PACIFIC JOURNAL OF MATHEMATICS
Vol 111, No. 2, 1984

GENERALIZED COMPLETE MAPPINGS, NEOFIELDS, SEQUENCEABLE GROUPS AND BLOCK DESIGNS. I

D. F. HSU AND A. D. KEEDWELL

The necessary and sufficient condition that the latin square formed by the Cayley multiplication table of a group has an orthogonal mate is that the group has a complete mapping. Here, we define two generalizations of the concept of a complete mapping and show how these generalizations are related to sequenceable groups and R-sequenceable groups respectively and that together they permit a complete characterization of left neofields. In the second part of the paper, we shall show that these generalizations also yield new constructions of block designs of Mendelsohn type.

Introduction. In [**11**] H. B. Mann introduced the concept of a *complete mapping* of a finite group $(G, \cdot)$ and showed that, when a group has such a complete mapping, the latin square formed by its Cayley multiplication table has a transversal and, hence, an orthogonal mate. See also §1.4 of [**1**]. Later, L. J. Paige [**13**] showed that complete mappings can also be used in the construction of neofields. This fact has been used extensively in [**6**].

More recently, it has been shown in [**10**] and [**2**] that a necessary condition for a finite group to be R-sequenceable is that it possess a complete mapping. Similarly, we prove below that a necessary condition for a finite group to be *sequenceable* is that it possess a *near complete mapping*. In general, both sequenceable and R-sequenceable groups permit the construction of neofields and the neofields so constructed are of special type.

In this first part of our paper, we define two generalizations of the concept of a complete mapping to be called a (K, λ) *complete mapping* and a (K, λ) *near complete mapping*, respectively, and we show that all of the above-mentioned concepts can be described in terms of these generalizations. We are also able to give a complete characterization for all left neofields. In the second part (to appear shortly), we show that these generalizations also yield new constructions of block designs of Mendelsohn type whose automorphism group contains a specified subgroup and we describe in more detail how (K, λ) generalized complete mappings and near complete mappings may be constructed.

We start with some definitions.

2. Basic concepts and definitions.

DEFINITION 2.1. A one-to-one mapping $g \to \theta(g)$ of a finite group $(G, \cdot)$ onto itself is said to be a *complete mapping* if the mapping $g \to \phi(g)$, where $\phi(g) = g \cdot \theta(g)$, is again a one-to-one mapping of G onto itself.

DEFINITION 2.2. A finite group $(G, \cdot)$ of order n is said to be *sequenceable* if its elements can be arranged in a sequence $a_0 = e, a_1, a_2, \ldots, a_{n-1}$ in such a way that the partial products $b_0 = a_0$, $b_1 = a_0 a_1$, $b_2 = a_0 a_1 a_2, \ldots, b_{n-1} = a_0 a_1 a_2 \cdots a_{n-1}$ are all distinct (and consequently are the elements of C in a new order). It is said to be *R-sequenceable* (see **[2]**) or *near-sequenceable* (see **[9]**) if its elements can be ordered in such a way that the partial products $b_0 = a_0$, $b_1 = a_0 a_1$, $b_2 = a_0 a_1 a_2, \ldots, b_{n-2} = a_0 a_1 a_2 \cdots a_{n-2}$ are all different and so that the product $b_{n-1} = a_0 a_1 a_2 \cdots a_{n-1} = b_0 = e$, where e is the identity element of G.

DEFINITION 2.3. A *finite neofield* N_v comprises a set N of v elements on which two binary operations, $(+)$ and $(\cdot)$ are defined such that $(N, +)$ is a loop, with identity element 0, say; $(N - \{0\}, \cdot)$ is a group; and $(\cdot)$ is both left and right distributive over $(+)$. A neofield whose multiplicative group is cyclic is called a *cyclic neofield*.

In particular, a Galois field is a finite cyclic neofield which has associative and commutative addition. The concept of a neofield was first introduced and studied by L. J. Paige in **[13]**. Cyclic neofields have been extensively studied in **[6]**.

We shall denote the order of a finite group $(G, \cdot)$ by $|G|$.

DEFINITION 2.4. A (K, λ) *complete mapping*, where $K = \{k_1, k_2, \ldots, k_s\}$ and the k_i are integers such that $\sum_{i=1}^{s} k_i = \lambda(|G| - 1)$, is an arrangement of the non-identity elements of G (each used λ times) into s cyclic sequences of lengths $k_1, k_2, \ldots, k_s$, say

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

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 λ times.

A (K, λ) *near complete mapping*, where $K = \{h_1, h_2, \ldots, h_r; k_1 k_2, \ldots, k_s\}$ and the h_i and k_j are integers such that $\Sigma_{i=1}^{r} h_i + \Sigma_{j=1}^{s} k_j = \lambda |G|$, is an arrangement of the elements of G (each used λ times) into r sequences with lengths $h_1, h_2, \ldots, h_r$ and s cyclic sequences with lengths $k_1, k_2, \ldots, k_s$, say

$$\left[g'_{11}\, g'_{12} \cdots g'_{1h_1}\right] \cdots \left[g'_{r1}\, g'_{r2} \cdots g'_{rh_r}\right]\left(g_{11}\, g_{12} \cdots g_{1k_1}\right) \cdots \left(g_{s1}\, g_{s2} \cdots g_{sk_s}\right)$$

such that the elements $(g'_{ij})^{-1} g'_{i,j+1}$ 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 λ times. (We have $\Sigma(h_i - 1) + \Sigma k_j = \lambda(|G| - 1)$ so it is immediate from the definition itself that $r = \lambda$.)

EXAMPLES. (2.1) $(a\ a^2\ a^4)(a^3\ a^6\ a^5)$ is a $(K, 1)$ complete mapping of the cyclic group $C_7 = \mathrm{gp}\{a: a^7 = e\}$, where $K = \{3, 3\}$.

(2.2) $(a\ a^2\ a^4)(a^3\ a^6\ a^5)(a\ a^3)(a^2\ a^6)(a^4\ a^5)$ is a $(K, 2)$ complete mapping of the cyclic group C_7, where $K = \{3, 3, 2, 2, 2\}$.

