Pacific Journal of Mathematics

COMBINATORIAL STRUCTURES IN LOOPS. II. COMMUTATIVE INVERSE PROPERTY CYCLIC NEOFIELDS OF PRIME-POWER ORDER

EUGENE CARLYLE JOHNSEN AND THOMAS FREDERICK STORER

Vol. 52, No. 1 January 1974

PACIFIC JOURNAL OF MATHEMATICS
Vol. 52, No. 1, 1974

COMBINATORIAL STRUCTURES IN LOOPS II. COMMUTATIVE INVERSE PROPERTY CYCLIC NEOFIELDS OF PRIME-POWER ORDER

E. C. JOHNSEN AND THOMAS STORER

In this paper we construct a large family of commutative inverse property, cyclic (CIP) neofields of prime-power order. Our purpose in doing so is to produce a class of algebraic systems which shall be useful in certain combinatorial constructions. One of these constructions is that of power-residue difference sets in the additive loops of finite CIP neofields which is a natural generalization of the corresponding constructions in the additive groups of finite fields. Another is that of cyclic Steiner triple systems, i.e., Steiner triple systems with a cyclic group of automorphisms sharply transitive on elements, which we discuss in the last section of this paper.

CIP neofields may be thought of as a first generalization of finite fields in that they share all of the familiar properties of the fields with the possible exception of additive associativity. The present approach, accordingly, is to begin with a finite field and modify the additive structure thereon so as to preserve these properties. We show that the number of nonisomorphic CIP neofields of prime-power order $v = p^\alpha$ goes to infinity with v and we exhibit proper (i.e., not the field) CIP neofields for every prime-power order $v = p^\alpha \geqq 11$ (every CIP neofield of order $v < 11$ is a field). For $p = 2$ the latter implies that there exists at least two nonisomorphic cyclic Steiner triple systems of order $2^\alpha - 1 \geqq 15$. The constructions of power-residue difference sets in finite CIP neofields appears in [5], the corresponding constructions in finite fields in [6], [9].

2. Preliminaries. *A neofield of order* v is a triple $N_v = \langle N, +, \cdot \rangle$, where N is a set of v elements including 0 and 1, and $+$ and $\cdot$ are binary operations on N such that $N(+)$ is a loop with identity element 0, $N^*(\cdot)$ (where $N^* = N - \{0\}$) is a group with identity element 1, and $\cdot$ is both left and right distributive over $+$. We also write N_v for N and N_v^* for N^*. It is easily verified that $0 \cdot x = 0 = x \cdot 0$ for every $x \in N_v$. The neofield N_v is said to have the *right inverse property* (RIP) if for each $y \in N_v$ there is an element $z \in N_v$ such that $(x + y) + z = x$ for all $x \in N_v$, and to have the *left inverse property* (LIP) if for each $y \in N_v$ there is an element $w \in N_v$ such that $w + (y + x) = x$ for all $x \in N_v$. If N_v has both the RIP and LIP then N_v is called an *inverse property* (IP) neofield. It is readily verified that in an RIP or LIP neofield N_v every $y \in N_v$ has a unique two-sided

negative $-y \in N_v$. In fact, in the above definitions the elements z and w are this element $-y$. In an RIP or LIP neofield N_v, $x + (-1)x = (1 + (-1))x = 0 = ((-1) + 1)x = (-1)x + x$, hence the negative of x is $-x = (-1)x$ for every $x \in N_v$. We call a neofield N_v *commutative* if $N_v(+)$ is commutative. The following result is probably known.

LEMMA 2.1. *An* IP *neofield is commutative.*

Proof. Let N_v be an IP neofield and let $x, y \in N_v$ with $x + y = z$. By the RIP we have $x = (x + y) + (-y) = z + (-y)$, by the LIP this becomes $(-z) + x = (-z) + (z + (-y)) = -y$, and by the RIP again we obtain $-z = ((-z) + x) + (-x) = (-y) + (-x)$ or $(-1)z = (-1)y + (-1)x = (-1)(y + x)$. Since $-1 \in N_v^*$ we obtain $z = y + x$. Hence $x + y = y + x$, and we see that N_v is commutative.

We call a neofield N_v *cyclic* when $N_v^*(\cdot)$ is cyclic. Let N_v be a cyclic neofield. A *presentation* of N_v based on the set N is the expression of N in terms of a multiplicative generator a, $N = \{0, 1, a, a^2, \cdots, a^{v-2}\}$ where $a^{v-1} = 1$, together with a function $T: N \to N$, called the *presentation function*, which is related to the addition in N_v by $1 + x \equiv T(x)$ for all $x \in N$. In a cyclic neofield the element 1 has a unique two-sided negative -1 where $-1 = 1$ if v is even and $-1 = a^{(v-1)/2}$ if v is odd ([7], p. 49, Theorem II2). Using the presentation of a cyclic neofield N_v we can construct the addition table $\hat{N}_v$ for $N_v(+)$. We choose the natural order $0, 1, a, a^2, \cdots, a^{v-2}$ for the first row and first column of $\hat{N}_v$. Then the second row of $\hat{N}_v$ consists of the elements $T(0) = 1, T(1), T(a), T(a^2), \cdots, T(a^{v-2})$ in this order. By the distributive laws we have

$$(2.1) \qquad a^r + a^s = a^r(1 + a^{s-r}) = a^r T(a^{s-r}) \; ; \quad 0 \leqq r, s \leqq v - 2 \, ,$$

hence the table $\hat{N}_v$ is completely determined by its first and second rows. A cyclic neofield N_v is thus completely determined by its presentation; henceforth, we shall give a presentation of N_v in terms of the first two rows of $\hat{N}_v$. Note, however, that an abstract cyclic neofield of order v may have more than one presentation. For example, the unique finite field of order 7 has the presentations

0	1	a	a^2	a^3	a^4	a^5
1	a^2	a^4	a	0	a^5	a^3

and

0	1	a	a^2	a^3	a^4	a^5
1	a^4	a^3	a	0	a^5	a^2

.

