DEMONSTRATIO MATHEMATICA
Vol. XXIV No 1-2 1991

A.D. Keedwell

# PROPER LOOPS OF ORDER n IN WHICH EACH NON-IDENTITY ELEMENT HAS LEFT ORDER n

When a latin square of order n is bordered by its own first row and first column, it becomes the multiplication table of a loop. Each column of the latin square may be regarded as a permutation of its first column. If each of these permutations consists of a single cycle of length n, this is equivalent to saying that each non-identity element of the loop has left-order n.

In the development of an idea for enumerating latin squares which was originally suggested by P.A. MacMahon, the question arose as to whether, when n is a prime p, a loop with the above property is necessarily isotopic to the cyclic group of order p.

In [4], it was shown that, for all $p \geq 7$, the answer is in the negative; and moreover that, for all positive integers $n \geq 7$, proper loops with every non-identity element of order n can quite easily be constructed. Here, we present a more elegant (and more algebraic) proof for the case when n is odd using the concept of a left-neofield.

First we dispose of the case when n is even and greater than 7. Tillson [7] has given a constructive method for separating the complete directed graph $K^*_{2m}$ on $n = 2m$ vertices into $2m-1$ disjoint Hamiltonian circuits for all $m \geq 4$. If we label the vertices of $K^*_{2m}$ with the integers $0,1,2,\ldots,2m-1$, these $2m-1$ Hamiltonian circuits define $2m-1$ discordant permutations each consisting of a single cycle of length $2m$. Since a group of even order contains at least one element of order 2 and since each loop isotopic to a group is isomorphic

to that group, a loop defined by permutations of order 2m cannot be group-isotopic and so we have a solution to our problem for even n.

When n is odd, our method is to a sequencing of the cyclic group of even order n-1 to construct a cyclic neofield of characteristic n. If the sequencing is chosen suitably, the addition loop of the neofield is not a group (provided that $n \geq 7$) and so we have a solution to our problem for odd n.

We shall require the following two definitions.

**Definition 1.** Let $(G,\cdot)$ be a finite group of order n and suppose that the elements $a_0,a_1,a_2,\ldots,a_{n-1}$ of G can be arranged in a sequence in such a way that the partial products $b_0=a_0=e$ (the identity element), $b_1=a_0a_1$, $b_2=a_0a_1a_2,\ldots,b_{n-1}=a_0a_1\ldots a_{n-1}$ are all different. The group $(G,\cdot)$ is then said to be sequenceable ([5], page 85).

**Definition 2.** A left-neofield $(N,+,\cdot)$ is an algebraic system comprising a set N on which two binary operations $(+)$ and $(\cdot)$ are defined such that

(i) $(N,+)$ is a loop, with identity element 0 say;

(ii) $(N\setminus\{0\},\cdot)$ is a group; and

(iii) $x(y+z)=xy+xz$ for all $x,y,z\in N$.

**Theorem 1.** Let $(G,\cdot)$ be a finite sequenceable group of n-1 elements with identity element denoted by 1. Let 0 be a symbol not in the set G and define $N=G\cup\{0\}$. Then we can construct a left neofield $(N,+,\cdot)$ of order and characteristic n. That is, each non-identity element of the loop $(N,+)$ has left-order n.

**Proof.** Let $a_0=1,a_1,a_2,\ldots,a_{n-1}$ be the sequencing of $(G,\cdot)$ with partial products $b_0=a_0$, $b_1=a_0a_1$, $b_2=a_0a_1a_2,\ldots$, $b_{n-1}=a_0a_1\ldots a_{n-1}$. Then the mapping $\theta : b_i \longrightarrow b_i^{-1}b_{i+1}=a_{i+1}$ for $i=0,1,\ldots,n-2$ is a near complete mapping of $(G,\cdot)$ (see Definition 4). If $\phi(g) = g\theta(g)$ for each $g\in G$, then $\phi : b_i \longrightarrow b_{i+1}$ for $i=0,1,\ldots,n-2$.

We define addition in N by the statement that $g+1=\phi(g)$

for each $g\in G$ except $b_{n-1}$. Also, $b_{n-1}+1=0$ and $0+1=1$. Further, for all $x,y\in N$,

$x+y=y(y^{-1}x+1)=y\phi(y^{-1}x)$ if $y\neq 0$ or $xb_{n-1}^{-1}$;

$=x\theta(y^{-1}x)$.

