Note di Matematica
Note Mat. **38** (2018) no. 2, 11–20.

ISSN 1123-2536, e-ISSN 1590-0932
doi:10.1285/i15900932v38n2p11

On a conjecture about the autotopism group of the Figueroa's presemifields of order p^n

Walter Meléndez
University of Puerto Rico, Río Piedras Campus
Mathematics Department, P. O. Box 70377
San Juan, PR 00936, USA
wflorian75@gmail.com

Moisés Delgado
University of Puerto Rico, Cayey Campus
Mathematics and Physics Department
Cayey, PR 00736, USA
moises.delgado@upr.edu

Received: 15.11.2016; accepted: 21.4.2018.

Abstract. In [14] was proved that the autotopism group of the Cordero-Figueroa semifield of order 3^6 is isomorphic to a subgroup of $\Gamma L(K) \times \Gamma L(K)$, where $K = GF(3^6)$. Also a conjecture was proposed for the general case, the autotopism group of a Figueroa's presemifield of order p^n. In this article, under a normality condition, we prove this conjecture.

Keywords: finite presemifield, finite semifield, autotopism, autotopism group, Cordero-Figueroa semifield, Figueroa's presemifields.

MSC 2000 classification: primary 12K10, secondary 17A35

1 Introduction

Finite presemifields and finite semifields are very important algebraic structures in many areas of mathematics. Although they have traditionally been considered in the context of finite geometries, new applications to coding theory, combinatorics, group theory, and graph theory (among others) have broadened potentially the interest in these structures. In fact, in the last few years there has been a renovated interest on its study with the help of computational methods (see, for example, [5]).

A *finite presemifield* $(P, +, *)$ consists of an additive group $(P, +)$ and a multiplication $*$ that satisfies both distributive laws and the condition: if $x*y = 0$ then $x = 0$ or $y = 0$. A finite presemifield with multiplicative identity is called *finite semifield*.

Throughout this article, the term presemifield (or semifield) will always be used to refer a finite presemifield (or a finite semifield).

Note that the multiplication in a presemifield or semifield is not assumed to be commutative or associative

In the earlier literature, semifields were known as 'nonassociative division rings', 'nonassociative division algebras' or 'distributive quasifields'. The term semifield was introduced by Knuth [13] in 1965.

A trivial example of semifield is a field. If the multiplication of the semifield is associative, then it becomes a field.

The first non-trivial examples of semifields were introduced by Dickson [7]. A complete study of semifields in the first decades of the 20th century can be found in [12]. Also, [11] provides an excellent survey of almost all the known presemifields and semifields, up to isotopism, until 2004. In the last years many new presemifields and semifields have been constructed (see, for example, [1], [3], [4], [14], [15], and [16]), some of which have been found with the help of computational tools (see, for example, [4] and [16]).

Two presemifields (or semifields) $(P, +, *)$ and $(P', +, \circ)$ are *isotopic* if there exist a triple (F, G, H) of bijective functions from P to P' which are additives and satisfy $G(x*y) = F(x) \circ H(y)$, for all $x, y \in P$. The triple (F, G, H) is called an *isotopism* from P to P'.

Any presemifield $(P, +, *)$ is isotopic to a semifield by defining a new operation $\circ$ as follows: $(x*e)\circ(e*y) = x*y$, where $e \in P$ is a fixed element, $e \neq 0$, and $x, y \in P$. Thus, $(P, +, \circ)$ is a semifield isotopic to $(P, +, *)$ with multiplicative identity $e * e$.

An isotopism from a presemifield (or semifield) P to itself is called an *autotopism* of P. The set of autotopisms of a presemifield (or semifield) P form a group under component-wise composition and it is known in the literature as the *autotopism group* of P. Let us denote this group by $\mathcal{A}(P)$.

In this paper, we will focus our attention on Figueroa's presemifields of order p^n and its autotopism group.

A *Figueroa's presemifield of order* p^n is defined in [14] as follows: let $\alpha \neq 1$ and $\beta \neq 1$, $\alpha \neq \beta$, be automorphisms of $K = GF(p^n)$, where $p \geqslant 3$ and $n \geqslant 4$, and let $A, B \in K^*$ be constants. Then, the product over K

$$x * y = xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha} \tag{1}$$

defines a presemifield $(K, +, *)$ if there exist α, β, A, and B, such that $x * y = 0$ implies $x = 0$ or $y = 0$. This presemifield in [14] is denoted by $P(K, \alpha, \beta, A, B)$.

