CHARACTERIZATION OF FOULSER’S \( \lambda \)-SYSTEMS

M. L. NARAYANA RAO

1. Introduction. In 1967 D. A. Foulser [1] defined a class of finite Veblen Wedderburn systems called \( \lambda \)-systems. These systems include regular nearfields and André systems. However, there are other finite Veblen Wedderburn (VW) systems which are not \( \lambda \)-systems. Hall systems and the new class of (C)-systems obtained from the exceptional (irregular) nearfields [3] are VW systems which are not \( \lambda \)-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 \( \lambda \)-system. Using this characterization it is shown in §3 that an isotopic or an anti-isotopic image of a \( \lambda \)-system is a \( \lambda \)-system.

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

(i) \( d = 2 \), \( q \) is a prime of the form \( 2^s - 1 \);
(ii) \( d = 6 \) and \( q = 2 \).

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

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

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

Proof. Since \( F(\cdot, \cdot) \) 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 \( 2^s \) and no element of \( GF(q) \) is of order \( 2^s \).

Received by the editors June 16, 1969.
Lemma 2.2. Let $F(\cdot, \cdot)$ 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 $\tau$, then the subgroup $G = \langle g \rangle$ generates $F(\cdot, \cdot)$ as a right vector space over $K$. Further the set $T = \{1, g, \ldots, g^{d-1}\}$ is a basis.

Proof [2, Theorem 2.1].

We now assume the following hypothesis.

Hypothesis 2.1. $F(\cdot, \cdot)$ is a (left) VW system of order $q^d$ with kern $K = GF(q)$ and $q \neq 2$ if $d = 6$. The group $N_1 \cap N_m$ contains a cyclic subgroup $G = \langle g \rangle$ of order $\tau$ with the property $x \cdot g = g^{t(x)} \cdot x$ for all $x \in F'$ where $t(x) = q^{\mu(x)} \pmod{\sigma}$ for some mapping $\mu : F' \to I_d$ (integers modulo $d$).

Using the fact that $g \in N_1 \cap N_m$ and $g$ is of order $\tau$ the property stated in Hypothesis 2.1 may be written as

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

The following is a consequence of Lemmas 2.1 and 2.2.

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

Let $F(\cdot, \cdot)$ be a VW system satisfying Hypothesis 2.1. Lemma 2.3 implies that if $x, y$ are arbitrary elements from $F(\cdot, \cdot)$, then there exist elements $a_i, b_i$ in $GF(q)$, $0 \leq i < d$, 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 `$\ast$' as

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

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

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

\[1 = x \cdot z = x \cdot \sum_{i=0}^{d-1} g^i \cdot a_i = \sum_{i=0}^{d-1} (g^{iq^{\mu(x)}(x)} \cdot a_i = \sum_{i=0}^{d-1} (g^{iq^{\mu(x)}(x)} \cdot g^{j} \cdot b_j) \cdot a_i = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} g^{iq^{\mu(x)}(x)+j} \cdot (a_i \cdot b_j) = y \ast x = x \ast y.\]
This completes the proof of the lemma.

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

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

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

**Lemma 2.5.** A VW system \( F(\cdot, \cdot) \) satisfying Hypothesis 2.1 is a \( \lambda \)-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

\[
x \cdot y = \sum_{i=0}^{d-1} g^i \cdot b_i = \sum_{i=0}^{d-1} (g^{iq^r(x)} \cdot x) \cdot b_i = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} g^{iq^r(x) + jq^r(x)} \cdot (a_i \cdot b_j)
\]

(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 \( F' \rightarrow I_d \) (integers modulo \( d \)).

**Lemma 2.6.** Let \( F(\cdot, \cdot) \) be a \( \lambda \)-system of order \( q^d \) with kern \( K = GF(q) \) and order \( q = p^s \), where \( p \) is a prime and \( d \) and \( s \) are natural numbers. Then the group \( N_1 \cap N_m \) contains a subgroup \( G = \langle g \rangle \) of order \( \tau \). If \( q^d \neq 9 \), the cyclic subgroup \( G \) is the unique subgroup of order \( \tau \) contained in \( N_1 \cap N_m \). If \( q^d = 9 \), then there are three cyclic subgroups of order \( \tau \) contained in \( N_1 \cap N_m \). Further \( x \circ g = g^{\lambda(x)} \circ x \) for all \( x \in F' \) where \( \lambda(x) \) is the mapping used to define the \( \lambda \)-system.

