CHARACTERIZATION OF FOULSER'S λ-SYSTEMS

M. L. NARAYANA RAO

1. **Introduction.** In 1967 D. A. Foulser [1] defined a class of finite Veblen Wedderburn systems called λ-systems. These systems include regular nearfields and André systems. However there are other finite Veblen Wedderburn (VW) systems which are not λ-systems. Hall systems and the new class of (C)-systems obtained from the exceptional (irregular) nearfields [3] are VW systems which are not λ-systems. The main aim of this paper is to deduce a set of necessary and sufficient conditions under which an arbitrary VW system is a λ-system. Using this characterization it is shown in §3 that an isotopic or an anti-isotopic image of a λ-system is a λ-system.

2. Throughout this paper Foulser's notation [1] is followed. Let $F(+, \cdot)$ be a left VW system of order q^d where $q=p^s$, p is a prime, d and s are natural numbers. Let σ be a prime such that σ divides $(p^{sd}-1)$ but does not divide $(p^{st}-1)$ for $0<t<d$. Prime σ exists except in the following cases (Foulser [1, Lemma 1.1, p. 380]):

(i) $d=2$, q is a prime of the form 2^x-1;

(ii) $d=6$ and $q=2$.

Definition 2.1. Let $\tau=\sigma$ in the nonexceptional case and $\tau=2^x$ in the exceptional case (i).

Exceptional case (ii) does not enter our discussion since Foulser [1] proved that there are no λ-systems of order 2^6 with kern $K=GF(2)$. Let N_l, N_m and K denote left nucleus, middle nucleus and kern in the VW system $F(+, \cdot)$ respectively.

Lemma 2.1. *Let $F(+, \cdot)$ be an arbitrary (left) VW system of order q^2 where q is a prime of the form 2^x-1 with* kern *$K=GF(q)$. If $N_l\cap N_m$ contains a subgroup $G=\langle g\rangle$ of order 2^x, then $F(+, \cdot)$ is generated by $\{g, 1\}$ as a right vector space over the* kern *K where 1 is the multiplicative identity in $F(+, \cdot)$.*

Proof. Since $F(+, \cdot)$ is a right vector space of dimension two over the kern K, the lemma is proved if it is shown that 1 and g are linearly independent over K. Suppose there exist a and b in $K=GF(q)$ such that $a+g\cdot b=0$ and at least one of a and b are distinct from 0. We then obtain that both a and b are distinct from 0 and $g=(-a)\cdot b^{-1} \in GF(q)$, a contradiction since g is of order 2^x and no element of $GF(q)$ is of order 2^x.

Received by the editors June 16, 1969.

LEMMA 2.2. *Let $F(+, \cdot)$ be a (left) Veblen Wedderburn system of order q^d with* kern K *of order $q=p^s$ where p is a prime, s and d are natural numbers, $d>2$ and if $p=2$ and $s=1$ then $d\neq 6$. If the loop $F'(\cdot)$ contains a power associative element g of order τ, then the subgroup $G=\langle g\rangle$ generates $F(+, \cdot)$ as a right vector space over K. Further the set $T=\{1, g, \cdots, g^{d-1}\}$ is a basis.*

PROOF [2, Theorem 2.1].

We now assume the following hypothesis.

HYPOTHESIS 2.1. $F(+, \cdot)$ is a (left) VW system of order q^d with kern $K=GF(q)$ and $q\neq 2$ if $d=6$. The group $N_l\cap N_m$ contains a cyclic subgroup $G=\langle g\rangle$ of order τ with the property $x\cdot g=g^{t(x)}\cdot x$ for all $x\in F'$ where $t(x)\equiv q^{\mu(x)} \pmod{\sigma}$ for some mapping $\mu\colon F'\to I_d$ (integers modulo d).

Using the fact that $g\in N_l\cap N_m$ and g is of order τ the property stated in Hypothesis 2.1 may be written as

$$x\cdot g^k = g^{kq^{\mu(x)}}\cdot x \quad \text{for all } x\in F'. \tag{2.1}$$

The following is a consequence of Lemmas 2.1 and 2.2.

LEMMA 2.3. *Let $F(+, \cdot)$ be a VW system satisfying Hypothesis* 2.1. *Then $F(+, \cdot)$ is generated by $\{1, g, \cdots, g^{d-1}\}$ as a right vector space over the* kern $K=GF(q)$.