It is evident that $(N\setminus\{0\},\cdot)\cong(G,\cdot)$ and so is a group. Also, the validity of the left distributive law is a consequence of the definition of $x+y$, since

$$zx+zy = zy[(zy)^{-1}zx+1] = zy(y^{-1}x+1) = z(x+y).$$

It remains to show that $(N,+)$ is a loop: that is, its Cayley table must be a latin square. Now, the values of $y\phi(y^{-1}x)$ are all distinct and different from y or 0 as x varies through the elements of N distinct from 0 and $yb_{n-1}$. When $x=0$, we have defined $x+y=0+y=y(0+1)=y$; and, when $x=yb_{n-1}$, we have $x+y=y(b_{n-1}+1)=0$. Thus, the elements of each column of the addition table of $(N,+)$ are distinct. Also, the values of $x\theta(y^{-1}x)$ are all distinct and different from x or 0 as y varies through the elements of N distinct from 0 and $xb_{n-1}^{-1}$. When $y=0$, we have $x+y=x+0=x$ and when $y=xb_{n-1}^{-1}$, we have $x+y=xb_{n-1}^{-1}(b_{n-1}+1)=0$. So, the elements of each row of the addition table of $(N,+)$ are all distinct. We conclude that $(N,+,\cdot)$ is a left-neofield.

Since $1+1=\phi(1)=b_1$ and $\phi(b_i)=b_{i+1}$ for $i=0,1,\ldots,n-2$, we find that the sum of $n-1$ 1's is $[\{(1+1)+1]+\ldots=b_{n-1}$. Hence, the sum of n 1's is $b_{n-1}+1=0$. From the left distributive law, each element of $(N,+,\cdot)$, except 0, has additive order n. This completes the proof.

It remains to choose the sequencing suitably so that the addition loop of the neofield is not a group. We use the following sequencing of the cyclic group $C_{2m}=\langle\alpha:\alpha^{2m}=1\rangle$:

$$1,\alpha,\alpha^{2m-2},\alpha^{3},\alpha^{2m-4},\alpha^{5},\alpha^{2m-6},\ldots,\alpha^{2m-3},\alpha^{2},\alpha^{2m-1}.$$

The mapping $\phi$ given by the partial products is then

$$\phi = [1\ \alpha\ \alpha^{2m-1}\ \alpha^{2}\ \alpha^{2m-2}\ \alpha^{3}\ \alpha^{2m-3}\ \alpha^{4}\ \ldots\ \alpha^{m-1}\ \alpha^{m+1}\ \alpha^{m}],$$

where the image of $\alpha^m$ is undefined.

Because $C_{2m}$ is abelian, the right distributive law holds and so we get a cyclic neofield of order $2m+1$ whose addition table is exhibited in Figure 1.

| | 0 | 1 | $\alpha$ | ... | ... | ... | $\alpha^{2m-1}$ |
|---|---|---|---|---|---|---|---|
| 0 | $\underline{0}$ | $\underline{1}$ | $\alpha$ | ... | ... | ... | $\alpha^{2m-1}$ |
| $\alpha^m$ | $\underline{\alpha^m}$ | $\underline{0}$ | $\underline{\alpha^{m+2}}$ | | | | $\alpha^{m-1}$ |
| $\alpha^{m+1}$ | $\alpha^{m+1}$ | $\underline{\underset{\sim}{\alpha^m}}$ | $\underline{0}$ | | | | $\alpha^{m-2}$ |
| . | . | . | . | | | | . |
| . | . | . | . | | | | . |
| $\alpha^{2m-1}$ | $\alpha^{2m-1}$ | $\alpha^2$ | $\alpha^4$ | | | | . |
| 1 | 1 | $\alpha$ | $\alpha^3$ | | | | . |
| $\alpha$ | $\alpha$ | $\alpha^{2m-1}$ | $\alpha^2$ | | | | . |
| $\alpha^2$ | $\alpha^2$ | $\alpha^{2m-2}$ | 1 | | | | . |
| . | . | . | . | | | | . |
| . | . | . | . | | | | . |
| $\alpha^{m-1}$ | $\alpha^{m-1}$ | $\alpha^{m+1}$ | $\alpha^{m+3}$ | | | | 0 |

Figure 1.

We observe that $0+0=\alpha^m+1$, $\alpha^m+0=\alpha^{m+1}+1$, $\alpha^m+1=\alpha^{m+1}+\alpha$ but $0+1\neq\alpha^m+\alpha$ except when $m=2$, since $1=\alpha^{m+2}$ implies that $m=2$. Thus, for all $m>2$, the quadrangle criterion is not satisfied by the quadrangles marked in Figure 1 and so we have a proper loop of order $2m+1$ with each non-identity element of order $2m+1$.

**Remark (1).** Note that the group $(G,\cdot)$ used in Theorem 1 can be any sequenceable group, not necessarily a cyclic group. The theory of sequenceable groups is still in its infancy but it is known that several infinite classes of groups are sequenceable such as the cyclic groups of even order, the dicyclic groups and the non-abelian groups of order pq, where p, q are distinct primes such that $p<q$ and 2 is a primitive root of p. The most recent major work on this topic has been

done by B.A. Anderson (see, for example [1] and [2]). Not all of this work has yet been published but a full account of present knowledge will be included in a forthcoming book by J. Dénes and the present author.

