JOURNAL OF NUMBER THEORY 8, 109–130 (1976)

Combinatorial Structures in Loops, III. Difference Sets in Special Cyclic Neofields

E. C. JOHNSEN*

Department of Mathematics, The University of California, Santa Barbara, California

AND

T. STORER†

Department of Mathematics, The University of Michigan, Ann Arbor, Michigan

Communicated by D. J. Lewis

Received October 27, 1972

1. INTRODUCTION

The notion of a difference set in a general finite group was introduced in [1] and has been extensively studied in the case where the group is abelian. In [2] we have generalized this concept to that of a loop difference set and discussed its relation to certain types of block systems and designs. The present paper discusses certain cases of the existence of these combinatorial structures in loops which are the additive structures of special cyclic neofields. More precisely, if $(-d)_R$ and $(-d)_L$ are the right and left negatives of the element d in an additive loop $\mathbb{L}$ of order v, then a $\langle v, k, \lambda\rangle$ right (left) loop difference set is a k-subset $D = \{d_1, d_2, \ldots, d_k\}$ of $\mathbb{L}$ with the property that each element of $\mathbb{L} - \{0\}$ occurs exactly λ times among the differences $d_i + (-d_j)_R((-d_i)_L + d_j)$, and $0 < \lambda < k < v - 1$. By an easy counting argument it is readily seen that here the parameters satisfy the equation

$$(v - 1)\lambda = k(k - 1). \tag{1.1}$$

We remark that, in contrast to the situation for groups, a right loop difference set need not, in general, be a left loop difference set. However, if $\mathbb{L}$ is a loop in which D is a right loop difference set then the anti-

* Supported in part by Air Force Office of Scientific Research Grants AFOSR 698-67 and 72-2163.

† Supported in part by an NSF Research Grant.

isomorphic copy of $\mathbb{L}$ is a loop in which D is a left loop difference set, and conversely. Thus, we shall without loss of generality, restrict our attention to loops which admit right loop difference sets.

Fundamental to the present approach is the introduction of further structure into the loops under consideration, and this is done by restricting our attention to loops which represent the additive structures of cyclic neofields of order v. We discuss the conditions under which the eth powers or the eth powers plus zero, $e \mid v - 1$, form a right loop difference set in these structures. These conditions are, in fact, an extension of Lehmer's criterion [4] to cyclic neofields. It is found that for $e = 2$ the squares and the squares plus zero form right loop difference sets in every cyclic neofield of order $v \equiv 3 \pmod 4$.

Essential to the successful application of Lehmer's criterion is the development of a workable cyclotomic theory for the structures under consideration. In Section 3 we construct a special family of right inverse property (RIP) cyclic neofields for every order $v > 5$ for which, unlike the situation for the finite field, the problem of cyclotomy is completely solved. Here the analysis yields the neofield analogue of residue difference sets for $e = 2$ for every set of Hadamard parameters v, $k = (v - 1)/2$, $\lambda = (v - 3)/4$, and complementary Hadamard parameters v, $k_c = (v + 1)/2$, $\lambda_c = (v + 1)/4$, with $v \equiv 3 \pmod 4$. In the last section we turn our attention to a special class [3] of commutative inverse-property, cyclic (CIP) neofields of prime-power order, where the problem of cyclotomy is solved if and only if it is solved for the corresponding field. Residue difference sets are investigated for the values $e = 2, 3, 4, 6$, and 8. With respect to the situation in the field, no new residue difference sets are obtained in the constructed neofields for $e = 2, 3, 4$, and 8. However, for $e = 6$ the sextic residues and the sextic residues plus zero are found to form difference sets in certain classes of these constructed neofields. This does not happen in the fields.

2. Preliminaries

For the terminology and notation concerning neofields the reader is referred to Section 2 of [3]. Let $\mathbb{N}_v(+, \cdot)$ be a cyclic neofield of order v with presentation given by $\mathbb{N}_v = \{0, 1, a, a^2, \ldots, a^{v-2}\}$, $a^{v-1} = 1$, and the presentation function $T(x) \equiv 1 + x$ for all $x \in \mathbb{N}_v$. We introduce a cyclotomic structure into $\mathbb{N}_v$ in a manner analogous to that for finite fields (see [6] for details). For any proper divisor e of $v - 1$, $1 < e < v - 1$, we write $v - 1 = ef$ and define the cyclotomic classes in $\mathbb{N}_v$ by

$$C_i = \{a^{es+i} \mid s = 0, 1, \ldots, f - 1\}, \qquad i = 0, 1, \ldots, e - 1. \qquad (2.1)$$

Note that the cyclotomic classes are pairwise disjoint, of the same cardinality, and that their union is $\mathbb{N}_v{}^*$. If b is a fixed element in $\mathbb{N}_v{}^*$, let $(C_i, b; C_j)$ denote the number of ordered pairs $(z_i, z_j) \in C_i \times C_j$ such that $z_i + b = z_j$, and $(b, C_i; C_j)$ denote the number of ordered pairs $(z_i, z_j) \in C_i \times C_j$ such that $b + z_i = z_j$. Noting that in a cyclic neofield every element x has a unique two-sided negative $-x$, where $-x = (-1)x$, we define the four types of cyclotomic numbers

$$\begin{aligned} &\text{(a)}\quad (i,j)_R^+ \equiv (C_i, 1; C_j), \qquad &&\text{(b)}\quad (i,j)_R^- \equiv (C_i, -1; C_j), \\ &\text{(c)}\quad (i,j)_L^+ \equiv (1, C_i; C_j), \qquad &&\text{(d)}\quad (i,j)_L^- \equiv (-1, C_i; C_j), \end{aligned} \tag{2.2}$$

where $0 \leqslant i, j \leqslant e - 1$. We shall also write $z + (-1)$ as $z - 1$. Note that $-1 = 1$ if v is even and that $-1 = a^{(v-1)/2}$ if v is odd [5]. Now, the cyclotomic class to which -1 belongs is given by

$$-1 \in \begin{cases} C_0, & \text{if } vf \text{ is even}, \\ C_{e/2}, & \text{if } vf \text{ is odd}. \end{cases} \tag{2.3}$$

The following lemma gives the elementary relations for the e^2 cyclotomic numbers of each type for a fixed cyclic neofield $\mathbb{N}_v$ of order v and fixed proper divisor $e \mid v - 1$.

LEMMA 2.1. *The four types of cyclotomic numbers, where (i, j) is a generic notation for any one of the four, satisfy the following elementary relations for a given $\mathbb{N}_v$ and e.*

(i) $(i + me, j + ne) = (i, j)$ *for all integers m and n.*

(ii) *If η_j and θ_i are defined by*

$$\eta_j = \begin{cases} 1, & j = 0, \\ 0, & \textit{otherwise}, \end{cases} \qquad \theta_i = \begin{cases} 1, & vf \textit{ even and } i = 0, \\ 1, & vf \textit{ odd and } i = e/2, \\ 0, & \textit{otherwise}, \end{cases}$$

then

(a) $$\sum_{i=0}^{e-1} (i,j)_R^+ = \sum_{i=0}^{e-1} (i,j)_L^+ = f - \eta_j.$$

(b) $$\sum_{i=0}^{e-1} (i,j)_R^- = \sum_{i=0}^{e-1} (i,j)_L^- = f - \theta_j.$$

(c) $$\sum_{j=0}^{e-1} (i,j)_R^+ = \sum_{j=0}^{e-1} (i,j)_L^+ = f - \theta_i.$$

(d) $\sum_{j=0}^{e-1} (i,j)_R^- = \sum_{j=0}^{e-1} (i,j)_L^- = f - \eta_i$.