Let $F(+, \cdot)$ be a VW system satisfying Hypothesis 2.1. Lemma 2.3 implies that if x, y are arbitrary elements from $F(+, \cdot)$, then there exist elements a_i, b_i in $GF(q)$, $0\leqq i<d$, such that $x=\sum_{i=0}^{d-1} g^i\cdot a_i$ and $y=\sum_{i=0}^{d-1} g^i\cdot b_i$. We now define a new multiplication '$*$' as

$$x*y = \sum_{i=0}^{d-1}\sum_{j=0}^{d-1} g^{i+j}\cdot(a_i\cdot b_j).$$

LEMMA 2.4. *Let $F(+, \cdot)$ be a VW system satisfying Hypothesis* 2.1. *Then $F(+, *)$ is a field.*

PROOF. Obviously $F(+, *)$ is a commutative ring with multiplicative unity. The unity of $F'(\cdot)$ is the unity of $F'(*)$. Let $0\neq x\in F$. We now show that there is a unique $y\in F'$ such that $x*y=1$. Since $0\neq x$, there is a unique $z\in F'$ such that $x\cdot z=1$. Let $z=\sum_{i=0}^{d-1} g^i\cdot a_i$, $x=\sum_{i=0}^{d-1} g^i\cdot b_i$ and $y=\sum_{i=0}^{d-1} g^{iq^{\mu(x)}}\cdot a_i$. Then

$$1 = x\cdot z = x\cdot \sum_{i=0}^{d-1} g^i\cdot a_i = \sum_{i=0}^{d-1} (g^{iq^{\mu(x)}}\cdot x)\cdot a_i = \sum_{i=0}^{d-1} \Big(g^{iq^{\mu(x)}}\cdot \sum_{j=0}^{d-1} g^j\cdot b_j\Big)\cdot a_i$$

$$= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1} g^{iq^{\mu(x)}+j}\cdot(a_i\cdot b_j) = y*x = x*y.$$

This completes the proof of the lemma.

For any $x\in F$ let x^{r*} be defined inductively as $x * x = x^{2*}$, $x * x^{(r-1)*} = x^{r*}$. The following are easy consequences of the definition of the multiplication $*$.

$$\text{(2.2)}\quad \begin{aligned} &\text{(i)}\ g^{r*} = g^r, \\ &\text{(ii)}\ g^r\cdot a = g^{r*} * a, \\ &\text{(iii) If } x = \sum_{i=0}^{d-1} g^i\cdot a_i, \text{ then } x^{q^{r*}} = \sum_{i=0}^{d-1} g^{iq^r}\cdot a_i \end{aligned}$$

where $\langle g\rangle = G$ of Hypothesis 2.1, a, $a_i\in GF(q)$, $0\leqq i<d$ and $x\in F$.

LEMMA 2.5. *A VW system $F(+,\ \cdot)$ satisfying Hypothesis* 2.1 *is a λ-system.*

PROOF. Let $x\neq 0\neq y$ be arbitrary elements of F with $x=\sum_{i=0}^{d-1} g^i\cdot a_i$ and $y=\sum_{i=0}^{d-1} g^i\cdot b_i$. Then

$$\begin{aligned} x\cdot y &= x\cdot \sum_{i=0}^{d-1} g^i\cdot b_i = \sum_{i=0}^{d-1} (g^{iq^{\mu(x)}}\cdot x)\cdot b_i = \sum_{i=0}^{d-1}\sum_{j=0}^{d-1} g^{i+jq^{\mu(x)}}\cdot(a_i\cdot b_j) \\ &= x * y^{q^{\mu(x)*}}. \end{aligned}$$

(Here we have used Equations (2.1) and (2.2).) The theorem now follows from Lemma 2.1 of Foulser [1] by taking $\mu(x)$ as the mapping $\lambda(x)$ from $F'\to I_d$ (integers modulo d).

LEMMA 2.6. *Let $F(+,\circ)$ be a λ-system of order q^d with* kern $K=GF(q)$ *of order $q=p^s$, where p is a prime and d and s are natural numbers. Then the group $N_l\cap N_m$ contains a subgroup $G=\langle g\rangle$ of order τ. If $q^d\neq 9$, the cyclic subgroup G is the unique subgroup of order τ contained in $N_l\cap N_m$. If $q^d=9$, then there are three cyclic subgroups of order τ contained in $N_l\cap N_m$. Further $x\circ g = g^{q^{\lambda(x)}}\circ x$ for all $x\in F'$ where $\lambda(x)$ is the mapping used to define the λ-system.*