2 The warm-up case $K = GF(3^6)$

The first example of a Figueroa's presemifield of order 3^6 was introduced in [8]. There in, a presemifield is defined by the product

$$x * y = xy + \gamma x^3 y^{27} + \gamma^{13} x^{27} y^3, \tag{2}$$

where $x, y \in GF(3^6)$ and $\gamma \in GF(3^6)$ is a primitive element such that $\gamma^6 = 1+\gamma$.

The idea of generating presemifields with this type of product arose in [6], where the authors proved that a semifield of order $p^n \neq 2^6$, for a prime number p and an integer $n \geq 3$, which admits an autotopism of order a p–primitive prime divisor h of $p^n - 1$ (that is, $h \mid (p^n - 1)$ but $h \nmid (p^i - 1)$ for each integer i with $1 \leqslant i \leqslant n-1$) is a presemifield with a product of the form

$$x * y = xy + \textstyle\sum_{i=1}^{n-1} a_i x^{p^i} y^{p^{e_i}},$$

where $x, y \in GF(p^n)$, $a_i \in GF(p^n)$ are constants, and $0 \leqslant e_i \leqslant n-1$.

The Figueroa's presemifield of order 3^6 defined by the product (2) is known in the literature of finite translation planes as *Cordero-Figueroa semifield of order* 3^6 (see Theorem 37.2 in [10]). For simplicity, from now on, this semifield will be called *Cordero-Figueroa semifield*.

Because of being the first one of its kind, in [14] we considered to study the autotopism group of this particular semifield and we showed that its autotopism group is isomorphic to a particular subgroup of $\Gamma L(K) \times \Gamma L(K)$, where $K = GF(3^6)$. We also suggested that the same fact should be fulfilled for the general case (i.e., for a Figueroa's presemifield of order p^n). Thus, we formally conjecture:

Conjecture 1. *If a Figueroa's presemifield of order p^n admits an autotopism of order a p-primitive prime divisor, then its autotopism group is isomorphic to a subgroup of $\Gamma L(K) \times \Gamma L(K)$, where $K = GF(p^n)$.*

The order and the form of the elements of the middle nucleus of a Figueroa's presemifield of order p^n (see Lemma 1 in [14]), as well as its normality, played an important role in the demonstration that the components of the autotopisms of the Cordero-Figueroa semifield are nonsingular semilinear transformations from K to K, where $K = GF(3^6)$ (see proof of Theorem 1 in [14]). Since, in (1), the parameters α, β, A, and B are unknown, a similar method can not be applied for the general case. For this reason, a different approach is taken in this paper.

Is our goal in this article to prove the Conjecture 1. In section 4, we provide a characterization for a Figueroa's presemifield of order p^n to admit a certain autotopism of order a p-primitive prime divisor of $p^n - 1$, which enable us to determine, in section 5, the form of the autotopisms of these presemifields.

3 Some preliminary results

In order to accomplish the characterization mentioned at the end of section 2, let us prove the following two propositions:

Proposition 1. *Let $P = P(K, \alpha, \beta, A, B)$ be a Figueroa's presemifield of order p^n. Assume that $\alpha^3 \neq 1$ if $\alpha\beta = 1$. If (f, g, h) is an autotopism of P with $f(x) = cx^\sigma$ and $g(y) = dy^\theta$, then $\sigma = \theta$, $h(n) = dc^{-1}n^\theta$, and*

$$dc^\beta A^\theta = Ac^\alpha d^\beta, \quad dc^\alpha B^\theta = Bc^\beta d^\alpha.$$

Proof. Since (f, g, h) is an autotopism of P,

$$d(x * n)^\theta = (cx^\sigma) * h(n).$$

Then

$$d(x^\theta n^\theta + A^\theta x^{\alpha\theta} n^{\beta\theta} + B^\theta x^{\beta\theta} n^{\alpha\theta}) = cx^\sigma h(n) + A(cx^\sigma)^\alpha h(n)^\beta + B(cx^\sigma)^\beta h(n)^\alpha.$$

Considering the exponent of the variable x in the last equation, let us denote the terms of this equation by $E_\theta = dx^\theta n^\theta, E_{\alpha\theta} = dA^\theta x^{\alpha\theta} n^{\beta\theta}$, and so on. Thus, we have the following cases:

If $E_\theta = E_\sigma$, then $\theta = \sigma$. So, $h(n) = dn^\theta/c$. Hence, $h(n) = dc^{-1}n^\theta$.

