Math. Z. 138, 1 – 14 (1974)

Combinatorial Structures in Loops

IV. Steiner Triple Systems in Neofields

Eugene C. Johnsen* and Thomas Storer**

1. Introduction

A *Steiner triple system* (STS) of order n, $\mathscr{T}_n = [S, \mathscr{S}]$, is an arrangement of the elements of an n-set S into a set $\mathscr{S}$ of triples such that every pair of elements in S occur together in exactly one triple of $\mathscr{S}$. A necessary and sufficient condition that an STS of order n exist is that $n \equiv 1, 3 \pmod 6$. An STS $\mathscr{T}_n$ which has a group of automorphisms G which is regular (sharply transitive) on the elements S is called *regular* and is denoted by $\langle \mathscr{T}_n, G \rangle$. It is simply called *cyclic* or *abelian* when the group G is respectively cyclic or abelian. For an excellent historical discussion and introduction to the literature on Steiner triple systems, the reader is referred to the first section of Doyen [10]. A *right neofield* of order v, $\mathbb{N}_v(+, \cdot)$, is an algebraic system of v elements including 0 and 1, $0 \neq 1$, with two binary operations $+$ (addition) and $\cdot$ (multiplication) such that $\mathbb{N}_v(+)$ is a loop with identity element 0, $\mathbb{N}_v^*(\cdot)$ (where $\mathbb{N}_v^* = \mathbb{N}_v - \{0\}$) is a group with identity element 1, every element of $\mathbb{N}_v$ is right distributive (i.e., every $x \in \mathbb{N}_v$ satisfies $(y+z) \cdot x = y \cdot x + z \cdot x$ for all $y, z \in \mathbb{N}_v$), and $x \cdot 0 = 0$ for all $x \in \mathbb{N}_v$. A right neofield in which every element is also left distributive is simply called a *neofield*. A right neofield $\mathbb{N}_v$ is said to have the inverse property (IP) and is called an IP *right neofield* if for each $y \in \mathbb{N}_v$ there is an element $z \in \mathbb{N}_v$ such that $(x+y)+z = x$ and $z+(y+x) = x$ for all $x \in \mathbb{N}_v$. In an IP right neofield every $y \in \mathbb{N}_v$ has a unique two-sided negative $-y \in \mathbb{N}_v$ and, in fact, z above is this element $-y$. We call a right neofield $\mathbb{N}_v$ *commutative* if $\mathbb{N}_v(+)$ is commutative. It is easy to show that an IP neofield is commutative [12]. A right neofield $\mathbb{N}_v$ and its additive loop $\mathbb{N}_v(+)$ are said to have *characteristic* m, written char $\mathbb{N}_v = m$, if

$$(\cdots \overbrace{((x+x)+x)+\cdots+x)+x}^{m \text{ terms}} = 0$$

* Supported in part by an Air Force Office of Scientific Research Grant.
** Supported in part by an NSF Research Grant.

for all $x \in \mathbb{N}_v$ and m is the least positive integer for which this is true. Finally, a neofield $\mathbb{N}_v$ is called *cyclic* or *abelian* if $\mathbb{N}_v^*(\cdot)$ is, respectively, cyclic or abelian, and a cyclic or abelian IP neofield is called, respectively, a CIP or AIP *neofield.*

In the next section we show that a regular STS $\langle \mathcal{T}_n, G \rangle$ of order $n \equiv 1, 3 \pmod 6$ is equivalent to a commutative IP right neofield $\mathbb{N}_v$ of order $v = n+1 \equiv 2, 4 \pmod 6$, char $\mathbb{N}_v = 2$, with $\mathbb{N}_v^*(\cdot)$ isomorphic to G. We determine the condition on $\langle \mathcal{T}_n, G \rangle$, called Z-regularity, for which $\mathbb{N}_v$ is in fact a neofield, and show that two Z-regular STSs are permutation isomorphic (i.e., are essentially the same combination of triple system and group) precisely when their corresponding neofields are isomorphic. Furthermore, an STS $\mathcal{T}_n$ which is regular with respect to two different groups G_1 and G_2 has $\langle \mathcal{T}_n, G_1 \rangle$ permutation isomorphic to $\langle \mathcal{T}_n, G_2 \rangle$ if and only if G_1 and G_2 are conjugate in the total automorphism group of $\mathcal{T}_n$, Aut$(\mathcal{T}_n)$. This shows that the two neofields corresponding to two Z-regular STSs $\langle \mathcal{T}_n, G_1 \rangle$ and $\langle \mathcal{T}_n, G_2 \rangle$ on the same STS are isomorphic if and only if G_1 and G_2 are conjugate in Aut$(\mathcal{T}_n)$.

In the third section we give a procedure for constructing AIP neofields which is an extension of the procedure previously used to construct CIP neofields from finite fields [12]. In his recent Ph. D. dissertation [9] Doner completed the determination of the orders for which CIP neofields exist and gave constructions of CIP neofields for all admissible orders. The above procedure can be applied to these CIP neofields and produces a sufficient number of different CIP neofields of each admissible order so that we can prove that the number of nonisomorphic CIP neofields of order v goes to infinity with v. The lower bound obtained in this proof, when used in conjunction with other known results, is sufficient to show that for all admissible orders $v \geqq 11$ except $v = 14$ there exists at least two nonisomorphic CIP neofields of order v.

In the last section we bring together some of these results to show that the number of nonisomorphic cyclic Steiner triple systems of order $n \equiv 1, 3 \pmod 6$ goes to infinity with n. The lower bound obtained in this proof shows that there exists at least two nonisomorphic cyclic Steiner triple systems for all orders $n \equiv 1, 3 \pmod 6$, $n \geqq 481$.

2. Regular Steiner Triple Systems

The following theorem gives an equivalent representation of regular STSs as commutative IP right neofields of even orders.

Theorem 2.1. *A regular Steiner triple system* $\langle \mathcal{T}_n, G \rangle$ *of order* $n \equiv 1, 3$ $\pmod 6$ *is equivalent to a commutative* IP *right neofield* $\mathbb{N}_v(+, \cdot)$ *of order* $v = n+1 \equiv 2, 4 \pmod 6$ *with* char$(\mathbb{N}_v) = 2$ *and* $\mathbb{N}_v^*(\cdot) \cong G$.