(2.3) $(a^3\ ba^2\ ba^3\ a)(ba\ b\ a^2)$ is a $(K, 1)$ complete mapping of the dihedral group $D_4 = \mathrm{gp}\{a, b: a^4 = b^2 = e, ab = ba^{-1}\}$, where $K = \{4, 3\}$.

(2.4) $[e\ a^4\ a^3](a\ a^2\ a^5)$ is a $(K, 1)$ near complete mapping of the cyclic group $C_6 = \mathrm{gp}\{a: a^6 = e\}$, where $K = \{3; 3\}$.

(2.5) $[e\ a^5\ a^4][e\ a^2\ a\ a^4](a\ a^3)(a^2\ a^6\ a^7)(a^3\ a^7\ a^5\ a^6)$ is a $(K, 2)$ near complete mapping of the cyclic group $C_8 = \mathrm{gp}\{a: a^8 = e\}$, where $K = \{3, 4; 2, 3, 4\}$.

(2.6) $[e\ ba][e\ ba^2](a^2\ b\ ba^2\ a)(a\ b\ ba\ a^2)$ is a $(K, 2)$ near complete mapping of the dihedral group $D_3 = \mathrm{gp}\{a, b: a^3 = b^2 = e, ab = ba^{-1}\}$, where $K = \{2, 2; 4, 4\}$.

DEFINITION 2.5. A (k, λ) *complete mapping* is a (K, λ) complete mapping such that $K = \{k, k, \ldots, k\}$. For such a generalized complete mapping, $s = \lambda(|G| - 1)/k$.

Similarly, a (k, λ) *near complete mapping* is a (K, λ) near complete mapping such that $K = \{h, h, \ldots, h; k, k, \ldots, k\}$ and $k - h = 1$.

EXAMPLES. (2.7) Example (1) above is a $(3, 1)$ complete mapping of the cyclic group C_7.

(2.8) $[e\ a^4][e\ a^4](a\ a^2\ a^7)(a^3\ a^6\ a^5)(a\ a^7\ a^6)(a^2\ a^3\ a^5)$ is a $(3, 2)$ near complete mapping of the cyclic group C_8.

Let $x \to \theta'(x)$ be a complete mapping of a group $(G, \cdot)$ with identity element denoted by e. Then the mapping θ such that $\theta(x) = \theta'(x)\theta'(e)^{-1}$

is also a complete mapping of G and $\theta(e) = e$. We shall call this the *canonical form* of the complete mapping θ'.

We easily see that

THEOREM 2.1. (i) *A* $(K, 1)$ *complete mapping of a group is equivalent to a complete mapping in canonical form.*

(ii) *The concept of k-regular complete mapping of a group introduced and discussed in* [3] *coincides with our concept of* $(k, 1)$ *complete mapping.*

(iii) *A finite group G is R-sequenceable if and only if it possesses a* $(|G| - 1, 1)$ *complete mapping.*

Proof. (i) Let $(c_{11}\, c_{12} \cdots c_{1k_1})(c_{21}\, c_{22} \cdots c_{2k_2}) \cdots (c_{s1}\, c_{s2} \cdots c_{sk_s})$ be a $(K, 1)$ complete mapping of a group G. Define $\theta(e) = e$ and $\theta(c_{ij}) = c_{ij}^{-1}c_{i,j+1}$, where the second suffix is added modulo k_i. Then θ is a complete mapping of G.

Conversely, let $x \to \theta(x)$ be the canonical form of a complete mapping of G. We suppose that the elements of G are $a_0 = e, a_1, a_2, \ldots, a_{n-1}$. Since $\theta(e) = e$, it follows that $\theta(a_1) = a_1^{-1}\phi(a_1) \neq e$ and so $\phi(a_1) = a_2 \neq a_1$. Then $\theta(a_1)\theta(a_2) = a_1^{-1}\phi(a_2)$. Let $\phi(a_2) = a_3 \neq a_2$ since $\phi(a_1) = a_2$. We have $\phi(a_2) \neq a_1$ unless $\theta(a_1)\theta(a_2) = e$. If $\theta(a_1)\theta(a_2) = e$, $(a_1\; a_2)$ forms one cyclic sequence of the generalized complete mapping. If not, we have $\theta(a_1)\theta(a_2)\theta(a_3) = a_1^{-1}\phi(a_3)$. Let $\phi(a_3) = a_4$. Then $\phi(a_3) \neq a_2$ or a_3 since $\phi(a_1) = a_2$, $\phi(a_2) = a_3$. Also, $\phi(a_3) \neq a_1$ unless $\theta(a_1)\theta(a_2)\theta(a_3) = e$. If $\theta(a_1)\theta(a_2)\theta(a_3) = e$, $(a_1\; a_2\; a_3)$ forms one cyclic sequence of the generalized complete mapping. If not, we have $\theta(a_1)\theta(a_2)\theta(a_3)\theta(a_4) = a_1^{-1}\phi(a_4)$. Eventually, we obtain a product $\theta(a_1)\theta(a_2) \cdots \theta(a_r) = e$ and a corresponding cyclic sequence $(a_1\; a_2 \cdots a_r)$ of the generalized complete mapping. Taking a_s distinct from the members of this cyclic sequence, we have $\theta(a_s) = a_s^{-1}\phi(a_s) \neq e$ and so $\phi(a_s) = a_{s+1} \neq a_s$ and not equal to any members of the previously constructed cyclic sequence $(a_1\; a_2 \cdots a_r)$ because ϕ is a bijection of G. Hence, by repetition of the process, we eventually separate the non-identity elements of G into disjoint cyclic sequences which form a $(K, 1)$ complete mapping.

(ii) The definition of a k-regular complete mapping given in [3] is exactly that of a $(k, 1)$ complete mapping.