If $E_{\alpha\theta} = E_{\sigma\alpha}$ and $E_{\beta\theta} = E_{\sigma\beta}$, then $dA^\theta = Ac^\alpha d^\beta/c^\beta$ and $dB^\theta = Bc^\beta d^\alpha/c^\alpha$. Hence, $dc^\beta A^\theta = Ac^\alpha d^\beta$ and $dc^\alpha B^\theta = Bc^\beta d^\alpha$.

If $E_{\alpha\theta} = E_{\sigma\alpha}$ and $E_\theta = E_{\sigma\beta}$, then $\theta = \sigma$ and $\theta = \sigma\beta$, which contradicts that $\beta \neq 1$. In the same fashion, $E_{\beta\theta} = E_{\sigma\beta}$ and $E_\theta = E_{\sigma\alpha}$ are not possible. The case $E_{\alpha\theta} = E_{\sigma\beta}$ and $E_{\beta\theta} = E_{\sigma\alpha}$ is also not possible since $\alpha \neq \beta$.

If $E_\theta = E_{\sigma\beta}$, $E_{\alpha\theta} = E_\sigma$, and $E_{\beta\theta} = E_{\sigma\alpha}$, then $\theta = \sigma\beta$, $\alpha\theta = \sigma$, and $\beta\theta = \sigma\alpha$. Therefore, $\alpha\beta = 1$ and $\alpha^3 = 1$, which is not possible by hypothesis. In the same fashion, $E_\theta = E_{\sigma\alpha}$, $E_{\alpha\theta} = E_{\sigma\beta}$, and $E_{\beta\theta} = E_\sigma$ can not occur. QED

Proposition 2. *Let $P = P(K, \alpha, \beta, A, B)$ be a Figueroa's presemifield of order p^n. If there exist an automorphism θ of K and constants $c, d \in K^*$ such that*

$$dc^\beta A^\theta = Ac^\alpha d^\beta, \quad dc^\alpha B^\theta = Bc^\beta d^\alpha \tag{3}$$

then the triple (f, g, h) with $f(x) = cx^\theta$, $g(y) = dy^\theta$, and $h(n) = dc^{-1}n^\theta$, is an autotopism of P.

Proof. From (3) we get

$$Ad^\beta c^{\alpha-\beta} = A^\theta d, \quad Bd^\alpha c^{\beta-\alpha} = B^\theta d. \tag{4}$$

Notice that

$$\begin{aligned} f(x) * h(n) &= (cx^\theta)(dc^{-1}n^\theta) + A(cx^\theta)^\alpha (dc^{-1}n^\theta)^\beta + B(cx^\theta)^\beta (dc^{-1}n^\theta)^\alpha \\ &= dx^\theta n^\theta + Ad^\beta c^{\alpha-\beta} x^{\alpha\theta} n^{\beta\theta} + Bd^\alpha c^{\beta-\alpha} x^{\beta\theta} n^{\alpha\theta} \\ &\overset{(4)}{=} dx^\theta n^\theta + A^\theta d x^{\alpha\theta} n^{\beta\theta} + B^\theta d x^{\beta\theta} n^{\alpha\theta} \\ &= d(x^\theta n^\theta + A^\theta x^{\alpha\theta} n^{\beta\theta} + B^\theta x^{\beta\theta} n^{\alpha\theta}) \\ &= d(xn + Ax^\alpha n^\beta + Bx^\beta n^\alpha)^\theta \\ &= d(x * n)^\theta \\ &= g(x * n). \end{aligned}$$

Obviously, f, g, and h, are biyective functions and additives. Hence, the triple (f, g, h) is an autotopism of P. QED

4 A characterization

As was mentioned before, the next theorem provides a characterization for the autotopism group of a Figueroa's presemifield of order p^n to admit an autotopism of order a p-primitive prime divisor.

