A QUESTION OF FOULSER ON λ-SYSTEMS OF CHARACTERISTIC TWO

M. L. NARAYANA RAO AND J. L. ZEMMER[1,2]

Introduction. In a recent paper [1], D. A. Foulser described a general construction of finite (left) Veblen-Wedderburn systems which contain the nonexceptional near-fields, the Andre VW systems, the finite Moulton systems, and other new VW systems. At one point in his work Foulser wishes to know whether or not there exist λ-systems of order 2^6 with kern $GF(2)$. He answers this question in the negative by proving that there is no λ-system of order 2^d, with kern $GF(2)$, where $d=a^xb^y$ and a, b are primes. At the same time he asks whether or not there exist proper λ-systems of order 2^d, with kern $GF(2)$, where d contains more than two distinct prime factors. It is the main object of this note to answer this question in the affirmative. More generally we give in §1 a construction of λ-systems of order q^d, with kern $GF(q)$, where $q=p^s$ is an arbitrary power of an arbitrary prime p, and d contains at least three distinct prime factors. In §2 an interesting property of the left and middle nuclei of these λ-systems is described.

Foulser's notation is, with one exception, followed throughout, and in order to save space this paper cannot be read independently. In particular, it is necessary to have at hand the first two sections plus the first lemma of §5 of Foulser's paper.

1. **A class of λ-systems.** Let p be an arbitrary prime, s an arbitrary natural number and $q=p^s$. Let d be a natural number, whose unique factorization as a product of primes is given by

$$d = r_1^{\alpha_1} r_2^{\alpha_2} \cdots r_t^{\alpha_t},$$

where $t \geqq 3$. Following Foulser's notation let $n=q^d$, and denote by I_{n-1} the integers modulo $n-1$. Similarly, denote by I_d the integers modulo d. To define a λ-system it is sufficient to define a mapping $\lambda: I_{n-1} \to I_d$ satisfying the conditions of Foulser's Lemma 2.1 [1, p. 382]. With this objective in mind we proceed to separate I_{n-1} into $k+1$ mutually disjoint subsets, where $3 \leqq k \leqq t$, and t is the number of distinct prime factors of d. In order to do this, the following notation is needed. Choose integers $\beta_1, \beta_2, \cdots, \beta_k$ such that

Received by the editors July 17, 1968.

[1] The research of the second author was supported by NSF Grant GP 7115.

[2] The authors wish to express their appreciation to the referee for several suggestions which have considerably improved the original version of this paper.

$$1 \leqq \beta_i \leqq \alpha_i, \qquad i = 1, 2, \cdots, k.$$

Let $u = r_1 r_2 \cdots r_k$, $v = r_1^{\beta_1} r_2^{\beta_2} \cdots r_k^{\beta_k}$,

$$u_i = u/r_i, \qquad v_i = v/r_i^{\beta_i}, \qquad i = 1, 2, \cdots, k,$$

and for $i \neq j$

$$u_{ij} = u/(r_i r_j), \qquad v_{ij} = v/(r_i^{\beta_i} r_j^{\beta_j}), \qquad i, j = 1, 2, \cdots, k.$$

Now, define $k+1$ subsets of I_{n-1} as follows:

$$X_i = \{x \in I_{n-1} \mid x \equiv i \pmod{q^{u_i} - 1}\}, \qquad i = 1, 2, \cdots, k,$$

$$X_{k+1} = \left\{x \in I_{n-1} \mid x \notin \bigcup_{i=1}^{k} X_i\right\}.$$

It is clear that for $i = 1, 2, \cdots, k$ $X_i \cap X_{k+1} = \varnothing$. To see that the remaining pairs of subsets have no common elements we will need two items from elementary number theory which are stated for future reference.

Item I. Any set of h distinct primes contains a prime $r \geqq h+1$.

Item II. If q, x are integers, $q, x \geqq 2$ then $q^x - 1 > x$.

It will now be shown that for $i, j = 1, 2, \cdots, k$ with $i \neq j$, we have $X_i \cap X_j = \varnothing$. Thus, suppose $i \neq j$ and $y \in X_i \cap X_j$. Then

$$y \equiv i \pmod{q^{u_i} - 1} \quad \text{and} \quad y \equiv j \pmod{q^{u_j} - 1},$$

whence

$$y = i + h_1(q^{u_i} - 1) = j + h_2(q^{u_j} - 1),$$

and hence

$$i - j = h_2(q^{u_j} - 1) - h_1(q^{u_i} - 1).$$

Now, clearly $u_{ij} \mid u_i$ and $u_{ij} \mid u_j$. Hence $q^{u_{ij}} - 1 \mid q^{u_i} - 1$ and $q^{u_{ij}} - 1 \mid q^{u_j} - 1$. Thus