(e) $(i,j)_R^- = \begin{cases} (i,j)_R^+, & vf \textit{ even}, \\ (e/2 + i, e/2 + j)_R^+, & vf \textit{ odd}. \end{cases}$

(f) $(i,j)_L^+ = (e - i, j - i)_R^+$.

(g) $(i,j)_L^- = \begin{cases} (e - i, j - i)_R^+, & vf \textit{ even}, \\ (e/2 - i, j - i)_R^+, & vf \textit{ odd}. \end{cases}$

Proof. (i) follows since $\mathbb{N}_v^*(\cdot)$ is cyclic. From the first four relations in (ii) we prove (c). The other three will follow in similar fashion. The expression

$$\sum_{j=0}^{e-1} (i,j)_R^+$$

counts the total number of elements of the cyclotomic class C_i that are followed additively by an element of some other cyclotomic class. Now $|C_i| = f$ and the only element of C_i not followed by an element from another cyclotomic class would be -1 when $-1 \in C_i$. By (2.3), $-1 \in C_i$ either when vf is even and $i = 0$ or when vf is odd and $i = e/2$. Thus, this first expression in (c) equals $f - \theta_i$. By virtually the same argument, the second expression in (c) also equals $f - \theta_i$. Relations (e), (f), and (g) follow algebraically from the definitions of the cyclotomic numbers and (2.3).

In the special case $e = 2$, the distribution of squares and nonsquares in the rows and columns of the addition table $\hat{\mathbb{N}}_v$ for a cyclic neofield $\mathbb{N}_v$ provides just enough additional information to combinatorially determine all of the cyclotomic numbers. We demonstrate this by exhibiting the numbers $(0, 0)_R^-$ for all cyclic neofields of order $v = 2f + 1$.

LEMMA 2.2. *For any cyclic neofield* $\mathbb{N}_v$ *of order* $v = 2f + 1$,

$$(0, 0)_R^- = \begin{cases} (v - 3)/4 = (f - 1)/2, & \textit{if} \quad v \equiv 3 \pmod 4, \\ (v - 5)/4 = (f - 2)/2, & \textit{if} \quad v \equiv 1 \pmod 4. \end{cases}$$

The relations of Lemma 2.1 *now suffice to determine all cyclotomic numbers for* $\mathbb{N}_v$ *with* $e = 2$.

Proof. Let $v \equiv 3 \pmod 4$. Here f is odd and the relations of Lemma 2.1 imply that $(0, 0)_R^- = (1, 1)_R^- = x$ and $(0, 1)_R^- + 1 = (1, 0)_R^- = y$, where $x + y = f$. Now, there are x squares in the set $Q_0 \equiv \{a^{2i} + (-1) \mid 0 \leqslant i \leqslant f - 1\}$, and since $0 \in Q_0$ there are $f - 1 - x$ nonsquares in Q_0.

Since -1 is a nonsquare, there are $f - 1 - (f - 1 - x) = x$ nonsquares in the set $Q_1 = \{a^{2i+1} + (-1) \mid 0 \leqslant i \leqslant f - 1\}$. Consider the number of elements $z \in \mathbb{N}_v$ such that $-1 + z$ is a nonsquare. One of these is $z = 0$. Suppose $z \neq 0$. Then the remaining number is the number of $z \in \mathbb{N}_v{}^*$ such that either $z^{-1} + (-1)$ is a square when z^{-1} is a square or $z^{-1} + (-1)$ is a nonsquare when z^{-1} is a nonsquare. By the above this number is $2x$; hence, the total number of nonsquares in $\{-1 + z \mid z \in \mathbb{N}_v\}$ is $2x + 1$. Since this number must be f we have $x = (f - 1)/2$, as asserted. The proof for $v \equiv 1 \pmod 4$ is entirely similar.

If the cyclic neofield, in addition, has the right inverse property (RIP) then further relations are obtained.

LEMMA 2.3. *If $\mathbb{N}_v$ is an RIP cyclic neofield, then the following relations hold in addition to those of Lemma* 2.1.

(i) $(i,j)_R^+ = \begin{cases} (j, i)_R^+, & vf \textit{ even}, \\ (j + e/2, i + e/2)_R^+, & vf \textit{ odd}. \end{cases}$

(ii) $(i,j)_R^- = (j, i)_R^+$.

Proof. We first prove (ii). Now $(i,j)_R^-$ is the number of pairs (r, s) such that

$$a^{er+i} + (-1) = a^{es+j}; \qquad 0 \leqslant r, s \leqslant f - 1.$$

By the RIP this is the number of pairs (r, s) such that

$$a^{es+j} + 1 = a^{er+i},$$

which is $(j, i)_R^+$. Now (i) follows from (ii) and Lemma 2.1(ii)e.

Further relations are also obtained when the cyclic neofield is (additively) commutative.

LEMMA 2.4. *If $\mathbb{N}_v$ is a commutative cyclic neofield, then the following relations hold in addition to those of Lemma* 2.1.

(i) $(i,j)_R^+ = (i,j)_L^+ = (e - i, j - i)_R^+$.

(ii) $(i,j)_R^- = (i,j)_L^- = \begin{cases} (i,j)_R^+, & vf \textit{ even}, \\ (i + e/2, j + e/2)_R^+, & vf \textit{ odd}. \end{cases}$

Proof. The first equations of (i) and (ii) are easy. The second equations follow by Lemma 2.1(ii)f and e.

When the cyclic neofield has both commutative and RIP addition, i.e., is a CIP neofield, then the content of Lemmas 2.1, 2.3, and 2.4 reduces to the elementary relations for the fields (cf. [6, p. 25]).

We now establish Lehmer's criterion for the existence of eth power right loop difference sets in cyclic neofields.

LEMMA 2.5. *C_0 is a $\langle v, (v-1)/e, (v-1-e)/e^2\rangle$ right loop difference set in the cyclic neofield $\mathbb{N}_v$ if and only if*

$$(0, i)_R^- = \lambda = (v-1-e)/e^2$$

for all $i = 0, 1, \ldots, e-1$.

Proof. For each u and i, $0 \leqslant u \leqslant f-1$, $0 \leqslant i \leqslant e-1$, the number of pairs (s, t) $0 \leqslant s, t \leqslant f-1$, for which

$$a^{es} - a^{et} = a^{eu+i}$$

is the same as the number for which

$$a^{e(s-t)} - 1 = a^{e(u-t)+i},$$

which is $(0, i)_R^-$. Hence, C_0 is a $\langle v, k, \lambda\rangle$ right loop difference set if and only if $(0, i)_R^- = \lambda$ for all $i = 0, 1, \ldots, e-1$. Since $k = f = (v-1)/e$ we have by (1.1) that $\lambda = (v-1-e)/e^2$.