PROOF. Let N_u and N_v be the subgroups of $N_l\cap N_m$ defined in [1, §2.4]. Let $\tau=2^x$. Then $u=(q-1)$ and $t=q+1=2^x=\tau$ and N_u itself is of order 2^x. In the nonexceptional case $\tau=\sigma$, the following congruences

$$u \equiv 0 \ (\text{mod } (q^d-1)) \quad \text{for } 0<m<d \text{ and } m\mid d,$$

$$q^d \equiv 1 \ (\text{mod } \sigma) \quad \text{and } q^k \not\equiv 1 \ (\text{mod } \sigma) \text{ for } 0<k<d$$

imply $((q^d-1)/u)=t\equiv 0$ (mod σ). From this congruence it follows that N_u contains a unique cyclic subgroup of order σ. Since $N_u\subseteq N_v$ and N_v is a cyclic subgroup (Foulser [1, §2.4]), we may conclude that

N_v contains a unique cyclic subgroup of order σ. Let H be a subgroup of N_l of order σ and $H=\langle h\rangle$. Since H is of prime order, it is generated by every nonidentity element of H. Let $\lambda(h)=k$. Here $\lambda(x)$ is the mapping used by Foulser to define the λ-system. Then $\lambda(x \circ y)\equiv\lambda(x)+\lambda(y) \pmod{d}$ for all $x\in N_l$ and all $y\in F'$ (Foulser [1, §5.1]). From this it follows that $\lambda(h^d)\equiv d\lambda(h)=dk \pmod{d}$ implying $\lambda(h)=0$. Since $\sigma>d$, h^d is not the identity and therefore $\langle h^d\rangle=H$. H is a subgroup of N_v since $h\in N_l$ and $\lambda(h)=0$ (Foulser [1, §5.1]). Thus in either case N_l contains a cyclic subgroup of order σ which is the unique subgroup of order σ contained in N_v. Foulser [1, Lemma 5.2, p. 387] has shown that N_v is the unique subgroup of order N_v contained in $N_l\cap N_m$ except in the case $q^d=9$ and $N_l\cap N_m$ contains three cyclic subgroups of order τ in the case $q^d=9$. The last part of the Lemma is a direct consequence of the definition of a λ-system.

Collecting the results of Lemmas 2.5 and 2.6 we may state the following

THEOREM 2.1. *An arbitrary VW system $F(+,\ \cdot)$ of order q^d with* kern $K=GF(q)$ *of order $q=p^s$ where p is a prime, d and s are natural numbers ($q\neq 2$, if $d=6$) is a λ-system if, and only if, the group $N_l\cap N_m$ contains a cyclic subgroup $G=\langle g\rangle$ of order τ with the property $x\cdot g=g^{t(x)}\cdot x$ for all $x\in F'$, where $t(x)\equiv q^{\mu(x)} \pmod{\tau}$ for some mapping $\mu\colon F'\to I_d$ (integers modulo d). If $q^d\neq 3^2$, the subgroup G is the unique cyclic subgroup of order τ contained in $N_l\cap N_m$.*

3. Let $F(+,\ \cdot)$ and $F_1(+,\circ)$ be two VW systems. Let R be a 1-1 additive mapping from F onto F_1, and $a,\ b\in F'$. If $(x\cdot y)R=(x\cdot a)R \circ (b\cdot y)R$ for all $x,\ y\in F$, then $(R,\ a,\ b)$ is said to be an isotopism of $F(+,\ \cdot)$ onto $F_1(+,\ \circ)$. If $\hat{x}R\circ(x\cdot y)R=(b\cdot y)R$ for all $x,\ y\in F'$, where $x\cdot\hat{x}=b\cdot a$, then $(R,\ a,\ b)$ is said to be an anti-isotopism from $F(+,\ \cdot)$ onto $F_1(+,\ \circ)$. The proof of the following lemma may be found in Foulser [1].

LEMMA 3.1. *Let $(R,\ a,\ b)$ be an isotopism (or anti-isotopism) from $F(+,\ \cdot)$ onto $F(+,\circ)$. Let N_l and N_m be left and middle nuclei respectively of $F(+,\ \cdot)$, N_{1l} and N_{1m} be left and middle nuclei respectively of $F_1(+,\circ)$. Then $(R,\ a,\ b)$ induces the following isomorphisms:*

(i) *$\sigma_l\colon x\to(x\cdot b\cdot a)R$ for all $x\in N_l$, σ_l is an isomorphism from N_l onto N_{1l} (or N_{1m}),*

(ii) *$\sigma_m\colon x\to(b\cdot x\cdot a)R$ for all $x\in N_m$, σ_m is an isomorphism from N_m onto N_{1m} (or N_{1l}).*

In what follows, let $F(+,\ \cdot)$ be a λ-system of order q^d with kern $GF(q)$ and $F_1(+,\circ)$ be an isotope (or an anti-isotope) of $F(+,\ \cdot)$ under $(R,\ a,\ b)$.

