Simplified method of construction of a complete set of MOLS

Prof. G. C. Bhimani[1] & Manisha H. Dave[2]
[1]Department of Statistics,Saurashtra University, Rajkot (Gujarat);
[2]M.K Amin Arts and Science college and college of commerce, Padra,
The Maharaja Sayajirao University, Baroda (Gujarat).

Received: May 13, 2018 Accepted: June 19, 2018

ABSTRACT *A complete set of MOLS(s) exists if s is p^n ; p is a prime number and n≥1 is an integer. Various methods of construction of a complete set of MOLS(s) have been discussed earlier. Here we discuss the algebraic method of construction of a complete set of MOLS(s) and its simplification with illustration.*

Keywords: *Prime number, Complete set of MOLS, Algebraic method, Primitive root, Element, Index.*

Introduction

We know that a complete set of MOLS(s) exists if s is p^n ; p is a prime number and n≥1 is an integer. To construct a complete set of MOLS(s) various methods are given by researchers. Here we discuss the algebraic method of construction of a complete set of MOLS(s) and its simplification with illustration. We also illustrate the saving in calculations and time due to the simplification.

Algebraic method

Let $s=p^n$; p is a prime number and n≥1 is an integer.
Obtain elements of GF (s):
a). Let n = 1 i.e. s is a prime number. Then
A complete set of incongruent residue mod p constitute elements of GF(s).
Hence elements of GF(s) are 0, 1, 2 . . . s-1. s We write them in standard order as
$\alpha_0=0, \alpha_1=1, \alpha_2=x, \alpha_3=x^2, \ldots, \alpha_{s-1}=x^{s-2}$, where x is a primitive root (p.r.) of GF (s).
Note that $x^{s-1}=1$.
b). Let n > 1 i.e. s is a prime power. Then
A complete set of incongruent residue mod minimum function of GF (p^n) constitute elements of GF(s= p^n).
Write them in a standard order as $\alpha_0=0, \alpha_1=1, \alpha_2=x, \alpha_3=x^2, \ldots, \alpha_{s-1}=x^{s-2}$, where x is a primitive root (p.r.) of GF (s). Note that $x^{s-1}=1$.
Now denote row and column numbers of an s × s square as 0, 1, 2, … s-1**.** There are two different approaches for the algebraic methods which are slightly different. We denote them as approaches A and B.

Approach A.
$(r,t)^{th}$ cell element of an s × s square L_i is **filled up by the index of the element/or the element**

$$\alpha_i\alpha_r + \alpha_t \ , i= 1, 2, \ldots s-1 \ ; r,t = 0, 1, 2, \ldots, s-1.$$

Approach B.
$(r,t)^{th}$ cell element of an s × s square L_i is **filled up by the indexof the element/or by the element**

$$\alpha_r+\alpha_i\alpha_t \ , i= 1, 2, \ldots s-1 \ ; r,t = 0, 1, 2, \ldots, s-1.$$

By these approaches, to obtain a complete set of MOLS(s) we have to obtain $s^2(s-1)$ cell elements of s-1 latin squares. The task is laborious and time consuming. Therefore we need simplification leading to reduction in time in the construction of a complete set of MOLS(s).

Simplification in the algebraic method

1. Consider $(r,t)^{th}$ cell element of L_1 by methods A and B.

By Approach A, $(r,t)^{th}$ cell element of L_1,

$$= \alpha_1\alpha_r + \alpha_t$$
$$= \alpha_r + \alpha_t \quad (\because \alpha_1=1) \qquad (1)$$

By Approach B, $(r,t)^{th}$ cell element of L_1,

$$= \alpha_r+\alpha_1\alpha_t$$
$$= \alpha_r + \alpha_t \quad (\because \alpha_1=1) \qquad (2)$$

From (1) and (2), it is clear that by both approaches A and B, obtained $(r,t)^{th}$ cell element of L_1 is same for ∀ r and t.

$\Rightarrow$ Approaches A and B give us same L_1.

2. Consider $(r,t)^{th}$ cell element of i^{th} LS L_i of a complete set of MOLS of order s.

$(r,t)^{th}$ cell element of L_i by Approach A

$$= \alpha_1\alpha_r + \alpha_t$$
$$= x^{i-1}\, x^{r-1} + x^{t-1}$$
$$= x^{i}\, x^{r-2} + x^{t-1}$$
$$= \alpha_{i+1}\, \alpha_{r-1} + \alpha_t$$
$$= (r\text{-}1,t)^{th} \text{ cell element of } L_i$$

$\Rightarrow \forall$ t, r^{th} row of L_i is same as $(r-1)^{th}$ row of L_{i+1} (3)

Consider $(1,t)^{th}$ cell element of i^{th} LS L_i of a complete set of MOLS of order s.

$(1,t)^{th}$ cell element of L_1

$$= \alpha_i\, \alpha_1 + \alpha_t$$
$$= x^{i-1} \cdot 1 + x^{t-1}$$
$$= x^{i-1} \cdot x^{s-1} + x^{t-1} \qquad \text{x being p.r. of GF (s)}$$
$$= x^{i} \cdot x^{s-2} + x^{t-1}$$
$$= \alpha_{i+1}\, \alpha_{s-1} + \alpha_t$$
$$= (s\text{-}1,t)^{th} \text{ cell element of } L_{i+1}$$

$\Rightarrow \forall$ t, 1^{st} row of L_i is same as last row of L_{i+1}. (4)

From (3) and (4), it is clear that

i. Keep zeroth row fixed,
ii. r^{th} row of $L_i = (r-1)^{th}$ row of L_{i+1}
iii. 1^{st} row of $L_i = (s-1)^{th}$ row of L_{i+1}

Summary. (a). Keep zeroth row fix. Now as proved above, by cyclic permutation of rows of L_i, we get L_{i+1}, i = 1,2,….,s-1.