Proof. Let $\langle \mathcal{T}_n, G\rangle$ be a regular STS of order $n \equiv 1, 3 \pmod 6$ where $\mathcal{T}_n = [S, \mathcal{S}]$ and G is regular on S. Let s be a fixed element of S. Then $S = \{(s)g \mid g \in G\}$, and $(s)g = (s)h$ for $g, h \in G$ implies that $g = h$. Now, the binary operation $\circ$ in S where $x \circ x = x$ and $x \circ y = z$ if $x \neq y$ and $\{x, y, z\} \in \mathcal{S}$, for all $x, y, z \in S$, makes $S(\circ)$ into an idempotent totally symmetric quasigroup of order n [8], with G acting on $S(\circ)$ as a regular automorphism group. The quasigroup $S(\circ)$, in turn, induces a binary operation $\circ$ in G as follows. For $g, h, k \in G$ we define $g \circ h \equiv k$ in $G(\circ)$ if and only if $(s)g \circ (s)h = (s)k$ in $S(\circ)$. The mapping φ: $(s)g \to g$, $g \in G$, is a bijection of S onto G such that φ: $(s)g \circ (s)h = (s)(g \circ h) \to g \circ h$, for all $g, h \in G$. Hence φ is a quasigroup isomorphism and $G(\circ)$ is an idempotent totally symmetric quasigroup isomorphic to $S(\circ)$. We now adjoin to G a new element 0 to obtain the set $\mathbb{N}_v = G \cup \{0\}$ and define a binary operation $+$ on $\mathbb{N}_v$ as follows:

(i) $g + h \equiv g \circ h$ for all $g, h \in G$, $g \neq h$,

(ii) $g + g \equiv 0$ for all $g \in G$,

(iii) $g + 0 = 0 + g \equiv g$ for all $g \in \mathbb{N}_v$.

Then $\mathbb{N}_v(+)$ is a totally symmetric loop of order $v = n + 1$ with identity element 0 [8]. Here $g + h = h + g$ and $(g + h) + h = g$ for all $g, h \in \mathbb{N}_v$, whence $\mathbb{N}_v(+)$ is a commutative IP loop with $x + x = 0$ for all $x \in \mathbb{N}_v$. Now, the composition operation in G induces a multiplication $\cdot$ in $\mathbb{N}_v$ given by

(iv) $g \cdot h \equiv gh$ for all $g, h \in G$,

(v) $g \cdot 0 = 0 \cdot g \equiv 0$ for all $g \in \mathbb{N}_v$.

Now, for $g, h \in \mathbb{N}_v$, $(g + 0) \cdot h = g \cdot h = g \cdot h + 0 \cdot h$, $(g + h) \cdot 0 = 0 = g \cdot 0 + h \cdot 0$, and $(g + g) \cdot h = 0 \cdot h = 0 = g \cdot h + g \cdot h$, and for $g, h, k \in G$, $g \neq h$, we have

$$(s)((g + h) \cdot k) = ((s)(g \circ h))\, k = ((s)\, g \circ (s)\, h)\, k = (s)\, gk \circ (s)\, hk$$
$$= (s)(gk \circ hk) = (s)(g \cdot k + h \cdot k),$$

or $(g + h) \cdot k = g \cdot k + h \cdot k$; hence every element of $\mathbb{N}_v(+, \cdot)$ is right distributive. Thus $\mathbb{N}_v(+, \cdot)$ is a commutative IP right neofield of order $v = n + 1 \equiv 2, 4 \pmod 6$, char $\mathbb{N}_v = 2$, and $\mathbb{N}_v^*(\cdot) \cong G$.

Now let $\mathbb{N}_v(+, \cdot)$ be a commutative IP right neofield of order $v = n + 1 \equiv 2, 4 \pmod 6$, which implies that char $\mathbb{N}_v = 2$. Let $S = \mathbb{N}_v^*$. We form the set $\mathcal{S}$ of all distinct triples $\{a_1, a_2, a_3\}$ for which $a_1 + a_2 = a_3$ and $a_1 \neq a_2 \neq a_3 \neq a_1$ in $\mathbb{N}_v^*$. Now $|S| = n = v - 1 \equiv 1, 3 \pmod 6$, and $\{a_1, a_2, a_3\} \in \mathcal{S}$ if and only if $a_{(1)\sigma} + a_{(2)\sigma} = a_{(3)\sigma}$ for all permutations σ of $\{1, 2, 3\}$, hence every pair of elements in S occur together in precisely one triple of $\mathcal{S}$. Thus $\mathcal{T}_n = [S, \mathcal{S}]$ is a Steiner triple system of order n. Now, for each $g \in \mathbb{N}_v^*$, the mapping R_g: $x \to x \cdot g$ for all $x \in \mathbb{N}_v^*$ is a bijection on S such that $(x + y) \cdot g = x \cdot g + y \cdot g$, hence R_g maps triples to triples in $\mathcal{S}$ and is thus an automorphism of $\mathscr{T}_n$. The set $G=\{R_g|g\in\mathbb{N}_v^*\}$ forms a group under composition of mappings which is regular on S. Since G is the right regular representation of $\mathbb{N}_v^*(\cdot)$, $\langle\mathscr{T}_n, G\rangle$ is a regular Steiner triple system with $G\cong\mathbb{N}_v^*(\cdot)$.

In the proof of Theorem 2.1 the addition in the constructed right neofields depends on the choice of fixed element $s\in S$. It is natural to ask whether there is any relationship among the right neofields constructed with respect to different fixed elements. Some information on this is given in the following result. We let $Z(G)$ denote the centralizer of G in the total automorphism group of $\mathscr{T}_n$, $\mathrm{Aut}(\mathscr{T}_n)$.

Lemma 2.2. *Let $\langle\mathscr{T}_n, G\rangle$ be a regular* STS *of order n and let $\mathbb{N}_{v,1}(+,\cdot)$ and $\mathbb{N}_{v,2}(\oplus,\cdot)$ be two right neofields of order $v=n+1$ obtained from $\langle\mathscr{T}_n, G\rangle$ according to Theorem* 2.1 *using fixed elements s_1 and s_2 in S, respectively. Then the following statements are equivalent:*

(i) $\mathbb{N}_{v,1}(+,\cdot)$ *and* $\mathbb{N}_{v,2}(\oplus,\cdot)$ *are the same right neofield* (i.e., $+$ *and* $\oplus$ *are identical additions).*

(ii) *There exists an $\alpha\in Z(G)$ such that $(s_1)\alpha=s_2$.*

(iii) *The element $k\in G$ for which $(s_1)k=s_2$ is left distributive in $\mathbb{N}_{v,1}(+,\cdot)$.*

