Construction, properties and applications of finite neofields

A.D. Keedwell

Abstract. We give a short account of the construction and properties of left neofields. Most useful in practice seem to be neofields based on the cyclic group and particularly those having an additional divisibility property, called *D-neofields*. We shall give examples of applications to the construction of orthogonal latin squares, to the design of tournaments balanced for residual effects and to cryptography.

Keywords: neofield, loop, orthomorphism, complete mapping, orthogonal latin squares, cryptography, balanced round robin tournament

Classification: 12K99, 20N05, 05B15, 05B30, 94A60

Introduction

A *left neofield* $(N, \oplus, .)$ of order n consists of a set N of n symbols on which two binary operations $(\oplus)$ and $(.)$ are defined such that $(N, \oplus)$ is a loop, with identity element 0 say, $(N \setminus \{0\}, .)$ is a group and $(.)$ distributes from the left over $(\oplus)$. (That is, $x(y \oplus z) = xy \oplus xz$ for all $x, y, z \in N$.)

If the right distributive law also holds, the structure is called a *neofield*. A left neofield (or neofield) whose multiplication group is $(G, .)$ is said to be *based on* that group. Clearly, every left neofield based on an abelian group is a neofield. Also, a neofield whose addition satisfies the associative law is a field. (In this article, all the structures discussed will be finite.)

The concept of a neofield was first introduced and developed by L. J. Paige [P1] in 1949. Paige hoped to use this structure as the co-ordinate system for a finite projective plane and so to construct new planes, possibly of non-prime-power order. It turns out, however, that a more natural structure to look at is a left neofield because, as was shown by Hsu and Keedwell [H2] in a paper published in 1984, left neofields are co-extensive with orthomorphisms and near orthomorphisms of groups. (The present author discovered later that the Ph.D. thesis of C.P. Johnson, a student of the late Trevor Evans, which was submitted in 1981 contains essentially the same idea.) Before proceeding, we shall need some further definitions:

A one-to-one mapping $g \to \phi(g)$ of a finite group $(G, .)$ onto itself is called an *orthomorphism* if the mapping $g \to \theta(g)$, where $\theta(g) = g^{-1}\phi(g)$, is again a one-to-one mapping of G onto itself. The orthomorphism is said to be in *canonical form* if $\phi(1) = 1$, where 1 is the identity element of G.

An orthomorphism in canonical form may be regarded as a permutation

$$\phi = (1)(g_{11}g_{12}\cdots g_{1k_1})(g_{21}g_{22}\cdots g_{2k_2})\cdots(g_{s1}g_{s2}\cdots g_{sk_s})$$

of G such that the elements $g_{ij}^{-1}g_{i,j+1}$ (where $i = 1, 2, \ldots, s$ and the second suffix j is added modulo k_i) comprise the non-identity elements of G each counted once. Then $\phi(g_{ij}) = g_{i,j+1}$ and $\theta(g_{ij}) = g_{ij}^{-1}g_{i,j+1}$. The mapping θ is the *complete mapping* associated with the orthomorphism ϕ.

If we express an orthomorphism in cycle form as above, we see that $\prod_{g\in G} g = \prod \theta(g_{ij}) = \prod(g_{ij}^{-1}g_{i,j+1}) = 1$. That is, the product of all the elements of G in some appropriate order is equal to the identity element.

The concept of an orthomorphism was first introduced explicitly in [D4] but the equivalent concept of complete mapping dates back to H.B. Mann [M2].

The historical significance of this concept as applied to a finite group G is that it guarantees the existence of, and can be used to construct, an orthogonal mate for the latin square formed by the multiplication table (Cayley table) of G.

As is implied by our earlier remarks and as we show in the next section, this concept (and also that of a near orthomorphism, defined below) plays a crucial role in the study of neofields because, in particular, the mapping defined by $1 \to 1$ and $w \to 1 \oplus w$ (for $w \neq 1$) is an orthomorphism of every left neofield for which $1 \oplus 1 = 0$.

Suppose now that the elements of the finite group $(G, .)$ can be arranged in the form of a sequence $[g'_1g'_2g'_3\cdots g'_h]$ followed by s cyclic sequences $(g_{11}g_{12}\cdots g_{1k_1})$, $(g_{21}g_{22}\cdots g_{2k_2})$, $\ldots$, $(g_{s1}g_{s2}\cdots g_{sk_s})$ such that the elements ${g'_j}^{-1}g'_{j+1}$ and $g_{ij}^{-1}g_{i,j+1}$ together with the elements $g_{ik_i}^{-1}g_{i1}$ comprise the non-identity elements of G each counted once. Then the mapping θ of $G \setminus \{g'_h\}$ onto $G \setminus \{1\}$ given by $\theta(g'_j) = {g'_j}^{-1}g'_{j+1}$ for $j = 1, 2, \ldots, h-1$ and $\theta(g_{ij}) = g_{ij}^{-1}g_{i,j+1}$ (where arithmetic of second suffices is modulo k_i) is called a *near complete mapping* of G. The associated mapping $\phi : g \to g\theta(g)$ of $G \setminus \{g'_h\}$ onto $G \setminus \{g'_1\}$ is called a *near orthomorphism* of G. It is said to be in *canonical form* if $g'_1 = 1$, where 1 is the identity element of G.

We shall represent a near orthomorphism ϕ in the following way:

$$\phi = [g'_1g'_2g'_3\cdots g'_h](g_{11}g_{12}\cdots g_{1k_1})(g_{21}g_{22}\cdots g_{2k_2})\cdots(g_{s1}g_{s2}\cdots g_{sk_s}).$$

When the near orthomorphism is in canonical form so that $g'_1 = 1$, we shall denote the element g'_h which has no image under the mapping by η and call it the *ex-domain element.*

It is immediate to see from the definition of θ that

$$\eta = \Bigg(\prod_{j=1}^{j=h-1}\theta(g'_j)\Bigg)\Bigg(\prod_{i=1}^{i=s}\prod_{j=1}^{j=k_s}\theta(g_{ij})\Bigg).$$

That is, η is the product of all the elements of G in some appropriate order.