(iii) Suppose that $(c_1\; c_2 \cdots c_{n-1})$ is the cyclic sequence which defines a $(|G| - 1,\ 1)$ complete mapping of a finite group G. Define $\theta(e) = e$, $\theta(c_i) = c_i^{-1}c_{i+1} = a_{i+1}$ for $i = 1, 2, \ldots, n-2$ and $\theta(c_{n-1}) = c_{n-1}^{-1}c_1 = a_1$. Then θ is a bijection of G by definition of a $(|G| - 1,\ 1)$ complete mapping. Also $b_0 = a_0 = e$, $b_1 = a_0a_1 = c_{n-1}^{-1}c_1$, $b_2 = a_0a_1a_2 = c_{n-1}^{-1}c_2$,

$b_3 = c_{n-1}^{-1}c_3, \ldots, b_{n-2} = c_{n-1}^{-1}c_{n-2}$ are all different and $b_{n-1} = a_0a_1a_2 \cdots a_{n-1} = c_{n-1}^{-1}c_{n-1} = e$, so G is R-sequenceable.

Conversely, if the finite group G is R-sequenceable, then if, with the notation of Definition 2.2, the element c is the one which does not occur among the distinct partial products $b_0 = e, b_1, b_2, \ldots, b_{n-2}$ the elements $c^{-1}, c^{-1}b_1, c^{-1}b_2, \ldots, c^{-1}b_{n-2}$ are the non-identity elements of G and form a cyclic sequence to define a $(|G|-1, 1)$ complete mapping of G.

THEOREM 2.2. *A finite group G is sequenceable if and only if it possesses a $(|G|+1, 1)$ near complete mapping.*

Proof. Suppose that $[c_0\ c_1 \cdots c_{n-1}]$ is the sequence which defines the $(|G|+1, 1)$ near complete mapping, where $n = |G|$. Define $a_0 = e$ and $a_i = c_{i-1}^{-1}c_i$ for $i = 1, 2, \ldots, n-1$. Then the a_i are all different by definition of a near complete mapping and the partial products $b_0 = a_0 = e$, $b_1 = a_0a_1 = c_0^{-1}c_1$, $b_2 = a_0a_1a_2 = c_0^{-1}c_2, \ldots,$ $b_{n-1} = a_0a_1 \cdots a_{n-1} = c_0^{-1}c_{n-1}$ are also all different, so G is sequenceable.

Conversely, suppose that G is sequenceable with sequencing $a_0 = e$, $a_1, a_2, \ldots, a_{n-1}$ and partial products $b_0 = a_0 = e$, $b_1 = a_0a_1$, $b_2 = a_0a_1a_2, \ldots, b_{n-1} = a_0a_1 \cdots a_{n-1}$. Then, the sequence $[b_0\ b_1 \cdots b_{n-1}]$ defines $a(|G|+1, 1)$ near complete mapping of G.

3. Construction of neofields.

DEFINITION 3.1. An algebraic structure $(N, +, \cdot)$ which differs from a neofield only in that right distributivity of multiplication over addition is not postulated is called a *left neofield.*

We note that a left neofield whose multiplicative group is abelian is a neofield.

Let $(G, \cdot)$ be a finite group of $v - 1$ elements which possesses a $(K, 1)$ complete mapping. Then there exists a left neofield $(N_v, +, \cdot)$ whose multiplicative group is G. Precisely we have

THEOREM 3.1. *Let $(G, \cdot)$ be a finite group with identity element denoted by 1 which possesses a $(K, 1)$ complete mapping and let $x \to \theta(x)$ be the corresponding complete mapping in canonical form whose existence is guaranteed by Theorem 2.1(i). Let 0 be a symbol not in the set G and define $N = G \cup \{0\}$. Then $(N - \{0\}, \cdot)$ is the given group $(G, \cdot)$ and we can define a second operation $(+)$ on N by the statements $1 + z = z\theta(z)$ for all*

$z \in N - \{0, 1\}$, $1 + 1 = 0$, $z + 0 = z = 0 + z$ for all $z \in N$, $x + y = x(1 + x^{-1}y)$ whenever x and y are non-zero. If we also define $0 \cdot x = 0 = x \cdot 0$ for all $x \in N$, then $(N, +, \cdot)$ is a left neofield.

Proof. We need to show that $(N, +)$ is a loop with identity element 0 and that multiplication is left distributive over addition.

The left distributivity of multiplication over addition follows immediately from the definition $x + y = x(1 + x^{-1}y)$, for we have

$$tu + tv = tu\left[1 + (tu)^{-1}tv\right] = tu(1 + u^{-1}v) = t\left[u(1 + u^{-1}v)\right] = t(u + v).$$

Since $1 + z = z\theta(z) = \phi(z)$ for all $z \neq 0, 1$, and since ϕ is a bijection of G with $\phi(1) = 1$ (because θ is a complete mapping in canonical form), the elements $1 + z$ are all distinct. Consequently, for $x \neq 0$, the elements $x + y = x(1 + x^{-1}y)$ as y varies are all distinct.

Thus the entries in each of the rows of the Cayley table of $(N, +)$ are all different.

Since for x, y non-zero, $x \neq y$, $x + y = x(1 + x^{-1}y) = x \cdot x^{-1}y \cdot \theta(x^{-1}y) = y \cdot \theta(x^{-1}y)$, and since $y + y = 0$, $0 + y = y$, the elements $x + y$ as x varies are all distinct. So the elements in each of the columns of the Cayley table of $(N, +)$ are all different.

The element 0 acts as identity for $(+)$, so $(N, +)$ is a loop. This completes the proof.

DEFINITION 3.2. A neofield or left neofield $(N, +, \cdot)$ for which $1 + 1 = 0$ and for which the mapping ϕ: $z \to 1 + z$, $z \neq 0, 1$, is a permutation of $N - \{0, 1\}$ consisting entirely of cycles of length k is said to be a neofield of *pseudo-characteristic* k.

We note that any finite left neofield constructed in the manner of Theorem 3.1 from a group $(G, \cdot)$ which possesses a $(k, 1)$ complete mapping is a left neofield of pseudo-characteristic k.

A Galois field of order 2^h has pseudo-characteristic 2. However, a neofield of pseudo-characteristic 2 is not necessarily a Galois field. In particular, some examples of cyclic neofields of pseudo-characteristic 2 will be found in **[6]**.

