$

and has order $2(p^2-1)^2$.

If $f_1^{2(p-1)} = 1$ then π admits a nonlinear autotopism; in particular, the semilinear transformation

$$\ell = \sigma\begin{bmatrix} z & 0 & & \\ 0 & 1 & & \\ & & v & 0 \\ & & 0 & (\frac{v}{z})^p \end{bmatrix}$$

where $v = \frac{f_0}{f_1}$ and z is an element in GF(p^2) such that $z^{p+1} = f_1^{p-1}$ and $\sigma \neq 1$ is a nonlinear autotopism of π. In this case,

$$\mathcal{A}(\pi) = \langle g, \ell \rangle \cdot H$$

and $|\mathcal{A}(\pi)| = 4(p^2-1)^2$.

We have completed the proof of the following theorem.

Theorem 2.1 *Let $\pi = \pi(f_0, f_1)$ be a p-primitive semifield plane and let $\mathcal{A}(\pi)$ be its autotopism group.*

Let

$$M(x,y,w) = \begin{bmatrix} x & 0 & & \\ 0 & y & & \\ & & xw & 0 \\ & & 0 & yw^p \end{bmatrix}$$

where $x, y, w \in GF(p^2) - \{0\}$.

(i) If $f_0 = 0$ and $f_1^{p-1} = -1$ then $\mathcal{A}(\pi) = \langle g, h, \ell \rangle \cdot H$ where

$$g = \begin{bmatrix} 0 & 1 & & \\ f_1 & 0 & & \\ & & 0 & 1 \\ & & f_1 & 0 \end{bmatrix}, \quad h = \begin{bmatrix} -1 & 0 & & \\ 0 & e & & \\ & & 0 & e \\ & & f_1 & 0 \end{bmatrix}, \quad |e| = 2(p+1)$$

$$\ell = \sigma\begin{bmatrix} 1 & 0 & & \\ 0 & d & & \\ & & 1 & 0 \\ & & 0 & d \end{bmatrix}$$

where $|d| = 2(p+1)$ and $\sigma \neq 1$, and $H = \langle M(x,y,w) : (x/y)^{p+1} = 1 \rangle$. In this case $|\mathcal{A}(\pi)| = 8(p^2-1)^2(p+1)$.

(ii) If $f_0 = 0$ and $f_1^{p-1} \neq -1$, then $\mathcal{A}(\pi) = \langle g, \ell \rangle \cdot H$ where g and H are as given above and ℓ is given by

$$\ell = \sigma\begin{bmatrix} 0 & 1 & & \\ f_1^p & 0 & & \\ & & 1 & 0 \\ & & 0 & 1 \end{bmatrix} \quad \textit{with } \sigma \neq 1.$$

Moreover, $|\mathcal{A}(\pi)| = 4(p^2-1)^2(p+1)$.

(iii) *If* $f_1 = 0$ *then* $\mathcal{A}(\pi) = \langle g, \ell\rangle \cdot H$ *where*

$$g = \begin{bmatrix} 0 & 1 & & \\ f_0 & 0 & & \\ & & 0 & f_0 \\ & & f_0^{p+1} & 0 \end{bmatrix}, \quad \ell = \sigma\begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & f_0 & 0 \\ & & 0 & f_0^p \end{bmatrix} \quad \text{with } \sigma \neq 1$$

and $H = \langle M(x,y,w) : (x/y)^{2(p+1)} = 1$ *and* $(y/xw)^{p-1} = 1\rangle$. $|\mathcal{A}(\pi)| = 8(p^2-1)^2$.

(iv) *If* $f_0 \neq 0$ *and* $f_1^{2(p-1)} \neq 1$, *then* $\mathcal{A}(\pi) = \langle g\rangle \cdot H$ *where*

$$g = \begin{bmatrix} 0 & 1 & & \\ s & 0 & & \\ & & 0 & u \\ & & u^p s & 0 \end{bmatrix} \quad \text{with } u = tf_0 \text{ and } s^{p+1} = f_1^{p+1} - f_0^{p+1}$$

and $H = \langle M(x,y,w) : (x/y)^{p+1} = 1$ *and* $(y/xw)^{p-1} = 1\rangle$. *Here* $|\mathcal{A}(\pi)| = 2(p^2-1)^2$.

(v) *If* $f_0 \neq 0$ *and* $f_1^{2(p-1)} = 1$, *then* $\mathcal{A}(\pi) = \langle g, \ell\rangle \cdot H$ *where* g *and* H *are as in (iv) and* ℓ *is given by*

$$\ell = \sigma\begin{bmatrix} z & 0 & & \\ 0 & 1 & & \\ & & v & 0 \\ & & 0 & (\frac{v}{z})^p \end{bmatrix} \quad \text{with } \sigma \neq 1,\ v = \frac{f_0}{f_1} \text{ and } z^{p+1} = f_1^{p-1}.$$

In this case, $|\mathcal{A}(\pi)| = 4(p^2-1)^2$.

Corollary 2.2 *Let* $\pi(f_0, f_1)$ *be a p-primitive semifield plane and let* $\mathcal{A}(\pi)$ *be its autotopism group. Then* $\mathcal{A}(\pi)$ *is solvable.*

Proof:

Notice that the subgroup H of $\mathcal{A}(\pi)$ is a normal abelian subgroup of $\mathcal{A}(\pi)$ and $\mathcal{A}(\pi)/H$ is also abelian. Thus $\mathcal{A}(\pi)$ is solvable.

References

[1] Cordero-Brana, M. On p-primitive semifield planes. Ph.D. thesis, University of Iowa, 1989.

[2] Cordero-Vourtsanis, M. Semifield planes of order p^4 that admit a p-primitive Baer collineation. Osaka J. Math (to appear).

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

[4] Hughes, D.R., Piper F. *Projective Planes*, Springer-Verlag, Berlin/ Heidelberg/ New York, 1973.

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