#### Mutually Orthogonal Quasigroup System and MOLS

#### Tomoko Adachi Shizuoka Institute of Science and Technology

*E-mail:* adachi.tomoko@sist.ac.jp

**Abstract** Restricted to a binary operator, quasigroups and Latin squares are equivalent. MOLS stands for mutually orthogonal Latin squares. In this paper, we describe about mutually orthogonal quasi-group system and MOLS.

#### 1 Introduction

A quasigroup with a binary operator is equivalent to a Latin square. That is, there exists a bijection between the set of all quasigroups of order q with binary operators and the set of all Latin squares with a size of  $q \times q$ .

Mutually orthogonal Latin squares are written abbreviated as MOLS. For quasigroups with binary operators, a mutually orthogonal quasigroup system is equivalent to MOLS.

Much research has been done on Latin squares and MOLS. But few research has been done on quasigroups with *n*-ary operators. Especially, in the case of  $n \geq 3$ , very few research has been done.

In this paper, we research for the definitions and property related to quasigroups with n-ary operators, and we describe about mutually orthogonal quasigroup system.

### 2 Definitons and property for Latin squares

We suggest that readers who wish to learn more about the definitions and property related to Latin squares discussed in this section refer to [3] and [2].

Let  $q(\geq 2)$  to be an integer and fixed.

**Definition 2.1** (Latin square). A Latin square of order q is an  $q \times q$  array in which q distinct symbols are arranged so that each symbol occurs in each row and column.

**Definition 2.2** (Quasigroup). A set Q is called a quasigroup if there is a binary operation \* defined in Q and if, when any two elements a, b of Q are given, the equations a \* x = b and y \* a = b each have exactly one solution.

**Theorem 2.3.** Evey multiplication table of a quasigroup is a Latin square and conversely, any bordered latin square is the multiplication table of a quasigroup.

We denote  $L = ||a_{ij}||$ , when an (i, j)-element of a Latin square L is written by  $a_{ij}$  as follows,

$$L = ||a_{ij}|| = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1q} \\ a_{21} & a_{22} & \cdots & a_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ a_{q1} & a_{q2} & \cdots & a_{qq} \end{bmatrix}$$

**Definition 2.4** (Orthogonal). Let  $L_1$  and  $L_2$  be Latin squares of the same order, sau  $q \ge 2$ . We say that  $L_1$  and  $L_2$  are orthogonal if, when superimposed, each of the possible  $q^2$  ordered pairs occurs exactly once. In the other word, two Latin squares  $L_1 = ||a_{ij}||$  and  $L_2 = ||b_{ij}||$  on q symbols are said to be orthogonal if evy ordered pair of symbols occurs exactly once among the  $q^2$  pairs  $(a_{ij}, b_{ij}), i, j = 1, 2, \dots, q$ .

The descriptive term orthogonal mate for a Latin square  $L_2$  which is orthogonal to a given Latin square  $L_1$  was first by [6].

For example, the following two Latin squares  $L_1$  and  $L_2$  are orthogonal. For given a Latin square  $L_1$ ,  $L_2$  is the orthogonal mate of  $L_1$ .

$$L_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, L_2 = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

**Definition 2.5** (MOLS). We say that a set  $\{L_1, L_2, \dots, L_t\}$  of  $t \ge 2$ Latin squares of order q is orthogonal if any two distinct squares are orthogonal, that is if  $L_i$  is orthogonal to  $L_j$  whenver  $i \ne j$ . Such a set of orthogonal squares is said to be a set of mutually orthogonal Latin squares (MOLS).

For example, the following set  $\{L_1, L_2, L_3\}$  is MOLS.

$L_1 =$	Γ0	1	2	3	$, L_2 =$	[0	1	2	3	$, L_{3} =$	0	1	2	3]
	1	0	3	2		2	3	0	1		3	2	1	0
	2	3	0	1		3	2	1	0		1	0	3	2
	3	2	1	0		1	0	3	2		2	3	0	1

**Definition 2.6** (N(q)). We denote the maximum possible number of MOLS of order q by N(q).

**Theorem 2.7.** For each  $q \ge 2$ ,  $N(q) \le q - 1$ 

**Definition 2.8** (Complete). If we have a set of q - 1 MOLS of order q, then the set is said to be complete.

Utilizing the property of orthogonal Latin squares and MOLS, several constructions of Sudoku solutions are obtain [1, 4, 5].

**Theorem 2.9** (Prime powers). For q a prime power the set of polynomials of the form  $f_a(x, y) = ax + y$  with  $a \neq 0 \in GF(q)$  represents a complete set of q - 1 MOLS of order q.