COROLLARY 2.6. *The set of squares is a $\langle v, (v-1)/2, (v-3)/4\rangle$ right loop difference set in every cyclic neofield of order $v \equiv 3 \pmod 4$.*

Proof. By Lemmas 2.5 and 2.2.

As in the case of the finite fields, there is an immediate criterion for the eth powers plus zero to be a right loop difference set in a cyclic neofield.

LEMMA 2.7. *$C_0 \cup \{0\}$ is a $\langle v, (v-1+e)/e, (v-1+e)/e^2\rangle$ right loop difference set in the cyclic neofield $\mathbb{N}_v$ if and only if*

(i) *for vf even, $(0, 0)_R^- + 2 = (0, i)_R^- = (v-1+e)/e^2$ for all i, $1 \leqslant i \leqslant e-1$.*

(ii) *for vf odd, $(0, 0)_R^- + 1 = (0, e/2)_R^- + 1 = (0, i)_R^- = (v-1+e)/e^2$ for all $i \neq 0, e/2$.*

Proof. Similar to the proof of Lemma 2.5. Here we have the additional differences $a^{er} - 0 = a^{er}$ and $0 - a^{er} = -a^{er}$, $0 \leqslant r \leqslant f-1$. These represent each element in C_0 twice if $-1 \in C_0$, i.e., vf is even, and represent each element in C_0 and in $C_{e/2}$ once if $-1 \in C_{e/2}$, i.e., vf is odd. Hence the lemma.

Corollary 2.8. *The set of squares plus zero is a* $\langle v, (v+1)/2, (v+1)/4\rangle$ *right loop difference set in every cyclic neofield of order* $v \equiv 3 \pmod 4$.

Proof. By Lemma 2.2 and part (ii) of Lemma 2.7.

Corollary 2.9. *If* $\mathbb{N}_v$ *is an* RIP *cyclic neofield then*

(i) C_0 *is a* $\langle v, (v-1)/e, (v-1-e)/e^2\rangle$ *right loop difference set in* $\mathbb{N}_v$ *if and only if* $(i, 0)_R^+ = (v-1-e)/e^2$ *for all* $i = 0, 1, \ldots, e-1$.

(ii) $C_0 \cup \{0\}$ *is a* $\langle v, (v-1+e)/e, (v-1+e)/e^2\rangle$ *right loop difference set in* $\mathbb{N}_v$ *if and only if*

(a) *for* vf *even,* $(0,0)_R^+ + 2 = (i,0)_R^+ = (v-1+e)/e^2$ *for all* i, $1 \leqslant i \leqslant e-1$,

(b) *for* vf *odd,* $(0,0)_R^+ + 1 = (e/2, 0)_R^+ + 1 = (i,0)_R^+ = (v-1+e)/e^2$ *for all* $i \neq 0, e/2$.

Proof. Lemmas 2.5, 2.7, and part (ii) of Lemma 2.3.

Lemma 2.10. *If* C_0 *or* $C_0 \cup \{0\}$ *is a right loop difference set in a cyclic neofield* $\mathbb{N}_v$, *then* $2 \nmid \gcd(e, f)$.

Proof. If v is even then e must be odd; while for v odd, $(f-1)/e$ or $(f+1)/e$ (i.e., λ) an integer implies that e and f cannot both be even.

The following result, which is used implicitly in the last section, follows directly from the work of Lehmer [4].

Lemma 2.11. *If* $\mathbb{N}_v$ *is a commutative cyclic neofield of odd order* v, *then exactly one of the cyclotomic numbers* $(0, h)_R^+$ *is odd.*

Proof. Suppose $z_0 + 1 = z_i$ where $z_0 \in C_0$ and $z_i \in C_i$. Then $z_0^{-1} + 1 = 1 + z_0^{-1} = (z_0+1)\, z_0^{-1} = z_i z_0^{-1}$ where $z_0^{-1} \in C_0$ and $z_i z_0^{-1} \in C_i$. These solutions z_0, z_0^{-1} pair up except when $z_0 = z_0^{-1}$ or $z_0 = \pm 1$. Since $-1 + 1 = 0 \notin C_i$, $z_0 = -1$ is ruled out, and since $1 \neq -1$ when v is odd we are left with $1 + 1 = z_h \neq 0$ for some h. Here $z_0 = 1$ is unpaired, whence $(0, h)_R^+$ must be odd.

In the subsequent sections we shall be concerned only with RIP cyclic neofields and right loop difference sets therein. We therefore restrict our attention to the cyclotomic numbers $(i, j)_R^+$ for these structures, and henceforth simply write the more usual (i, j) for them.

3. A Class of Cyclic RIP Neofields

In this section we construct a special infinite family of cyclic RIP neofields and show that here, unlike the case for the finite field, the problem of cyclotomy (and hence the existence of eth power difference sets) is completely solvable. Let $\mathbb{N}_v = \{0, 1, a, a^2, \ldots, a^{v-2}\}$ be the set of elements written in terms of the multiplicative generator a, $a^{v-1} = 1$, where $0 \cdot x = x \cdot 0 = 0$ for all $x \in \mathbb{N}_v$. For $v > 5$ we construct the presentation function $T\colon \mathbb{N}_v \to \mathbb{N}_v$ as follows:

(1) If v is even

$$T(x) = \begin{cases} 1, & x = 0, \\ 0, & x = 1, \\ a^{2j}, & x = a^j \text{ and } 1 \leqslant j \leqslant v-2. \end{cases}$$

(2) If v is odd

$$T(x) = \begin{cases} 1, & x = 0, \\ a^{2j+1}, & x = a^j \text{ and } 0 \leqslant j \leqslant (v-3)/2, \\ 0, & x = -1 = a^{(v-1)/2}, \\ a^{2j}, & x = a^j \text{ and } (v+1)/2 \leqslant j \leqslant v-2. \end{cases}$$

The addition in $\mathbb{N}_v$ is introduced by $0 + x = x + 0 = x$ and $1 + x = T(x)$ for all $x \in \mathbb{N}_v$ and is extended to all of $\mathbb{N}_v$ by distributivity. Clearly the function T is onto. It is easy to verify that for no $x, y \in \mathbb{N}_v$, $x \neq 1$, do we have $xT(y) = T(xy)$, whence $\mathbb{N}_v(+)$ is a loop and thus $\mathbb{N}_v(+, \cdot)$ is a cyclic neofield. It remains to be shown that these neofields have the RIP.

LEMMA 3.1. *The neofields $\mathbb{N}_v$ constructed above have the* RIP.