Proof. First assume (i) that $\mathbb{N}_{v,2}(+,\cdot)$ and $\mathbb{N}_{v,2}(\oplus,\cdot)$ are the same right neofield. Then $a+b=a\oplus b$ or $(s_2)(a+b)=(s_2)(a\oplus b)=(s_2)\,a\circ(s_2)\,b$ for all $a, b\in G$, $a\neq b$. We define the mapping α on S by $\big((s_1)\,g\big)\alpha\equiv(s_2)\,g$ for all $g\in G$. Since the elements in $\{(s_1)\,g|g\in G\}$ and in $\{(s_2)\,g|g\in G\}$ are distinct and $|G|=|S|$, α is well defined and bijective and $(s_1)\alpha=s_2$. Let $x, y\in S$, $x\neq y$, where $x=(s_1)\,a$ and $y=(s_1)\,b$, $a, b\in G$, $a\neq b$. Then

$$(x\circ y)\,\alpha=\big((s_1)\,a\circ(s_1)\,b\big)\,\alpha=\big((s_1)(a+b)\big)\,\alpha=(s_2)(a+b)=(s_2)\,a\circ(s_2)\,b$$
$$=\big((s_1)\,a\big)\,\alpha\circ\big((s_1)\,b\big)\,\alpha=(x)\,\alpha\circ(y)\,\alpha,$$

whence α is an automorphism of $\mathscr{T}_n$, and since $(s_1)\,g\alpha=(s_2)\,g=(s_1)\,\alpha g$ or $g\alpha=\alpha g$ for all $g\in G$, we have $\alpha\in Z(G)$, which proves (ii). Next assume (ii) that there exists an $\alpha\in Z(G)$ such that $(s_1)\,\alpha=s_2$. Let $k\in G$ be the element such that $(s_1)\,k=s_2=(s_1)\,\alpha$. Then for all $g, h\in G$, $g\neq h$,

$$(s_1)\big(k\cdot(g+h)\big)=(s_1)\,\alpha(g+h)=(s_1)(g+h)\,\alpha=\big((s_1)\,g\circ(s_1)\,h\big)\,\alpha$$
$$=(s_1)\,g\,\alpha\circ(s_1)\,h\,\alpha=(s_1)\alpha\,g\circ(s_1)\,\alpha h$$
$$=(s_1)k\,g\circ(s_1)\,k\,h=(s_1)(k\cdot g+k\cdot h)$$

or $k\cdot(g+h)=k\cdot g+k\cdot h$. Further, $k\cdot(g+0)=k\cdot(0+g)=k\cdot g=k\cdot g+k\cdot 0$ $=k\cdot 0+k\cdot g$ and $k\cdot(g+g)=k\cdot 0=0=k\cdot g+k\cdot g$ for all $g\in G\cup\{0\}$. Hence k is left distributive in $\mathbb{N}_{v,1}(+,\cdot)$, and we have (iii). Finally, assume (iii) that the element $k\in G$ for which $(s_1)\,k=s_2$ is left distributive in $\mathbb{N}_{v,1}(+,\cdot)$.

Then for any $g, h \in G$, $g \neq h$,

$$(s_2)(g+h)=(s_1)\,k(g+h)=(s_1)(k\cdot g+k\cdot h)=(s_1)\,k\,g\circ(s_1)\,k\,h$$
$$=(s_2)\,g\circ(s_2)\,h=(s_2)(g\oplus h)$$

or $g+h=g\oplus h$. Further, $g+0=0+g=g=g\oplus 0=0\oplus g$ and $g+g=0=g\oplus g$ for all $g\in G\cup\{0\}$. Hence the additions in $\mathbb{N}_{v,1}(+,\cdot)$ and $\mathbb{N}_{v,2}(\oplus,\cdot)$ are identical, which proves (i). This completes the proof of the lemma.

Corollary 2.3. *Let $\langle\mathcal{T}_n, G\rangle$ be a regular* STS *of order n and let $\mathbb{N}_v(+,\cdot)$ be a right neofield of order $v=n+1$ obtained from $\langle\mathcal{T}_n, G\rangle$ according to Theorem* 2.1. *Then $\mathbb{N}_v(+,\cdot)$ is a neofield if and only if $Z(G)$ is transitive on S. Furthermore, if $\langle\mathcal{T}_n, G\rangle$ yields a neofield with respect to some $s\in S$, according to Theorem* 2.1, *then it yields the same neofield with respect to every $s\in S$.*

Proof. If $\mathbb{N}_v(+,\cdot)$ is a neofield then every $k\in G$ is left distributive in $\mathbb{N}_v(+,\cdot)$. Since G is transitive on S there exists for every $s_2\in S$ and $\alpha\in Z(G)$ such that $(s_1)\alpha=s_2$, by Lemma 2.2 (ii), hence $Z(G)$ is transitive on S. Conversely, suppose that $Z(G)$ is transitive on S. Then, by Lemma 2.2 (iii), the unique element $k\in G$ for which $(s_1)\,k=s_2$ is left distributive in $\mathbb{N}_v(+,\cdot)$, for every $s_2\in S$. Since this includes all elements of G and 0 is always left distributive in $\mathbb{N}_v(+,\cdot)$, this says that $\mathbb{N}_v(+,\cdot)$ is a neofield. Now suppose that $\langle\mathcal{T}_n, G\rangle$ yields a neofield with respect to some $s\in S$. Then for each $s_2\in S$ the element $k\in G$ such that $(s)\,k=s_2$ is left distributive in $\mathbb{N}_v(+,\cdot)$, whence by Lemma 2.2 (i) the neofield $\mathbb{N}_v(\oplus,\cdot)$ obtained from $\langle\mathcal{T}_n, G\rangle$ using the fixed element s_2 is the same neofield as the one obtained using the fixed element s. Hence $\langle\mathcal{T}_n, G\rangle$ yields the same neofield with respect to every $s\in S$.

Corollary 2.4. *An abelian (cyclic)* STS $\langle\mathcal{T}_n, G\rangle$ *of order $n\equiv 1, 3 \pmod 6$ is equivalent to a unique commutative* AIP (CIP) *neofield $\mathbb{N}_v(+,\cdot)$ of order $v=n+1\equiv 2, 4 \pmod 6$ with* char $\mathbb{N}_v=2$ *and $\mathbb{N}_v^*(\cdot)\cong G$.*

We shall call a regular STS $\langle\mathcal{T}_n, G\rangle$ *Z-regular* when $Z(G)$ is transitive on S.