Construction and properties

The concepts of orthomorphism and near orthomorphism of a group enable us to characterize left neofields in the following way:

Theorem N. *Let $(N, \oplus, .)$ be a finite left neofield with multiplicative group $(G, .)$, where $G = N \setminus \{0\}$. Then, if $1 \oplus 1 = 0$ in N, N defines an orthomorphism (and corresponding complete mapping) of $(G, .)$, which is in canonical form. If $1 \oplus 1 \neq 0$ but $1 \oplus \eta = 0$, N defines a near orthomorphism of G in canonical form and with η as ex-domain element.*

Conversely, let $(G, .)$ be a finite group with identity element 1 which possesses an orthomorphism ϕ (in canonical form). Let 0 be a symbol not in the set G and define $N = G \cup \{0\}$. Then $(N, \oplus, .)$ is a left neofield, where we define $\psi(w) = 1 \oplus w = \phi(w)$ for all $w \neq 0, 1$ and $\psi(0) = 1$, $\psi(1) = 0$. Also, $x \oplus y = x(1 \oplus x^{-1}y)$ for $x \neq 0$, $0 \oplus y = y$ and $0.x = 0 = x.0$ for all $x \in N$.

Alternatively, let $(G, .)$ possess a near orthomorphism ϕ in canonical form. Then, with N defined as before, $(N, \oplus, .)$ is a left neofield, where we define $\psi(w) = 1 \oplus w = \phi(w)$ for all $w \neq 0, \eta$, where η is the ex-domain element of ϕ and $\psi(0) = 1$, $\psi(\eta) = 0$. Also, $x \oplus y = x(1 \oplus x^{-1}y)$ for $x \neq 0$, as before, $0 \oplus y = y$ and $0.x = 0 = x.0$ for all $x \in N$.

Proof of Theorem N (first part; neofield given):

Case when $1 \oplus 1 = 0$.

In $N \setminus \{0\}$, define $\phi(w) = 1 \oplus w$ for $w \neq 1$ and $\phi(1) = 1$. Since $(N, \oplus)$ is a loop, the equation $\phi(w) = 1 \oplus w = z$ has a unique solution for w and $w \neq 1$ if $z \neq 0$, so ϕ is a one-to-one mapping of $G = N \setminus \{0\}$ onto itself.

Then $\theta(w) = w^{-1}\phi(w) = w^{-1} \oplus 1$ if $w \neq 1$, and $\theta(1) = 1$. Since $(N, \oplus)$ is a loop, the equation $\theta(w) = w^{-1} \oplus 1 = z$ has a unique solution for w and $w \neq 1$ if $z \neq 0$, so θ is a one-to-one mapping of $G = N \setminus \{0\}$ onto itself.

It follows that ϕ is an orthomorphism in canonical form of $G = N \setminus \{0\}$ with θ as corresponding complete mapping.

Case when $1 \oplus 1 \neq 0$, $1 \oplus \eta = 0$.

In $N \setminus \{0\}$, define $\phi(w) = 1 \oplus w$ for $w \neq \eta$. Since $(N, \oplus)$ is a loop, the equation $\phi(w) = 1 \oplus w = z$ has a unique solution for w with $w \neq 0, \eta$ when $z \in G \setminus \{1\}$, where $G = N \setminus \{0\}$. Thus, ϕ is a one-to-one mapping from $G \setminus \{\eta\}$ to $G \setminus \{1\}$.

Then $\theta(w) = w^{-1}\phi(w) = w^{-1} \oplus 1$ if $w \neq 0, \eta$. Since $(N, \oplus)$ is a loop, the equation $\theta(w) = w^{-1} \oplus 1 = z$ has a unique solution for w with $w \neq 0, \eta$ when $z \in G \setminus \{1\}$. So θ is a one-to-one mapping from $G \setminus \{\eta\}$ to $G \setminus \{1\}$. [Note that $\eta^{-1} \oplus 1 = 0$ in $(N, \oplus, .)$.]

It follows that ϕ is a near orthomorphism in canonical form mapping $G \setminus \{\eta\}$ onto $G \setminus \{1\}$ with θ as corresponding near complete mapping. Since the identity element 1 of G has no pre-image, the near orthomorphism is in canonical form.

Proof of Theorem N (second part; mapping of group given):

We require to show that $(N, \oplus)$ is a loop with identity element 0 and that multiplication is left-distributive over addition.

We have $tu \oplus tv = tu(1 \oplus (tu)^{-1}tv) = tu(1 \oplus u^{-1}v) = t(u \oplus v)$ from the definition $x \oplus y = x(1 \oplus x^{-1}y)$, so the left distributive law holds.

Also, in the case when ϕ is an orthomorphism,

$\psi(w) = 1 \oplus w = \phi(w)$ for $w \neq 0, 1$;
$\psi(1) = 1 \oplus 1 = 0$;
$\psi(0) = 1 \oplus 0 = 1$. [Note that $\phi(1) = 1$ since ϕ is in canonical form.]

Therefore, the elements $a \oplus y = a(1 \oplus a^{-1}y) = a\psi(a^{-1}y)$ are distinct as y varies.

When $x \neq 0, a$; $x \oplus a = x(1 \oplus x^{-1}a) = x\phi(x^{-1}a) = x.x^{-1}a\theta(x^{-1}a) = a\theta(x^{-1}a)$. These are all different as x varies and none is equal to 0 or a. Also, $a \oplus a = a(1 \oplus 1) = 0$ and $0 \oplus a = a$. Therefore, the elements $x \oplus a$ are all distinct as x varies.