$$i - j \equiv 0 \pmod{q^{u_{ij}} - 1}. \tag{1}$$

Since u_{ij} is a product of $k-2$ primes, it follows from Item I that at least one of the primes, say $r_\nu \geqq k-1$ and hence $u_{ij} \geqq k-1$. Since $k \geqq 3$, we have $u_{ij} \geqq k-1 \geqq 2$. Further, it is clear that $q \geqq 2$ and it follows from Item II that $q^{u_{ij}} - 1 > u_{ij} \geqq k-1$. Thus,

$$q^{u_{ij}} - 1 > k - 1. \tag{2}$$

Since $i, j = 1, 2, \cdots, k$ and $i \neq j$, we have $0 < |i-j| \leqq k-1$, which together with (1) gives $q^{u_{ij}} - 1 \leqq k-1$. This contradicts (2) and hence proves that $X_i \cap X_j = \varnothing$ for $i \neq j$. We see then that the $k+1$ subsets

X_i, $i=1, 2, \cdots, k+1$ are mutually disjoint. Further it is clear that none of them is empty and $I_{n-1}=\bigcup_{i=1}^{k+1} X_i$.

These $k+1$ subsets of I_{n-1} are now used to define a mapping $\lambda: I_{n-1}\to I_d$ as follows:

$$\begin{aligned} \lambda(x) &= 0 \qquad \text{if } x \in X_{k+1}, \\ &= v_i \qquad \text{if } x \in X_i, \qquad i = 1, 2, \cdots, k. \end{aligned} \tag{3}$$

To see that this mapping defines a λ-system it will now be shown that it satisfies the conditions of Lemma 2.1 [1, p. 382]. These are, (i) $\lambda(0)=0$; and (ii) for $i, j\in I_{n-1}$, if $i\not\equiv j$ then $i\not\equiv j \pmod{q^h-1}$ where $h=(d, \lambda(i)-\lambda(j))$. That (i) is satisfied will follow from the fact that for $i=1, 2, \cdots, k$ we have $0\not\equiv i \pmod{q^{u_i}-1}$. To see this suppose $i\equiv 0 \pmod{q^{u_i}-1}$, and let $u_\mu=\min\{u_i \mid i=1, 2, \cdots, k\}$. Then clearly, $q^{u_i}-1\geqq q^{u_\mu}-1$. Since u_μ is a product of $k-1$ distinct primes, it follows from Item I that $u_\mu\geqq k$. From Item II we have $q^{u_\mu}-1>u_\mu$. We also have $k\geqq i$ and the assumption $i\equiv 0 \pmod{q^{u_i}-1}$ implies $i\geqq q^{u_i}-1$. Stringing these inequalities together we have

$$k \geqq i \geqq q^{u_i} - 1 \geqq q^{u_\mu} - 1 > u_\mu \geqq k,$$

which gives $k>k$, a contradiction. Thus $0\notin X_i$, $i=1, 2, \cdots, k$, which implies $\lambda(0)=0$. To see that condition (ii) is satisfied, we must show that for $x, y \in I_{n-1}$, if $x \not\equiv y$ then $x\not\equiv y \pmod{q^h-1}$ where $h=(d, \lambda(x)-\lambda(y))$. To prove this we consider three cases.

Case 1. Suppose $x, y\in X_i$. Then $\lambda(x)=\lambda(y)$, and $h=(d, 0)=d$. Since $q^d-1=n-1$, it is clear that $x\not\equiv y$, $x, y\in I_{n-1}$, imply $x\not\equiv y \pmod{q^d-1}$.

Case 2. Suppose $x\in X_{k+1}$, $y\in X_i\not\equiv X_{k+1}$. In this case $\lambda(x)=0$ and $\lambda(y)=v_i$. We then have $h=(d, \lambda(x)-\lambda(y))=v_i$. Suppose that $x\equiv y \pmod{q^{v_i}-1}$. Since $u_i \mid v_i$, $q^{u_i}-1 \mid q^{v_i}-1$, and hence $x\equiv y \pmod{q^{u_i}-1}$, but $y\in X_i$ implies $y\equiv i \pmod{q^{u_i}-1}$. These last two congruences give $x\equiv i \pmod{q^{u_i}-1}$ which implies $x\in X_i$, a contradiction. Hence $x\not\equiv y \pmod{q^h-1}$.