Now let $\langle\mathcal{T}_{n,1}, G_1\rangle$ and $\langle\mathcal{T}_{n,2}, G_2\rangle$ be two regular Steiner triple systems where $\mathcal{T}_{n,1}=[S_1, \mathcal{S}_1]$ and $\mathcal{T}_{n,2}=[S_2, \mathcal{S}_2]$. We say that $\langle\mathcal{T}_{n,1}, G_1\rangle$ and $\langle\mathcal{T}_{n,2}, G_2\rangle$ are *permutation isomorphic*, written $\langle\mathcal{T}_{n,1}, G_1\rangle\cong\langle\mathcal{T}_{n,2}, G_2\rangle$, if there is an isomorphism τ of $\mathcal{T}_{n,1}$ onto $\mathcal{T}_{n,2}$ (mapping elements to elements and preserving triples) and a group isomorphism γ of G_1 onto G_2 such that $(x)\,g=y$ in $\langle\mathcal{T}_{n,1}, G_1\rangle$ if and only if $((x)\tau)((g)\gamma)=(y)\tau$ in $\langle\mathcal{T}_{n,2}, G_2\rangle$ for $x, y\in S_1$ and $g\in G_1$. Clearly, permutation isomorphism is an equivalence relation on regular Steiner triple systems.

Lemma 2.5. *Let $\langle\mathcal{T}_n, G\rangle$ be a regular* STS *of order n and let $\mathbb{N}_v(+,\cdot)$ be a corresponding right neofield of order $v=n+1$ as given by Theorem* 2.1.

Let N_v^+ be the STS *determined by the nonzero elements in* $\mathbb{N}_v(+)$ *and let* $\mathcal{R}_G$ *be the right regular representation of* $G\cong\mathbb{N}_v^*(\cdot)$. *Then* $\langle\mathcal{T}_n, G\rangle\cong\langle N_v^+, \mathcal{R}_G\rangle$.

Proof. Let τ be the isomorphism from $\mathcal{T}_n$ onto N_v^+ given by $\tau\colon t\to g$ where $(s)g=t$ in $\mathcal{T}_n$, s the fixed element of S. Let γ be the isomorphism of G onto $\mathcal{R}_G$ given by $\gamma\colon g\to R_g$ where $R_g\colon u\to u\cdot g$ for all $u\in G=N_v^+$. Then $(x)g=y$ in $\mathcal{T}_n$ if and only if $(s)\xi g=(s)\eta$ where $x=(s)\xi$, $y=(s)\eta$, and $\xi,\eta\in G$, if and only if $\xi\cdot g=\eta$ in $G=N_v^+$ if and only if $((x)\tau)((g)\gamma)=(\xi)R_g=\xi\cdot g=\eta=(y)\tau$ for $x, y\in\mathcal{T}_n$ and $g\in G$. Thus $\langle\mathcal{T}_n, G\rangle\cong\langle N_v^+, \mathcal{R}_G\rangle$.

Theorem 2.6. *Let* $\langle\mathcal{T}_{n,1}, G_1\rangle$ *and* $\langle\mathcal{T}_{n,2}, G_2\rangle$ *be two Z-regular Steiner triple systems of order n and let* $\mathbb{N}_{v,1}(+,\cdot)$ *and* $\mathbb{N}_{v,2}(\oplus,\odot)$ *be the corresponding neofields of order* $v=n+1$ *as given by Theorem* 2.1. *Then* $\langle\mathcal{T}_{n,1}, G_1\rangle\cong\langle\mathcal{T}_{n,2}, G_2\rangle$ *if and only if* $\mathbb{N}_{v,1}(+,\cdot)\cong\mathbb{N}_{v,2}(\oplus,\odot)$.

Proof. Let $\langle\mathcal{T}_{n,1}, G_1\rangle\cong\langle\mathcal{T}_{n,2}, G_2\rangle$ and let $\mathbb{N}_{v,1}(+,\cdot)$ and $\mathbb{N}_{v,2}(\oplus,\odot)$ be the respective corresponding neofields. Then by Lemma 2.5 $\langle N_{v,1}^+, \mathcal{R}_{G_1}\rangle\cong\langle N_{v,2}^+, \mathcal{R}_{G_2}\rangle$, whence there exists an isomorphism $\tau\colon N_{v,1}^+\to N_{v,2}^+$ and an isomorphism $\gamma\colon\mathcal{R}_{G_1}\to\mathcal{R}_{G_2}$ such that $(x)R_g=y$ in $N_{v,1}^+$ if and only if $((x)\tau)((R_g)\gamma)=(y)\tau$ in $N_{v,2}^+$. Now, γ induces an isomorphism

$$\varphi\colon\ \mathbb{N}_{v,1}^*(\cdot)\to\mathbb{N}_{v,2}^*(\odot)\quad\text{where }(g)\varphi=h$$

exactly when $(R_g)\gamma=R_h(=R_{(g)\varphi})$. Thus $(x)R_g=y$ in $N_{v,1}^+$ if and only if $((x)\tau)R_{(g)\varphi}=(y)\tau$ or $((x)\tau)\odot(g)\varphi=(y)\tau$. In particular, $(1)\tau\odot(g)\varphi=(g)\tau$. We now extend φ to the mapping

$$\Phi\colon\ x\to\begin{cases}(x)\varphi, & x\neq 0\\ 0, & x=0\end{cases}$$

from $\mathbb{N}_{v,1}\to\mathbb{N}_{v,2}$. Since

$$(0\cdot x)\Phi=(x\cdot 0)\Phi=(0)\Phi=0=(0)\Phi\odot(x)\Phi=(x)\Phi\odot(0)\Phi,$$

Φ is an isomorphism from $\mathbb{N}_{v,1}(\cdot)$ onto $\mathbb{N}_{v,2}(\odot)$. Now, we have

$$(x+0)\Phi=(0+x)\Phi=(x)\Phi=(x)\Phi\oplus(0)\Phi=(0)\Phi\oplus(x)\Phi$$

and

$$(x+x)\Phi=(0)\Phi=0=(x)\Phi\oplus(x)\Phi.$$

Also, for $0\neq x\neq y\neq 0$,

$$\begin{aligned}(1)\tau\odot((x+y)\varphi)&=(x+y)\tau=(x)\tau\oplus(y)\tau\\ &=[(1)\tau\odot(x)\varphi]\oplus[(1)\tau\odot(y)\varphi]=(1)\tau\odot[(x)\varphi\oplus(y)\varphi];\end{aligned}$$

whence, since $(1)\tau\neq 0$, $(x+y)\varphi=(x)\varphi\oplus(y)\varphi$ or $(x+y)\Phi=(x)\Phi\oplus(y)\Phi$. Thus Φ is also an isomorphism of $\mathbb{N}_{v,1}(+)$ onto $\mathbb{N}_{v,2}(\oplus)$. Thus Φ is a neofield isomorphism, which yields $\mathbb{N}_{v,1}(+,\cdot)\cong\mathbb{N}_{v,2}(\oplus,\odot)$.