In the case when ϕ is a near orthomorphism,

$\psi(w) = 1 \oplus w = \phi(w)$ when $w \neq 0, \eta$;
$\psi(\eta) = 1 \oplus \eta = 0$;
$\psi(0) = 1 \oplus 0 = 1$. [Note that $\phi(\eta)$ is not defined since η is exdomain element and that $\phi(w) \neq 1$ for $w \in G$ since ϕ is in canonical form.]

Therefore, the elements $a \oplus y = a(1 \oplus a^{-1}y) = a\psi(a^{-1}y)$ are distinct as y varies.

When $x^{-1}a \neq 0, \eta$; $x \oplus a = x(1 \oplus x^{-1}a) = x\phi(x^{-1}a) = x.x^{-1}a\theta(x^{-1}a) = a\theta(x^{-1}a)$. These are all different as x varies and none is equal to 0 or a. Furthermore, $x^{-1}a = \eta \Rightarrow x = a\eta^{-1}$ and $a\eta^{-1} \oplus a = a\eta^{-1}(1 \oplus \eta) = 0$. Also, $0 \oplus a = a$. Therefore, the elements $x \oplus a$ are all distinct as x varies.

We conclude that $(N, \oplus)$ is a loop with 0 as two-sided identity. □

Note. The mapping $\psi : z \to 1+z$ is called the *presentation function* of the neofield because it determines the complete addition table of the neofield by virtue of the fact that $x + y = x(1 + x^{-1}y)$.

Remarks.

(1) It is interesting to note here that, by a theorem of R.H. Bruck [B1], a loop which has a transitive automorphism group is either simple (that is, without normal subloops) or else is an elementary abelian group.

Since the mapping $g \to ag$, where a is any non-zero fixed element, defines an automorphism of the additive loop of a left neofield, it follows that this loop always has a transitive automorphism group. The case when the loop is an elementary abelian group occurs when and only when the neofield is a finite field. The multiplication group is then cyclic.

(2) In a recently submitted paper [K5], the present author has investigated the properties that an orthomorphism or near orthomorphism of a cyclic group must have to enable it to define a finite field rather than just a cyclic neofield. (For abelian groups, the existence of orthomorphisms or near orthomorphisms are mutually exclusive according as the group has not or has a unique element of

order two. This follows from the fact that the product of all the elements of a finite abelian group is equal to the identity except when the group has a unique element of order two.)

(3) In the case of a left neofield which is defined by a near orthomorphism of a group, we have $1 \oplus \eta = 0$, $\eta \neq 1$ and so the exdomain element η plays the role of the element -1 in a finite field. Since $(-1)^2 = 1$ in a field, we might expect that η would have multiplicative order two. However, it was shown in [K3] that infinitely many so-called *pathological left neofields* exist in which η has prime order distinct from two. Such left neofields were called pathological because they do not have the left or right inverse properties, are not commutative for addition or multiplication and cannot be (two-sided) neofields.

(4) A left neofield becomes a neofield if the right distributive law holds. It was shown in [H2] that necessary and sufficient conditions for this are that the complete mapping (in the case when $1 \oplus 1 = 0$) or the near complete mapping (in the case when $1 \oplus \eta = 0$, $\eta \neq 1$) of the group G which defines the neofield maps conjugacy classes to conjugacy classes and additionally in the latter case that η is in the centre of G.

Most useful in practice are cyclic neofields: that is, neofields whose multiplication group is cyclic. Such neofields have been investigated in considerable detail by D.F. Hsu in his book [H1].

Observation. Suppose that $1 \oplus \eta = 0$ in a cyclic neofield of odd order $m = n+1$ based on the group $G = \langle \alpha : \alpha^n = 1 \rangle$. Then, because η is the product of all the elements of G, it is equal to the unique element of order two in G. That is, $\eta = \alpha^{n/2}$. We shall use this fact in the following sections.

An application of cyclic neofields to cryptography

One future application of cyclic neofields is likely to be to cryptography because, unlike finite fields, cyclic neofields exist of all finite orders. The following example (taken from [D2]) indicates one cryptographic situation in which use of a cyclic neofield has advantages over use of a group.

Example 1. Let $(N, \oplus, .)$ be a finite Galois field or a cyclic neofield. Then each non-zero element u of the additive group or loop $(N, \oplus)$ can be represented in the form $u = \alpha^v$, where α is a generator of the multiplicative group $(N \setminus \{0\}, .)$. v is called the *discrete logarithm* of u to the base α or, sometimes, the *exponent* or *index* of u (see page 85 of [M1]). Given v and α, it is easy to compute u in a finite field but, if the order of the field is a sufficiently large prime p and also is appropriately chosen, it is believed to be difficult to compute v when u (as a residue modulo p) and α are given (see [O1]). Since the multiplicative structure of a cyclic neofield is the same as that of a finite field, the same remark applies to a cyclic neofield of the same prime order.

Let $A, B, C, \ldots,$ be persons who wish to send each other encrypted messages, let p be a large prime number and let α be a primitive root of p. T. ElGamal in [E1] has proposed the following public key encryption scheme.

Each of $A, B, C, \ldots,$ has a secret key $x(i)$, $i = a, b, c, \ldots,$ and a public key, $y(i) = \alpha^{x(i)}$, $i = a, b, c, \ldots$. Suppose that A wishes to send B a block M_j of a message M, where $0 \leq M_j \leq p-1$. He chooses randomly a message key k, $0 < k < p-1$, and computes $y(b)^k = (\alpha^{x(b)})^k \bmod p$. He then sends (C'_j, C_j), where $C'_j = \alpha^k \bmod p$ and $C_j = y(b)^k M_j$ or $y(b)^k + M_j$ according as multiplication or addition is used in the enciphering process.

On receipt of the enciphered message, B first computes $(C'_j)^{x(b)} = \alpha^{k.x(b)} = y(b)^k$ and hence he obtains $M_j = C_j / y(b)^k$ or $M_j = C_j - y(b)^k$.