Different presentations of a cyclic neofield N_v, of course, correspond to different definitions of addition on the set N. Finally, we call a cyclic IP neofield a CIP neofield.

3. Construction of a family of CIP neofields. Let $F_v = \langle F, +, \cdot \rangle$ be the finite field of order $v = p^\alpha \geqq 11$, p prime, $\alpha \geqq 1$ integral, with presentation given by $F = \{0, 1, a, a^2, \cdots, a^{v-2}\}$ and the presentation function T for which $T(x) = 1 + x$ for all $x \in F$. We define the functions T' and T_0 on F as follows:

$$T'(x) \equiv (-1) + x\,, \quad x \in F\,, \tag{3.1}$$

$$T_0(x) \equiv \begin{cases} T(x),\ x = 0, -1 \\ \dfrac{x}{T(x)},\ \text{otherwise}\,, \end{cases} \tag{3.2}$$

and define a new addition $\oplus$ on F according to

$$x \oplus y \equiv \begin{cases} y;\ y \in F,\ x = 0 \\ xT_0(x^{-1}y);\ x, y \in F,\ x \neq 0\,. \end{cases} \tag{3.3}$$

Also, we define

$$T_0'(x) \equiv (-1) \oplus x,\ x \in F\,. \tag{3.4}$$

We note that $F_v^{(0)} = \langle F, \oplus, \cdot \rangle$ is also the field of order $v = p^\alpha$ which, as the image of the mapping $0 \to 0$, $x \to x^{-1}$ for all $x \neq 0$ in F, is an isomorph but not an automorph of $F_v(+, \cdot)$. We let the corresponding presentation of $F^{(0)}$ be given by $F = \{0, 1, a, a^2, \cdots, a^{v-2}\}$ and the presentation function T_0. We shall be concerned with compositions of the functions T, T', and T_0 on the set F. We need the following two results for the neofield construction which is to follow.

LEMMA 3.1. *For all* $x \in F$, $(T'T_0)^3(x) = x$.

Proof. We easily verify that $T'T_0(0) = 0$ and $T'T_0(-1) = -1$, hence the lemma holds for $x = 0, -1$. We now take $x \neq 0, -1$. Then a straightforward computation yields $T'T_0(x) = -(1 + x)^{-1}$. Since $-(1 + x)^{-1} \neq 0, -1$, a second application of $T'T_0$ yields $(T'T_0)^2(x) = -(1 + x)x^{-1}$. Finally, since $-(1 + x)x^{-1} \neq 0, -1$, a third application of $T'T_0$ yields $(T'T_0)^3(x) = x$; hence the lemma.

We now determine those $x \in F$ for which $T'T_0(x) = x$.

LEMMA 3.2. *We have* $(T'T_0)(x) = x$ (i.e., $T(x) = T_0(x)$) *in the set* F_v, $v = p^\alpha$, *precisely when*

(1) $x = 0, -1$. (*This includes* $1 = -1$ *when* $p = 2$.)

(2) $p = 3$ *and* $x = 1$. (*Here* $T(1) = -1$.)

(3) $p^\alpha \equiv 1 \pmod 3$ *and* x *is a primitive cube root of unity in* F_v. (*Here* $T(x) = -x^2$ *is a primitive sixth root of unity in* F_v *when* $p \neq 2$.)

Proof. We already have (1) from the proof of the previous lemma. When $1 \neq -1$ v is odd and $T'T_0(1) = 1$ if and only if $p = \text{char}(\boldsymbol{F}_v) = 3$ and $T(1) = -1$. When $x \neq 0, 1, -1$ we have $T'T_0(x) = x$ if and only if $1 + x + x^2 = 0$. Here x is a primitive cube root of unity in $\boldsymbol{F}_v$, and $x^3 = 1$ implies that $3 \mid v - 1$ or $p^\alpha \equiv 1 \pmod 3$. Also, $T(x) = 1 + x = -x^2$ satisfies $(1 + x)^2 - (1 + x) + 1 = 0$ and is thus a primitive sixth root of unity in $\boldsymbol{F}_v$ when $p \neq 2$.

COROLLARY 3.3. *Let* $S = \{x \in F \mid (T'T_0)(x) \neq x\}$. *Then* S *is partitioned into triples* $\{y, T'T_0(y), (T'T_0)^2(y)\}$, *whence* $|S| \equiv 0 \pmod 3$.

Proof. The elements y, $T'T_0(y)$, and $(T'T_0)^2(y)$ are distinct except when y is one of the elements given in Lemma 3.2 and thus satisfies $T'T_0(y) = y$. Hence S is partitioned into triples and $|S| \equiv 0 \pmod 3$.

We now change viewpoint and assume that $\boldsymbol{N}_v = \langle F, \boxplus, \cdot \rangle$ is a cyclic neofield of order $v = p^\alpha$ with presentation given by F and the presentation function T_* satisfying

(i) $T_* \not\equiv T$ and $T_* \not\equiv T_0$ on F,

(ii) for each $x \in F$, either $T_*(x) = T(x)$ or $T_*(x) = T_0(x)$. We inquire as to what other conditions T_* must satisfy on F. Immediate restrictions are obtained in the following result.