LEMMA 3.2. *The mapping σ_l maps $N_l \cap N_m$ onto $N_{1l} \cap N_{1m}$ isomorphically.*

PROOF. Let $x \in N_l \cap N_m$. Then $x\sigma \in N_{1l(m)}$ by Lemma 3.1. It may be easily verified that $x \cdot b = b \cdot x^t$ where $t \equiv q^{d-\lambda(b)}$ (mod τ) and $x^t \in N_m$ $\cdot x\sigma_l = (x \cdot b \cdot a)R = (b \cdot x^t \cdot a)R = x^t \sigma_m \in N_{1m(l)}$ by Lemma 3.1. It then follows that $x\sigma_l \in N_{1l} \cap N_{1m}$. Obviously σ_l is an isomorphism from $N_l \cap N_m$ onto $N_{1l} \cap N_{1m}$.

LEMMA 3.3. *$N_{1l} \cap N_{1m}$ contains a cyclic subgroup G_1 of order τ.*

PROOF. $N_l \cap N_m$ contains a cyclic subgroup G of order τ by Theorem 2.1. It follows from Lemma 3.2 that $G\sigma_l$ is a desired cyclic subgroup of $N_{1l} \cap N_{1m}$.

LEMMA 3.4. *Let (R, a, b) be an isotopism and $z \in F'$, $x \in N_l \cap N_m$. Then $((b \cdot z) \cdot a)R \circ (x \cdot b \cdot a)R = (b \cdot x^t \cdot a)R \circ ((b \cdot z) \cdot a)R$ where $t \equiv q^{t_1}$ (mod τ), with $t_1 = \lambda(b \cdot z) - \lambda(b)$.*

PROOF.

$$\begin{aligned} ((b\cdot z)\cdot x)R &= ((b\cdot z)\cdot a)R \circ (b\cdot x)R \\ &= ((b\cdot z)\cdot a)R \circ ((b\cdot x\cdot a)R) \circ (b)R. \end{aligned} \tag{3.1}$$

A simple computation gives $(b \cdot z) \cdot x = x^m \cdot (b \cdot z) = (x^m \cdot b) \cdot z = b \cdot x^t \cdot z$ where $m = q^{\lambda(b \cdot z)}$, $t \equiv q^{t_1}$ (mod τ) with $t_1 = \lambda(b \cdot z) - \lambda(b)$ (mod d). We then have

$$\begin{aligned} ((b\cdot z)\cdot x)R &= (b\cdot x^t\cdot z)R = (b\cdot x^t\cdot a)R \circ (b\cdot z)R \\ &= ((b\cdot x^t\cdot a)R \circ ((b\cdot z)\cdot a)R) \circ (b)R. \end{aligned} \tag{3.2}$$

From (3.1) and (3.2), it follows that

$$((b\cdot z)\cdot a)R \circ (x\cdot b\cdot a)\, R = (b\cdot x^t\cdot a)R \circ ((b\cdot z)\cdot a)R.$$

LEMMA 3.5. *Let (R, a, b) be an isotopism and $y \in N_{1l} \cap N_{1m}$ and $u \in F'$. Then $u \circ y = y^l \circ u$ with $l \equiv q^{\mu(u)}$ (mod τ) where $\mu(u)$ is a mapping from F' into I_d.*

PROOF. $(b \cdot x^t \cdot a)R = (x^{t \cdot q^{\lambda(b)}} \cdot b \cdot a)R = ((x \cdot b \cdot a)R)^m$ where $m = t \cdot q^{\lambda(b)}$ $= q^{t_1 + \lambda(b)} = q^{\lambda(b \cdot z)}$ since σ_l is an isomorphism. Let $u = ((b \cdot z) \cdot a)R$, $(x \cdot b \cdot a)R = y$. From Lemma 3.4 we obtain

$$u \circ y = y^l \circ u \quad \text{where} \quad l = q^{\lambda(b\cdot z)} = q^{\mu(u)}. \tag{3.3}$$

Since the mapping R is 1-1 and onto, by letting z range over F' and x range over $N_l \cap N_m$, we obtain that (3.3) is true for arbitrary $u \in F'$ and arbitrary $y \in N_{1l} \cap N_{1m}$. Hence the lemma.