Now suppose that $\mathbb{N}_{v,1}(+,\cdot)\cong\mathbb{N}_{v,2}(\oplus,\odot)$ under the isomorphism Φ. We define the mappings $\tau\colon N_{v,1}^{+}\to N_{v,2}^{+}$ and $\gamma\colon \mathscr{R}_{G_1}\to\mathscr{R}_{G_2}$ by $(x)\tau=(x)\Phi$ for all $x\neq 0$ in $\mathbb{N}_{v,1}$ and $(R_g)\gamma=R_{(g)\Phi}$ for all $g\in\mathbb{N}_{v,1}^{*}$. Clearly τ and γ are bijective. Then for $0\neq x\neq y\neq 0$,

$$(x+y)\tau=(x+y)\Phi=(x)\Phi\oplus(y)\Phi=(x)\tau\oplus(y)\tau,$$

and for $g,h\in\mathbb{N}_{v,1}^{*}$,

$$(R_g R_h)\gamma=(R_{gh})\gamma=R_{(gh)\Phi}=R_{(g)\Phi\odot(h)\Phi}=R_{(g)\Phi}R_{(h)\Phi}=(R_g)\gamma(R_h)\gamma$$

whence τ is an isomorphism from the STS $N_{v,1}^{+}$ onto the STS $N_{v,2}^{+}$ and γ is an isomorphism of the right regular representation $\mathscr{R}_{G_1}$ of $\mathbb{N}_{v,1}^{*}(\cdot)$ onto the right regular representation $\mathscr{R}_{G_2}$ of $\mathbb{N}_{v,2}^{*}(\odot)$. Further, $(x)R_g=y$ in $N_{v,1}^{+}$ if and only if $x\cdot g=y$ in $G_1=N_{v,1}^{+}$ if and only if $(x)\Phi\odot(g)\Phi=(y)\Phi$ if and only if

$$((x)\tau)(R_g)\gamma=((x)\tau)R_{(g)\Phi}=(y)\tau \quad\text{in}\quad G_2=N_{v,2}^{+}.$$

Hence $\langle N_{v,1}^{+},\mathscr{R}_{G_1}\rangle\cong\langle N_{v,2}^{+},\mathscr{R}_{G_2}\rangle$ and, by Lemma 2.5, $\langle\mathscr{T}_{n,1},G_1\rangle\cong\langle\mathscr{T}_{n,2},G_2\rangle$.

We now consider an STS $\mathscr{T}_n$ which has two regular automorphism groups which are isomorphic.

Theorem 2.7. *Let $\mathscr{T}_n$ be a regular Steiner triple system with respect to two isomorphic regular automorphism groups G_1 and G_2. Then $\langle\mathscr{T}_n,G_1\rangle\cong\langle\mathscr{T}_n,G_2\rangle$ if and only if G_1 and G_2 are conjugate in* $\operatorname{Aut}(\mathscr{T}_n)$.

Proof. Let $\langle\mathscr{T}_n,G_1\rangle\cong\langle\mathscr{T}_n,G_2\rangle$ where τ is the automorphism of $\mathscr{T}_n$ and γ is the isomorphism from G_1 onto G_2 for which $(x)g=y$ in $\langle\mathscr{T}_n,G_1\rangle$ if and only if $((x)\tau)((g)\gamma)=(y)\tau$ in $\langle\mathscr{T}_n,G_2\rangle$. This means that

$$((x)\tau)(\tau^{-1}g\tau)=(y)\tau=((x)\tau)((g)\gamma)$$

for all $x\in S$ and all $g\in G_1$, or $(g)\gamma=\tau^{-1}g\tau\in G_2$ for all $g\in G_1$, and since $|G_1|=|G_2|$, G_1 and G_2 are conjugate in $\operatorname{Aut}(\mathscr{T}_n)$. Conversely, suppose that G_1 and G_2 are conjugate in $\operatorname{Aut}(\mathscr{T}_n)$ where $\tau^{-1}G_1\tau=G_2$, $\tau\in\operatorname{Aut}(\mathscr{T}_n)$. Then $(x)g=y$ in $\langle\mathscr{T}_n,G_1\rangle$ if and only if

$$(y)\tau=((x)g)\tau=((x)\tau)(\tau^{-1}g\tau)=((x)\tau)((g)\gamma)$$

in $\langle\mathscr{T}_n,G_2\rangle$ for all $g\in G_1$, where $\gamma\colon g\to\tau^{-1}g\tau$, $g\in G_1$, is an isomorphism from G_1 onto G_2. Hence $\langle\mathscr{T}_n,G_1\rangle\cong\langle\mathscr{T}_n,G_2\rangle$, which proves the theorem.

Corollary 2.8. *Let $\mathscr{T}_n$ be a Z-regular* STS *with respect to two isomorphic regular automorphism groups G_1 and G_2 and let $\mathbb{N}_{v,1}(+,\cdot)$ and $\mathbb{N}_{v,2}(\oplus,\odot)$ be the corresponding neofields obtained according to Theorem* 2.1 *from $\langle\mathscr{T}_n,G_1\rangle$ and $\langle\mathscr{T}_n,G_2\rangle$, respectively. Then $\mathbb{N}_{v,1}(+,\cdot)\cong\mathbb{N}_{v,2}(\oplus,\odot)$ if and only if G_1 and G_2 are conjugate in* $\operatorname{Aut}(\mathscr{T}_n)$.

Proof. By Theorem 2.6, $\mathbb{N}_{v,1}(+,\cdot)\cong\mathbb{N}_{v,2}(\oplus,\odot)$ if and only if $\langle\mathcal{T}_n, G_1\rangle\cong\langle\mathcal{T}_n, G_2\rangle$, and by Theorem 2.7 $\langle\mathcal{T}_n, G_1\rangle\cong\langle\mathcal{T}_n, G_2\rangle$ if and only if G_1 and G_2 are conjugate in $\mathrm{Aut}(\mathcal{T}_n)$. Hence we have the corollary.

We shall be using Corollary 2.8 to obtain lower bounds for the number of nonisomorphic cyclic Steiner triple systems of order n.

3. Construction of AIP Neofields from AIP Neofields

In [12] we gave a construction of CIP neofields from finite fields. This construction is, in fact, much more general and can be used to obtain further AIP neofields from given finite AIP neofields. Since this construction generalizes with no essential change we give here just a description of the construction and the statements of the corresponding results obtained.