Proof. Since $\mathbb{N}_v{}^*(\cdot)$ is cyclic and both distributive laws hold, it suffices to prove that for all j, $0 \leqslant j \leqslant v-2$, we have

$$(a^j + 1) + (-1) = a^j.$$

We give details for the (more difficult) case where v is odd; the analysis for even v being entirely similar. For $j = 0$ we have, by construction

$$\begin{aligned}(1 + 1) + (-1) &= T(1) + (-1) \\ &= a(1 + a^{(v-3)/2}) = aT(a^{(v-3)/2}) = 1.\end{aligned}$$

For $1 \leqslant j \leqslant v-2$ we use the relation $a^j + 1 = a^j T(a^{-j})$, whence

$$a^j + 1 = \begin{cases} a^{v-j-1}, & 1 \leqslant j \leqslant (v-3)/2, \\ 0, & j = (v-1)/2, \\ a^{v-j}, & (v+1)/2 \leqslant j \leqslant v-2, \end{cases}$$

and then

$$(a^j + 1) + (-1) = \left\{\begin{array}{ll} a^{(v-1)/2}(a^{(v-1)/2-j} + 1), & 1 \leqslant j \leqslant (v-3)/2, \\ a^{(v-1)/2}, & j = (v-1)/2, \\ a^{(v-1)/2}(a^{(v-1)/2-j+1} + 1), & (v+1)/2 \leqslant j \leqslant v-2, \end{array}\right\}$$

$$= a^j.$$

The additive class structure for this collection of neofields is completely determined by the following theorem.

THEOREM 3.2. *Let* $v = ef + 1 > 5$, *and let* $\mathbb{N}_v$ *be the cyclic* RIP *neofield of order* v *constructed above. Then, the nonzero cyclotomic numbers* (i, j), $0 \leqslant i, j \leqslant e-1$, *for* $\mathbb{N}_v$ *and* e *are given by*

(i) *v even*:

$$(0, 0) + 1 = (k, e-k) = f \quad \textit{for} \quad k = 1, 2, \ldots, e-1.$$

(ii) *v odd*:

(a) *If f is even,*

$$1 + (0, 0) = (0, 1) = (k, e-k)$$
$$= (k, e-k+1) = f/2 \quad \textit{for} \quad k = 1, 2, \ldots, e-1.$$

(b) *If f is odd,*

$$(e/2, e/2) = (e/2, e/2 + 1) = (f-1)/2,$$

and

$$(k, e-k) = (k, e-k+1) + 1$$
$$= (f+1)/2 \quad \textit{for} \quad k = 1, 2, \ldots, (e-2)/2,$$

while

$$(k, e-k) + 1 = (k, e-k+1) = (f+1)/2$$
$$\textit{for} \quad k = (e+2)/2, (e+4)/2, \ldots, e-1, e.$$

Proof. We present the proof for v odd, the proof for v even being similar. By construction, $0 + 1 = 1$, $1 + 1 = a$, and

$$a^j + 1 = \begin{cases} a^{v-j-1}, & 1 \leqslant j \leqslant (v-3)/2, \\ 0, & j = (v-1)/2, \\ a^{v-j}, & (v+1)/2 \leqslant j \leqslant v-2. \end{cases}$$

Now, $a + 1 = a^{v-2} \in C_{e-1}$ since $v - 2 \equiv ef + 1 - 2 \equiv -1 \pmod{e}$, whence, for $1 \leqslant 1 + ke \leqslant (v-3)/2$,

$$a^{1+ke} + 1 = a^{v-2-ke} \in C_{e-1}$$

also. Now

$$(v-3)/2 = [f/2]e - 1 + \tfrac{1}{2}e\delta_f$$

where

$$\delta_f = \begin{cases} 0, & f \text{ even}, \\ 1, & f \text{ odd}, \end{cases}$$

whence, if f is even, there are $(f-2)/2$ complete residue systems modulo e plus the residues $1, 2, \ldots, e-1$ among the exponents j, $1 \leqslant j \leqslant (v-3)/2$, while, if f is odd, there are $(f-1)/2$ complete residue systems modulo e plus the residues $1, 2, \ldots, (e-2)/2$ among these exponents.

Similarly,

$$v - 2 - (v+1)/2 + 1 = (v-3)/2 = [f/2]e - 1 + \tfrac{1}{2}e\delta_f$$

and

$$(v+1)/2 = ef/2 + 1 \equiv \begin{cases} 1 \pmod{e}, & f \text{ even}, \\ e/2 + 1 \pmod{e}, & f \text{ odd}, \end{cases}$$

whence

$$a^{(v+1)/2} + 1 = a^{(v-1)/2} \in \begin{cases} C_0, & f \text{ even}, \\ C_{e/2}, & f \text{ odd}. \end{cases}$$

Thus, if f is even there are again $(f-2)/2$ complete residue systems mod e plus the residues $1, 2, \ldots, e-1$ among the exponents j, while if f is odd, there are $(f-1)/2$ complete residue systems mod e plus the residues $e/2 + 1, e/2 + 2, \ldots, e-1$ among these exponents. Collecting these results yields the theorem.

The *cyclotomic matrix* for $\mathbb{N}_v$ and e is defined to be the $e \times e$ matrix $\mathbf{C}_e$ whose i, j entry is the cyclotomic number (i, j), $0 \leqslant i, j \leqslant e-1$. As illustrative examples, we exhibit the matrices $\mathbf{C}_e$ for v odd and $e = 2, 3, 4$.

$$e = 2: \quad \begin{array}{|c|c|} \hline \frac{v-5}{4} & \frac{v-1}{4} \\ \hline \frac{v-1}{4} & \frac{v-1}{4} \\ \hline \end{array} \qquad \begin{array}{|c|c|} \hline \frac{v-3}{4} & \frac{v+1}{4} \\ \hline \frac{v-3}{4} & \frac{v-3}{4} \\ \hline \end{array}$$

f even $\qquad$ f odd

$e = 3$:

$\frac{v-7}{6}$	$\frac{v-1}{6}$	0
$\frac{v-1}{6}$	0	$\frac{v-1}{6}$
0	$\frac{v-1}{6}$	$\frac{v-1}{6}$

f even

$e = 4$:

$\frac{v-9}{8}$	$\frac{v-1}{8}$	0	0
$\frac{v-1}{8}$	0	0	$\frac{v-1}{8}$
0	0	$\frac{v-1}{8}$	$\frac{v-1}{8}$
0	$\frac{v-1}{8}$	$\frac{v-1}{8}$	0

f even

$\frac{v-5}{8}$	$\frac{v+3}{8}$	0	0
$\frac{v-5}{8}$	0	0	$\frac{v+3}{8}$
0	0	$\frac{v-5}{8}$	$\frac{v-5}{8}$
0	$\frac{v-5}{8}$	$\frac{v+3}{8}$	0

f odd

Theorem 3.2 and Corollary 2.9 give immediate necessary and sufficient conditions for the eth-powers or the eth-powers plus 0 to form a right loop difference set in the above cyclic RIP neofields.