Theorem 1. *Let $P = P(K, \alpha, \beta, A, B)$ be a Figueroa's presemifield of order p^n. Assume that $p^n - 1$ has a p-primitive prime divisor s and $\alpha^3 \neq 1$ if $\alpha\beta = 1$. Then $\mathcal{A}(P)$ admits the autotopism $(f_0 x,\ f_0^2 y,\ f_0 n)$ of order s, with $f_0 \in K^*$, if and only if s divides $(\beta - 1) + (\alpha - 1)$.*

Proof. Let us assume that $\mathcal{A}(P)$ admits the autotopism $(f_0 x,\ f_0^2 y,\ f_0 n)$ of order s, with $f_0 \in K^*$. Then, the order of f_0 is s. By Proposition 1,

$$f_0^2 f_0^\beta A = A f_0^\alpha f_0^{2\beta}, \quad f_0^2 f_0^\alpha B = B f_0^\beta f_0^{2\alpha}.$$

Thus, $f_0^{\beta+\alpha} = f_0^2$. Then, $\beta + \alpha \equiv 2 \bmod s$. Therefore, s divides $(\beta - 1) + (\alpha - 1)$.

Conversely, let us assume that s divides $(\beta - 1) + (\alpha - 1)$. Since s is prime and divides the order of K^*, there exist $f_0 \in K^*$ of order s. Moreover, since s is p-primitive prime divisor of $p^n - 1$,

$$gcd(\beta - \alpha, s) = 1 = gcd(\alpha - 1, s).$$

Then

$$\langle f_0 \rangle = \langle f_0^{\beta-\alpha} \rangle = \langle f_0^{\alpha-1} \rangle.$$

Thus, there exist natural numbers i and j, $1 \leq i, j < s$, such that $f_0^{\beta-\alpha} = f_0^j$ and $f_0^{-j} = (f_0^{\alpha-1})^i$. Therefore,

$$f_0^{\beta-\alpha}(f_0^i)^{\alpha-1} = 1. \tag{5}$$

Since s divides $(\beta-1)+(\alpha-1)$, we have that

$$-i(\alpha-1) \equiv i(\beta-1) \bmod s.$$

Then $f_0^{-i(\alpha-1)} = f_0^{i(\beta-1)}$. Therefore, from (5), we get

$$f_0^{\alpha-\beta}(f_0^i)^{\beta-1} = 1. \tag{6}$$

Let us denote $g_0 = f_0^i$. Then the equations (5) and (6) become

$$f_0^{\beta-\alpha}g_0^{\alpha-1} = 1, \quad f_0^{\alpha-\beta}g_0^{\beta-1} = 1. \tag{7}$$

On the other hand, from (5) and (6), we find that

$$f_0^{2(\beta-\alpha)} = f_0^{i(\beta-\alpha)}.$$

Then

$$i(\beta-\alpha) \equiv 2(\beta-\alpha) \bmod s. \tag{8}$$

Since $gcd(\beta-\alpha, s) = 1$, s does not divide $(\beta-\alpha)$. Therefore, from (8), we have that $i \equiv 2 \bmod s$. Thus, $g_0 = f_0^2$.

Now, from equation (7), it is not difficult to verify that the hypothesis of Proposition 2 is satisfied with $\theta = i$ (the identity automorphism from K to K), $c = f_0$, and $d = g_0$. Hence, (f_0x, f_0^2y, f_0n) is the autotopism of P of the required order s. QED

5 Main result

The previous characterization allows as to establish our main result:

Theorem 2. *Let $P = P(K, \alpha, \beta, A, B)$ be a Figueroa's presemifield of order p^n. Assume that $\mathcal{A}(P)$ admits the autotopism of order s referred in Theorem 1. If the subgroup generated by this autotopism is normal in $\mathcal{A}(P)$, then*

$$\mathcal{A}(P) = \{(ux^\phi, uvy^\phi, vn^\phi) : u, v \in K^*,\ \phi \in Aut(K)\},$$

and hence, it is isomorphic to a subgroup of $\Gamma L(K) \times \Gamma L(K)$.