LEMMA 3.4. *The function* T_* *is bijective on* F, *and for all* $x, y \in F$ *we must have*

(1) $T_*(x) \neq x$,

(2) $xT_*(y) \neq T_*(xy)$ *for* $x \neq 1$.

Furthermore, $\boldsymbol{N}_v$ *is commutative if and only if*

(3) $xT_*(x^{-1}) = T_*(x)$ *for all* $x \neq 0$ *in* F.

Proof. That T_* is bijective and satisfies (1) and (2) is obvious. In $\boldsymbol{N}_v$ we automatically have $x \boxplus 0 = 0 \boxplus x$ for all $x \in F$. Suppose $x, y \in F$ where $x \neq 0 \neq y$. Then

$$x \boxplus y = x(1 \boxplus x^{-1}y) = y(xy^{-1})T_*((xy^{-1})^{-1})$$

and $y \boxplus x = y(1 \boxplus xy^{-1}) = yT_*(xy^{-1})$. Hence $x \boxplus y = y \boxplus x$ if and only if $(xy^{-1})T_*((xy^{-1})^{-1}) = T_*(xy^{-1})$. Let $z = xy^{-1}$. As x and y run over $\boldsymbol{N}_v^*$ so does z, and as z runs over $\boldsymbol{N}_v^*$ all pairs $x, y \in \boldsymbol{N}_v^*$ are obtained. Hence, $\boldsymbol{N}_v$ is commutative if and only if $zT_*(z^{-1}) = T_*(z)$ for all $z \neq 0$ in F, which is (3).

For $y \in S = \{x \in F \mid T'T_0(x) \neq x\}$ we define the *orbit* of y to be the set $\theta(y) \equiv \{y, T'T_0(y), (T'T_0)^2(y)\}$. A simple computation shows that $\theta(y) = \{y, (-1)/T(y), (-1)/T_0(y)\}$. We now show that T_* is identically T or T_0 on the orbits in S.

LEMMA 3.5. *If T_* agrees with T (or T_0) at $y \in S$, then T_* agrees with T (or T_0) on $\theta(y)$.*

Proof. We first note that for $y \in S$, the two sets

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

and

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

are equal, since

$$T_0(y) = T(T'T_0)(y),\ T_0(T'T_0)(y) = T(T'T_0)^2(y)\ ,$$

and $T_0(T'T_0)^2(y) = T(T'T_0)^3(y) = T(y)$. Suppose $T_*(y) = T(y)$. If $T_*(T'T_0)^2(y) = T_0(T'T_0)^2(y)$ then $T_*(T'T_0)^2(y) = T(y)$, contrary to the fact that T_* is injective. Hence $T_*(T'T_0)^2(y) = T(T'T_0)^2(y)$. Further, if $T_*(T'T_0)(y) = T_0(T'T_0)(y)$ then $T_*(T'T_0)(y) = T(T'T_0)^2(y)$, again contrary to T_* being injective. Hence $T_*(T'T_0)(y) = T(T'T_0)(y)$. Thus, if T_* agrees with T at $y \in S$ then T_* agrees with T on $\theta(y)$. Similarly, if T agrees with T_0 at $y \in S$ then T_* agrees with T_0 on $\theta(y)$.

When N_v is commutative the condition $xT(x^{-1}) = T(x)$ (or $xT_0(x^{-1}) = T_0(x)$) effects a further agreement of T_* and T (or T_0) on the orbits in S.

LEMMA 3.6. *Suppose N_v is commutative. If T_* agrees with T (or T_0) at $y \in S$, then T_* agrees with T (or T_0) on $\theta(y) \cup \theta(y^{-1})$. Thus, the orbits in S are paired except when $1 \in S$. In the latter case $\theta(1)$ is paired with itself.*

Proof. Suppose $T_*(y) = T(y)$. Then, by Lemma 3.5, T_* agrees with T on $\theta(y)$. Since N_v is commutative we have, by Lemma 3.4(3), that $yT_*(y^{-1}) = T_*(y)$, whence $yT_*(y^{-1}) = T(y) = yT(y^{-1})$ or $T_*(y^{-1}) = T(y^{-1})$. Again, by Lemma 3.5, T_* agrees with T on $\theta(y^{-1})$. Hence T_* agrees with T on $\theta(y) \cup \theta(y^{-1})$. Now, $\theta(y) = \theta(y^{-1})$ if and only if one of $y = y^{-1}$, $y = T'T_0(y^{-1}) = -1/T(y^{-1})$, or

$$y = (T'T_0)^2(y^{-1}) = (-1)/T_0(y^{-1})$$

holds.

Case 1. $y = y^{-1}$. Here $y^2 = 1$, hence $y = 1$ since $-1 \notin S$, whence $\theta(y) = \theta(1)$.

Case 2. $y = (-1)/T(y^{-1})$. Here $y = -1/(1 + y^{-1}) = (-y)/(y + 1)$ or $y = -2$, whence $\theta(y) = \{-2, 1, -2^{-1}\} = \theta(1)$.

Case 3. $y = (-1)/T_0(y^{-1})$. Here $y = (-y)(1 + y^{-1}) = -y - 1$ or $y = -2^{-1}$, whence $\theta(y) = \{-2^{-1}, -2, 1\} = \theta(1)$.
Clearly, when $1 \in S$, $\theta(1)$ is paired with itself. A similar argument goes through when $T_*(y) = T_0(y)$.