THEOREM 3.3. *The set of eth-powers and the set of eth-powers plus* 0 *in the special class of cyclic* RIP *neofields* $\mathbb{N}_v$ $(v > 5)$ *constructed above form a right loop difference set if and only if* $e = 2$ *and* $v \equiv 3 \pmod 4$, *in which case the parameters of the difference set are* v, $k = (v-1)/2$, $\lambda = (v-3)/4$ *and* v, $k = (v+1)/2$, $\lambda = (v+1)/4$, *respectively.*

We remark that for $v = 7$ we have

$$\begin{aligned} C_0 &= \{1, a^2, a^4\}, & a^3 + C_0 &= \{0, 1, a\}, \\ 1 + C_0 &= \{a, a^2, a^5\}, & a^4 + C_0 &= \{1, a^3, a^5\}, \\ a + C_0 &= \{0, a^4, a^5\}, & a^5 + C_0 &= \{0, a^2, a^3\}, \\ a^2 + C_0 &= \{a, a^3, a^4\}, \end{aligned}$$

which is a $\langle 7, 3, 1\rangle$ block design, by inspection; we also have the $\langle 7, 4, 2\rangle$ block design $\{x + D\}$ for $D = C_0 \cup \{0\}$ and $x \in \mathbb{N}_v$. For $v \neq 7$, however, we have

$$1 + C_0 = \{a^j\colon 1 \leqslant j \leqslant v - 2 \text{ and } j \equiv 1, 2 \pmod 4\},$$
$$a^2 + C_0 = \{a^i\colon 3 \leqslant i \leqslant v - 3 \text{ and } i \equiv 0, 3 \pmod 4\} \cup \{a\},$$

and

$$1 + \{C_0 \cup \{0\}\} = \{1 + C_0\} \cup \{1\},$$
$$a^2 + \{C_0 \cup \{0\}\} = \{a^2 + C_0\} \cup \{a^2\},$$

whence

$$\{1 + C_0\} \cap \{a^2 + C_0\} = \{a\},$$

and $\lambda = (v - 3)/4 > 1$ implies that C_0 is not the initial block of a $\langle v, (v - 1)/2, (v - 3)/4\rangle$ right loop design. Further,

$$(1 + \{C_0 \cup \{0\}\}) \cap (a^2 + \{C_0 \cup \{0\}\}) = \{a, a^2\},$$

and $\lambda = (v + 1)/4 > 2$ implies that $C_0 \cup \{0\}$ is not the initial block of a $\langle v, (v + 1)/2, (v + 1)/4\rangle$ right loop design. Nevertheless, by Theorem 3.2 of [2], we have that

$$| C_0 \cap (x + C_0)| = \lambda \qquad \text{for all} \quad x \in \mathbb{N}_v, x \neq 0,$$

whenever C_0 is a right loop difference set in a cyclic neofield with the RIP.

4. Cyclotomy in a Family of CIP Neofields

Let $\mathbb{F}_v(+, \cdot)$ be a finite field of order $v = ef + 1 \geqslant 11$ with presentation given by $\mathbb{F}_v = \{0, 1, a, a^2, \ldots, a^{v-2}\}$ and the presentation function $T(x) = 1 + x$, $x \in \mathbb{F}_v$. Define T_0 on $\mathbb{F}_v$ by

$$T_0(x) = \begin{cases} T(x), & x = 0, -1, \\ x/T(x), & \text{otherwise}, \end{cases}$$

and T' by

$$T'(x) = -1 + x, \qquad x \in \mathbb{F}_v.$$

Let $S = \{x \in \mathbb{F}_v \mid T'T_0(x) \neq x\}$, and for $x \in S$ define the *orbit* $\theta(x)$ of x by

$$\theta(x) = \{x, T'T_0(x), (T'T_0)^2(x)\}.$$

The following theorem was proved in [3].

THEOREM 4.1. *Let $\mathbb{F}_v(+, \cdot)$ be a field of order $v \geqslant 11$ with presentation function T, and let T_* be any mapping on $\mathbb{F}_v$ satisfying*

(a) $T_* \not\equiv T$ *and* $T_* \not\equiv T_0$ *on* $\mathbb{F}_v$,

(b) *for each* $x \in \mathbb{F}_v$, *either* $T_*(x) = T(x)$ *or* $T_*(x) = T_0(x)$,

(c) *if* T_* *agrees with* T (*or* T_0) *at* $x \in S$, *then* T_* *agrees with* T (*or* T_0) *on* $\theta(x) \cup \theta(x^{-1})$.

Then T_* *is the presentation function for a* CIP *neofield* $\mathbb{N}_v(\boxplus, \cdot)$ *where* $\mathbb{N}_v(\cdot)$ *is identical to* $\mathbb{F}_v(\cdot)$.

In order to discuss the cyclotomic structure of the neofields $\mathbb{N}_v$ constructed by Theorem 4.1, we assume that the cyclotomic structure for $\mathbb{F}_v$ and e is known. For $x \in S$ we have

$$\theta(x) \cup \theta(x^{-1}) = \{x, -1/T(x), -T(x)/x, 1/x, -x/T(x), -T(x)\},$$

which reduces to a triple

$$\theta(1) = \{1, -1/T(1), -T(1)\}$$

precisely when $x \in \theta(1)$. If T_* is the presentation function of a fixed neofield $\mathbb{N}_v$ constructed by Theorem 4.1, and if $x \in S - \theta(1)$ is an element of $\mathbb{N}_v$ for which $T_*(x) = T_0(x)$, then the cyclotomic relations for $\mathbb{F}_v$ and e are altered in a regular manner depending upon the cyclotomic classes to which x and $T(x)$ belong. For $x \in C_i$ and $T(x) \in C_j$, we have Table I.

TABLE I

$\theta(x) \cup \theta(x^{-1})$	$T\{\theta(x) \cup \theta(x^{-1})\}$	$T_0\{\theta(x) \cup \theta(x^{-1})\}$
$x \in C_i$	$T(x) \in C_j$	$\dfrac{x}{T(x)} \in C_{i-j}$
$\dfrac{-1}{T(x)} \in \begin{cases} C_{e-j} \text{ } vf \text{ even} \\ C_{e/2-j} \text{ } vf \text{ odd} \end{cases}$	$\dfrac{x}{T(x)} \in C_{i-j}$	$\dfrac{-1}{x} \in \begin{cases} C_{e-i} \text{ } vf \text{ even} \\ C_{e/2-i} \text{ } vf \text{ odd} \end{cases}$
$\dfrac{-T(x)}{x} \in \begin{cases} C_{j-i} \text{ } vf \text{ even} \\ C_{e/2+j-i} \text{ } vf \text{ odd} \end{cases}$	$\dfrac{-1}{x} \in \begin{cases} C_{e-i} \text{ } vf \text{ even} \\ C_{e/2-i} \text{ } vf \text{ odd} \end{cases}$	$T(x) \in C_j$
$\dfrac{1}{x} \in C_{e-i}$	$\dfrac{T(x)}{x} \in C_{j-i}$	$\dfrac{1}{T(x)} \in C_{e-j}$
$\dfrac{-x}{T(x)} \in \begin{cases} C_{i-j} \text{ } vf \text{ even} \\ C_{e/2+i-j} \text{ } vf \text{ odd} \end{cases}$	$\dfrac{1}{T(x)} \in C_{e-j}$	$-x \in \begin{cases} C_{i} \text{ } vf \text{ even} \\ C_{e/2+i} \text{ } vf \text{ odd} \end{cases}$
$-T(x) \in \begin{cases} C_{j} \text{ } vf \text{ even} \\ C_{e/2+j} \text{ } vf \text{ odd} \end{cases}$	$-x \in \begin{cases} C_{i} \text{ } vf \text{ even} \\ C_{e/2+i} \text{ } vf \text{ odd} \end{cases}$	$\dfrac{T(x)}{x} \in C_{j-i}$

Hence, replacement of T by T_0 on $\theta(x) \cup \theta(x^{-1})$ effects the changes in the cyclotomic relations for $\mathbb{F}_v$ and e as shown in Table II.