**Proof.** Let \( N_u \) and \( N_* \) be the subgroups of \( N_1 \cap N_m \) defined in [1, §2.4]. Let \( \tau = 2^s \). Then \( u = (q - 1) \) and \( t = q + 1 = 2^s = \tau \) and \( N_u \) itself is of order \( 2^s \). In the nonexceptional case \( \tau = \sigma \), the following congruences

\[
\begin{align*}
& u \equiv 0 \pmod{(q^d - 1)} \quad \text{for } 0 < m < d \text{ and } m \mid d, \\
& q^d \equiv 1 \pmod{\sigma} \quad \text{and } q^k \neq 1 \pmod{\sigma} \quad \text{for } 0 < k < d
\end{align*}
\]

imply \( ((q^d - 1)/u) = t \equiv 0 \pmod{\sigma} \). From this congruence it follows that \( N_u \) contains a unique cyclic subgroup of order \( \sigma \). Since \( N_u \subseteq N_* \) and \( N_* \) is a cyclic subgroup (Foulser [1, §2.4]), we may conclude that
contains a unique cyclic subgroup of order $\sigma$. Let $H$ be a subgroup of $N_t$ of order $\sigma$ 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 $\lambda$-system. Then $\lambda(x \circ y) = \lambda(x) + \lambda(y) \pmod{d}$ for all $x \in N_t$ and all $y \in F'$ (Foulser [1, §5.1]). From this it follows that $\lambda(h^d) = d\lambda(h) = dk \pmod{d}$ 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 $N_t$ since $h \in N_t$ and $\lambda(h) = 0$ (Foulser [1, §5.1]). Thus in either case $N_t$ contains a cyclic subgroup of order $\sigma$ which is the unique subgroup of order $\sigma$ contained in $N_t$. Foulser [1, Lemma 5.2, p. 387] has shown that $N_t$ is the unique subgroup of order $\sigma$ contained in $N_t \cap N_m$ except in the case $q^d = 9$ and $N_t \cap N_m$ contains three cyclic subgroups of order $\tau$ in the case $q^d = 9$. The last part of the Lemma is a direct consequence of the definition of a $\lambda$-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 $\lambda$-system if, and only if, the group $N_t \cap N_m$ contains a cyclic subgroup $G = \langle g \rangle$ of order $\tau$ with the property $x \cdot g = g^{t(x)} \cdot x$ for all $x \in F'$, where $t(x) \equiv g^{\mu(x)} \pmod{\tau}$ for some mapping $\mu: F' \to I_d$ (integers modulo $d$). If $q^d \neq 3^2$, the subgroup $G$ is the unique cyclic subgroup of order $\tau$ contained in $N_t \cap N_m$.

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 $xR \circ (x \cdot y)R = (b \cdot y)R$ for all $x, y \in F'$, where $x \cdot x = b - a$, 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) $\sigma_1: x \mapsto (x \cdot b \cdot a)R$ for all $x \in N_l$, $\sigma_1$ is an isomorphism from $N_l$ onto $N_{1l}$ (or $N_{1m}$),

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

In what follows, let $F(+, \cdot)$ be a $\lambda$-system of order $q^d$ with kern $GF(q)$ and $F_1(+, \circ)$ be an isotope (or an anti-isotope) of $F(+, \cdot)$ under $(R, a, b)$. License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Lemma 3.2. The mapping $\sigma_i$ maps $N_i \cap N_m$ onto $N_{1i} \cap N_{1m}$ isomorphically.

Proof. Let $x \in N_{1i} \cap N_m$. Then $x \sigma \in N_{11(m)}$ by Lemma 3.1. It may be easily verified that $x \cdot b = b \cdot x^t$ where $t \equiv q^{d(i)}$ (mod $\tau$) and $x^t \in N_m$.

Lemma 3.3. $N_{1i} \cap N_{1m}$ contains a cyclic subgroup $G_i$ of order $\tau$.

Proof. $N_{1i} \cap N_m$ contains a cyclic subgroup $G$ of order $\tau$ by Theorem 2.1. It follows from Lemma 3.2 that $G \sigma_i$ is a desired cyclic subgroup of $N_{1i} \cap N_{1m}$.

Lemma 3.4. Let $(R, a, b)$ be an isotopism and $z \in F'$, $x \in N_{1i} \cap N_m$. Then $(b \cdot z) \cdot a) R \circ (x \cdot b \cdot a) R R \circ ((b \cdot z) \cdot a) R$ where $t \equiv q^t$ (mod $\tau$), with $t_1 = \lambda(b \cdot z) - \lambda(b)$. 

Proof.