We now show that if N_v is commutative then it inherits the IP from the field. Since N_v is cyclic -1 is also the negative of 1 in $N_v(\boxplus)$; whence, $-y = (-1)y$ is the negative of y in $N_v(\boxplus)$ for every $y \in N_v$.

LEMMA 3.7. *If N_v is commutative, then N_v is an* IP *neofield.*

Proof. Since N_v is assumed to be commutative, we only need to prove that N_v has the LIP. Now $(-y) \boxplus (y \boxplus 0) = 0$ for all $y \in F$ and $(-0) \boxplus (0 \boxplus x) = x$ for all $x \in F$, hence we are left with proving $(-y) \boxplus (y \boxplus x) = x$ for all $x \neq 0 \neq y$. Now, $(-y) \boxplus (y \boxplus x) = x$ if and only if $(-1) \boxplus (1 \boxplus xy^{-1}) = xy^{-1}$ or $T'_* T_*(xy^{-1}) = xy^{-1}$, where T'_* is defined by $T'_*(w) = (-1) \boxplus w$ for all $w \in F$. Let $z = xy^{-1}$. As x and y run over N_v^* so does z, and as z runs over N_v^* every pair $x, y \in N^*$ is obtained. Hence N_v has the IP if and only if $T'_* T_*(z) = z$ for all $z \neq 0$ in N_v. If $T'T_0(z) = z$ then $T_*(z) = T(z) = T_0(z)$, and regardless of whether T'_* agrees with T' or T'_0 on $T_*(z)$ we have $T'_* T_*(z) = z$. Otherwise, $T'T_0(z) \neq z$ and z has an orbit $\theta(z) = \{z, (-1)/T(z), (-1)/T_0(z)\}$. For such z, $(-1) \boxplus (1 \boxplus z) = (1 \boxplus z) \boxplus (-1) = (1 \boxplus z)(1 \boxplus (-1)/(1 \boxplus z))$ or $T'_* T_*(z) = T_*(z)T_*((-1)/T_*(z))$, and, by Lemma 3.5 and the commutativity and IP of $F_v(+)$ and $F_v^{(0)}(\oplus)$, we have

$$T'_* T_*(z) = \begin{cases} T(z)T((-1)/T(z)) = T'T(z) = z & \text{if} \quad T_*(z) = T(z) \\ T_0(z)T_0((-1)T_0(z)) = T'_0 T_0(z) = z & \text{if} \quad T_*(z) = T_0(z)\,. \end{cases}$$

Hence $T'_* T_*(z) = z$ for all $z \neq 0$ in N_v, whence N_v has the IP, as was to be shown.

We now have enough information on the neofield $N_v = \langle F, \boxplus, \cdot \rangle$ obtained from F_v and $F_v^{(0)}$ according to (i) and (ii) to give a construction of CIP neofields for every prime-power order $v = p^\alpha \geqq 11$.

THEOREM 3.8. *Let $F_v = \langle F, +, \cdot \rangle$ and $F_v^{(0)} = \langle F, \oplus, \cdot \rangle$, $F = \{0, 1, a, a^2, \cdots, a^{v-2}\}$, $a^{v-1} = 1$, be two copies of the finite field of order $v \geqq 11$ with presentation functions T and T_0, respectively, where T_0 is related to T by*

$$T_0(x) = \begin{cases} T(x), \; x = 0, -1 \\ \dfrac{x}{T(x)}, \; x \neq 0, -1\,. \end{cases} \tag{3.5}$$

Let T_* be any mapping on F satisfying

$$(3.6)\quad \begin{cases} \text{(a)} & T_* \not\equiv T \text{ and } T_* \not\equiv T_0 \text{ on } F, \\ \text{(b)} & \text{for each } x \in F, \text{ either } T_*(x) = T(x) \text{ or } T_*(x) = T_0(x)\,, \\ \text{(c)} & \text{if } T_* \text{ agrees with } T \text{ (or } T_0) \text{ at } x \in S, \text{ then } T_* \text{ agrees with } T \text{ (or } T_0) \text{ on } \theta(x) \cup \theta(x^{-1})\,. \end{cases}$$

Then T_* is the presentation function for a CIP *neofield $N_v = \langle F, \boxplus, \cdot \rangle$.*

Proof. Let $N_v(\boxplus)$ be the groupoid on F defined by

$$(3.7)\qquad x \boxplus y \equiv \begin{cases} y, & x = 0 \\ xT_*(x^{-1}y), & x \neq 0 \end{cases}$$