Proof. Let S be the subgroup of $\mathcal{A}(P)$ generated by the autotopism $(f_0x,\ f_0^2 y,\ f_0n)$ of order s, where $f_0 \in K^*$, as in Theorem 1. First we show that the components of any element of $\mathcal{A}(P)$ are nonsingular semilinear transformations from K to K.

In fact, let $(\Phi, \Psi, \Upsilon) \in \mathcal{A}(P)$. Let us denote $f(x) = f_0x$, the first component of the autotopism $(f_0x,\ f_0^2y,\ f_0n)$ of order s. Since S is normal in $\mathcal{A}(P)$, there exist $t \in \mathbb{N}$, $1 \leq t < s$, such that

$$\Phi f \Phi^{-1} = f^t.$$

Then, for $1 \leq m < s$,

$$\Phi f^m \Phi^{-1} = f^{mt}.$$

Therefore, for $x \in K$,

$$\Phi(f_0^m x) = \Phi(f^m(x)) = f^{mt}(\Phi(x)) = f_0^{mt}\Phi(x). \tag{9}$$

Let $\Phi(1) = u$. Then, for $x = 1$, (9) implies that

$$\Phi(f_0^m) = f_0^{mt}u.$$

Hence

$$f_0^{mt} = u^{-1}\Phi(f_0^m).$$

Thus, from (9) we obtain that

$$\Phi(f_0^m x) = u^{-1}\Phi(x)\Phi(f_0^m).$$

Let us define $\phi : K \to K$ by $\phi(x) = u^{-1}\Phi(x)$. It is not difficult to verify that ϕ is a linear transformation from K over $GF(p)$. Then

$$\begin{aligned}\phi(f_0^m x) &= u^{-1}\Phi(f_0^m x)\\ &= u^{-1}(u^{-1}\Phi(x)\Phi(f_0^m))\\ &= (u^{-1}\Phi(f_0^m))(u^{-1}\Phi(x))\\ &= \phi(f_0^m)\phi(x).\end{aligned}$$

Since $GF(p^n) = GF(p)(f_0)$, any element in $GF(p^n)$ is a polynomial expression of f_0 over $GF(p)$ with degree less than s. Consequently, if $x, y \in K$, then writing y in terms of f_0, the equation $\phi(f_0^m x) = \phi(f_0^m)\phi(x)$ implies that $\phi(xy) = \phi(x)\phi(y)$. Therefore, $\phi \in Aut(K)$. Since $\phi(x) = u^{-1}\Phi(x)$, we have that $\Phi(x) = ux^{\phi}$. Thus, Φ is a nonsingular semilinear transformation from K to K.

Similarly, it can be proved that Ψ and Υ are also nonsingular semilinear transformation from K to K. Hence, the components of any element of $\mathcal{A}(P)$ are nonsingular semilinear transformations from K to K.

On the other hand, let $(F, G, H) \in \mathcal{A}(P)$. From the previous discussion, we note that F and H must have similar forms; i.e.,

$$F(x) = ux^{\phi}, \quad H(n) = vn^{\psi},$$

where $u = F(1)$, $v = H(1)$, and $\phi, \psi \in Aut(K)$.

By Lemma 8.9 in [9], there exist $a, b \in K^*$ such that

$$F(y) = bG(y), \quad H(y) = aG(y). \tag{10}$$

These two equations imply that

$$a^{-1}vy^{\psi} = b^{-1}uy^{\phi}. \tag{11}$$

If $\psi \neq \phi$, from (11) we get

$$a^{-1}v = 0 = b^{-1}u. \tag{12}$$

Since $a \neq 0$ and $b \neq 0$, from (12) we have that $u = v = 0$. Therefore $F = G = H = 0$, which contradicts the nonsingularity of those functions. Hence $\psi = \phi$. Then

$$F(x) = ux^{\phi}, \quad H(n) = vn^{\phi}$$

and from (10)

$$G(y) = b^{-1}uy^{\phi} \ \text{ or } \ G(y) = a^{-1}vy^{\phi}.$$

If $G(y) = b^{-1}uy^{\phi}$, then by Proposition 1

$$H(n) = \frac{b^{-1}u}{u}n^{\phi} = b^{-1}n^{\phi},$$

which implies that $b^{-1} = v$, and therefore $G(y) = uvy^{\phi}$. Similarly, if $G(y) = a^{-1}vy^{\phi}$, then $a^{-1} = u$, and therefore $G(y) = uvy^{\phi}$. In any case,

$$G(y) = uvy^{\phi}.$$

Hence

$$\mathcal{A}(P) = \{(ux^{\phi}, uvy^{\phi}, vn^{\phi}) : u, v \in K^*,\ \phi \in Aut(K)\}.$$