If there exists an R-sequenceable group of order $v - 1$, then there exists a left neofield of order v of the maximum possible pseudo-characteristic: namely, pseudo-characteristic $v - 2$.

Next, we have the following:

THEOREM 3.2. *Let $(G, \cdot)$ be a finite group of $v - 1$ elements which possesses a $(K, 1)$ near complete mapping such that $K = \{h; k_1, k_2, \ldots, k_s\}$. Then there exists a left neofield $(N_v, +, \cdot)$ whose multiplicative group is G.*

Proof. Let the near complete mapping be as follows:

$$[g_1' \, g_2' \cdots g_h'](g_{11} \, g_{12} \cdots g_{1k_1})(g_{21} \, g_{22} \cdots g_{2k_2}) \cdots (g_{s1} \, g_{s2} \cdots g_{sk_s}).$$

We suppose that this has been put into canonical form with g_1' equal to the identity of the group G. (A $(K, 1)$ near complete mapping can always be put into this canonical form by premultiplying each element in the sequences by $g_1'^{-1}$.) Define a mapping θ of G into itself by the statements $\theta(g_i') = g_i'^{-1}g_{i+1}'$ for $i = 1, 2, \ldots, h-1$; $\theta(g_{ij}) = g_{ij}^{-1}g_{i,j+1}$ for $i = 1, 2, \ldots, s$, where the second suffix j is added modulo k_i. Then, by definition of a near complete mapping, θ maps $G - \{g_h'\}$ one-to-one onto $G - \{1\}$, where 1 denotes the identity element of $(G, \cdot)$.

Let 0 be a symbol not in the set G and define $N = G \cup \{0\}$. Then $(N - \{0\}, \cdot)$ is the given group $(G, \cdot)$ and we can define a second operation $(+)$ on N by the statements $1 + z = z\theta(z)$ for all $z \in N - \{0, g_h'\}$, $1 + g_h' = 0$, $z + 0 = z = 0 + z$ for all $z \in N$, $x + y = x(1 + x^{-1}y)$ whenever x and y are non-zero. We also define $0 \cdot x = 0 = x \cdot 0$ for all $x \in N$.

Since $1 + 0 = 1 = g_1'$; $1 + g_i' = g_{i+1}'$ for $i = 1, 2, \ldots, h-1$; $1 + g_h' = 0$; $1 + g_{ij} = g_{i,j+1}$ for $i = 1, 2, \ldots, s$ where the second suffix j is added modulo k_i, it follows that the elements $1 + z$ are all distinct. Consequently, for $x \neq 0$, the elements $x + y = x(1 + x^{-1}y)$ as y varies are all distinct. So the entries in each of the rows of the Cayley table of $(N, +)$ are all different.

Since $x + y = x(1 + x^{-1}y) = y \cdot \theta(x^{-1}y) \neq y$ if x and y are not zero and $\neq 0$ unless $x^{-1}y = g_h'$ and, since $0 + y = y$, the elements $x + y$ as x varies are all distinct. So the elements in each of the columns of the Cayley table of $(N, +)$ are all different.

The remainder of the proof is exactly similar to that of Theorem 3.1.

DEFINITION 3.4. A neofield $(N, +, \cdot)$ for which the mapping ϕ: $z \to 1 + z$ is a permutation of N consisting entirely of cycles of length k is said to be a neofield of *characteristic k*.

THEOREM 3.3. *A finite left neofield constructed in the manner of Theorem* 3.2 *from a group* $(G, \cdot)$ *which possesses a* $(k, 1)$ *near complete mapping is a left neofield of characteristic k.*

Proof. Let the canonical form of the $(k, 1)$ near complete mapping be

$$[1 \, g_2' \, g_3' \cdots g_{k-1}'](g_{11} \, g_{12} \cdots g_{1k})(g_{21} \, g_{22} \cdots g_{2k}) \cdots (g_{s1} \, g_{s2} \cdots g_{sk}).$$

Then, from the definition of the mapping θ and the facts $1 + z = z\theta(z)$ for $z \neq 0$, g'_{k-1} and $1 + 0 = 1$, $1 + g'_{k-1} = 0$, it follows that the mapping $\phi: z \to 1 + z$ is given by the permutation

$$(0\ 1\ g'_2\ g'_3 \cdots g'_{k-1})(g_{11}\ g_{12} \cdots g_{1k})(g_{21}\ g_{22} \cdots g_{2k}) \cdots (g_{s1}\ g_{s2} \cdots g_{sk}),$$

which consists entirely of cycles of length k.

We note that a Galois field of order p^h has characteristic p, but, of course, a neofield of prime characteristic is not necessarily a Galois field. As an example, the following example of a cyclic neofield of order 9 and of characteristic 3 is given in [**6**]:

z	0	1	a	a^2	a^3	a^4	a^5	a^6	a^7
$1+z$	1	a^4	a^7	a	a^5	0	a^6	a^3	a^2

Addition in this neofield is neither associative nor commutative.

If there exists a sequenceable group of order $v - 1$, then there exists a left neofield of order v of the maximum possible characteristic: namely, characteristic v. Conversely, the existence of a left neofield of order and characteristic v based on a group $(G, \cdot)$ implies that G is a sequenceable group.

The concept of characteristic of a neofield was first introduced in [**8**] where it was shown (among other things) that property D neofields of the maximum possible characteristic exist of orders 9, 15 and 17, but not of orders 3, 5, 7, or 11. (A property D neofield is a cyclic neofield with the additional property that

$$\frac{1 + x^t}{1 + x^{t-1}} = \frac{1 + x^u}{1 + x^{u-1}} \Rightarrow t = u.)$$

THEOREM 3.4. *A finite left neofield constructed in the manner of Theorems* 3.1 *or* 3.2 *from a group* $(G, \cdot)$ *is a neofield if and only if the mapping* θ *maps conjugacy classes of G to conjugacy classes and, in the case of Theorem* 3.2, *if and only if we have additionally that the element* g'_h *is in the centre of G.*