Case 3. Suppose $x\in X_i$, $y\in X_j$ and $i\not\equiv k+1\not\equiv j\not\equiv i$. In this case $\lambda(x)=v_i$, $\lambda(y)=v_j$ and $h=(d, v_i-v_j)=m\cdot v_{ij}$. Since $u_{ij} \mid v_{ij}$, we see that u_{ij} is a factor of h and hence $x\equiv y \pmod{q^h-1}$ implies

$$x \equiv y \pmod{q^{u_{ij}} - 1}. \tag{4}$$

Further, since $u_{ij} \mid u_i$ and $u_{ij} \mid u_j$, we also have

$$x \equiv i \pmod{q^{u_{ij}} - 1}, \tag{5}$$

and

$$y \equiv j \pmod{q^{u_{ij}} - 1}. \tag{6}$$

It follows from (4), (5) and (6) that

$$i - j \equiv 0 \pmod{q^{u_i j} - 1}. \tag{7}$$

From Items I and II, we obtain, as before, the inequality

$$q^{u_i j} - 1 > k - 1. \tag{8}$$

The same argument used to show that (1) and (2) lead to a contradiction, will show that (7) and (8) produce a contradiction. Thus $x \not\equiv y \pmod{q^k - 1}$. We see then that condition (ii) is satisfied for all $x, y \in I_{n-1}$, and it follows that the mapping λ, defined above, does indeed give rise to a λ-system, in the manner prescribed by Foulser.

It remains to show that this λ-system, Q_λ, has kern $K = GF(q)$. By Foulser's Lemma 2.5 [1, p. 382] we see that the kern of Q_λ is the fixed field of the group of automorphisms of $GF(q^d)$ generated by the $\rho^{\lambda(i)}$ where ρ is the automorphism $x \to x^q$. Since the nonzero values taken by $\lambda(i)$, namely $v_1, v_2, \cdots, v_k$ are relatively prime it follows that $\langle \rho^{\lambda(i)} \rangle = \langle \rho \rangle$. Hence we have $K = GF(q)$.

Since $q = p^s$ is arbitrary, we note that for $q = 2$ our construction gives λ-systems of order 2^d with kern $GF(2)$, thus answering the question of Foulser mentioned in the introduction.

2. **The left and middle nuclei of Q_λ.** Following Foulser's notation denote by N_l and N_m, respectively the left and middle nuclei of a VW system. For a λ-system, let w be the least positive integer such that for $i, j \in I_{n-1}$, $i \equiv j \pmod{w}$ implies $\lambda(i) = \lambda(j)$. (In referring to Foulser's paper note that v is used instead of w.) Further let ω be a generator of the multiplicative group of $GF(q^d)$. Foulser has shown [1, Lemma 5.1, p. 387] that the cyclic subgroup of $GF(q^d)$, $N_w = \{\omega^i : w \mid i\}$ is a subgroup of both N_l and N_m in any λ-system. In this section it will be shown that for the λ-systems constructed in §1, we have $N_w = N_l = N_m$. To prove that $N_w = N_m$ we will need an expression for w in terms of q and the u_i, $i = 1, 2, \cdots, k$. We proceed first to do this.

It will now be shown that for the λ-systems constructed in §1, the integer w is given by

$$w = \mathrm{LCM}(q^{u_i} - 1, i = 1, 2, \cdots, k). \tag{9}$$

To prove this let $x \in I_{n-1}$, $x = 1, 2, \cdots, k$. By the definition of w, $\lambda(x) = \lambda(x + w)$. It follows that $x \equiv x + w \pmod{q^{u_x} - 1}$ or that $w \equiv 0 \pmod{q^{u_x} - 1}$ for $x = 1, 2, \cdots, k$. Thus w is a common multiple of the $q^{u_i} - 1$, $i = 1, 2, \cdots, k$. Next, let f be any common multiple of the $q^{u_i} - 1$, $i = 1, 2, \cdots, k$, and let x be any element of I_{n-1}. Then clearly if h is an arbitrary integer, we have $x + hf \equiv x \pmod{q^{u_i} - 1}$ for i

$=1, 2, \cdots, k$. If $x\in X_j$, $j=1, 2, \cdots, k$, it follows that $x+hf\in X_j$ also and hence that $\lambda(x+hf)=\lambda(x)$. If $x\in X_{k+1}$, so that $\lambda(x)=0$, then $x+hf\in X_{k+1}$ also, for otherwise we have $(x+hf)\in X_i$, where $1\leqq i\leqq k$, which implies that $x+hf\equiv i \pmod{q^{u_i}-1}$ and hence, since $f\equiv 0 \pmod{q^{u_i}-1}$, that $x\equiv i \pmod{q^{u_i}-1}$. This in turn implies that $x\in X_i$, a contradiction. Thus, for all $x\in I_{n-1}$ we have $\lambda(x+hf)=\lambda(x)$. In other words, if $i\equiv j \pmod f$, for $i, j\in I_{n-1}$, then $\lambda(i)=\lambda(j)$. This proves that f is a multiple of w, and hence (9) is proved.