ElGamal points out that it is not advisable to use the same key k for enciphering more than one block of the message since, if k is used more than once, knowledge of one block M_1 of the message would enable an intruder to compute other blocks because then $M_2/M_1 = C_2/C_1$ or $M_2 - M_1 = C_2 - C_1$ according as multiplication or addition is used. However, this problem does not arise if a cyclic neofield is used and $C_j = y(b)^k \oplus M_j$ since $(\oplus)$ does not satisfy the associative law and so $C_2 - C_1 = (y(b)^k \oplus M_2) - (y(b)^k \oplus M_1) \neq M_2 - M_1$.

Suppose, for example, that a cyclic neofield of odd prime order p whose addition is a crossed-inverse loop is used. [Crossed inverse loops were first introduced by R. Artzy in [A2]. A neofield $(N, \oplus, .)$ is said to have the *right crossed inverse property* if, for each $g \in N$, there exists an element $g'_R \in N$ such that $(g \oplus h) \oplus g'_R = h$ for all $h \in N$. A neofield which has the right crossed inverse property also has the left crossed inverse property. If the neofield is cyclic of odd order, $1 \oplus \eta = 0$ and then, putting $h = 0$, we see that $g'_R = g\eta$.] Since the order of the neofield is an odd prime p, each element g of the neofield has $g\eta = g\alpha^{(p-1)/2}$ as its crossed inverse. The modified ElGamal scheme is then as follows:

A chooses a key k, $0 < k < p-1$, and sends (C'_j, C_j), where $C'_j = \alpha^k \bmod p$ and $C_j = y(b)^k \oplus M_j$. On receipt of this encrypted block of the message, B computes $(C'_j)^{x(b)} = \alpha^{k.x(b)} = y(b)^k$ and thence $C_j \oplus (C'_j)^{x(b)}\eta = (y(b)^k \oplus M_j) \oplus y(b)^k \alpha^{(p-1)/2} = M_j$.

The same key k can now be used for each block of the message without providing any help to an intruder who acquires a knowledge of M_1 because

$$C_2 \oplus C_1\eta = (y(b)^k \oplus M_2) \oplus (y(b)^k \oplus M_1)\eta \neq M_2 \oplus M_1\eta.$$

Applications of cyclic neofields which have a special divisibility property

A cyclic neofield (of order $m = n+1$) based on the group $\langle x : x^n = 1 \rangle$ is said to have *property D* if $(1 \oplus x^{r+1})/(1 \oplus x^r) = (1 \oplus x^{s+1})/(1 \oplus x^s) \Leftrightarrow r \equiv s \bmod n$, where r, s are any positive integers. For brevity, we shall call such a neofield, a *D-neofield.* It is almost certain, but still unproved, that such neofields exist of every finite order except 2 and 6.

Historically, such neofields were introduced by the present author in order to provide an explanation for the non-existence of orthogonal latin squares of order six because the latin square formed by the addition table of a D-neofield always has an orthogonal mate. (We prove this later when discussing round robin tournaments.) It is easy to see that D-neofields do not exist of orders 2 and 6 but they can be constructed of all other small orders up to at least order 20. To show this, we use the following theorem which generalizes to all cyclic neofields the theorem first given in [K1].

Note. In Figure 1 below, we have written $(+)$ in place of $(\oplus)$. We shall continue to use this less formal notation throughout the subsequent part of the paper.

Theorem 1. *A necessary and sufficient set of conditions for a cyclic neofield of order $m = n + 1$ to exist is that $n - 2$ (not necessarily distinct) residues modulo n from the set $\{2, 3, \ldots n - 1\}$ can be arranged in a sequence P such that:*

(i) *the partial sums of the first one, two, … , $n - 2$ elements are all distinct and non-zero modulo n; and*

(ii) *when each element of the sequence is reduced by one, the new sequence, P' say, also satisfies* (i).

Furthermore, the cyclic neofield has property D if and only if the elements of P are all distinct.

Proof: Suppose first that a cyclic neofield of order $m = n + 1$ exists based on the cyclic group $C_n = \langle x : x^n = 1\rangle$. Its addition table can be written in the form shown in Figure 1, where $1 \oplus x^h = 0$ (so that $h = 0$ or $n/2$ according as n is odd or even). Figure 2 represents the same addition table except that powers of x have been replaced by their indices (with $x^0 = 1$) and the element 0 has been replaced by n. Comparison of the two tables shows that $a_{i+1,j+1} = a_{ij} + 1$, where arithmetic of indices is modulo n.

Let $p_1 = a_{02} - a_{01}$. Then $p_1' = p_1 - 1 = a_{02} - (a_{01} + 1) = a_{02} - a_{12} = a_{n-3,n-1} - a_{n-2,n-1}$.

$p_2 = a_{03} - a_{02}$. $p_2' = p_2 - 1 = a_{03} - (a_{02} + 1) = a_{03} - a_{13} = a_{n-4,n-1} - a_{n-3,n-1}$.

$p_3 = a_{04} - a_{03}$. $p_3' = p_3 - 1 = a_{04} - (a_{03} + 1) = a_{04} - a_{14} = a_{n-5,n-1} - a_{n-4,n-1}$.

… … … … … …

$p_{n-2} = a_{0,n-1} - a_{0,n-2}$. $p_{n-2}' = p_{n-2} - 1 = a_{0,n-1} - (a_{0,n-2} + 1) = a_{0,n-1} - a_{1,n-1}$.