Proof. We have

$$ut + vt = ut\left[1 + (ut)^{-1}vt\right] = ut(1 + t^{-1}u^{-1}vt) = ut\phi(t^{-1}u^{-1}vt),$$

where $\phi(z) = 1 + z = z\theta(z)$ for all $z \neq 0, 1$ in Theorem 3.1 and for all $z \neq 0$, g'_h in Theorem 3.2. So, $ut + vt = vt\theta(t^{-1}u^{-1}vt)$ except for two special values of $t^{-1}u^{-1}vt$. Also,

$$(u+v)t = u(1+u^{-1}v)t = u\phi(u^{-1}v)t = v\theta(u^{-1}v)t$$

except for two special values of $u^{-1}v$. Consequently, the right distributive law holds if and only if $\theta(t^{-1}u^{-1}vt) = t^{-1}\theta(u^{-1}v)t$ for all except two special values of $t^{-1}u^{-1}vt$. For the special value $t^{-1}u^{-1}vt = 0$, we have $v = 0$ or $t = 0$ and in that case $ut + vt = (u+v)t$ always. For the special value $t^{-1}u^{-1}vt = 1$ in Theorem 3.1, we have $u = v$ and then $ut + vt = ut(1+1) = 0$ and $(u+v)t = u(1+1)t = 0$, so $ut + vt = (u+v)t$ in this case also. Since $\theta(1) = 1$, the conjugacy class $\{1\}$ of G is preserved by θ. So, it is clear that, for the case of Theorem 3.1, if the complete mapping θ (in canonical form) maps conjugacy classes of G onto conjugacy classes then the right distributive law holds for all elements of $(N, +, \cdot)$.

For the special value $t^{-1}u^{-1}vt = g_h'$ in Theorem 3.2 we have $ut + vt = ut(1+g_h') = 0$ and $t \neq 0$ so $ut + vt = (u+v)t$ if and only if $u^{-1}v = g_h'$. Consequently in Theorem 3.2 we require the extra condition that $\{g_h'\}$ be a complete conjugacy class.

COROLLARY 1. *A necessary condition that the right distributive law hold in the left neofield constructed by the method of Theorem* 3.2 *is that the elements g_2' and g_h' of the $(K, 1)$ near complete mapping be both in the centre of the multiplicative group $(G, \cdot)$.*

Proof. We have already shown that g_h' must be in the centre. Since $\theta(1) = g_2'$ and since conjugacy classes are mapped to conjugacy classes, so also g_2' must be in the centre.

COROLLARY 2. *If $(G, \cdot)$ is a finite non-abelian group of odd order then there exists a neofield whose multiplicative group is G.*

Proof. For such a group, the identity mapping is a complete mapping and it maps conjugacy classes to conjugacy classes.

THEOREM 3.5. *For abelian groups the constructions of Theorems* 3.1 *and* 3.2 *are mutually exclusive. An abelian group $(G, \cdot)$ has a $(K, 1)$ complete mapping if and only if the product of all its elements is the identity element e. It has a $(K, 1)$ near complete mapping if and only if it has a unique element of order* 2 *and then the product of all its elements is this unique element of order* 2.

Proof. Suppose that $(G, \cdot)$ is abelian and has a $(K, 1)$ complete mapping

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

Then the elements $g_{11}^{-1}g_{12}$, $g_{12}^{-1}g_{13}, \ldots, g_{1k_1}^{-1}g_{11}$, $g_{21}^{-1}g_{22}$, $g_{22}^{-1}g_{23}, \ldots,$ $g_{2k_2}^{-1}g_{21}, \ldots, g_{s1}^{-1}g_{s2}$, $g_{s2}^{-1}g_{s3}, \ldots, g_{sk_s}^{-1}g_{s1}$ are the non-identity elements of G each counted once. It is clear that the products of these elements is e. Conversely, by a theorem of L. J. Paige [**12**], if the product of the elements of an abelian group G is e, then G has a complete mapping and, hence, by Theorem 2.1(i), it has a $(K, 1)$ complete mapping.

Secondly, suppose that $(G, \cdot)$ is abelian and has a $(K, 1)$ near complete mapping

$$[g_1'\, g_2' \cdots g_h'](g_{11}\, g_{12} \cdots g_{1k_1}) \cdots (g_{s1}\, g_{s2} \cdots g_{sk_s}).$$

Then the elements $g_1'^{-1}g_2'$, $g_2'^{-1}g_3', \ldots, g_{h-1}'^{-1}g_h'$, $g_{11}^{-1}g_{12}$, $g_{12}^{-1}g_{13}, \ldots,$ $g_{1k_1}^{-1}g_{11}, \ldots, g_{s1}^{-1}g_{s2}$, $g_{s2}^{-1}g_{s3}, \ldots, g_{sk_s}^{-1}g_{s1}$ are the non-identity elements of G each counted once. The product of these elements is $g_1'^{-1}g_h' \neq e$. But, by another theorem due to L. J. Paige [**12**], the product of all the elements of an abelian group is equal to e unless the group has a unique element of order 2. In the latter case, the product is equal to the unique element of order 2. We deduce immediately that an abelian group has a $(K, 1)$ near complete mapping only if it has a unique element of order 2 and that then it does not have a $(K, 1)$ complete mapping. Conversely, by a theorem due to B. Gordon [**4**], an abelian group which has a unique element of order 2 is sequenceable. So such a group has a $(|G| + 1, 1)$ near complete mapping. That is, it has a $(K, 1)$ near complete mapping for at least one choice of K.

COROLLARY. *If an abelian group $(G, \cdot)$ has a $(K, 1)$ near complete mapping in canonical form as required for Theorem* 3.2, *then the element g_h' is the unique element of order* 2 *in G.*

Proof. The product of all the elements of G is $g_1'^{-1}g_h'$ and, when the near complete mapping is in canonical form, $g_1' = e$.

We end this section by proving that left neofields are co-extensive with $(K, 1)$ complete mappings and near complete mappings of groups.