TABLE II

vf even		vf odd	
decrease by 1	increase by 1	decrease by 1	increase by 1
(i,j)	$(i, i-j)$	(i,j)	$(i, i-j)$
$(e-j, i-j)$	$(e-j, e-i)$	$\left(\frac{e}{2}-j, i-j\right)$	$\left(\frac{e}{2}-j, \frac{e}{2}-i\right)$
$(j-i, e-i)$	$(j-i, j)$	$\left(\frac{e}{2}+j-i, \frac{e}{2}-i\right)$	$\left(\frac{e}{2}+j-i, j\right)$
$(e-i, j-i)$	$(e-i, e-j)$	$(e-i, j-i)$	$(e-i, e-j)$
$(i-j, e-j)$	$(i-j, i)$	$\left(\frac{e}{2}+i-j, e-j\right)$	$\left(\frac{e}{2}+i-j, \frac{e}{2}+i\right)$
(j,i)	$(j, j-i)$	$\left(\frac{e}{2}+j, \frac{e}{2}+i\right)$	$\left(\frac{e}{2}+j, j-i\right)$

If we now denote by $\Theta(i,j)$ the *orbit* of the cyclotomic number (i,j) under the elementary cyclotomic relationships for commutative IP neofields

(a) $(i,j) = (e-i, j-i)$,

(b) $(i,j) = \begin{cases} (j,i), & vf \text{ even}, \\ (e/2+j, e/2+i), & vf \text{ odd}, \end{cases}$

we find

$\underline{\Theta(i,j)}$

$$\begin{tikzcd}
(i,j) \arrow[r, leftrightarrow, "a"] \arrow[d, leftrightarrow, "b"'] & (e-i, j-i) \arrow[d, leftrightarrow, "b"] \\
(j,i) \arrow[d, leftrightarrow, "a"'] & (j-i, e-i) \arrow[d, leftrightarrow, "a"] \\
(e-j, i-j) \arrow[r, leftrightarrow, "b"] & (i-j, e-j)
\end{tikzcd}$$

vf even

$$\begin{tikzcd}
(i,j) \arrow[r, leftrightarrow, "a"] \arrow[d, leftrightarrow, "b"'] & (e-i, j-i) \arrow[d, leftrightarrow, "b"] \\
\left(\frac{e}{2}+j, \frac{e}{2}+i\right) \arrow[d, leftrightarrow, "a"'] & \left(\frac{e}{2}+j-i, \frac{e}{2}-i\right) \arrow[d, leftrightarrow, "a"] \\
\left(\frac{e}{2}-j, i-j\right) \arrow[r, leftrightarrow, "b"] & \left(\frac{e}{2}+i-j, e-j\right)
\end{tikzcd}$$

vf odd

Direct comparison shows that $\Theta(i,j)$ and $\Theta(e-i, e-j)$ comprise the entries under "decrease by 1" and "increase by 1," respectively, in the above table; thus the orbits $\Theta(i,j)$ and $\theta(x) \cup \theta(x^{-1})$ are intimately connected. We remark that the orbits under Θ are $\{(0,0)\}$ for vf even, $\{(0, e/2)\}$ for vf odd; $\{(e/3, 2e/3), (2e/3, e/3)\}$ for vf even, $\{(e/3, e/6), (2e/3, 5e/6)\}$ for vf odd, when $e \equiv 0 \pmod 3$; $\{(i,0), (e-i, e-i), (0,i)\}$ for vf even, $\{(i, e/2), (e-i, e/2-i), (0, e/2+i)\}$ for vf odd, when $i \not\equiv 0 \pmod e$; and the proper sextuples $\Theta(i,j)$ otherwise. In the first two cases we have $\Theta(i,j) = \Theta(e-i, e-j)$, whence the choice $T_* = T_0$ on the corresponding sextuples leaves the cyclotomic numbers for the parent field structure unaltered. In the third case we have $\Theta(i,j) = \Theta(e-i, e-j)$ if and only if e is even and $i = e/2$, while if $\Theta(i,j)$ is a proper sextuple we find $\Theta(i,j) = \Theta(e-i, e-j)$ for exactly the schemes

$\underline{\Theta(i,j)}$

$$\begin{tikzcd}
(2i,i) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & (e-2i, e-i) \arrow[d, leftrightarrow] \\
(i,2i) \arrow[d, leftrightarrow] & (e-i, e-2i) \arrow[d, leftrightarrow] \\
(e-i, i) \arrow[r, leftrightarrow] & (i, e-i)
\end{tikzcd}$$

vf even

$$\begin{tikzcd}
(2i,i) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & (e-2i, e-i) \arrow[d, leftrightarrow] \\
\left(\frac{e}{2}+i, \frac{e}{2}+2i\right) \arrow[d, leftrightarrow] & \left(\frac{e}{2}-i, \frac{e}{2}-2i\right) \arrow[d, leftrightarrow] \\
\left(\frac{e}{2}-i, i\right) \arrow[r, leftrightarrow] & \left(\frac{e}{2}+i, e-i\right)
\end{tikzcd}$$

vf odd

where neither i nor $2i \equiv 0 \pmod e$. In every remaining case the choice $T_* = T_0$ on the relevant sextuple $\theta(x) \cup \theta(x^{-1})$ alters the field cyclotomic numbers by ± 2 or ± 1 depending on whether or not $\Theta(i,j)$ is a triple or a sextuple; the (inequivalent) cyclotomic numbers affected are the representatives of $\Theta(i,j)$ and $\Theta(e-i, e-j)$, respectively. Finally, if $T(1) = 2 \in C_j$, then the choice $T_* = T_0$ on $\theta(1)$ effects the change as shown by Table III,

TABLE III

vf even		vf odd	
decrease by 1	increase by 1	decrease by 1	increase by 1
$(0,j)$	$(0, e-j)$	$(0,j)$	$(0, e-j)$
$(e-j, e-j)$	$(e-j, 0)$	$\left(\frac{e}{2}-j, e-j\right)$	$\left(\frac{e}{2}-j, \frac{e}{2}\right)$
$(j,0)$	(j,j)	$\left(\frac{e}{2}+j, \frac{e}{2}\right)$	$\left(\frac{e}{2}+j, j\right)$

which leaves the cyclotomic numbers for the field unaltered if and only if $j = 0$ where $|\Theta(0, 0)| = 1$ or $j = e/2$ where $|\Theta(0, e/2)| = 3$ for vf even; $j = 0$ where $|\Theta(0, 0)| = 3$ or $j = e/2$ where $|\Theta(0, e/2)| = 1$ for vf odd. We remark that, for small values of e, the eth power character of $T(1) = 2$ is known, and thus j is explicitly determined by v (see [6], for example).

