ON THE SINGER 1-PERMUTATION

A. Hedayat
Cornell University

Abstract

This paper gives a simple method of constructing a linear set of
directrices of the n-sided Latin square $A = (a_{ij})$ whose rows are the
successive cyclic permutations of the integers 0, 1, ..., n-1, so that
$a_{ij} = i + j \pmod{n}$. Therefore it gives a lower bound on the total
number $N(n)$ of directrices which $A$ contains.

Paper No. BU-176 in the Biometrics Unit series, and No. 572 in the
Department of Plant Breeding and Biometry.
ON THE SINGER 1-PERMUTATION
A. Hedayat
Cornell University

0. Summary

This paper gives a simple method of constructing a linear set of directrices of the n-sided Latin square $A = (a_{ij})$ whose rows are the successive cyclic permutations of the integers $0,1,\ldots,n-1$, so that $a_{ij} \equiv i + j \pmod{n}$. Therefore it gives a lower bound on the total number $N(n)$ of directrices which $A$ contains.

1. Introduction

An $n$-sided Latin square (L.sq.) is an arrangement of $n$ distinct symbols into an $n \times n$ matrix $B = (b_{ij})$ in such a way that no row and no column contains any symbol twice. Two $n$-sided L.sqs. $B = (b_{ij})$, $C = (c_{ij})$ are mutually orthogonal if the $n^2$ ordered pairs $(b_{ij}, c_{ij})$ are all distinct. A set $\{A_1, A_2, \ldots, A_t\}$ of $n$-sided L.sqs. is called orthogonal if $A_i$ and $A_j$ are orthogonal for all $i \neq j$. It is easy to see that $t \leq n-1$. If $n$ is a power of a prime, then it is well known that there exists a set of $n-1$ mutually orthogonal L.sqs.
A collection of n cells in an n-sided L.sq. such that no row and no column contains two cells of the collection, and no two cells of the collection contain the same symbol is called a directrix\(^1\) \((d)\) of the L.sq. Two directrices are said to be parallel if they have no cell in common. A set \(\{d_1, d_2, \ldots, d_r\}\) of directrices of a L.sq. is called a linear set if \(d_i\) and \(d_j\) are either parallel or they have only one cell in common for \(i \neq j\). We denote such a set by \(L\).

We define the arithmetic function \(N(n)\) to be the total number of directrices which a given n-sided L.sq. contains.

2. The Problem

Let \(A = (a_{ij})\) be the n-sided L.sq. whose rows are the successive cyclic permutations of the integers \(0, 1, \ldots, n-1\) so that \(a_{ij} \equiv i + j \pmod{n}\). The Singer problem [3] can be stated as follows: Given \(n\), what is the value of \(N(n)\) for \(A\). Singer [3] has easily shown that

\[N(n) = 0 \text{ if } n \equiv 0 \pmod{2}.\]

For \(n \equiv 1 \pmod{2}\) Singer [3] gives the following values, \(N(1) = 1, N(3) = 3, N(5) = 15, N(7) = 133, N(9) = 2025,\)

\(^1\) Some writers prefer to call such a collection a transversal or a \(1\)-permutation. But for the historical reasons, we prefer to use the term directrix.
N(ll) = 37,851, and in an effort to shed some light on the values of \( N(n) \) for large values of \( n \) he has related the problem to a special group \( \mathcal{G} \) of order \( 6n^2\varphi(n) \), where \( \varphi(n) \) is the familiar Euler \( \varphi \)-function.

In this paper, we give an explicit method of constructing a non-empty linear set of directrices for all \( n \equiv 1 \pmod{2} \) and hence a lower bound (obviously crude for large \( n \)) on the values of \( N(n) \). The construction to be presented relies on an appreciation of orthogonal L.sqs.

3. **Group Solution of the Problem**

Consider for each positive integer \( n \) an abstract group \( G \) of order \( n \). Let \( \Omega \) be the collection of all one-to-one mappings of \( G \) into itself.

**Definition 1.** Two maps \( \alpha \) and \( \beta \) in \( \Omega \) are said to be orthogonal if for any \( g \in G \),

\[
(\alpha z)\#(\beta z)^{-1} = g
\]

has a unique solution \( z \in G \).

**Definition 2.** A non-empty subset \( \omega \) of \( \Omega \) is said to be a mutually orthogonal subset (m.o.sub.) if any two nonidentical maps of \( \omega \) are orthogonal.
**Definition 3.** A m.o.sub. \( w^* \) of \( \Omega \) is said to be a maximal mutually orthogonal subset (m.m.o.sub.) if the number of maps in \( w^* \) is at least as large as the number of maps in \( H \), for any other m.o.sub.

**Remark.** The identification of \( w^* \) is an unsolved problem at the present, except when the order of \( G \) is a power of a prime.

Let \( L(\cdot) \) be an n x n square. We make a one-to-one correspondence between the rows of \( L(\cdot) \) and the elements of \( G \). Thus, by row \( x \) we shall mean the row corresponding to the element \( x \) in \( G \). Similarly we make a one-to-one corresponding between the columns of \( L(\cdot) \) and the elements of \( G \). The cell of \( L(\cdot) \) which occurs in the intersection of row \( x \) and column \( y \) is called the cell \( (x,y) \).