THEOREM 3.6. *Let $(N, +, \cdot)$ be a left neofield with multiplicative group $(G, \cdot)$ where $G = N - \{0\}$. Then, if $1 + 1 = 0$ in N, N defines a $(K, 1)$ complete mapping of G. If $1 + 1 \neq 0$, N defines a $(K, 1)$ near complete mapping of G.*

Proof. Let Q: $z \to 1 + z$ be the permutation of N induced by the presentation function of $(N, +, \cdot)$. If $1 + 1 = 0$, Q takes the form

$$Q = (0\ 1)(g_{11}\, g_{12} \cdots g_{1k_1})(g_{21}\, g_{22} \cdots g_{2k_2}) \cdots (g_{s1}\, g_{s2} \cdots g_{sk_s})$$

when written as a product of cycles, where $1 + g_{hi} = g_{h,i+1}$. Define $\theta(g_{hi}) = g_{hi}^{-1} g_{h,i+1}$ and $\theta(1) = 1$. Then θ is a complete mapping of G and

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

is a $(K, 1)$ complete mapping. Since $\phi(g_{hi}) = g_{hi} \cdot \theta(g_{hi}) = g_{h,i+1}$, it is sufficient to prove that $\theta(g_{hi}) \neq \theta(g_{lj})$ unless $g_{hi} = g_{lj}$.

We have

$$\theta(g_{hi}) = \theta(g_{lj}) \Rightarrow g_{hi}^{-1}(1 + g_{hi}) = g_{lj}^{-1}(1 + g_{lj})$$
$$\Rightarrow g_{hi}^{-1} + 1 = g_{lj}^{-1} + 1 \Rightarrow g_{hi} = g_{lj}$$

since multiplication is left distributive over addition and addition is a loop.

If $1 + 1 \neq 0$, Q takes the form

$$Q = (0\ 1\ g_2'\, g_3' \cdots g_h')(g_{11}\, g_{12} \cdots g_{1k_1}) \cdots (g_{s1}\, g_{s2} \cdots g_{sk_s}),$$

where $1 + 1 = g_2'$ and $1 + g_h' = 0$. Then

$$[1\ g_2'\, g_3' \cdots g_h'](g_{11}\, g_{12} \cdots g_{1k_1}) \cdots (g_{s1}\, g_{s2} \cdots g_{sk_s})$$

is a $(K, 1)$ near complete mapping of G. We define $\theta(g_{hi}) = g_{hi}^{-1} g_{h,i+1}$ as before and $\theta(1) = g_2'$, $\theta(g_i') = g_i'^{-1} g_{i+1}'$ for $i = 2, 3, \ldots, h - 1$. An argument exactly similar to that above shows that θ is a one-to-one mapping from $G - \{g_h'\}$ onto $G - \{1\}$ so we have a $(K, 1)$ near complete mapping.

4. Examples. Since the left distributive law holds in any neofield or left neofield $(N, +, \cdot)$, the neofield is completely defined by its multiplicative group and by the function ϕ: $z \to 1 + z$. This was pointed out in **[8]** and, in that paper, ϕ was given in the form of a permutation Q of the elements of N. In **[6]** and **[7]**, ϕ has been called the *presentation function* of the neofield.

When Q is a regular permutation consisting entirely of cycles of length k, the corresponding neofield has characteristic k. When Q comprises the transposition $(0\ 1)$ and a set of cycles each of length k, the corresponding neofield has pseudo-characteristic k.

EXAMPLE 4.1. The $(3, 1)$ complete mapping $(a\ a^2\ a^4)(a^3\ a^6\ a^5)$ of the cyclic group $C_7 = \mathrm{gp}\{a\colon a^7 = e\}$ defines a neofield of order 8 and pseudo-characteristic 3. Its presentation function is

z	0	1	a	a^2	a^3	a^4	a^5	a^6
$\phi(z)$	1	0	a^2	a^4	a^6	a	a^3	a^5

We have $Q = (0\ 1)(a\ a^2\ a^4)(a^3\ a^6\ a^5)$ and we note that the associated complete mapping in canonical form is the identity mapping.

EXAMPLE 4.2. The (3, 1) near complete mapping $[e\ a^4](a\ a^2\ a^7)\cdot(a^3\ a^6\ a^5)$ of the cyclic group $C_8 = \mathrm{gp}\{a\colon a^7 = e\}$ defines a neofield of order 9 and characteristic 3. Its presentation function is

z	0	1	a	a^2	a^3	a^4	a^5	a^6	a^7
$\phi(z)$	1	a^4	a^2	a^7	a^6	0	a^3	a^5	a

We have $Q = (0\ 1\ a^4)(a\ a^2\ a^7)(a^3\ a^6\ a^5)$.

EXAMPLE 4.3. The (5, 1) near complete mapping

$$[e\ a^6\ a^{18}\ a^{12}](a\ a^{22}\ a^{15}\ a^2\ a^{17})(a^7\ a^8\ a^4\ a^{23}\ a^{21}) \times (a^{19}\ a^9\ a^{11}\ a^{16}\ a^{20})(a^{13}\ a^5\ a^{14}\ a^3\ a^{10})$$

of the cyclic group $C_{24} = \mathrm{gp}\{a\colon a^{24} = e\}$ defines a neofield of order 25 and characteristic 5. This is the Galois field GF[25], where a is a primitive element satisfying $a^2 = a - 2$.

EXAMPLE 4.4. The (6, 1) complete mapping $(a^2\ a\ a^3\ a^6\ a^4\ a^5)$ of the cyclic group $C_7 = \mathrm{gp}\{a\colon a^7 = e\}$ is constructed from the R-sequencing e, a^6, a^2, a^3, a^5, a, a^4 of C_7 in the manner of Theorem 2.1(iii). It defines a neofield of order 8 of the maximum pseudo-characteristic 6. Its presentation function is

z	0	1	a	a^2	a^3	a^4	a^5	a^6
$\phi(z)$	1	0	a^3	a	a^6	a^5	a^2	a^4

We note that every cyclic group of odd order is R-sequenceable. For proofs, see **[2]**, **[6]** and **[10]**.