To see that $N_w=N_l$ it is sufficient, in view of Foulser's Lemma 5.1 (4), to show that for every $c\in N_l$, $\lambda(c)=0$. Let $c=\omega^f$, $x=\omega^i$. Since $c\in N_l$ we have

$$\lambda(\omega^f \circ \omega^j) \equiv \lambda(\omega^f) + \lambda(\omega^j) \pmod d \tag{10}$$

for all $j\in I_{n-1}$, by (2) of Foulser's Lemma 5.1. Suppose $\lambda(c)=\lambda(f)\neq 0$. Then $\lambda(f)=v_x$ for some $x=1, 2, \cdots, k$. Since $k\geqq 3$, we can choose j so that $j\neq x$ and $r_j>2$. With this choice of j the congruence (10) becomes

$$\lambda(\omega^f \circ \omega^j) \equiv v_x + v_j \pmod d. \tag{11}$$

Now, let $r_x'=r_x^{\beta_x}$ and $r_j'=r_j^{\beta_j}$. Since $r_x'\geqq 2$ and $r_j'>2$, we have

$$v_x + v_j = v(1/r_x' + 1/r_j') < v(\tfrac{1}{2} + \tfrac{1}{2}) = v \leqq d$$

or $v_x+v_j<d$. Further, $0<v_x+v_j$. It then follows from (11) that $\lambda(\omega^f \circ \omega^j)=v_h\neq 0$, and that $v_h\equiv v_x+v_j \pmod d$. But $v_h<d$, and hence this last congruence implies

$$v_h = v_x + v_j. \tag{12}$$

Again let $r_h'=r_h^{\beta_h}$. A simple computation then shows that (12) implies

$$r_x' r_j' = r_h'(r_x' + r_j'). \tag{13}$$

Since $j\neq x$, $(r_j', r_x')=1$ which implies that $(r_j', r_x'+r_j')=1$. This together with (13) implies that r_j' is a factor of r_h' and hence that $r_j'=r_h'$. Equation (13) then gives $r_x'=r_x'+r_j'$ which implies $r_j'=0$, a contradiction. We conclude that $\lambda(c)=\lambda(f)=0$ and hence that $N_w=N_l$.

Using (3) of Foulser's Lemma 5.1, and an argument similar to the above, it can be shown that if $c\in N_m$ then $\lambda(c)=0$. To see that this implies $N_w=N_m$, let $c=\omega^f\in N_m$, so that $\lambda(c)=\lambda(f)=0$. Let $x=\omega^i$ be an arbitrary nonzero element of Q_λ. Then, by Lemma 5.1 (3) [1, p. 387], we have

$$\lambda(x \circ c) \equiv \lambda(x) \pmod d. \tag{14}$$

Further, $x \circ c = \omega^i \circ \omega^f = \omega^{i+fq^{\lambda(i)}}$, and hence (14) may be written

$$\lambda(i + fq^{\lambda(i)}) \equiv \lambda(i) \pmod{d}. \tag{15}$$

Since $0 \leqq \lambda(y) < d$ for all $y \in I_{n-1}$, (15) implies that $\lambda(i+fq^{\lambda(i)}) = \lambda(i)$. Further, this holds for all $i \in I_{n-1}$, and in particular for $i = 1, 2, \cdots, k$ we have $i+fq^{\lambda(i)} \in X_i$. This implies that

$$i + fq^{\lambda(i)} \equiv i \pmod{q^{u_i} - 1} \tag{16}$$

holds for $i = 1, 2, \cdots, k$, and hence that $fq^{\lambda(i)} \equiv 0 \pmod{q^{u_i}-1}$ for such i. Since $(q^{\lambda(i)}, q^{u_i}-1) = 1$, we have $f \equiv 0 \pmod{q^{u_i}-1}$, that is, f is a common multiple of the $q^{u_i}-1$. It follows that $f = hw$, since w is the least common multiple of the $q^{u_i}-1$. This proves that $N_m \subseteq N_w$, which together with $N_w \subseteq N_m$ (as mentioned above) gives $N_w = N_m$. This completes the proof that $N_w = N_l = N_m$.

Reference

1. D. A. Foulser, *A generalization of Andre's systems*, Math. Z. **100** (1967), 380–395.

University of Missouri, Columbia