**Theorem 2.10** (Nonprime powers). If there is a pair of MOLS of order  $q_1$  and a pair of MOLS of order  $q_2$ , then there is a pair of MOLS of order  $q_1q_2$ 

**Theorem 2.11** (Nonprime powers). If  $q \equiv 0, 1, 3 \pmod{4}$ , then  $N(q) \geq 2$ .

**Theorem 2.12** (Nonprime powers). For all q except 2 and 6, there is a pair of MOLS of order q; that is, for all q except 2 and 6,  $N(q) \ge 2$ .

**Theorem 2.13** (Nonprime powers). Let  $q_1 \times q_2 \times \cdots \times q_r$  be the factorization of q into distinct prime powers with  $q_1 < q_2 < \cdots < q_r$ . Then  $N(q) \ge q_1 - 1$ 

**Theorem 2.14** (Nonprime powers). For  $q_1, q_2 \ge 2$ , it holds that  $N(q_1q_2) \ge min\{N(q_1), N(q_2)\}$ .

# 3 Definitons and property for quasigroups with *n*-ary operators

We suggest that readers who wish to learn more about the definitions and property related to quasigroups discussed in this section refer to [7].

Let  $n(\geq 2)$  to be an integer and fixed. Generally, when A is an *n*-ary operation on a non-empty set G, we write  $A(x_1, x_2, \dots, x_n)$ , for any elements  $x_1, x_2, \dots, x_n \in G$ . Especially, when A is a binary operation on a non-empty set G, we often write x \* y instead of A(x, y), for any elements  $x, y \in G$ .

**Definition 3.1** (*n*-aray Groupoid). An *n*-ary groupoid (G, A) is a nonempty set G together with an *n*-ary operation A.

**Definition 3.2** (order). The order of an *n*-ary groupoid (G, A) is cardinarity |G| of the carrier set G. An *n*-ary groupoid (G, A) is said to be finite if its order is finite.

**Definition 3.3** (Binary Quasigroup). A binary groupoid  $(Q, \circ)$  is called a *quasigroup* if for any ordered pair  $(a, b) \in Q^2$  there exist unique solutions  $x, y \in Q$  to the equations  $x \circ a = b$  and  $a \circ y = b$ .

**Definition 3.4** (*n*-ary Quasigroup). An *n*-ary groupoid (Q, A) with *n*-ary operation A such that in the equality  $A(x_1, x_2, \dots, x_n) = x_{n+1}$  the fact of knowing any *n* elements of the set  $\{x_1, x_2, \dots, x_n, x_{n+1}\}$  uniquely speccifies the remaining one element is called an *n*-ary quasigroup.

**Definition 3.5** (Isotopism of isotopy). An *n*-ary groupoid (G, f) is an isotope of an *n*-ary groupoid (G, g) (in other words (G, f) is an isotopic image of (G, g)), if there exsit permutations  $\mu_1, \mu_2, \dots, \mu_n, \mu$  of the set G such that

$$f(x_1, x_2, \cdots, x_n) = \mu^{-1}g(\mu_1 x_1, \mu_2 x_2, \cdots, \mu_n x_n)$$

for all  $x_1, x_2, \dots, x_n \in G$ . We can also write this fact in the form (G, f) = (G, g)T where  $T = (\mu_1, \mu_2, \dots, \mu_n, \mu)$ . The ordered (n + 1)-tuple T is called isotopy of n-ary groupoids.

**Example 3.6.** We give an example of a ternary quasigroup (Q, A) of order 4 using four binary operators  $A_0, A_1, A_2, A_3$  on the set  $Q = \{0, 1, 2, 3\}$ .

At first, we give the following four binary operators  $A_0, A_1, A_2, A_3$  on the set  $Q = \{0, 1, 2, 3\}$ . These multiplication tables are all Latin squares of order 4. Hence, the set  $Q = \{0, 1, 2, 3\}$  is a quasigroup with each binary operator  $A_i$  (i = 0, 1, 2, 3). That is,  $(Q, A_0)$ ,  $(Q, A_1)$ ,  $(Q, A_2)$ ,  $(Q, A_3)$  are four quasigroups of order 4,

3
2
3
0
1
3
0
1
2
3
<u>-</u> 32L) <u>2</u> L)32

Next, the ternary operator A of the set  $Q = \{0, 1, 2, 3\}$  is given by  $A(i, j, k) = A_i(j, k)$ . For example, we have  $A(1, 2, 3) = A_1(2, 3) = 0$ . Therefore, (Q, A) is a ternary quasigroup of order 4.