**Remark (2).** The construction described in Theorem 1 above is a special case of a more general construction due to D.F. Hsu and the present writer (see [6]) which establishes a one-to-one correspondence between left neofields based on a given group $(G,\cdot)$ and certain kinds of mappings of that group called orthomorphisms and near-orthomorphisms in canonical form. We shall describe this briefly.

**Definition 3.** Let $(G,\cdot)$ be a finite group. A complete mapping of $(G,\cdot)$ is a permutation $\theta$ of G such that the mapping $\phi : x \longrightarrow x\theta(x)$ is another permutation of G ([5], page 28). The mapping $\phi$ is called an orthomorphism of $(G,\cdot)$.

A finite group which has a complete mapping is called admissible ([3], page 115). A complete mapping (or orthomorphism) is in canonical form if $\theta(e)=e$, where e is the identity element of $(G,\cdot)$.

**Definition 4.** A near-complete mapping (in canonical form) of a finite group $(G,\cdot)$ is a one-to-one mapping $\theta$ from the set $G\backslash\{g\}$, where g is some non-identity of G called the exdomain element, onto the set $G\backslash\{e\}$, where e is the identity element of G, such that the mapping $\phi : x \longrightarrow x.\ \theta(x)$ is a mapping of the same kind. The mapping $\phi$ is called a near-orthomorphism of $(G,\cdot)$.

**Example** ([6], page 331). The mapping

$$\theta = \begin{pmatrix} e & a & a^2 & a^3 & a^4 & a^5 & a^6 & b & ba & ba^2 & ba^3 & ba^4 & ba^5 & ba^6 \\ ba^3 & a^3 & a^6 & ba^4 & a^5 & b & ba^5 & ba^6 & a^4 & a^2 & . & ba^2 & ba & a \end{pmatrix}$$

is a near-complete mapping of the dihedral group $D_7=\langle a,b : a^7=b^2=e,\ ab=ba^{-1}\rangle$.

The corresponding near-orthomorphism can be written in semi-cyclic form as follows:

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

In [6], it is proved that "there is a one-to-one correspondence between left neofields based on a group $(G,\cdot)$ and orthomorphisms and near-orthomorphisms of $(G,\cdot)$. Each left neofield for which $1+1=0$ corresponds to an orthomorphism of $(G,\cdot)$ and each left neofield for which $1+1\neq 0$ corresponds to a near-orthomorphism; and conversely."

If each element of the additive loop of a left neofield for which $1+1\neq 0$ has the same left-order k, then the neofield is said to have characteristic k. This includes and generalizes the concept of characteristic of a Galois field). Our example above gives rise to a left neofield of order 15 and characteristic 3 based on the dihedral group $D_7$.

## REFERENCES

[1] B.A. Anderson: Sequencings of dicyclic groups, Ars Combinatoria 23 (1987), 131-142.

[2] B.A. Anderson: $S_5$, $A_5$ and all non-abelian groups of order 32 are sequenceable, Congressus Numerantium 58 (1987), 53--68.

[3] V.D. Belousov: Basic theory of quasigroups and loops. Moscow, 1967. (in Russian).

[4] J. Dénes, A.D. Keedwell: Latin squares and one-factorizations of complete graphs: (II) Enumerating one-factorizations of the complete directed graph $K_n^*$ using MacMahon's double partition idea, Utilitas Math. 34 (1988), 73-83.

[5] J. Dénes, A.D. Keedwell: Latin squares and their applications. Akadémiai Kiadó, Budapest /English Universities Press, London/ Academic Press, New York, 1974.

[6] D.F. Hsu, A.D. Keedwell: Generalized complete mappings, neofields, sequenceable groups and block designs I, Pacific J. Math. 111 (1984) 317-332.

[7] T.W. Tillson: A Hamiltonian decomposition of $K_{2m}^*$, $2m\geq 8$, J. Combinatorial Theory B 29 (1980) 68-74.

**Added in proof**

(1) Since this paper was written (in 1989), P.J. Owens and D.A. Preece have shown that, for certain prime orders of the form 8k+3, there exist latin squares with much more remarkable properties than those constructed in the above paper as examples of loops with every element of left order n. Not only do the Owens/Preece squares have the required property that each column (except the first), when regarded as a permutation of the first column, consists of a single cycle but also they have the much stronger property that, for every pair of positive integers r, s with $0<r<s\leq n$, the sth column, when regarded as a permutation of the rth column, consists of a single cycle. Moreover, because the Owens/Preece squares are symmetric, they have the same remarkable property with respect to every pair of distinct rows.

Owens conjectures that squares of this kind exist for all prime orders of the form 8k+3 but also so far examples have been constructed only for the orders 11, 19 and 43.

(2) In Remark (1), we referred to a forthcoming book. This has now been published as Annals of Discrete Mathematics, Volume 46, 1991.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SURREY, GUILDFORD SURREY GU25XH, ENGLAND.

Received June 27, 1989.