Thus, having obtained L_1, we can easily obtain a complete set of MOLS by cyclic permutation of rows as under:

L_2 from L_1
L_3 from L_2
L_4 from L_3
...
...
L_{s-1} from L_{s-2}

(b). OR we can obtain L_2, L_3, … L_{s-1} from L_1 as follows:
Having obtained L_1, where zeroth row is in natural order; L_i can obtained by i - step cyclic permutation of rows of L_1, i= 2, 3, … s-1. Note that zeroth row of L_i is same as L_1.
(c). This method is applicable to both LS's obtained by filling index of the element or by filing the element.

Note that by above simplification we need to obtain only L_1, that is we need to obtain only s^2 cell elements instead $s^2(s-1)$ entries. Thus we save labour and time of obtaining $s^2(s-1) - s^2 = s^2(s-2)$ cell elements. If s = 9, then we save time and labour of obtaining 567 cell elements, a tremendous reduction.

llustrations

Approach A: $s=9=3^2$.

GF(3) = 0, 1, 2.

Minimum function of GF (9) is $x^2 + x + 2$.

GF (9) : $\alpha_0=0$, $\alpha_1=1$, $\alpha_2=x$, $\alpha_3=x^2=2x+1$, $\alpha_4=x^3=2x+2$, $\alpha_5=x^4=2$, $\alpha_6=x^5=2x$, $\alpha_7=x^6=x+2$, $\alpha_8=x^7=x+1$

Illustation 1.

Let $(r,t)^{th}$ cell element of an s × s square L_1 is filled up by the element

$\alpha_1\, \alpha_r + \alpha_t$, i= 1, 2, … s-1 ; r,t = 0, 1, 2, … , s-1.

L_1 - Element filling

	$\alpha_0=0$	$\alpha_1=1$	$\alpha_2=x$	$\alpha_3=x^2=2x+1$	$\alpha_4=x^3=2x+2$	$\alpha_5=x^4=2$	$\alpha_6=x^5=2x$	$\alpha_7=x^6=x+2$	$\alpha_8=x^7=x+1$
$\alpha_0=0$	0	1	x	2x+1	2x+1	2	2x	x+2	x+1
$\alpha_1=1$	1	2	x+1	2x+2	2x	0	2x+1	x	x+2
$\alpha_2=x$	X	x+1	2x	1	2	x+2	0	2x+2	2x+1
$\alpha_3=x^2=2x+1$	2x+1	2x+2	1	x+2	X	2x	x+1	0	2
$\alpha_4=x^3=2x+2$	2x+2	2x	2	x	x+1	2x+1	x+2	1	0
$\alpha_5=x^4=2$	2	0	x+2	2x	2x+1	1	2x+2	x+1	x
$\alpha_6=x^5=2x$	2x	2x+1	0	x+1	x+2	2x+2	x	2	1
$\alpha_7=x^6=x+2$	x+2	x	2x+2	0	1	x+1	2	2x+1	2x
$\alpha_8=x^7=x+1$	x+1	x+2	2x+1	2	0	x	1	2x	2x+2

Illustration 2

Let $(r,t)^{th}$ cell element of an s × s square L_1 is filled up by the index of

$\alpha_1\alpha_r + \alpha_t$, i= 1, 2, ... s-1 ; r,t = 0, 1, 2, ... , s-1.

L_1 - Index filling

	$\alpha_0=0$	$\alpha_1=1$	$\alpha_2=x$	$\alpha_3=x^2=2x+1$	$\alpha_4=x^3=2x+2$	$\alpha_5=x^4=2$	$\alpha_6=x^5=2x$	$\alpha_7=x^6=x+2$	$\alpha_8=x^7=x+1$
$\alpha_0=0$	0	1	2	3	4	5	6	7	8
$\alpha_1=1$	1	5	8	4	6	0	3	2	7
$\alpha_2=x$	2	8	6	1	5	7	0	4	3
$\alpha_3=x^2=2x+1$	3	4	1	7	2	6	8	0	5
$\alpha_4=x^3=2x+2$	4	6	5	2	8	3	7	1	0
$\alpha_5=x^4=2$	5	0	7	6	3	1	4	8	2
$\alpha_6=x^5=2x$	6	3	0	8	7	4	2	5	1
$\alpha_7=x^6=x+2$	7	2	4	0	1	8	5	3	6
$\alpha_8=x^7=x+1$	8	7	3	5	0	2	1	6	4

From $L_1(9)$ obtained above either by filling the element or the index of the element, the rest 8 LSs from a complete set can be obtained by the simplification methods discussed above . thus there is saving of time and labour of obtaining 81 x 7 = 567 = $s^2(s-2)$.

In Approach B, there is column permutation instead roe permutation.

References

1. Damaraju Raghavarao, 1988. Constructions and Combinatorial Problems in Design of Experiments (corrected reprint of the 1971 John Wiley Series in Probability and mathematical statistics). New York: Dover. ISBN 0-486-65685-3. MR 1102899.
2. Dwivedi Lokesh, Mutually orthogonal latin squares and their uses. I.A.S.R.I., Library Avenue, New Delhi