# 4 Orthogonallity of quasigroups with binary operations

We suggest that readers who wish to learn more about orthogonallity of quasigroups with binary operations discussed in this section refer to [3] and [7].

In this section, we let G is a groupoid, Q is a quasigroup, A, B,  $A_1, A_2, \dots, A_t$  are binary operators on G or Q. In this section, we rewrite the definitions and property for Latin squares in section 2, in the terms of quasigroups with binary operations.

**Definition 4.1** (Binary Orthogorality). Two binary groupoids (G, A) and (G, B) are called orthogonal, if the system of equations

$$\begin{cases} A(x,y) = a\\ B(x,y) = b \end{cases}$$

has a unique solution  $(x_0, y_0)$  for any fixed pair of elements  $a, b \in G$ .

When two binary quasigroups (Q, A) and (Q, B) are orthogonal, and  $L_A, L_B$  are the multiplication tables of quasigroups (Q, A), (Q, B), respectively, two Latin squares  $L_A$  and  $L_B$  are orthogonal.

**Definition 4.2** (Basis square). A Latin square for which an orthogonal Latin square exsists is called a basis square.

**Definition 4.3** (Mutual Orthogonarity). A set of quasigroups  $\{(Q, A_1), (Q, A_2), \dots, (Q, A_t)\}$  over Q is called to be a mutually orthogonal quasigroup system when  $A_i$  and  $A_j$  are orthogonal for any i, j where  $i \neq j$ .

When a set  $\{(Q, A_1), (Q, A_2), \dots, (Q, A_t)\}$  over Q is a mutually orthogonal quasigroup system, and each  $L_i$  is the multiplication table of each quasigroup  $(Q, A_i)$  for  $i = 1, 2, \dots, t$ , a set  $\{L_1, L_2, \dots, L_t\}$  is MOLS.

**Definition 4.4** (N(q)). We denote by N(q) the largest number N such that there exists a mutually orthogonal quasigroup system  $\{(Q, A_1), (Q, A_2), \dots, (Q, A_t)\}$  where q = |Q|.

The above definition is equivalent to Definition 2.6 in Section 2.

Theorem 4.5. The followings hold.

- $N(q) \leq (q-1);$
- If q is prime, then N(q) = (q-1);
- $N(q_1q_2) \ge min\{N(q_1), N(q_2)\}$ , in particular, if  $q = q_1 \cdots q_t$  is the canonical decomposition of q, then  $N(q) \ge min\{q_1 1, \cdots, q_t 1\}$ ;
- $N(q) \ge q^{10/143} 2;$
- $N(q) \ge 3$ , if  $q \notin \{2, 3, 6, 10\}$ ;
- $N(q) \ge 6$  whenever q > 90;
- $N(q) \ge q^{10/148}$  for sufficiently large q.

## 5 Orthogonallity of quasigroups with *n*-ary operations

Finally, we describe about mutually orthogonal quasigroups with *n*-ary operations. In this section, we let G is a groupoid, Q is a quasigroup,  $f_1, f_2, \dots, f_n, A, B, C$  are *n*-ary operators on G or Q.

**Definition 5.1** (*n*-aray Orthogonality). *n*-aray groupoids  $(G, f_1), (G, f_2), cdots, (G, f_n)$  are called orthogonal, if for any fixed *n*-tuple  $a_1, a_2, \dots, a_n$  the following system of equations

 $\begin{cases} f_1(x_1, x_2, \cdots, x_n) = a_1 \\ f_2(x_1, x_2, \cdots, x_n) = a_2 \\ \vdots \\ f_n(x_1, x_2, \cdots, x_n) = a_n \\ \vdots \\ nue \text{ solution.} \end{cases}$ 

has a unique solution.

The above definition is can use in the both cases whenever the set G is finite or infinite. When the set G is finite, that is |G| = q, there exist  $(q^n)!$  systems.

**Definition 5.2.** For fixed k  $(2 \leq k \leq n)$ , *n*-aray groupoids  $(G, f_1)$ ,  $(G, f_2)$ , *cdots*,  $(G, f_k)$  given on a set G of order m are called orthogonal if the system of equations

 $\begin{cases} f_1(x_1, x_2, \cdots, x_n) = a_1 \\ f_2(x_1, x_2, \cdots, x_n) = a_2 \\ \vdots \\ f_k(x_1, x_2, \cdots, x_n) = a_k \end{cases}$ 

has exactly  $m^{n-k}$  solutions for any k-tuple  $a_1, a_2, \dots, a_k$ , where  $a_1, a_2, \dots, a_k \in G$ .