Since no two entries of the second row of the addition table are equal, no one of the p_i's is equal to zero. Since no two entries of the last column of the addition table are equal, no one of the p_i''s is equal to zero. Thus, for each i, $p_i \neq 0$ or 1; so each $p_i \in \{2, 3, \dots, n-1\}$. Also, the partial sums $p_1 = a_{02} - a_{01}$, $p_1 + p_2 = a_{03} - a_{01}, \dots\dots, p_1 + p_2 + \dots p_{n-2} = a_{0,n-1} - a_{01}$ are all distinct and non-zero modulo n. Furthermore, the partial sums $p_1' = a_{n-3,n-1} - a_{n-2,n-1}$, $p_1' + p_2' = a_{n-4,n-1} - a_{n-2,n-1}, \dots \dots, p_1' + p_2' + \dots p_{n-2}' = a_{0,n-1} - a_{n-2,n-1}$ are all distinct and non-zero modulo n.

Since $1 + x^{h+r} = x^s$, where $s = a_{0r}$, and $1 + x^{h+r-1} = x^t$, where $t = a_{0,r-1}$, we have $(1 + x^{h+r})/(1 + x^{h+r-1}) = x^{s-t}$, where $s - t = p_{r-1}$. It follows that the elements of the set $P = \{p_1, p_2, \dots p_{n-2}\}$ are all distinct if and only if the neofield has property D.

	0	x^h	x^{h+1}	x^{h+2}	x^{h+3}	...	x^{h-1}
0	0	x^h	x^{h+1}	x^{h+2}	x^{h+3}	...	x^{h-1}
1	1	0	$1+x^{h+1}$	$1+x^{h+2}$	$1+x^{h+3}$	...	$1+x^{h-1}$
x	x	$x+x^h$	0	$x+x^{h+2}$	$x+x^{h+3}$	...	$x+x^{h-1}$
x^2	x^2	x^2+x^h	x^2+x^{h+1}	0	x^2+x^{h+3}	...	x^2+x^{h-1}
•	•	•	•	•	•	...	•
•	•	•	•	•	•	...	•
x^{n-2}	x^{n-2}	$x^{n-2}+x^h$	$x^{n-2}+x^{h+1}$	$x^{n-2}+x^{h+2}$	$x^{n-2}+x^{h+3}$	...	$x^{n-2}+x^{h-1}$
x^{n-1}	x^{n-1}	$x^{n-1}+x^h$	$x^{n-1}+x^{h+1}$	$x^{n-1}+x^{h+2}$	$x^{n-1}+x^{h+3}$	...	0

Figure 1

	n	h	$h+1$	$h+2$	$h+3$	$\dots$	$h-1$
n	n	h	$h+1$	$h+2$	$h+3$	$\dots$	$h-1$
0	0	n	a_{01}	a_{02}	a_{03}	$\dots$	$a_{0,n-1}$
1	1	a_{10}	n	a_{12}	a_{13}	$\dots$	$a_{1,n-1}$
2	2	a_{20}	a_{21}	n	a_{23}	$\dots$	$a_{2,n-1}$
•	•	•	•	•	•	$\dots$	•
•	•	•	•	•	•	$\dots$	•
$n-2$	$n-2$	$a_{n-2,0}$	$a_{n-2,1}$	$a_{n-2,2}$	$a_{n-2,3}$	$\dots$	$a_{n-2,n-1}$
$n-1$	$n-1$	$a_{n-1,0}$	$a_{n-1,1}$	$a_{n-1,2}$	$a_{n-1,3}$	$\dots$	n

Figure 2

Conversely, given a sequence $p_1, p_2, \dots, p_{n-2}$ of residues modulo n with the properties stated in the theorem, we can construct a cyclic neofield in the following way:

In Figure 2, the entries of the second row are 0, n, a_{01}, $a_{01} + p_1$, $a_{01} + (p_1 + p_2), \dots, a_{01} + (p_1 + p_2 + \cdots + p_{n-2})$. Clearly, none of the $n-1$ indices $a_{01}, a_{01} +$

$p_1, a_{01} + (p_1 + p_2), \ldots, a_{01} + (p_1 + p_2 + \cdots + p_{n-2})$ must be equal to 0 modulo n and this determines a_{01}. We may then fill in the second row of the table shown in Figure 2 and also all its remaining rows using the fact that $a_{i+1,j+1} = a_{ij} + 1$. From the properties of the sequences P and P', it follows that the table so obtained is an $(n+1) \times (n+1)$ latin square and so the corresponding Figure 1 represents the addition table of a cyclic neofield.

It is helpful to illustrate the second part of the above proof by means of examples.

Let $n = 7$ and let P be the sequence $4, 6, 5, 5, 3$. Then P' is the sequence $3, 5, 4, 4, 2$. Each of these sequences has distinct partial sums and we have $0, n, a_{01}$, $a_{01} + 4, a_{01} + 3, a_{01} + 1, a_{01} + 6, a_{01} + 2$ as elements of the second row in Figure 2. Since $a_{01} + 5$ does not occur, we have $a_{01} + 5 \equiv 0$ (or 7) $\bmod 7$. Therefore, $a_{01} = 2$ and the second row of the table is $0, n, 2, 6, 5, 3, 1, 4$. We may complete the Figure 2 so obtained to the table shown in Figure 3. Since n is odd, $h = 0$ and so the corresponding neofield has presentation function

$$\psi = \begin{pmatrix} 0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\ 1 & 0 & x^2 & x^6 & x^5 & x^3 & x & x^4 \end{pmatrix}.$$

	7	0	1	2	3	4	5	6
7	7	0	1	2	3	4	5	6
0	0	7	2	6	5	3	1	4
1	1	5	7	3	0	6	4	2
2	2	3	6	7	4	1	0	5
3	3	6	4	0	7	5	2	1
4	4	2	0	5	1	7	6	3
5	5	4	3	1	6	2	7	0
6	6	1	5	4	2	0	3	7

Figure 3

	6	3	4	5	0	1	2
6	6	3	4	5	0	1	2
0	0	6	5	3	2	4	1
1	1	2	6	0	4	3	5
2	2	0	3	6	1	5	4
3	3	5	1	4	6	2	0
4	4	1	0	2	5	6	3
5	5	4	2	1	3	0	6