for all $x, y \in F$. Now, by (3.7), $0 \boxplus y = y$ and $x \boxplus 0 = xT_*(0) = xT(0) = xT_0(0) = x \cdot 1 = x$ for all $x, y \in N_v$; hence 0 is the identity element in $N_v(\boxplus)$ and 0 commutes with every element in N_v. Let $x \neq 0$ in N_v and suppose that $T_*(x) = T(x)$. Then, by (3.6)(c), $T_*(x^{-1}) = T(x^{-1})$, hence $xT_*(x^{-1}) = xT(x^{-1}) = T(x) = T_*(x)$. If $T_*(x) = T_0(x)$ we again obtain $xT_*(x^{-1}) = T_*(x)$. By the proof of (3) of Lemma 3.4, this implies that $N_v(\boxplus)$ is commutative. Now, $0 \boxplus x = b$ has the unique solution $x = b$ for any $b \in N_v$. By (3.7), $a \boxplus x = b$ for $a, b \in N_v$, $a \neq 0$, has a unique solution $x \in N_v$ if and only if $T_*(a^{-1}x) = a^{-1}b$ has, that is, if and only if T_* is bijective on N_v. Suppose for $w, z \in N_v$, $w \neq z$, we have $T_*(w) = T_*(z)$. Now T_* agrees with one of T and T_0 at w and, since both T and T_0 are bijective, T_* must agree with the other at z. We may assume that $T_*(w) = T(w)$ and $T_*(z) = T_0(z)$. Then $T_0(z) = T(w)$ or $T'T_0(z) = w \neq z$, hence z has an orbit $\theta(z)$ and $w \in \theta(z)$. By (3.6) (c) this means that T_* agrees with T_0 at w, whence $T_0(w) = T_*(w) = T_*(z) = T_0(z)$, which contradicts the fact that T_0 is bijective. Hence, T_* is bijective on N_v and, by the commutativity of $N_v(\boxplus)$, $x \boxplus a = a \boxplus x = b$ always has a unique solution $x \in N_v$ for every choice of elements $a, b \in N_v$. Hence $N_v(\boxplus)$ is a commutative loop. Now, for any $w \neq 0$, $x, y \in N_v$ we have, by (3.7), that $0 \cdot (x \boxplus y) = 0 = 0 \cdot x \boxplus 0 \cdot y$ and

$$w \cdot (x \boxplus y) = \begin{cases} w \cdot y = w \cdot 0 \boxplus w \cdot y = w \cdot x \boxplus w \cdot y, & x = 0 \\ w \cdot xT_*(x^{-1}y) = wxT_*((wx)^{-1}(wy)) = wx \boxplus wy, & x \neq 0\,, \end{cases}$$

hence, since $N_v(\cdot)$ is commutative, $\boxplus$ is both left and right distributive over $\cdot$. Thus $N_v(\boxplus, \cdot)$ is a cyclic commutative neofield. By (3.6) (a) and (b), N_v satisfies the implicit conditions of Lemma 3.7, hence $N_v = \langle F, \boxplus, \cdot \rangle$ is a CIP neofield with presentation function T_*.

For F_v and $F_v^{(0)}$ of order $v = p^\alpha \leqq 9$ we have $|S|/3 \leqq 2$, and so condition (3.6) (a) cannot be satisfied. For $v = 11$ and 13 we have $|S|/3 = 3$ and $\theta(1)$ is paired with itself. Here, fixing $T_* = T$ (or T_0)

on $S - \theta(1)$ and $T_* = T_0$ (or T) on $\theta(1)$ yields what we shall call a *special* CIP neofield. We remark that special CIP neofields exist for every order $v = p^\alpha \geqq 11$ where $p \neq 2, 3$. The construction produces non-special CIP neofields for every order $v = p^\alpha \geqq 16$. At this point we do not know whether this construction produces neofields which are not isomorphs of the corresponding field. This question is taken up in the next section.

4. Proper CIP neofields. A neofield is called *proper* if it is not a field. It is natural to inquire as to which of the CIP neofields constructed by Theorem 3.8 are proper and how many nonisomorphic proper CIP neofields are obtained. So far we do not have the complete answer to these questions; however, we can obtain some information of value. Let φ denote the Euler phi-function. We need the following preliminary result.

LEMMA 4.1. *A cyclic neofield* $N_v = \langle N, +, \cdot \rangle$, $N = \{0, 1, a, a^2, \cdots, a^{v-2}\}$, *of order* $v > 1$ *has at most* $\varphi(v-1)$ *presentations based on the set* N.

Proof. Let T_0 be the presentation function for $N_v^{(0)} = \langle N, \oplus, \cdot \rangle$, where $N_v^{(0)}$ is isomorphic to N_v. Let Ψ denote the isomorphism from N_v onto $N_v^{(0)}$. Then Ψ induces an isomorphism from $N_v^*(\cdot)$ onto $N_v^{(0)*}(\cdot)$. In terms of the generator a of $N_v^*(\cdot)$ we have $\Psi: a \to a^r$ where a^r is a generator of $N_v^{(0)*}(\cdot)$. Since $|N_v^{(0)*}(\cdot)| = v - 1$ we must have $\gcd(r, v-1) = 1$. Since Ψ is completely determined by its effect on a multiplicative generator, the number of different presentations of N_v on the set N is at most the number of different integers r, $1 \leqq r \leqq v - 1$ such that $\gcd(r, v-1) = 1$, which is $\varphi(v-1)$.

THEOREM 4.2. *The number of nonisomorphic* CIP *neofields of order* $v = p^\alpha$ *constructed by Theorem* 3.8 *goes to infinity with* v.

Proof. In the construction of Theorem 3.8, let u denote the number of elements x such that $T'T_0(x) \neq x$ and $x \notin \theta(1)$ if $\theta(1)$ exists. Then $u/6$ is the number of orbit pairs $\theta(x) \cup \theta(x^{-1})$ on which a choice of either T or T_0 can be made. If $\theta(1)$ exists then the total number of neofield presentations constructed is $2^{(u/6)+1} - 2$ and if $\theta(1)$ does not exist, this number is $2^{u/6} - 2$. Now, the value of u is $3^\alpha - 3 = v - 3$ if $p = 3$, $2^\alpha - 4 = v - 4$ if $p = 2$ and $p^\alpha \equiv 1 \pmod 3$, $p^\alpha - 7 = v - 7$ if $p \neq 2$ and $p^\alpha \equiv 1 \pmod 3$, $2^\alpha - 2 = v - 2$ if $p = 2$ and $p^\alpha \equiv 2 \pmod 3$, and $p^\alpha - 5 = v - 5$ if $p \neq 2$ and $p^\alpha \equiv 2 \pmod 3$. Since $\theta(1)$ exists only for $p \neq 2, 3$, the resulting number of neofield presentations is, respectively, $2^{(v-3)/6} - 2$, $2^{(v-4)/6} - 2$, $2^{(v-1)/6} - 2$, $2^{(v-2)/6} - 2$, and $2^{(v+1)/6} - 2$.