THEOREM 3.1. *An isotopic image of a λ-system is a λ-system.*

PROOF. Let $F(+,\cdot)$ be a λ-system and $F_1(+,\circ)$ is an isotopic image of $F(+,\cdot)$ under (R, a, b). From Lemmas 3.3 and 3.5, it follows that the group $N_{1l}\cap N_{1m}$ contains a cyclic subgroup G_1 of order τ satisfying conditions of Theorem 2.1. Hence the theorem.

LEMMA 3.6. *Let (R, a, b) be an anti-isotopism and $z\in F'$, $x\in N_l \cap N_m$. Then $((b\cdot z)\cdot a)R\circ(x\cdot b\cdot a)R=(b\cdot x^t\cdot a)R\circ((b\cdot z)\cdot a)R$, where $t\equiv q^{t_1}$ (mod τ) with $t_1=-\lambda(u)-\lambda(b)$ (mod α) where u is the solution of the equation $u\cdot((b\cdot u)\cdot a)=b\cdot a$.*

PROOF. Since (R, a, b) is an anti-isotopism we have

$$\hat{x}R\circ(x\cdot y)R = (b\cdot y)R \quad \text{for all } x, y\in F' \text{ where } x\cdot\hat{x} = b\cdot a. \tag{3.4}$$

From (3.4) and the relations $\hat{u}=((b\cdot z)\cdot a)$, $u\cdot v=x\cdot b\cdot a$, and $u\cdot\hat{u}=b\cdot a$ we obtain

$$((b\cdot z)\cdot a)R\circ(x\cdot b\cdot a)R = (b\cdot x^{q^{d-\lambda(u)}}\cdot((b\cdot z)\cdot a))R \tag{3.5}$$

where $u\cdot((b\cdot z)\cdot a)=b\cdot a$. Similarly (4.15) and the relations $\hat{w}=b\cdot x^t\cdot a$, $w\cdot e=(b\cdot z)\cdot a$, and $w\cdot\hat{w}=b\cdot a$ imply

$$(b\cdot x^t\cdot a)R\circ((b\cdot z)\cdot a)R = (b\cdot x^{q^{d-\lambda(u)}}\cdot((z\cdot b)\cdot a))R \tag{3.6}$$

where $u\cdot((z\cdot b)\cdot a)=b\cdot a$. The lemma follows from (3.5) and (3.6).

LEMMA 3.7. *Let (R, a, b) be an anti-isotopism and $y\in N_{1l}\cap N_{1m}$ and $w\in F_1'$. Then $w\circ y=y^l\circ w$ with $l\equiv q^{\mu(w)}$ (mod τ), where $\mu(w)$ is a mapping from F_1' into I_d.*

PROOF: Since σ_l is an isomorphism from N_l onto N_m, it follows that $(b\cdot x^t\cdot a)R=(x^t\cdot q^{\lambda(b)}\cdot b\cdot a)R=((x\cdot b\cdot a)R)^m$, where $m\equiv t\cdot q^{\lambda(b)}$ (mod τ). Let $w=((b\cdot z)\cdot a)R$ and $y=(x\cdot b\cdot a)R$ where $z\in F'$ and $x\in N_l\cap N_m$. Then from Lemma 3.6 we obtain

$$w\circ y = y^l\circ w \quad \text{where} \quad l\equiv q^{d-\lambda(u)} = q^{\mu(w)}. \tag{3.7}$$

Since the mapping is 1-1 onto, by letting z range over F' and x over $N_l\cap N_m$, we obtain that (3.7) is true for arbitrary $u\in F'$ and arbitrary $y\in N_{1l}\cap N_{1m}$. Hence the lemma.

THEOREM 3.2. *An anti-isotopic image of a λ-system is a λ-system.*

The proof follows from Lemmas 3.3 and 3.7 and Theorem 2.1.

References

1. D. A. Foulser, *A generalization of André's systems*, Math. Z. **100** (1967), 380–395. MR **37** #3436.

2. M. L. Narayana Rao, *A question on finite Moufang Veblen Wedderburn systems*, J. Algebra **13** (1969).

3. M. L. Narayana Rao, D. J. Rodabaugh, F. W. Wilke and J. L. Zemmer, *A new class of finite translation planes obtained from the exceptional near-fields*, J. Combinatorial Theory (to appear).

University of Missouri