Figure 4

Secondly, let $n = 6$ and let P be the sequence $4, 5, 2, 3$. Then P' is the sequence $3, 4, 1, 2$. Each of these sequences has distinct partial sums and we have

$0, n, a_{01}, a_{01}+4, a_{01}+3, a_{01}+5, a_{01}+2$ as elements of the second row in Figure 2. Since $a_{01}+1$ does not occur, we have $a_{01}+1 \equiv 0$ (or 6) mod 6. Therefore, $a_{01} = 5$ and the second row of the table is $0, n, 5, 3, 2, 4, 1$. We may complete the Figure 2 so obtained to the table shown in Figure 4. Since n is even, $h = n/2 = 3$ and so the corresponding neofield has presentation function

$$\psi = \begin{pmatrix} 0 & x^3 & x^4 & x^5 & 1 & x & x^2 \\ 1 & 0 & x^5 & x^3 & x^2 & x^4 & x \end{pmatrix}.$$

Since the elements of the sequence P are distinct, the neofield has property D. It is in fact the finite field of order 7 and the generating element is 3 (which is a primitive root of 7).

Note. The smallest order for which there exists a D-neofield which is not a field is 9. (See [K2] for a table of finite D-neofields which are not fields.)

The special case of the above theorem which applies to D-neofields is due to the present author. It appears both in [K1] and also as Theorems 7.5.2 and 7.5.3 of [D1]. D. Bedford observed (in his Ph.D. thesis of 1991) that the theorem can be generalised to apply to all cyclic neofields as above.

As regards the explanation for the non-existence of D-neofields of order 6 and consequent non-existence of pairs of orthogonal latin squares of that order based on the addition table of a D-neofield, we quote from [K1]: "Since [*use of D-neofields*] provides a standard method for constructing pairs of mutually orthogonal latin squares of all orders up to 20 at least, we shall expect it to throw some light on the reason for the non-existence of pairs of orthogonal latin squares of order 6. We observe [*using the theorem above*] that the method fails when $m = 6$ because the integers $2, 3, 4$ and 2–1, 3–1, 4–1 cannot be simultaneously re-ordered so that their partial sums taken modulo 5 are all distinct and non-zero. Essentially, this is due to the fact that the integers $2, 3$ occur in each triad and must occur consecutively in one or the other. Thus, the non-existence of orthogonal latin squares of order 6 appears to be a consequence of nothing more profound than the paucity of combinatorial arrangements of the integers 0 to 4."

A more recent, and quite surprising, application of D-neofields is to the construction of round robin games tournaments balanced for residual effects. K.G. Russell [R1] was the first to investigate the existence of such tournaments.

Suppose that player x (or team x) meets player y (team y) in one round of the tournament and immediately afterwards meets player z in the next round. Then it is likely that x's performance against z will have been affected by y. For example, if y is very strong relative to x, x's morale will have been shaken and so he will perform less well than is to be expected against z. Because of this, it is desirable that z should profit by the carry-over effect of y no more than once in the whole tournament. If we represent the tournament by a latin square, we see that it will be "best possible" if we can arrange that each player has carry-over from each other at most once. Let us define a matrix as follows: place k in cell

(i, j) if j plays k in the ith round of the tournament. When there are an even number of players, everyone plays in every round so, if we denote the rounds by $1, 2, \ldots, 2n-1$, and the players by $0, 1, 2, \ldots, 2n-1$, every player occurs in the ith row and every player except j occurs in the jth column (since a player cannot play against himself). In this representation of the tournament, player z suffers a carry-over effect from player y when and only when y, z are consecutive entries of the same column. Since player y occurs in every row, he creates $2n-2$ carry-overs (there is no carry-over from the last row) so it ought to be possible to arrange that these carry-overs are all different. However, there is a snag. If j plays k in the ith round of the tournament, then k plays j in the ith round. In other words, our matrix must have the property that if cell (i, j) contains k then also cell (i, k) contains j. Despite this, a matrix which meets all the requirements is known to exist when $m = 2n$ is a power of two and for at least some other even values. (When there are an odd number of players, we can delete one player, say player 0, and take that player's opponent in round i (as given by the matrix) to be the player who has a bye in that round.)

	0	1	2	3	4	5	6	7
0	<u>0</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>
1	1	0	4	7	2	6	5	3
2	2	4	0	5	1	3	7	6
3	3	7	5	0	6	2	4	1
4	4	2	1	6	0	7	3	5
5	5	6	3	2	7	0	1	4
6	6	5	7	4	3	1	0	2
7	7	3	6	1	5	4	2	0

Figure 5

A solution for eight players (or seven players with byes) is shown in Figure 5. It is immediately obvious that, if an additional first row is adjoined to our matrix with players in the same order as the row border, then the matrix becomes a latin square. By suitably labelling the players, we can also arrange that the first column of the square is in the same order as the column border (as in Figure 5) and then the latin square represents the addition table of a loop such that $i + j = k \Leftrightarrow i + k = j$: that is, a loop with the left keys property: namely, one for which $i + (i + k) = k$. (See, for example, [D1, page 58] for more details.) Since each symbol is to follow each other at most once in the columns when the first row is omitted, it is necessary and sufficient to have a latin square which satisfies the left keys law and becomes a column complete $(m-1) \times m$ latin rectangle when its first row is deleted.

One way of achieving this is by means of a suitable and suitably arranged group of order $m = 2n$ (with elements which we may denote by $0, 1, \ldots, 2n-1$, where 0 is the identity element) which satisfies the left keys law and whose Cayley table is the latin square. This is the method used by Russell but, unfortunately, a group can only satisfy the left keys law if all its elements have order two: that is, if it is elementary abelian. Consequently, this method of attack can only give solutions when m is a power of two. (For more details of this method of obtaining solutions, see Russell's original paper or the survey paper [K4] of the present author.)