Now, by Lemma 4.1, a given neofield of order v can occur among these presentations at most $\varphi(v-1)$ times, hence the construction yields at least

$$\frac{2^{(v-r)/6}-2}{\varphi(v-1)} > \frac{2^{(v-r)/6}-2}{v-1}$$

nonisomorphic neofields of order v, where $r = -1, 1, 2, 3,$ or 4. In any of these cases we clearly have

$$\lim_{v\to\infty} \frac{2^{(v-r)/6}-2}{v-1} = \infty ,$$

hence the theorem.

In the case of a field $\boldsymbol{F}_v$ of order $v = p^\alpha$ the number of different presentations given by the various isomorphisms $\Psi_r\colon a \to a^r$, $\gcd(r, v-1) = 1$, is $\alpha^{-1}\varphi(p^\alpha - 1)$ since the mappings $\Psi_{p^i}\colon a \to a^{p^i}$, $i = 1, 2, 3, \cdots, \alpha$, are all automorphisms and automorphisms preserve presentations. The number of presentations of neofields of order $v = p^\alpha$ constructed by Theorem 3.8 is larger than $\alpha^{-1}\varphi(p^\alpha - 1) - 2$ for all $p^\alpha \geqq 11$ except 11, 13, and 17 and for these orders the theorem constructs proper neofields by inspection. Hence, for all orders $v \geqq 11$, proper CIP neofields are constructed by Theorem 3.8. In the following theorems we give actual constructions of proper CIP neofields for each order $v = p^\alpha \geqq 11$, divided into the three cases where $p > 7$, $p = 3, 5, 7$, and $p = 2$. The three analyses are rather distinct; each is based on particular properties of the case involved.

THEOREM 4.3. *Let $v = p^\alpha \geqq 11$ where $p > 7$. Then $2 \notin \theta(1)$ and any neofield $\boldsymbol{N}_v$ of order v constructed by Theorem 3.8 with $T_* = T$ on $\theta(1)$ and $T_* = T_0$ on $\theta(2)$ has the property that*

$$1 \boxplus (1 \boxplus (1 \boxplus 1)) \neq (1 \boxplus 1) \boxplus (1 \boxplus 1) \tag{4.1}$$

and is, hence, not the field of order v.

Proof. We note that $\boldsymbol{F}_p \subseteqq \boldsymbol{F}_{p^\alpha} = \boldsymbol{F}_v$ and that for $x \in \boldsymbol{F}_v$, $x \in \boldsymbol{F}_p$ if and only if $\theta(x) \subseteqq \boldsymbol{F}_p$. Since $p \neq 2, 3$, $\theta(1)$ exists and $\theta(1) = \{1, -2^{-1}, -2\}$; hence $2 \in \theta(1)$ iff $5 = 0$ or $4 = 0$, i.e., $p = 2$ or $p = 5$. Thus, choosing $T_* = T$ on $\theta(1)$ and $T_* = T_0$ on $\theta(2)$,

$$1 \boxplus (1 \boxplus (1 \boxplus 1)) = T_* T_* T_*(1) = T_* T_0 T(1) = T_*\left(\frac{2}{3}\right)$$

and

$$(1 \boxplus 1) \boxplus (1 \boxplus 1) = (1 \boxplus 1)(1 \boxplus 1) = T_*(1) T_*(1) = T(1) T(1) = 4 .$$

If $T_*(2/3) = T(2/3) = 5/3$ then $T_*(2/3) = 4$ implies that $7 = 0$, and if $T_*(2/3) = T_0(2/3) = 2/5$ then $T_*(2/3) = 4$ implies that $2 = 0$ or $3 = 0$, all of which are contradictions. Hence $T_*(2/3) \neq 4$, which is (4.1).

THEOREM 4.4. *Let $v = p^\alpha > 11$ where $p = 3, 5,$ or 7. Let $x \in \boldsymbol{F}_v$ where $x \notin \boldsymbol{F}_p$ and $x \neq -1 \pm \sqrt{-1}$, $x \neq 2^{-1}(-1 \pm \sqrt{5})$, $x \neq 2^{-1}(-3 \pm \sqrt{5})$, $x \neq 2^{-1}(-3 \pm \sqrt{-3})$, in case any of these elements exist in $\boldsymbol{F}_v$ and are not in $\boldsymbol{F}_p$. Then $T(x) \notin \theta(x) \cup \theta(x^{-1})$, and any neofield $\boldsymbol{N}_v$ of order v constructed by Theorem 3.8 with $T_* = T$ on $\theta(1) \cup \theta(x) \cup \theta(x^{-1})$ and $T_* = T_0$ on $\theta(T(x)) \cup \theta((T(x))^{-1})$ has the property that*

$$1 \boxplus (1 \boxplus x) \neq (1 \boxplus 1) \boxplus x \tag{4.2}$$

and is, hence, not the field of order v.