Let $\mathbb{N}_v(+,\cdot)$ be a neofield of order v. We write the set of elements of the neofield as $\mathbb{N}_v=\{0, 1, a_1, a_2, \ldots, a_{v-2}\}$ where the multiplication of these elements is given explicitly, either in terms of generators or of a multiplication table. Then the addition in $\mathbb{N}_v(+,\cdot)$ is completely determined by the function $T(x)\equiv 1+x$, $x\in\mathbb{N}_v$, since $0+x=x$ for all $x\in\mathbb{N}_v$ and $y+z=y(1+y^{-1}z)=y\cdot T(y^{-1}z)$ for all $y,z\in\mathbb{N}_v$, $y\neq 0$. Such an expression of $\mathbb{N}_v(+,\cdot)$ in terms of the set $\mathbb{N}_v$ with explicitly given multiplication and the function T on $\mathbb{N}_v$ is called a *presentation* of the neofield and T is called its *presentation function.* A neofield is completely determined algebraically by its presentation, which may be given in terms of the first two rows of its addition table. As was seen in [12], a neofield may have more than one presentation. The different presentations in fact correspond to the different definitions of addition on the set $\mathbb{N}_v$.

Let $\mathbb{N}_v(+,\cdot)$ be an AIP neofield of order $v\geqq 10$ (all AIP neofields of orders $v\leqq 9$ are fields), with presentation given by

$$\mathbb{N}_v=\{0, 1, a_1, a_2, \ldots, a_{v-2}\}$$

and the presentation function $T(x)=1+x$ for all $x\in\mathbb{N}_v$. We define the functions T' and T_0 on $\mathbb{N}_v$ by

$$T'(x)\equiv(-1)+x, \qquad x\in\mathbb{N}_v, \tag{3.1}$$

and

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

and define a new addition $\oplus$ on $\mathbb{N}_v$ by

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

It is straightforward to verify that $\mathbb{N}_v(\oplus, \cdot)$ is an AIP neofield of order v which is isomorphic to $\mathbb{N}_v(+, \cdot)$ under the mapping $0 \to 0$, $x \to x^{-1}$ for all $x \neq 0$ in $\mathbb{N}_v$. We let the corresponding presentation of $\mathbb{N}_v(\oplus, \cdot)$ be given by $\mathbb{N}_v = \{0, 1, a_1, a_2, \ldots, a_{v-2}\}$ and the presentation function $T_0(x) = 1 \oplus x$, $x \in \mathbb{N}_v$. We now state the results which give the construction of further AIP neofields. The proofs of all except one of these results are identical to those in §3 of [12] and will not be repeated. These proofs carry over because the full associativity of addition which occurs in the fields is really not needed.

Lemma 3.1. *For all* $x \in \mathbb{N}_v$, $(T' T_0)^3(x) = x$.

The following lemma is the only result here whose proof varies from that in [12].

Lemma 3.2. *We have* $T' T_0(x) = x$ (i.e., $T(x) = T_0(x)$) *in the set* $\mathbb{N}_v$ *precisely when*

1) $x = 0, -1$. *(This includes* $1 = -1$ *when* v *is even.)*

2) $(1+x) + x^2 = 1 + (x + x^2) = 0$, *which implies* $x^3 = 1$; $x \neq 0, -1$.

Proof. 1) is obvious. When $x \neq 0, -1$ we have $T' T_0(x) = x$ if and only if $1 + (x + x^2) = (1 + x) + x^2 = 0$. This equation implies $x^3 = -(x + x^2) = 1$.

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

We now assume that $\mathbb{N}_v(\boxplus, \cdot)$ is an abelian neofield of order v with presentation given by $\mathbb{N}_v = \{0, 1, a_1, a_2, \ldots, a_{v-2}\}$ and the presentation function $T_*(x) \equiv 1 \boxplus x$ satisfying

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

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

Lemma 3.4. *The function* T_* *is bijective on* $\mathbb{N}_v$, *and for all* $x, y \in \mathbb{N}_v$, *satisfies*

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

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

Furthermore, $\mathbb{N}_v(\boxplus)$ *is commutative if and only if*

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

For $y \in S$, $S = \{x \in \mathbb{N}_v \mid T' T_0(x) \neq x\}$, we define the *orbit* of y to be the set $\theta(y) = \{y, T' T_0(y), (T' T_0)^2(y)\}$. A simple computation shows that $\theta(y) = \{y, -(T(y))^{-1}, -(T_0(y))^{-1}\}$.

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

Lemma 3.6. *Suppose* $\mathbb{N}_v(\boxplus)$ *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.*

Lemma 3.7. *If $\mathbb{N}_v(\boxplus)$ is commutative, then $\mathbb{N}_v(\boxplus)$ is an* IP *neofield.*

The above gives us enough information to construct AIP neofields $\mathbb{N}_v(\boxplus, \cdot)$ for $v \geqq 10$ according to (i) and (ii) whenever $\mathbb{N}_v(+, \cdot)$ and $\mathbb{N}_v(\oplus, \cdot)$ have distinct presentations.

Theorem 3.8. *Let $\mathbb{N}_v(+, \cdot)$ and $\mathbb{N}_v(\oplus, \cdot)$, $\mathbb{N}_v = \{0, 1, a_1, a_2, \ldots, a_{v-2}\}$ be two copies of a finite* AIP *neofield of order $v \geqq 10$ with presentation functions T and T_0, respectively, where T_0 is related to T by*

$$T_0(x) = \begin{cases} T(x), & x = 0, -1 \\ x(T(x))^{-1}, & x \neq 0, -1. \end{cases} \tag{3.4}$$

Let T_* be any mapping on $\mathbb{N}_v$ satisfying

a) *$T_* \neq T$ and $T_* \neq T_0$ on $\mathbb{N}_v$,*

b) *for each $x \in \mathbb{N}_v$, 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 an AIP *neofield $\mathbb{N}_v(\boxplus, \cdot)$ whose multiplication is identical to that of $\mathbb{N}_v(+, \cdot)$ and $\mathbb{N}_v(\oplus, \cdot)$.*

Theorem 3.8 constructs new presentations of AIP neofields whenever there exists an AIP neofield $\mathbb{N}_v(+, \cdot)$ for which S has at least two orbits. This rules out $v = 10$. More specially, this rules out $\mathbb{N}_v(+, \cdot)$ whenever $T' T_0(x) = x$ for all $x \in \mathbb{N}_v$. By Lemma 3.2 this only occurs when $T(x) = x^2$ and $x^3 = 1$ for every $x \neq 0, -1$ in $\mathbb{N}_v$, which means that for $v \geqq 10$, $\mathbb{N}_v^*(\cdot)$ is an elementary abelian 3-group and $|\mathbb{N}_v| = 3^\alpha + 1$, $\alpha \geqq 2$. AIP neofields of this type have been obtained by Paige [14].

4. CIP Neofields

The following result was proved in [12], where ϕ is Euler's phi-function.