$((b \cdot z) \cdot x) R = ((b \cdot z) \cdot a) R \circ (b \cdot x) R
\tag{3.1}$

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

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 $m = q^{(b \cdot z)}$, $t \equiv q^t$ (mod $\tau$) with $t_1 = \lambda(b \cdot z) - \lambda(b)$ (mod $d$). We then have

$((b \cdot z) \cdot x) R = (b \cdot x^t \cdot z) R = (b \cdot x^t \cdot a) R \circ (b \cdot z) R\tag{3.2}$

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

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 $y \in N_{11} \cap N_{1m}$ and $u \in F'$. Then $u \circ y = y^l \circ u$ with $l \equiv q^{\mu(u)}$ (mod $\tau$) 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 $m = t \cdot q^{\lambda(b)} = q^{l + \lambda(b)} = q^{\lambda(b \cdot z)}$ since $\sigma_i$ 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 $N_{11} \cap N_m$, we obtain that (3.3) is true for arbitrary $u \in F'$ and arbitrary $y \in N_{11} \cap N_{1m}$. Hence the lemma.
Theorem 3.1. An isotopic image of a $\lambda$-system is a $\lambda$-system.

Proof. Let $F(+, \cdot)$ be a $\lambda$-system and $F_1(\pm, \circ)$ is an isotopic image of $F(+, \cdot)$ under $(R, a, b)$. From Lemmas 3.3 and 3.5, it follows that the group $N_{11} \cap N_{1m}$ contains a cyclic subgroup $G_1$ of order $\tau$ satisfying conditions of Theorem 2.1. Hence the theorem.

Lemma 3.6. Let $(R, a, b)$ be an anti-isotopism and $z \in F'$, $x \in N_{11} \cap N_{1m}$. Then $(b \cdot z) \cdot a \circ (x \cdot b \cdot a) = R = (b \cdot x^t \cdot a) \circ ((b \cdot z) \cdot a)$, where $t = q^{\tau_t}$ (mod $\tau$) with $t = -\lambda(u) - \lambda(b)$ (mod $\alpha$) where $u$ is the solution of the equation $u \cdot (b \cdot u) = b \cdot a$.

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

$(3.4) \quad xR \circ (x \cdot y)R = (b \cdot y)R$ for all $x, y \in F'$ where $x \cdot x = b \cdot a$.

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

$(3.5) \quad ((b \cdot z) \cdot a) \circ (x \cdot b \cdot a) = R = (b \cdot x^{d-\lambda(u)} \cdot ((b \cdot z) \cdot a))$ where $u \cdot ((b \cdot z) \cdot a) = b \cdot a$. Similarly (4.15) and the relations $w = b \cdot x^t \cdot a$, $w \cdot e = (b \cdot z) \cdot a$, and $w \cdot w = b \cdot a$ imply

$(3.6) \quad (b \cdot x^t \cdot a) \circ ((b \cdot z) \cdot a) = R = (b \cdot x^{d-\lambda(u)} \cdot ((b \cdot z) \cdot a))$ where $u \cdot ((b \cdot z) \cdot a) = b \cdot a$. The lemma follows from (3.5) and (3.6).

Lemma 3.7. Let $(R, a, b)$ be an anti-isotopism and $y \in N_{11} \cap N_{1m}$ and $w \in F'_1$. Then $w \circ y = y^t \circ w$ with $l = q^{\mu(w)}$ (mod $\tau$), where $\mu(w)$ is a mapping from $F'_1$ into $I_a$.

Proof: Since $\sigma_1$ is an isomorphism from $N_{11}$ onto $N_{1m}$, it follows that $(b \cdot x^t \cdot a) = R = (x^t \cdot q^{h(b)} \cdot b \cdot a) = R = ((x \cdot b \cdot a) \circ ((b \cdot z) \cdot a))$, where $m \equiv t \cdot q^{h(b)}$ (mod $\tau$). Let $w = ((b \cdot z) \cdot a) \circ (x \cdot b \cdot a) \circ (w \cdot w = b \cdot a)$ where $z \in F'$ and $x \in N_{11} \cap N_{1m}$. Then from Lemma 3.6 we obtain

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

Since the mapping is 1-1 onto, by letting $z$ range over $F'$ and $x$ over $N_{11} \cap N_{1m}$, we obtain that (3.7) is true for arbitrary $u \in F'$ and arbitrary $y \in N_{11} \cap N_{1m}$. Hence the lemma.

Theorem 3.2. An anti-isotopic image of a $\lambda$-system is a $\lambda$-system.

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


University of Missouri