Proof. We first note that the element x must be different from at most $p + 8$ elements of $\boldsymbol{F}_v$. Since the minimal values of 3^α, 5^β, and 7^γ are 27, 25, and 49 and $p + 8 \leqq 15$, such an element x exists. Since $T(x) \notin \boldsymbol{F}_p$ we have $T(x) \notin \theta(1)$. Furthermore, $T(x) \in \theta(x) \cup \theta(x^{-1})$ implies that either $x \in \boldsymbol{F}_p$ or x is one of the first six forbidden values. Thus, choosing $T_* = T$ on $\theta(1) \cup \theta(x) \cup \theta(x^{-1})$ and $T_* = T_0$ on $\theta(T(x)) \cup \theta((T(x))^{-1})$,

$$1 \boxplus (1 \boxplus x) = T_* T_*(x) = T_0 T(x) = (x + 1)(x + 2)^{-1}$$

and

$$\begin{aligned}(1 \boxplus 1) \boxplus x &= x \boxplus (1 \boxplus 1) = x(1 \boxplus (x^{-1} \boxplus x^{-1})) \\ &= x T_*(x^{-1} T(1)) = x T_*(2x^{-1}) .\end{aligned}$$

If $T_*(2x^{-1}) = T(2x^{-1}) = 1 + 2x^{-1}$ then $xT_*(2x^{-1}) = (x + 1)(x + 2)^{-1}$ implies that $x^2 + 3x + 3 = 0$ or x is one of the last two forbidden values, and if $T_*(2x^{-1}) = T_0(2x^{-1}) = 2(x + 2)^{-1}$ then $xT_*(2x^{-1}) = (x + 1)(x + 2)^{-1}$ implies that $x = 1$, both of which are contradictions. Hence $(x + 1)(x + 2)^{-1} \neq xT_*(2x^{-1})$, which is (4.2).

THEOREM 4.5. *Let $v = 2^\alpha > 11$ and let x be any element in $\boldsymbol{F}_v$ which is not in the largest of the subfields $\boldsymbol{F}_2$, $\boldsymbol{F}_4$, or $\boldsymbol{F}_8$ contained in $\boldsymbol{F}_v$. Then $x^2 \notin \theta(x) \cup \theta(x^{-1})$ and any neofield $\boldsymbol{N}_v$ of order v constructed by Theorem 3.8 with $T_* = T$ on $\theta(x) \cup \theta(x^{-1})$ and $T_* = T_0$ on $\theta(x^2) \cup \theta(x^{-2})$ has the property that*

$$(x \boxplus 1) \boxplus x^2 \neq x \boxplus (1 \boxplus x^2) \tag{4.3}$$

and is, hence, not the field of order v.

Proof. Since x is not in any subfield $\boldsymbol{F}_2$, $\boldsymbol{F}_4$, or $\boldsymbol{F}_8$ of $\boldsymbol{F}_v$, x satisfies

no cubic or lower degree equation over $\boldsymbol{F}_2$. If $x^2 \in \theta(x) \cup \theta(x^{-1}) = \{x, -(1+x)^{-1}, -(1+x)x^{-1}, x^{-1}, -x(1+x^{-1}), -(1+x)\}$, this condition is clearly violated. Thus, choosing $T_* = T$ on $\theta(x) \cup \theta(x^{-1})$ and $T_* = T_0$ on $\theta(x^2) \cup \theta(x^{-2})$,

$$\begin{aligned}(x \boxplus 1) \boxplus x^2 = x^2 \boxplus (1 \boxplus x) &= x^2 T_*(x^{-2} T_*(x)) \\ &= x^2 T_*(x^{-2} T(x)) = x^2 T_*(x^{-1} + x^{-2})\end{aligned}$$

and

$$x \boxplus (1 \boxplus x^2) = x T_*(x^{-1} T_*(x^2)) = x T_*(x^{-1} T_0(x^2)) = x T_*(x(1+x^2)^{-1}) .$$

If $x^2 T_*(x^{-1} + x^{-2}) = x^2 T(x^{-1} + x^{-2}) = x^2 + x + 1$ and $x T_*(x(1+x^2)^{-1}) = x T(x(1+x^2)^{-1}) = x + x^2(1+x^2)^{-1}$ then $x^2 T_*(x^{-1} + x^{-2}) = x T_*(x(1+x^2)^{-1})$ implies that $x^2 + x + 1 = 0$, a contradiction. If

$$x^2 T_*(x^{-1} + x^{-2}) = x^2 T(x^{-1} + x^{-2}) = x^2 + x + 1$$

and $x T_*(x(1+x^2)^{-1}) = x T_0(x(1+x^2)^{-1}) = x^2(1+x+x^2)^{-1}$ then

$$x^2 T_*(x^{-1} + x^{-2}) = x T_*(x(1+x^2)^{-1})$$

implies that $x^2 + 1 = 0$, another contradiction. If $x^2 T_*(x^{-1} + x^{-2}) = x^2 T_0(x^{-1} + x^{-2}) = (x^2 + x^3)(1 + x + x^2)^{-1}$ and $x T_*(x(1+x^2)^{-1}) = x T(x(1+x^2)^{-1}) = x + x^2(1+x^2)^{-1}$ then $x^2 T_*(x^{-1} + x^{-2}) = x T_*(x(1+x^2)^{-1})$ implies that $x^3 + x + 1 = 0$, also a contradiction. Finally, if $x^2 T_*(x^{-1} + x^{-2}) = x^2 T_0(x^{-1} + x^{-2}) = (x^2 + x^3)(1 + x + x^2)^{-1}$ and $x T_*(x(1+x^2)^{-1}) = x T_0(x(1+x^2)^{-1}) = x^2(1+x+x^2)^{-1}$ then $x^2 T_*(x^{-1} + x^{-2}) = x T_*(x(1+x^2)^{-1})$ implies that $x = 0$, again a contradiction. Hence $x^2 T_*(x^{-1} + x^{-2}) \neq x T_*(x(1+x^2)^{-1})$ which establishes (4.3).