EXAMPLE 4.5. The (9, 1) near complete mapping $[e\ a^2\ a^5\ a\ a^7\ a^6\ a^3\ a^4]$ of the cyclic group $C_8 = \mathrm{gp}\{a\colon a^8 = e\}$ is constructed from the sequencing e, a^2, a^3, a^4, a^6, a^7, a^5, a. It defines a neofield of order 9 which has property D and also has the maximum possible characteristic of 9. In order to exhibit that it has property D, we exhibit its presentation function in the following way, where the last line gives the values of $(1 - a^{t-1})/(1 - a^t)$.

z	a^3		a^2		a		1		a^7		a^6		a^5		a^4		0
$\phi(z)$	a^4		a^5		a^7		a^2		a^6		a^3		a		0		1
		a		a^2		a^3		a^4		a^5		a^6		0			

We remark that every cyclic group of even order is sequenceable (see, for instance, [**4**] or [**1**]) but that, in general, the sequencings do not give neofields which have property D.

EXAMPLE 4.6. The dihedral group

$$D_6 = \mathrm{gp}\{a, b \colon a^6 = b^2 = e, ab = ba^{-1}\}$$

is both R-sequenceable and sequenceable. Consequently, it permits the constuction of a left neofield of order 13 and maximal pseudo-characteristic 11 (Theorem 3.1) and also a left neofield of order 13 and maximal characteristic 13 (Theorem 3.2). We exhibit the presentation function for one example of each kind.

z	0	1	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5
$\phi(a)$	1	0	b	a^4	ba^2	a^3	ba^5	a^2	ba^4	ba^3	ba	a^5	a

$$Q = (0\ 1)(a^2\, a^4\, a^3\, ba^2\, ba^3\, ba\, ba^4\, a^5\, ba^5\, a\, b)$$

z	0	1	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5
$\phi(z)$	1	a	a^3	ba^5	ba^3	0	ba^4	a^2	a^4	ba	b	ba^2	a^5

$$Q = (0\ 1\ a\ a^3\ ba^3\ b\ a^2\ ba^5\ a^5\ ba^4\ ba^2\ ba\ a^4)$$

It is known that a dihedral group is R-sequenceable if and only if it is of doubly even order (see [**10**]). It is conjectured that all dihedral groups of orders greater than 8 are sequenceable. There is strong evidence for this conjecture in the case of dihedral groups of singly even order (see [**5**]).

TABLE 1

(+)	0	1	a	a^2	a^3	a^4	a^5	a^6	b	ba	ba^2	ba^3	ba^4	ba^5	ba^6	b^2	b^2a	b^2a^2	b^2a^3	b^2a^4	b^2a^5	b^2a^6
0	0	1	a	a^2	a^3	a^4	a^5	a^6	b	ba	ba^2	ba^3	ba^4	ba^5	ba^6	b^2	b^2a	b^2a^2	b^2a^3	b^2a^4	b^2a^5	b^2a^6
1	1	0	a^2	a^4	a^6	a	a^3	a^5	b^2	b^2a^3	b^2a^6	b^2a^2	b^2a^5	b^2a	b^2a^4	b	ba^5	ba^3	ba	ba^6	ba^4	ba^2
a	a	a^6	0	a^3	a^5	1	a^2	a^4	b^2a^5	b^2a	b^2a^4	b^2	b^2a^3	b^2a^6	b^2a^2	ba^3	ba	ba^6	ba^4	ba^2	b	ba^5
a^2	a^2	a^5	1	0	a^4	a^6	a	a^3	b^2a^3	b^2a^6	b^2a^2	b^2a^5	b^2a	b^2a^4	b^2	ba^6	ba^4	ba^2	b	ba^5	ba^3	ba
a^3	a^3	a^4	a^6	a	0	a^5	1	a^2	b^2a	b^2a^4	b^2	b^2a^3	b^2a^6	b^2a^2	b^2a^5	ba^2	b	ba^5	ba^3	ba	ba^6	ba^4
a^4	a^4	a^3	a^5	1	a^2	0	a^6	a	b^2a^6	b^2a^2	b^2a^5	b^2a	b^2a^4	b^2	b^2a^3	ba^5	ba^3	ba	ba^6	ba^4	ba^2	b
a^5	a^5	a^2	a^4	a^6	a	a^3	0	1	b^2a^4	b^2	b^2a^3	b^2a^6	b^2a^2	b^2a^5	b^2a	ba	ba^6	ba^4	ba^2	b	ba^5	ba^3
a^6	a^6	a	a^3	a^5	1	a^2	a^4	0	b^2a^2	b^2a^5	b^2a	b^2a^4	b^2	b^2a^3	b^2a^6	ba^4	ba^2	b	ba^5	ba^3	ba	ba^6
b	b	b^2	b^2a^5	b^2a^3	b^2a	b^2a^6	b^2a^4	b^2a^2	0	ba^2	ba^4	ba^6	ba	ba^3	ba^5	1	a^3	a^6	a^2	a^5	a	a^4
ba	ba	b^2a^3	b^2a	b^2a^6	b^2a^4	b^2a^2	b^2	b^2a^5	ba^6	0	ba^3	ba^5	b	ba^2	ba^4	a^5	a	a^4	1	a^3	a^6	a^2
ba^2	ba^2	b^2a^6	b^2a^4	b^2a^2	b^2	b^2a^5	b^2a^3	b^2a	ba^5	b	0	ba^4	ba^6	ba	ba^3	a^3	a^6	a^2	a^5	a	a^4	1
ba^3	ba^3	b^2a^2	b^2	b^2a^5	b^2a^3	b^2a	b^2a^6	b^2a^4	ba^4	ba^6	ba	0	ba^5	b	ba^2	a	a^4	1	a^3	a^6	a^2	a^5
ba^4	ba^4	b^2a^5	b^2a^3	b^2a	b^2a^6	b^2a^4	b^2a^2	b^2	ba^3	ba^5	b	ba^2	0	ba^6	ba	a^6	a^2	a^5	a	a^4	1	a^3
ba^5	ba^5	b^2a	b^2a^6	b^2a^4	b^2a^2	b^2	b^2a^5	b^2a^3	ba^2	ba^4	ba^6	ba	ba^3	0	b	a^4	1	a^3	a^6	a^2	a^5	a
ba^6	ba^6	b^2a^4	b^2a^2	b^2	b^2a^5	b^2a^3	b^2a	b^2a^6	ba	ba^3	ba^5	b	ba^2	ba^4	0	a^2	a^5	a	a^4	1	a^3	a^6
b^2	b^2	b	ba^3	ba^6	ba^2	ba^5	ba	ba^4	1	a^5	a^3	a	a^6	a^4	a^2	0	b^2a^2	b^2a^4	b^2a^6	b^2a	b^2a^3	b^2a^5
b^2a	b^2a	ba^5	ba	ba^4	b	ba^3	ba^6	ba^2	a^3	a	a^6	a^4	a^2	1	a^5	b^2a^6	0	b^2a^3	b^2a^5	b^2	b^2a^2	b^2a^4
b^2a^2	b^2a^2	ba^3	ba^6	ba^2	ba^5	ba	ba^4	b	a^6	a^4	a^2	1	a^5	a^3	a	b^2a^5	b^2	0	b^2a^4	b^2a^6	b^2a	b^2a^3
b^2a^3	b^2a^3	ba	ba^4	b	ba^3	ba^6	ba^2	ba^5	a^2	1	a^5	a^3	a	a^6	a^4	b^2a^4	b^2a^6	b^2a	0	b^2a^5	b^2	b^2a^2
b^2a^4	b^2a^4	ba^6	ba^2	ba^5	ba	ba^4	b	ba^3	a^5	a^3	a	a^6	a^4	a^2	1	b^2a^3	b^2a^5	b^2	b^2a^2	0	b^2a^6	b^2a
b^2a^5	b^2a^5	ba^4	b	ba^3	ba^6	ba^2	ba^5	ba	a	a^6	a^4	a^2	1	a^5	a^3	b^2a^2	b^2a^4	b^2a^6	b^2a	b^2a^3	0	b^2
b^2a^6	b^2a^6	ba^2	ba^5	ba	ba^4	b	ba^3	ba^6	a^4	a^2	1	a^5	a^3	a	a^6	b^2a	b^2a^3	b^2a^5	b^2	b^2a^2	b^2a^4	0