Lemma 4.1. *A cyclic neofield $\mathbb{N}_v(+, \cdot)$, $\mathbb{N}_v = \{0, 1, a, a^2, \ldots, a^{v-2}\}$ of order $v > 1$ has at most $\phi(v-1)$ different presentations based on the set $\mathbb{N}_v$.*

Doner [9] has recently completed the determination of the orders for which CIP neofields exist. They exist precisely for all orders $v \geqq 2$ satisfying $v \neq 0, 6, 12, 15, 18, 21 \pmod{24}$ and $v \neq 10$. The restriction $v \neq 0, 6, 12, 18 \pmod{24}$ was obtained previously by Hughes [11] and the existence for $v \equiv 2, 4 \pmod{6}$, $v \neq 10$, was essentially shown earlier (if we invoke Corollary 2.4) by Peltesohn [15]. Thus, for every admissible order v we can apply the construction theorem of the preceding section to obtain further CIP neofields. We now obtain some information about the number of nonisomorphic CIP neofields constructed by Theorem 3.8.

For this the following refinement of Lemma 3.2 for CIP neofields is needed. The proof is straightforward and will be omitted. Note that if $\mathbb{N}_v^*(\cdot)$ is cyclic and $x^3=1$ for some $x\in\mathbb{N}_v^*$, $x\neq 1$, then $\mathbb{N}_v^*(\cdot)$ has a unique subgroup of order 3 $\{1,\zeta,\zeta^2\}$ where ζ is a primitive cube root of unity.

Lemma 4.2. *When* $\mathbb{N}_v(+,\cdot)$ *and* $\mathbb{N}_v(\oplus,\cdot)$ *are* CIP *neofields we have* $T'T_0(x)=x$ *in the set* $\mathbb{N}_v$ *precisely when*

1) $v\equiv 1 \pmod 6$ *and* $x=0, -1, \zeta, \zeta^2$. *Here* $\theta(1)=\{1, -2, -2^{-1}\}$.

2) $v\equiv 2 \pmod 6$ *and* $x=0, -1\ (=1)$. *Here*

$$\operatorname{char}\mathbb{N}_v(+)=\operatorname{char}\mathbb{N}_v(\oplus)=2.$$

3) $v\equiv 3 \pmod 6$ *and* $x=0, -1, 1$. *Here* $\operatorname{char}\mathbb{N}_v(+)=\operatorname{char}\mathbb{N}_v(\oplus)=3$.

4) $v\equiv 4 \pmod 6$ *and* $x=0, -1\ (=1), \zeta, \zeta^2$. *Here*

$$\operatorname{char}\mathbb{N}_v(+)=\operatorname{char}\mathbb{N}_v(\oplus)=2.$$

5) $v\equiv 5 \pmod 6$ *and* $x=0, -1$. *Here* $\theta(1)=\{1, -2, -2^{-1}\}$.

Theorem 4.3. *The number of nonisomorphic* CIP *neofields of order* v *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, including the original two, is $2^{(u/6)+1}$ and if $\theta(1)$ does not exist this number is $2^{u/6}$. Now, in the cyclic group $\mathbb{N}_v^*(\cdot)$ there are at most two elements of order 3; hence, by Lemma 4.2, the value of u is at least $v-4-3=v-7$ if $\theta(1)$ exists and $v-4$ if $\theta(1)$ does not exist, whence the resulting number of CIP neofield presentations obtained by Theorem 3.8 is at least $2^{(v-4)/6}$, including the original two. Now, by Lemma 4.1, a given CIP neofield of order v can occur among these presentations at most $\phi(v-1)$ times, hence the construction yields at least

$$\frac{2^{(v-4)/6}}{\phi(v-1)}>\frac{2^{(v-4)/6}}{v-1}$$

nonisomorphic CIP neofields of order v. Since

$$\lim_{v\to\infty}\frac{2^{(v-4)/6}}{v-1}=\infty,$$

we have the theorem.

Now, by Lemma 4.2 and the proof of Theorem 4.3, the number of nonisomorphic CIP neofields constructed by Theorem 3.8 is at least $\dfrac{2^{(v-r)/6}}{\phi(v-1)}$

when $v \equiv r \pmod 6$, $r = -1, 1, 2, 3, 4$. This value is greater than 1 for all admissible orders $v \geqq 19$ except $v = 20, 22, 26$, and 28, and hence there exist at least two nonisomorphic CIP neofields for these orders. Further, from the results in [12] there are at least two nonisomorphic CIP neofields for all admissible orders $11 \leqq v < 19$ except $v = 14$ where only one exists, and from the work of Bays [1, 2, 5] we see by Corollary 2.4 that the number of nonisomorphic CIP neofields of orders $n = 20, 22, 26$, and 28 is at least two. Hence, for all admissible orders $v \geqq 11$ except $v = 14$ there exists at least two nonisomorphic CIP neofields of order v.

5. Cyclic Steiner Triple Systems

Let $\mathscr{T}_n = [S, \mathscr{S}]$ be an STS of order $n = v - 1$ where $2^\alpha - 1 \leqq n < 2^{\alpha+1}$ and so $\alpha \leqq \log_2 v < \alpha + 1$. We want to determine how small the number of elements of S which generate $\mathscr{T}_n$ can be. Now, two elements generate a $\mathscr{T}_3$ and three elements not in a triple generate at least a $\mathscr{T}_7$. In general, a $\mathscr{T}_m = [S_m, \mathscr{S}_m]$ with an element $x \notin S_m$ generate at least a $\mathscr{T}_{2m+1}$, since the third element z in the triples $\{a, x, z\}$, $a \in S_m$, must be distinct and lie outside of $S_m \cup \{x\}$, thus yielding an extension of $\mathscr{T}_m$ having at least $2m+1$ elements. By induction, then, there exists for each integer β satisfying $3 \leqq 2^\beta - 1 \leqq n$ a set of at most β elements of S which generate at least a $\mathscr{T}_{2^\beta - 1}$.

Lemma 5.1. *Let $\mathscr{T}_n = [S, \mathscr{S}]$ be an* STS *of order n where $2^\alpha - 1 \leqq n < 2^{\alpha+1} - 1$, $\alpha \geqq 2$ an integer. Then there exists a set of at most α elements of S which generate $\mathscr{T}_n$.*

Proof. There exists a set of at most α elements of S which generate a $\mathscr{T}_m = [S_m, \mathscr{S}_m]$ with $2^\alpha - 1 \leqq m \leqq n$. If $m < n$ there exists an $x \in S - S_m$ such that $\mathscr{T}_m$ and x generate at least a $\mathscr{T}_{2m+1}$ in $\mathscr{T}_n$ where $2m + 1 \geqq 2^{\alpha+1} - 1 > n$, a contradiction. Hence $m = n$ and we have the lemma.