In order to see that $\mathcal{A}(P)$ is isomorphic to a subgroup of $\Gamma L(K) \times \Gamma L(K)$, let us define the application $\Theta : \mathcal{A}(P) \to \Gamma L(K) \times \Gamma L(K)$ by

$$\Theta(ux^{\phi}, uvy^{\phi}, vn^{\phi}) = (ux^{\phi}, vn^{\phi}),$$

where $u, v \in K^*$ and $\phi \in Aut(K)$. It is not difficult to show that Θ is an isomorphism. QED

Remark 1. We conclude this article with two comments:

(a) Theorem 2, and consequently the Conjecture 1, is verified for the Cordero-Figueroa semifield. This Figueroa's presemifield of order 3^6 admits the autotopism $(\gamma^{104}x, \gamma^{208}y, \gamma^{104}n)$ of order 7, a 3-primitive prime divisor of $3^6 - 1$. The subgroup generated by this autotopism is normal in the autotopism group of the Cordero-Figueroa semifield [14]. A similar argument applies for a Figueroa's presemifield of order 5^6 that is not a generalized twisted field.

(b) The Conjecture 1 is also confirmed for Figueroa's presemifields of orders 7^6, 11^6, and 13^6. For these orders, the Figueroa's presemifields are generalized twisted fields, and it is already known that their autotopism groups are isomorphic to a subgroup of $\Gamma L(K) \times \Gamma L(K)$ (see [2]).

References

[1] J. Bierbrauer: *New semifields, PN and APN functions*, Des. Codes. Cryptogr., **54** (2010), 189-200.

[2] M. Biliotti, V. Jha, N. Johnson: *The collineation groups of generalized twisted field planes*, G. Dedicata, **76** (1999), 91-126.

[3] L. Budaghyan, T. Helleseth: *New conmutative semifields defined by new PN multinomials*, Cryptogr. Commun., **3** (2011), 1-16.

[4] E.F. Combarro, I.F. Rúa, J. Ranilla: *Finite semifields with* 7^4 *elements*, International Journal of Computer Mathematics, **89** (2012), 1865-1878.

[5] E.F. Combarro, I.F. Rúa, J. Ranilla: *New advances in the computational exploration of semifields*, International Journal of Computer Mathematics, **88** (2011), 1990-2000

[6] M. Cordero, R. Figueroa: *Towards a characterization of the generalized twisted field planes*, J. Geom., **52** (1995), 54-63.

[7] L.E. Dickson: *Linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc., **7** (1906), 370-390.

[8] R. Figueroa: *A characterization of the generalized twisted field planes of characteristic* $\geqslant 5$, Geom. Dedicata, **50** (1994), 205-216.

[9] D. R. Hughes, F. C. Piper: Projective planes, Springer-Verlag, New York 1973.

[10] N. Jhonson, V. Jha, M. Biliotti: Handbook of finite translation planes, Chapman & Hall/CRC, Boca Ratón 2007.

[11] W. M. Kantor: Finite semifields, Proceeding of the conference 'Finite Geometries, Groups, and Computation', Walter de Gruyter GmbH & Co., Pingree Park CO. 2006.

[12] E. Kleinfeld: *A history of finite semifields*, Lecture Notes in Pure and Appl. Math., **82** (1983), 275-278.

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

[14] W. Meléndez, R. Figueroa, M. Delgado: *On the autotopism group of Cordero-Figueroa semifield of order* 3^6, Discuss. Math. General Algebra and Appl., **36** (2016), 117-126.

[15] A. Pott, Y. Zhou: *A new family of semifields with 2 parameters*, Adv. Math., **234** (2013), 43-60.

[16] I.F. Rúa and E.F. Combarro: *Commutative semifields of order* 3^5, Communications in Algebra, **40** (2012), 988-996.