Combination of the preceding remarks shows that the cyclotomic structure of any neofield $\mathbb{N}_v$ constructed from the field $\mathbb{F}_v$ by Theorem 4.1 is determined by the corresponding structure in $\mathbb{F}_v$; in fact we have proved the following theorem.

THEOREM 4.2. *Let $\mathbb{N}_v$ be a fixed neofield constructed from the field $\mathbb{F}_v$ of order $v = p^\alpha = ef + 1$ by Theorem 4.1, let $X = \{x_1, x_2, ..., x_n\}$ be an ordered system of representatives for the orbit pairs $\theta(x) \cup \theta(x^{-1})$ from S on which $T_* = T_0$, and let $|X_{i,j}|$ be the number of elements $x_k \in X$, $x_k \notin \theta(1)$ for which $x_k' \in C_i$ and $T(x_k') \in C_j$ for some $x_k' \in \theta(x_k) \cup \theta(x_k^{-1})$. Finally, let*

$$\mathfrak{A} = \{A_{i,j} \mid A_{i,j} \text{ a representative of } \Theta(i,j)\}$$

and

$$\mathfrak{A}' = \{A'_{i,j} \mid A'_{i,j} \text{ a representative of } \Theta(i,j)\}$$

be the inequivalent cyclotomic numbers for $\mathbb{F}_v$, e and $\mathbb{N}_v$, e respectively. Then we have

$$A'_{i,j} = A_{i,j}$$

if

(1) $|\Theta(i,j)| < 3$,

(2) $|\Theta(i,j)| = 3$ *and* $(e/2, 0) \in \Theta(i,j)$,

(3) $|\Theta(i,j)| = 6$ *and for some* i', $(2i', i') \in \Theta(i,j)$.

Otherwise,

$$A'_{ij} = A_{ij} + \frac{6}{|\Theta(i,j)|}(|X_{i,i-j}| - |X_{i,j}|) - \delta_{ij}$$

where

$$\delta_{i,j} = \begin{cases} 1, & \text{if } \theta(1) \cap X \neq \varnothing \text{ and } 2 \in C_{j'} \\ & \qquad \text{for some } (0,j') \in \Theta(i,j), j' \neq 0, e/2, \\ -1, & \text{if } \theta(1) \cap X \neq \varnothing \text{ and } 2 \in C_{e-j'} \\ & \qquad \text{for some } (0,j') \in \Theta(i,j), j' \neq 0, e/2, \\ 0, & \text{otherwise.} \end{cases}$$

We now apply Theorem 4.2 to the neofields $\mathbb{N}_v$ and those e, namely $e = 2, 3, 4, 6$, and 8, which have proven themselves interesting combinatorially in the case of the fields $\mathbb{F}_v$. We then discuss the resulting combinatorial structures in $\mathbb{N}_v$ and their relationship to the corresponding field structures in these cases. We have, in the following corollaries, used the known cyclotomic structure for $\mathbb{F}_v$ and e (as in [6]).

COROLLARY 4.3. *When $e = 2$, the cyclotomic matrices for the neofields $\mathbb{N}_v$ have the forms*

A	B
B	B

vf even

A	B
A	A

vf odd

and the inequivalent cyclotomic numbers are given by

$$4A = v - 5, \qquad 4A = v - 3,$$

$$4B = v - 1, \qquad 4B = v + 1,$$

f even $\qquad$ f odd.

COROLLARY 4.4. *When $e = 3$, the cyclotomic numbers for $\mathbb{N}_v$ are given by the matrix*

A	B	C
B	C	D
C	D	B

and the relations

$$9A = v - 8 + c,$$

$$18B = 2v - 4 - c - 9d - 18\epsilon,$$

$$18C = 2v - 4 - c + 9d + 18\epsilon,$$

$$9D = v + 1 + c,$$

where

$$\epsilon = \delta_{0,1} + 2(|X_{0,1}| - |X_{0,2}|),$$

and $4p^\alpha = c^2 + 27d^2$ *with* $c \equiv 1 \pmod 3$; *the sign of d is ambiguously determined.*

We remark that, using the cubic character of $2 \in \mathbb{F}_v$, we have

$$\delta_{0,1} = \begin{cases} 1, & \text{for } \Theta(1) \cap X \neq \varnothing \text{ and } c + d \equiv 0 \pmod 4, \\ -1, & \text{for } \Theta(1) \cap X \neq \varnothing \text{ and } c - d \equiv 0 \pmod 4, \\ 0, & \text{otherwise.} \end{cases}$$

COROLLARY 4.5. *When $e = 4$, the cyclotomic numbers for $\mathbb{N}_v$ are given by the matrices*

A	B	C	D
B	D	E	E
C	E	C	E
D	E	E	B

vf even

A	B	C	D
E	E	D	B
A	E	A	E
E	D	B	E

vf odd

and the relations

$16A = v - 11 - 6x,$	$16A = v - 7 + 2x,$
$16B = v - 3 + 2x + 8y + 16\epsilon,$	$16B = v + 1 + 2x - 8y + 16\epsilon,$
$16C = v - 3 + 2x,$	$16C = v + 1 - 6x,$
$16D = v - 3 + 2x - 8y - 16\epsilon,$	$16D = v + 1 + 2x + 8y - 16\epsilon,$
$16E = v + 1 - 2x,$	$16E = v - 3 - 2x,$

where

$$\epsilon = \delta_{0,3} + 2(|X_{0,3}| - |X_{0,1}|)$$

and $v = p^\alpha = x^2 + 4y^2$ *with* $x \equiv 1 \pmod 4$; *the sign of y is ambiguously determined.*

In the cases $e = 6$ and 8 below, we present the results only for the combinatorially interesting case vf odd (cf. Lemma 2.10); the analysis for vf even is entirely similar.

COROLLARY 4.6. *When $e = 6$ and vf is odd, the cyclotomic numbers for $\mathbb{N}_v$ are given by the matrix*

A	B	C	D	E	F
G	H	I	E	C	I
H	J	G	F	I	B
A	G	H	A	G	H
G	F	I	B	H	J
H	I	E	C	I	G

and the numbers $(i, 0) = \{A, G, H\}$ are given by

$$\begin{array}{ll} 36A = v - 11 + 4C, & 72A = 2v - 22 - c - 9d, \\ 36G = v - 5 - 2c + 9d + 36\epsilon, & 72G = 2v - 10 + 5c + 9d + 72\epsilon, \\ 36H = v - 5 - 2c - 9d - 36\epsilon, & 72H = 2v - 10 - 4c - 72\epsilon, \\ \textit{if } 2 \in C_0 \textit{ or } C_3 & \textit{if } 2 \in C_2 \textit{ or } C_5 \end{array}$$

$$\begin{aligned} 72A &= 2v - 22 - c + 9d, \\ 72G &= 2v - 10 - 4c + 72\epsilon, \\ 72H &= 2v - 10 + 5c - 9d - 72\epsilon, \end{aligned}$$

$$\textit{if } 2 \in C_1 \textit{ or } C_4$$

where

$$\epsilon = |X_{1,1}| - |X_{1,0}|$$

and $v = p^\alpha$, where $4p^\alpha = c^2 + 27d^2$ with $c \equiv 1 \pmod 3$; the sign of d is ambiguously determined.