An alternative idea is to use a loop instead of a group. More precisely, an idea proposed by A. Tripke [T1] is to use the addition table of a cyclic neofield. Tripke pointed out that a sufficient condition that a balanced tournament for $m = 2n$ players should exist is that there exists a latin square L which satisfies the left keys law and is *cyclically orthogonal with respect to rows*; by which is meant that the latin square obtained from L by effecting the permutation $P = (0)(2n-1\ 2n-2 \ldots 2\ 1)$ of its rows is orthogonal to L. The latter concept is due to Tripke himself who has pointed out in his Diploma Thesis (of the Ruhr Universität in Bochum) that such a latin square can be constructed from a D-neofield of order m and characteristic two. A cyclic neofield has *characteristic* 2 if its presentation function $\psi(z) = 1 + z$ consists entirely of cycles of length 2, so that $1 + (1 + z) = z$. Since multiplication distributes over addition, this implies that the left keys law holds. We have $x^h + (x^h + x^{h+k}) = x^{h+k}$, where $z = x^k$, and so $x^h + (x^h + x^l) = x^l$ for every pair of non-zero elements x^h and x^l. The addition table of such a neofield takes the form shown in Figure 6.

	0	1	x	x^2	...	x^{m-3}	x^{m-2}
0	0	1	x	x^2	...	x^{m-3}	x^{m-2}
1	1	$1+1$	$1+x$	$1+x^2$	...	$1+x^{m-3}$	$1+x^{m-2}$
x	x	$x+1$	$x+x$	$x+x2$	...	$x+x^{m-3}$	$x+x^{m-2}$
x^2	x^2	x^2+1	x^2+x	x^2+x^2	...	x^2+x^{m-3}	x^2+x^{m-2}
•	•	•	•	•	•	...	•
•	•	•	•	•	•	...	•
x^{m-3}	x^{m-3}	$x^{m-3}+1$	$x^{m-3}+x$	$x^{m-3}+x^2$	...	$x^{m-3}+x^{m-3}$	$x^{m-3}+x^{m-2}$
x^{m-2}	x^{m-2}	$x^{m-2}+1$	$x^{m-2}+x$	$x^{m-2}+x^2$	...	$x^{m-2}+x^{m-3}$	$x^{m-2}+x^{m-2}$

Figure 6

We shall show that the latin square of Figure 6 is cyclically orthogonal with respect to both rows and columns. (It will then follow that Figure 6 provides a tournament scheduling of the kind we are seeking.) To see this, note first that, if the 0th row and 0th column of the latin square are disregarded, the remainder of the main left-to-right diagonal consists entirely of zeros (since the neofield has characteristic two) and each of the other broken left-to-right diagonals consists of powers of x in ascending natural order. Because the neofield has property D, the differences between the indices of x of adjacent elements of the row prefixed by 1 are all different and non-zero modulo $m-1$. Also, none of them is equal to 1 because $(1 + x^{r+1})/(1 + x^r) = x$ would imply that $1 = x$. Since succeeding rows of the matrix (excluding the 0th column) are obtained by adding 1 to the indices of x of the entries, excluding 0, of the previous row and shifting the elements thus obtained one step to the right, every ordered pair (x^u, x^{u+t}), $0 \le u \le m-2$, $2 \le t \le m-2$, where the indices are added modulo $m-1$, occurs once among the rows $1, 2, \ldots, m-1$ when the columns are read cyclically. Also, because all the entries of the main left-to-right diagonal are equal to 0, whereas those of the adjoining broken diagonals are all different, every ordered pair $(0, x^u)$ and every ordered pair $(x^u, 0)$, $0 \le u \le m-2$, occurs. Finally, because the indices of the entries in the row prefixed by 0 all differ by 1, every ordered pair (x^u, x^{u+1}), $0 \le u \le m-2$, occurs. It follows that the latin square is cyclically orthogonal with respect to columns. We easily show that it is also cyclically orthogonal with respect to rows. From the property $(1+x^{r+1})/(1+x^r) = (1+x^{s+1})/(1+x^s) \Leftrightarrow r \equiv s \bmod m-1$, we get

$$(1+x^{m-r-2})/(1+x^{m-r-1}) = (1+x^{m-s-2})/(1+x^{m-s-1}) \Leftrightarrow m-r-1 \equiv m-s-1,$$

and hence $(x^{r+1}+1)/(x^{r+1}+x) = (x^{s+1}+1)/(x^{s+1}+x) \Leftrightarrow r \equiv s$, since $x^{m-1} = 1$. The latter implication is equivalent to $(x^{r+1}+1)/(x^r+1) = (x^{s+1}+1)/(x^s+1) \Leftrightarrow r \equiv s$, and we can immediately deduce that the transpose of the given latin square is cyclically orthogonal with respect to columns or, equivalently, that the given square is cyclically orthogonal with respect to rows. To transform Figure 6 to the form shown in the example of Figure 5, we replace x^u by the integer $u+1$ for $0 \le u \le m-2$. (For example, to obtain Figure 5 itself, we take $m = 8$ and the neofield to be the Galois field $GF[2^3]$ with x as a primitive root which satisfies the equation $x^3 = x + 1$.)

We state this result as a theorem:

Theorem 2. *A sufficient condition for the existence of a round robin tournament for $m = 2n$ players which is balanced for carry-over effects is that there exists a property D cyclic neofield of order m and characteristic two.*

Because $1 + 1 = 0$ in a cyclic neofield of even order, to say that such a neofield has the left inverse property is equivalent to saying that it has characteristic two, as we observed above. Such a neofield need not have the right inverse property as was first shown by Hsu who, in [H1], gave explicit constructions for cyclic neofields of every finite order which have the left inverse property but not the right inverse property. Hsu called them *LXP-neofields*. However, the LXP-neofields constructed by Hsu do not have property D.