**Lemma 1.** ([1],[2]). Let \( \alpha \in \Omega \). Put in the cell \( (x,y) \) of \( L(\cdot) \) the element \( (\alpha x)^*y \) of \( G \). Call the resulting square \( L(\alpha) \). Then \( L(\alpha) \) is a L.sq.

**Lemma 2.** ([1],[2]). If \( \alpha \) and \( \beta \) are in \( \Omega \). Then \( L(\alpha) \) and \( L(\beta) \) form a pair of orthogonal L.sqs. if and only if \( \alpha \) and \( \beta \) are orthogonal.
Remark. Since there are at most $n-1$ L.sqs. in any set of orthogonal L.sqs of side $n$, it is obvious by lemma 2 that the number of maps in any m.m.o.sub. $w^*$ is at most $n-1$, where $n$ is the order of $G$.

In the sequel, for a given $n$, we restrict $G$ to be the set $\{0,1,\cdots,n-1\}$ with addition (mod $n$) as the binary operation. We also suppose the standard order of taking the elements of $G$ to be $0,1,\cdots,n-1$. In addition, let $I$ denote the identity map in $G$, i.e.

$$I(i) = i, \quad i=0,1,\cdots,n-1$$

Lemma 3. If $n > 2$ and if

$$n = p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}$$

is the prime decomposition of $n$, then $2I,3I,\cdots,(p_m-1)I$ all belong to $\Omega$, where

$$p_m = \min(p_1,p_2,\cdots,p_r).$$

Proof. Suppose there exist $i \leq p_m-1$ such that $iI \notin \Omega$. Then this implies that there exists $x$ and $y$ in $G$ such that $x \neq y$ but
ix \equiv iy \pmod{n}.

Since i and n are relatively prime this implies that \( x \equiv y \pmod{n} \) and consequently \( x = y \), which is a contradiction.

Q.E.D.

**Theorem 1.** Let \( n \) be the same as in lemma 3. Then L.sqs. \( L(I), L(2I), \ldots \) \( L((p_m - 1)I) \) are mutually orthogonal.

**Proof.** Let \( S = \{I, 2I, \ldots, (p_m - 1)I\} \). Then by lemma 3, \( S \subseteq \Omega \). Hence by lemma 1, \( L(I), L(2I), \ldots, L((p_m - 1)I) \) are L.sqs. Now it is sufficient to prove that \( S \) is a m.o.sub. or we have to show that for any \( \alpha \) and \( \beta \) in \( S \),

\[
(1) \quad (\alpha z) \ast (\beta z) = g
\]

has a unique solution \( z \) in \( G \). With respect to the operation in our new \( G \) equation (1) becomes

\[
\alpha z - \beta z = g
\]
or

\[
(\alpha - \beta)z = g.
\]
Equivalently, we have to prove that $\alpha - \beta \in \Omega$. But this is true, since if $\alpha = kI$ and $\beta = \ell I$ ($k > \ell$ without loss of generality), then

$$\alpha - \beta = (k-\ell)I.$$

Since $k \leq p_m - 1$, $\ell \leq p_m - 1$, $k \neq \ell$ it is clear that $(k-\ell)I$ belongs to $S$ and hence belongs to $\Omega$.

Q.E.D.

Remark. Note that $L(I) = A$ as was defined in section 2.

Theorem 2. Let $n$ be the same as in lemma 3. Then there exists for $L(I) = A$ a linear set $L$ with $n(p_m - 2)$ elements. Hence $n(p_m - 2)$ is a lower bound on $N(n)$.

Proof. By construction. By theorem 1, $A = L(I), L(2I), \ldots, L((p_m - 1)I)$ are mutually orthogonal. Now consider the cells in $L(kI)$, $k \neq 1$, which contain the same integer "i". Then the corresponding cells of $L(I)$ form a directrix of $L(I)$, since $L(I)$ and $L(kI)$ are orthogonal. Since "i" and "k" can take $n$ and $p_m - 2$ distinct values respectively, we can exhibit $n(p_m - 2)$ directrices for $A$. In addition, these directrices are either parallel or have one cell in common, since $A = L(I), L(2I), \ldots, L((p_m - 1)I)$ are mutually orthogonal.
Remark. For $n = 3, 5$ the above procedure gives the exact values of $N(n)$ which have been computed by Singer [3].

Example. Let $n = 3$, then

$$
A = L(I) = \begin{pmatrix}
0 & 1 & 2 \\
1 & 2 & 0 \\
2 & 0 & 1
\end{pmatrix}, \quad L(2I) = \begin{pmatrix}
0 & 1 & 2 \\
2 & 0 & 1 \\
1 & 2 & 0
\end{pmatrix}.
$$

Then the cells

$(0,0), (1,1), (2,2)$ form a directrix of $A$ associated with $0$ of $L(2I)$,

$(0,1), (1,2), (2,0)$ form a directrix of $A$ associated with $1$ of $L(2I)$, and

$(0,2), (1,0), (2,1)$ form a directrix of $A$ associated with $2$ of $L(2I)$.

References