COROLLARY 4.7. *When $e = 8$ and vf is odd, the cyclotomic numbers for $\mathbb{N}_v$ are given by the matrix*

A	B	C	D	E	F	G	H
I	J	K	L	F	D	L	M
N	O	N	M	G	L	C	K
J	O	O	I	H	M	K	B
A	I	N	J	A	I	N	J
I	H	M	K	B	J	O	O
N	M	G	L	C	K	N	O
J	K	L	F	D	L	M	I

and the numbers $(i, 0) = \{A, I, N, J\}$ are given by

$$\begin{array}{ll}
64A = v - 15 - 2x, & 64A = v - 15 - 10x - 8a, \\
64I = v - 7 + 2x + 4a + 64\epsilon, & 64I = v - 7 + 2x + 4a + 16y + 64\epsilon, \\
64J = v - 7 + 2x + 4a - 64\epsilon, & 64J = v - 7 + 2x + 4a - 16y - 64\epsilon, \\
64N = v - 7 - 2x - 8a, & 64N = v - 7 + 6x, \\
\quad \text{if } 2 \in C_0 \text{ or } C_4 & \quad \text{if } 2 \notin C_0, C_4
\end{array}$$

where

$$\epsilon = | X_{1,1} | - | X_{1,0} |$$

and $v = p^\alpha = x^2 + 4y^2 = a^2 + 2b^2$ with $x \equiv a \equiv 1 \pmod 4$; the signs of y and b are ambiguously determined.

The Lehmer criterion (Corollary 2.9), in conjunction with Theorem 4.2, gives immediate necessary and sufficient conditions on the order v that the set of eth-powers or eth-powers plus 0 for $e = 2, 3, 4, 6$, and 8 form a right (and left) loop difference set in the commutative IP neofields $\mathbb{N}_v$ constructed from Theorem 4.1.

THEOREM 4.8. *The neofields $\mathbb{N}_v$ with $v = p^\alpha = ef + 1$ arising from Theorem* 4.1 *admit the* eth-*powers or the* eth-*powers plus* 0 *as right* (*and left*) *loop difference sets for $e = 2, 3, 4, 6$, and* 8 *as follows*:

(1) $e = 2$; $v = p^\alpha \equiv 3 \pmod 4$ *and all* $\mathbb{N}_v$.

(2) $e = 3$; $C_0 + \{0\}$ *is a difference set in* $\mathbb{F}_{16}$ *only.*

(3) $e = 4$; *If* C_0 *or* $C_0 + \{0\}$ *is a difference set in the field* $\mathbb{F}_v$, *then it is a loop difference set in every neofield* $\mathbb{N}_v$ *arising from Theorem* 4.1 *and conversely. Explicitly,* C_0 *is a difference set for* $v = p^\alpha = 1 + 4t^2$ *with t odd and* $C_0 + \{0\}$ *for* $v = p^\alpha = 9 + 4t^2$ *with t odd.*

(4) $e = 6$; C_0 *is a loop difference set in* $\mathbb{N}_v$ *when* $v = p^\alpha = 108\eta^2 + 36\eta + 7$ *and* $\lambda = 3\eta^2 + \eta$; $C_0 + \{0\}$ *is when* $v = p^\alpha = 108\eta^2 + 108\eta + 175$ *and* $\lambda = 3\eta^2 + 5\eta + 5$, *where* $\eta = \pm\epsilon$ *and* $2 \notin C_0$ *or* C_3.

(5) $e = 8$; *If* C_0 *or* $C_0 + \{0\}$ *is a difference set in the field* $\mathbb{F}_v$, *then it is a loop difference set in every neofield* $\mathbb{N}_v$ *arising from Theorem* 4.1 *for which* $\epsilon = 0$, *and conversely. Explicitly,* C_0 *is a difference set for* $v = p^\alpha = 9 + 64y^2 = 1 + 8b^2$ *with y, b odd, and* $C_0 + \{0\}$ *for* $v = p^\alpha = 441 + 64y^2 = 49 + 8b^2$ *with y, b odd.*

Proof. We first note that when e is even, v and f are both odd, and when e is odd, v is even and f is odd. Then (1) is trivial and (2) follows from Corollary 4.4 and inspection of the field and neofield tables. For (3) note in Corollary 4.5 that A and E are invariant under the neofield constructions of Theorem 4.1. There are no 6th power difference sets in the fields $\mathbb{F}_v$; here, in (4) from Corollary 4.6 for C_0 we have for $2 \in C_1$ or C_4: $A = G$ and $A = H$ if and only if $c + 3d = 4 + 24\epsilon$ and $-c + 3d = 2 - 12\epsilon$, respectively. Hence $c = 1 + 18\epsilon \equiv 1 \pmod 3$ and $d = 1 + 2\epsilon$ implies $4p^\alpha = (1 + 18\epsilon)^2 + 27(1 + 2\epsilon)^2$, or $p^\alpha = 108\epsilon^2 + 36\epsilon + 7$, and by Corollary 2.9, $\lambda = 3\epsilon^2 + \epsilon$. Similarly for $C_0 \cup \{0\}$ where we take $2 \in C_2$ or C_5. Case (5) follows the analysis for the field.

The cases (1), (3), and (5) of the theorem, being direct analogues of the fields, are not very interesting combinatorially since the difference sets in the fields are already $\langle v, k, \lambda \rangle$ designs. In case (2) for $e = 3$, the single example is for the field GF(16) (see [6, p. 36]) and there is no corresponding loop difference set in the proper commutative IP neofield $\mathbb{N}_{16}$. In case (4), however, for $e = 6$, many new examples occur, the smallest for the 6th-powers in the $3.2^{10} \approx 2^{11}$ distinct neofields $\mathbb{N}_{79}$. A computer search has revealed, however, that C_0 and its translates do not form a design in any of these neofields.

As a final remark, since $12^2 + 12 + 1 = 157$ and $15^2 + 15 + 1 = 241$ are primes, and $18^2 + 18 + 1 = 343 = 7^3$, we have examined the commutative IP neofields of these orders obtained by Theorem 4.1, and have found that the 12th-powers, the 16th-powers plus 0, and the 18th-powers, respectively, form loop difference sets in none of these. The method is thus too restrictive to attack the problem of the existence of projective planes of orders 12, 15, and 18.

References

1. R. H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.* **78** (1955), 464–481.
2. E. C. Johnsen and T. F. Storer, Combinatorial structures in loops, I. Elements of the decomposition theory, *J. Combinatorial Theory* (A) **14** (1973), 149–166.
3. E. C. Johnsen and T. F. Storer, Combinatorial structures in loops, II. Commutative inverse-property cyclic neofields of prime-power order, *Pacific J. Math.* **52** (1974), 115–127.
4. E. Lehmer, On residue difference sets, *Canad. J. Math.* **5** (1953), 425–432.
5. L. J. Paige, Neofields, *Duke Math. J.*, **16** (1949), 39–60.
6. T. Storer, "Cyclotomy and Difference Sets," Markham, Chicago, 1967.

Printed in Belgium