On the other hand, if a cyclic neofield of characteristic two has both the left and right inverse properties, then and only then it is commutative for addition (Lemma I.14 of [H1] or Theorem 2.1 (1) of [K5]). Such neofields exist of all even orders which are not multiples of 6 except order 10. (This was first proved by J.R. Doner [D3] in his Ph.D. thesis of 1972.) An easy proof of non-existence if $m \equiv 0 \bmod 6$ is as follows:

Since the neofield is cyclic of even order, $1 + 1 = 0$ and so each element is its own additive inverse as already remarked. If x, y are non-zero elements of the addition loop and $x + y = z$, then, by adding x on the left of this equality, we get $y = x + z$ and, by adding y on the right, we get $x = z + y$. Also, addition is commutative and so $y+x = z$, $z+x = y$, $y+z = x$. Thus, the additive loop of the neofield is totally symmetric and so its non-zero elements define a Steiner triple system whose triples x, y, z are such that the sum in the additive loop of any two is the third. A Steiner triple system of order $m - 1$ exists only if $m - 1 \equiv 1$ or $3 \bmod 6$ so only $m \equiv 2$ or $4 \bmod 6$ are possible.

Tripke reported in his Diploma Thesis that he had carried out a search for commutative D-neofields of characteristic two for all orders m that are not multiples of 6 up to order 54 inclusive. He found two commutative D-neofields of order 20 and two of order 22 but no further examples. In fact, each of these pairs of examples of the same order are complementary. The presentation function ψ of one is obtained from that of the other by replacing each transposition $(a\ b)$ by the transposition $(m-1-a\ \ m-1-b)$. More recently, I. Anderson [A1], unaware of Tripke's work, has looked at this same problem of finding tournaments balanced for carry-over effects from a different point of view. With the aid of a computer programme written by N. Finizio, he has found (in effect) the same commutative D-neofields of characteristic two of orders 20 and 22 but no others, though the search was not exhaustive for $m > 22$. In the meantime, I had asked a young student (Ganesh Sittampalam) of mine to write his own computer programme for this same purpose. He obtained the same results!

The question remains open as to whether non-commutative D-neofields of characteristic two exist and also for what orders greater than 22 (if any) commutative ones exist.

Acknowledgement. The author wishes to thank the referee for a number of helpful suggestions.

References

[A1] Anderson I., *Balancing carry-over effects in tournaments*, in Combinatorial Designs and their Applications, Eds. F.C. Holroyd, K.A.S. Quinn, C.Rowley, B.S. Webb, Chapman and Hall/CRC Research Notes in Mathematics, CRC Press, 1999, pp. 1–16.

[A2] Artzy R., *On loops with a special property*, Proc. Amer. Math. Soc. **6** (1955), 448–453.

[B1] Bruck R.H., *Loops with transitive automorphism groups*, Pacific J. Math. **1** (1951), 481–483.

[D1] Dénes J., Keedwell A.D., *Latin Squares and their Applications*, Akadémiai Kiadó, Budapest; English Universities Press, London; Academic Press, New York, 1974.

[D2] Dénes J., Keedwell A.D., *Some applications of non-associative algebraic systems in cryptology*, submitted.

[D3] Doner J.R., *CIP-neofields and Combinatorial Designs*, Ph.D. Thesis, University of Michigan, U.S.A., 1972.

[D4] Dulmage A.L., Mendelsohn N.S., Johnson D.M., *Orthomorphisms of groups and orthogonal latin squares I*, Canad. J. Math. **13** (1961), 356–372.

[E1] ElGamal T., *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Information Theory IT–31, 1985, pp. 469–472.

[H1] Hsu D.F., *Cyclic neofields and combinatorial designs*, Lecture Notes in Mathematics No. 824, Springer, Berlin, 1980.

[H2] Hsu D.F., Keedwell A.D., *Generalized complete mappings, neofields, sequenceable groups and block designs I, II.*, Pacific J. Math. **111** (1984), 317–332 and **117** (1985), 291–311.
[K1] Keedwell A.D., *On orthogonal latin squares and a class of neofields*, Rend. Mat. e Appl. (5) **25** (1966), 519–561.
[K2] Keedwell A.D., *On property D neofields*, Rend. Mat. e Appl. (5) **26** (1967), 383–402.
[K3] Keedwell A.D., *The existence of pathological left neofields*, Ars Combinatoria **B16** (1983), 161–170.
[K4] Keedwell A.D., *Designing Tournaments with the aid of Latin Squares: a presentation of old and new results*, Utilitas Math., to appear.
[K5] Keedwell A.D., *A characterization of the Jacobi logarithms of a finite field*, submitted.
[M1] MacWilliams F.J., Sloane N.J.A., *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.
[M2] Mann H.B., *The construction of orthogonal latin squares*, Ann. Math. Statist. **13** (1942), 418–423.
[O1] Odlyzko A.M., *Discrete logarithms in finite fields and their cryptographic significance*, in Lecture Notes in Computer Science No. 209; Advances in Cryptology, Proc. Eurocrypt 84, Eds. T. Beth, N. Cot, I. Ingemarsson, Springer, Berlin, 1955, pp. 224–314.
[P1] Paige L.J., *Neofields*, Duke Math. J. **16** (1949), 39-60.
[R1] Russell K.G., *Balancing carry-over effects in round robin tournaments*, Biometrika **67** (1980), 127–131.
[T1] Tripke A., *Algebraische and Kombinatorische Structuren von Spielplänen mit Anwendung auf ausgewogen Spielpläne*, Diploma Thesis, Ruhr-Universität in Bochum, 1983.

Department of Mathematics and Statistics, University of Surrey,
Guildford GU2 7XH, Surrey, United Kingdom

(*Received* August 26, 1999, *revised* December 6, 1999)