EXAMPLE 4.7. The identity mapping is a complete mapping of the non-abelian group of order 21. It gives rise to a $(K, 1)$ complete mapping, where $K = \{3, 3, 2, 2, 2, 2, 2, 2, 2\}$, and hence to a neofield of order 22. (See Theorem 3.4, Corollary 2).

We have $G = \mathrm{gp}\{a, b\colon a^7 = b^3 = e,\ ab = ba^2\}$ and the $(K, 1)$ complete mapping is

$$(a\,a^2\,a^4)(a^3\,a^6\,a^5)(b\,b^2)(ba\,b^2a^3)(ba^2\,b^2a^6)$$
$$(ba^3\,b^2a^2)(ba^4\,b^2a^5)(ba^5\,b^2a)(ba^6\,b^2a^4).$$

The complete addition table of the neofield is given in Table 1. The reader may check that the right distributive law holds.

EXAMPLE 4.8. The (3, 1) near complete mapping

$$[e\,ba^3](a^2\,a\,a^4)(a^3\,ba\,ba^5)(a^6\,ba^6\,b)(a^5\,ba^2\,ba^4)$$

of the dihedral group $D_7 = \mathrm{gp}\{a, b\colon a^7 = b^2 = e,\ ab = ba^{-1}\}$ defines a left neofield of order 15 and characteristic 3. Its presentation function is

z	0	1	a	a^2	a^3	a^4	a^5	a^6	b	ba	ba^2	ba^3	ba^4	ba^5	ba^6
$\phi(z)$	1	ba^3	a^4	a	ba	a^2	ba^2	ba^6	a^6	ba^5	ba^4	0	a^5	a^3	b

REFERENCES

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

[2] R. J. Friedlander, B. Gordon and M. D. Miller, *On a group sequencing problem of Ringel*, Proc. Ninth S.E. Conf. on Combinatorics, Graph Theory and Computing. Florida Atlantic Univ., Boca Raton, 1978. (Congressus Numerantium XXI, Utilitas Math., 1978), pages 307–321.

[3] R. J. Friedlander, B. Gordon and P. Tannenbaum, *Partitions of groups and complete mappings*, Pacific J. Math., **92** (1981), 283–293.

[4] B. Gordon, *Sequences in groups with distinct partial products*, Pacific J. Math., **11** (1961), 1309–1313.

[5] G. B. Hoghton and A. D. Keedwell, *On the sequenceability of dihedral groups*, Annals of Discrete Math., **15** (1982), 259–264.

[6] D. F. Hsu, *Cyclic Neofields and Combinatorial Designs*, (Springer-Verlag, 1980, Lecture Notes in Mathematics, No. 824.)

[7] E. C. Johnsen and T. Storer, *Combinatorial structures in loops II. Commutative inverse property cyclic neofields of prime power order*, Pacific J. Math., **52** (1974), 115–127.

[8] A. D. Keedwell, *On property D neofields*, Rend. Mat. e Appl., (5) **26** (1967), 383–402.

[9] _____, *On the sequenceability of non-abelian groups of order pq*, Discrete Math., **37** (1981), 203–216.

[10] ______, *On R-sequenceability and R_h-sequenceability of groups*, Atti del Convegno Internazionale Geometrie Combinatorie e Loro Applicazioni, Roma, 7–12 Giugno, 1981. Annals of Discrete Math., **18** (1983), 535–548.

[11] H. B. Mann, *The construction of orthogonal latin squares*, Ann. Math. Statist., **12** (1942), 418–423.

[12] L. J. Paige, *A note on finite abelian groups*, Bull. Amer. Math. Soc., **53** (1947), 590–593.

[13] ______, *Neofields*, Duke Math. J., **16** (1949), 39–60.

Received May 3, 1982. The work of the first author was supported in part by Fordham University Faculty Research Grant #071225.

FORDHAM UNIVERSITY
BRONX, NY 10458
U.S.A.

AND

UNIVERSITY OF SURREY
GUILDFORD, SURREY, GU2 5XH
ENGLAND