It is natural to inquire as to the orders for which CIP neofields exist. The order need not be a prime-power as the following presentation for the lone CIP neofield of order 14 shows:

x	0	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
$T_*(x)$	1	0	a^4	a^7	a^{12}	a	a^{11}	a^8	a^2	a^6	a^{10}	a^9	a^5	a^3

.

Recently, John R. Doner has obtained CIP neofields for all orders $v \geqq 2$ satisfying $v \not\equiv 0, 6, 12, 15, 18, 21 \pmod{24}$ and $v \neq 10$ and has shown that no CIP neofields exist for these forbidden orders. Hughes [4] had earlier shown that the orders $v \equiv 0, 6, 12, 18 \pmod{24}$ were forbidden, and the authors, among perhaps others, had earlier observed that order $v = 10$ is also forbidden.

5. Cyclic Steiner triple systems. A Steiner triple system of order n, $S(n)$, is an arrangement of a set of n elements into triples

such that every pair of elements occur together in precisely one triple. A necessary and sufficient condition that an $S(n)$ exist is that $n \equiv 1, 3 \pmod 6$. An $S(n)$ is called *cyclic* if it has a cyclic group of automorphisms which is sharply transitive on the elements. For an excellent historical discussion and introduction to the literature on Steiner triple systems in general and cyclic Steiner triple systems in particular, the reader is referred to the first section of Doyen [3]. Here we note that a cyclic Steiner triple system $S(n)$ is known to exist for all orders $n \equiv 1, 3 \pmod 6$ except $n = 9$ [8]. Now, a CIP neofield $N_v = \{0, 1, a, a^2, \cdots, a^{v-2}\}$ of order $v = 2^\alpha$ has the property that $x + x = 0$ or $-x = x$ for all $x \in N_v$, and so if $x, y, z \in N_v$ satisfy $x + y = z$ then also $y + x = z$, $x + z = z + x = y$, and $y + z = z + y = x$. This means that $N_v(+)$ is a totally symmetric loop. The set of elements $N_v^* = N_v - \{0\}$ formed into the triples $\{x, y, z\}$ where $x + y = z$ thus yields a Steiner triple system $S(n)$ of order $n = v - 1$ [2]. Furthermore, the right regular representation of $N_v^*(\cdot)$ is a cyclic group of automorphisms of $N_v(+)$, hence also of $S(n)$, which is sharply transitive on the elements of $S(n)$. Hence, a CIP neofield of order $v = 2^\alpha \geqq 4$ naturally yields a cyclic Steiner triple system of order $n = v - 1$. Now, CIP neofields of order $v = 2^\alpha$ with nonisomorphic additive loops yield nonisomorphic cyclic Steiner triple systems of order $n = 2^\alpha - 1$, and by Theorem 4.5 there exists both the field of order v and a proper CIP neofield of order v for every order $v = 2^\alpha \geqq 16$. Hence, we obtain the following result, which is a more specific version of a theorem of Assmus and Mattson [1].

THEOREM 5.1. *There exists at least two nonisomorphic cyclic Steiner triple systems for each order* $n = 2^\alpha - 1 \geqq 15$.

Although the number of nonisomorphic CIP neofields of order $v = 2^\alpha$ goes to infinity with v, we cannot immediately conclude from this that the number of nonisomorphic cyclic Steiner triple systems of order $v - 1$ does the same, since we must ascertain the number of nonisomorphic additive loops among the nonisomorphic CIP neofields of order v. By further investigation, however, the authors have determined that this number does go to infinity with v. This will be presented in a subsequent paper.

REFERENCES

1. E. F. Assmus, Jr. and H. F. Mattson, *On the number of inequivalent Steiner triple systems*, J. Combinatorial Theory, **1** (1966), 301-305; Errata, **2** (1967), 394.
2. R. H. Bruck, *What is a loop?*, in *Studies in Modern Algebra* (M. A. A. Studies in Mathematics, 2), Prentice-Hall, Inc., Englewood Cliffs, N. J., (1963), 59-99.
3. Jean Doyen, *Sur la croissance du nombre de systèmes triples de Steiner non isomorphes*, J. Combinatorial Theory, **8** (1970), 424-441.

4. D. R. Hughes, *Planar division neo-rings*, Trans. Amer. Math. Soc., **80** (1955), 502-527.
5. E. C. Johnsen and Thomas Storer, *Combinatorial structures in loops III. Difference sets in special cyclic neofields*, J. Number Theory, to appear.
6. Emma Lehmer, *On residue difference sets*, Canad. J. Math., **5** (1953), 425-432.
7. Lowell J. Paige, *Neofields*, Duke Math. J., **16** (1949), 39-60.
8. Rose Peltesohn, *Eine Lösung der beiden Heffterschen Differenzenprobleme*, Compositio Math., **6** (1939), 251-257.
9. Thomas Storer, *Cyclotomy and Difference Sets*, Markham Publishing Co., Chicago, 1967.

Received December 12, 1972. The first author was supported in part by Air Force Office of Scientific Research Grants AFOSR 698-67 and 72-2163. The second author was supported in part by an NSF Research Grant.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA
AND
UNIVERSITY OF MICHIGAN, ANN ARBOR

PACIFIC JOURNAL OF MATHEMATICS

Printed in Japan by Intarnational Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics
Vol. 52, No. 1 January, 1974