Now let $\mathscr{T}_n$ be a cyclic STS. Suppose we obtain an upper bound for the total number of distinct cyclic regular automorphism groups of $\mathscr{T}_n$. This will be an upper bound for the maximum number of cyclic regular automorphism groups of $\mathscr{T}_n$ which are pairwise nonconjugate in $\mathrm{Aut}(\mathscr{T}_n)$, whence an upper bound for the number of nonisomorphic CIP neofields of order $v = n + 1$ with a given additive loop $\mathbb{N}_v(+)$, by Corollary 2.8. Now, a generator for a cyclic regular automorphism group of $\mathscr{T}_n$ is completely determined by its action on a set of at most α generating elements of $\mathscr{T}_n$. Since no generating element of $\mathscr{T}_n$ can be mapped to itself by a generator, there are no more than

$$(n-1)(n-1)(n-2)\ldots(n-\alpha+1) = (v-2)(v-2)(v-3)\ldots(v-\alpha) \qquad (5.1)$$

generators altogether. The number of different generators for a cyclic group of order n is $\phi(n)$, hence there are no more than

$$\frac{(n-1)(n-1)(n-2)\ldots(n-\alpha+1)}{\phi(n)}=\frac{(v-2)(v-2)(v-3)\ldots(v-\alpha)}{\phi(v-1)}\equiv v_v \tag{5.2}$$

different cyclic regular automorphism groups on $\mathscr{T}_n$. Now, the number of nonisomorphic CIP neofields of order $v\equiv 2,4 \pmod 6$ constructed by Theorem 3.8 is, by the proof of Theorem 4.3, at least $\frac{2^{(v-4)/6}}{\phi(v-1)}$. Since there are no more than v_v nonisomorphic CIP neofields of order v with a given additive loop, there are at least

$$\begin{aligned}\frac{2^{(v-4)/6}}{\phi(v-1)\cdot v_v}&=\frac{2^{(v-4)/6}}{(v-2)(v-2)(v-3)\ldots(v-\alpha)}\\&>2^{-2/3}\cdot\frac{2^{v/6}}{v^{\alpha}}>2^{-2/3}\cdot\frac{2^{v/6}}{v^{\log_2 v}}\end{aligned} \tag{5.3}$$

distinct CIP neofields of order $v\equiv 2,4 \pmod 6$ with nonisomorphic additive loops $\mathbb{N}_v(+)$. Let

$$\frac{2^{v/6}}{v^{\log_2 v}}=\frac{2^{v/6}}{2^{(\log_2 v)^2}}=2^w \tag{5.4}$$

where

$$w=(\log_2 v)^2\left\{\frac{v}{6(\log_2 v)^2}-1\right\}. \tag{5.5}$$

Now $(\log_2 v)^2\to\infty$ and $\frac{v}{(\log_2 v)^2}\to\infty$ as $v\to\infty$, whence

$$\lim_{v\to\infty}\frac{2^{v/6}}{v^{\log_2 v}}=\lim_{v\to\infty}2^w=\infty. \tag{5.6}$$

Since CIP neofields exist and the construction of further CIP neofields by Theorem 3.8 can be carried out for all orders $v\equiv 2,4 \pmod 6$, $v>10$, we have the following result.

Theorem 5.1. *The number of nonisomorphic cyclic Steiner triple systems of order* $n=v-1\equiv 1,3 \pmod 6$ *goes to infinity with* n.

This result was previously known for the subclass of prime orders $n\equiv 1 \pmod 6$ [3, 13].

We note that for all $v\equiv 2,4 \pmod 6$, $v\geqq 482$, the expression on the right side of (5.3) is greater than 1, which shows that for all $n\equiv 1,3 \pmod 6$, $n\geqq 481$, there exist at least two nonisomorphic cyclic Steiner triple systems of order n. This result was previously known for all $n=2^\alpha-1\geqq 15$ [12] and for a number of low values of n [1-7], as well as for all prime $n=6k+1\geqq 19$ [3, 13].

References

1. Bays, S.: Sur les systèmes cycliques de triples de Steiner. C. r. Acad. Sci., Paris **165**, 543-545 (1917); **171**, 1363-1365 (1920); **175**, 936-939 (1922)
2. Bays, S.: Sur les systèmes cycliques de triples de Steiner. Ann. sci. Ecole Norm. sup. III Sér. **40**, 55-96 (1923)
3. Bays, S.: Recherche des systèmes cycliques de triples de Steiner différents pour N premier (ou puissance de nombre premier) de la forme $6n+1$. J. Math. pures appl. IX. Sér. **2**, 73-98 (1923)
4. Bays, S.: Sur les systèmes cycliques de triples de Steiner différent pour N premier (ou puissance de nombre premier) de la forme $6n+1$. Ann. Fac. Sci. Univ. Toulouse III. Sér. **17**, 23-61 (1925)
5. Bays, S.: Sur les systèmes cycliques de triples de Steiner différents pour N premier (ou puissance de nombre premier) de la forme $6n+1$. Commentarii math. Helvet. **2**, 294-306 (1930); **3**, 22-41, 122-147, 307-325 (1931)
6. Bays, S.: Sur les systèmes cycliques de triples de Steiner différents pour N premier de la forme $6n+1$. Commentarii math. Helvet. **4**, 183-194 (1932)
7. Bays, S., Belhôte, G.: Sur les systèmes cycliques de triples de Steiner différents pour N premier de la forme $6n+1$. Commentarii math. Helvet. **6**, 28-46 (1933)
8. Bruck, R.H.: What is a loop? In: *Studies in Modern Algebra* (A.A. Albert, Ed.), pp. 59-99. Math. Assoc. Amer. Engelwood Cliffs: Prentice-Hall 1963
9. Doner, J.R.: CIP Neofields and Combinatorial Designs. Ph. D. dissertation, University of Michigan, 1972
10. Doyen, J.: Sur la croissance du nombre de systèmes triples de Steiner non isomorphes. J. combinat. Theory **8**, 424-441 (1970)
11. Hughes, D.R.: Planar division neo-rings. Trans. Amer. math. Soc. **80**, 502-527 (1955)
12. Johnsen, E.C., Storer, T.: Combinatorial structures in loops II. Commutative inverse-property cyclic neofields of prime-power order. Pacific J. Math., to appear
13. Lambossy, P.: Sur une manière de différencier les fonctions cycliques d'une forme donnée. Commentarii math. Helvet. **3**, 69-102 (1931)
14. Paige, L.: Neofields. Duke math. J., **16**, 39-60 (1949)
15. Peltesohn, R.: Eine Lösung der beiden Heffterschen Differenzenprobleme. Compositio math. **6**, 251-257 (1939)

Professor E.C. Johnsen
Department of Mathematics
University of California
Santa Barbara, California 93106
USA

Professor Thomas Storer
Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48104
USA

(Received March 13, 1974)