**Example 5.3.** We give an example of mutually orthogonal ternary groupoids (G, A), (G, B), (G, C) of order 4.

At first, we give four binary operators  $A_0, A_1, A_2, A_3$  on the set  $G = \{0, 1, 2, 3\}$ , such as Example 3.6. The ternary operator A of the set  $G = \{0, 1, 2, 3\}$  is given by  $A(i, j, k) = A_i(j, k)$ . Then, (G, A) is a ternary groupoid of order 4. Moreover, we note that each multiplication table of each binary operation  $A_i$  (i = 0, 1, 2, 3) is Latin square of order 4. and (G, A) is also a ternary quasigroup of order 4.

Secondly, we give the following four binary operators  $B_0, B_1, B_2, B_3$ on the set  $G = \{0, 1, 2, 3\}$ , as follows. These multiplication tables of binary operations  $B_i$  (i = 0, 1, 2, 3) are no Latin squares, but are all closed in  $G = \{0, 1, 2, 3\}$ . Hence,  $(G, B_0), (G, B_1), (G, B_2), (G, B_3)$  are binary groupoids, not quasigroups. The ternary operator B of the set  $G = \{0, 1, 2, 3\}$  is given by  $B(i, j, k) = B_i(j, k)$ . Then, (G, B) is a ternary groupoid of order 4.

$B_0$	0	1	2	3	$B_1$	1	0	1	2	3
0	3	0	1	3	0		2	1	1	0
1	0	2	3	0	1		2	3	3	0
2	1	2	1	3	2		0	2	1	3
3	1	1	2	2	3		0	0	3	1
$B_2$	0	1	2	3	Ba	3	0	1	2	3
0	1	2	0	0	0		3	3	2	2
1	2	0	3	1	1		0	1	2	1
0										
2	0	2	3	2	2		0	2	0	3

Thirdly, we give the following four binary operators  $C_0, C_1, C_2, C_3$ on the set  $G = \{0, 1, 2, 3\}$ , as follows. These multiplication tables of binary operations  $C_i$  (i = 0, 1, 2, 3) are no Latin squares, but are all closed in  $G = \{0, 1, 2, 3\}$ . Hence,  $(G, C_0)$ ,  $(G, C_1)$ ,  $(G, C_2)$ ,  $(G, C_3)$  are binary groupoids, not quasigroups. The ternary operator C of the set  $G = \{0, 1, 2, 3\}$  is given by  $C(i, j, k) = C_i(j, k)$ . Then, (G, C) is a ternary groupoid of order 4.

$C_0$	0	1	2	3	$C_1$	0	1	2	3
0	3	1	2	0	0	1	2	1	3
1	2	1	1	2	1	1	2	3	1
2	0	1	0	1	2	0	2	2	0
3	3	1	2	3	3	1	3	1	1
$C_{2}$	0	1	2	3	$C_3$	0	1	2	3
$\frac{-2}{0}$	3	3	0	0	0	2	1	0	0
1	2	1	0	1	1	2	0	2	3
2	3	3	2	0	2	3	3	2	0

Therefore, the three ternaray groupoids (G, A), (G, B), (G, C) are mutually orthogonal, since the following system of equations

 $\begin{cases} A(x_1, x_2, x_3) = a_1 \\ B(x_1, x_2, x_3) = a_2 \\ C(x_1, x_2, x_3) = a_3 \end{cases}$ 

has a unique solution for any 3-tuple  $(a_1, a_2, a_3) \in G^3$ .

### References

- D. Keedwell (2010); Constructions of complete sets of orthogonal diagonal Sudoku squares, Australasian Journal of Combinatorics, Vol. 47, pp. 227–238.
- [2] D. Keedwell and J. Dénes (2015); Latin Squares and their applications, (second edition), North-Holland publications.
- [3] C. F. Laywine and G. L. Mullen (1998); Discrete Mathematics Using Latin Squares, John Weiley & Sons, INC.

- [4] J. Lorch (2009); Mutually orthogonal families of linear sudoku solutions, Journal of the Australian Mathematical Society, Vol. 87, pp. 409–420.
- [5] J. Lorch (2010); Orthogonal combings of linear sudoku solutions, Australasian Journal of Combinatorics, Vol. 47, pp. 247–264.
- [6] E. T. Parker (1963); Computer investigation of orthogonal Latin squares of order ten. *Proc. Sympos. Appl. Math.*, Vol. 15, pp. 73-81.
- [7] V. Shcherbacov (2017); *Elements of Quasigroup Theory and Applications*, Chapman and Hall/CRC.