International J.Math. Combin. Vol.3(2015), 55-61

Variations of Orthogonality of Latin Squares

Vadiraja Bhatta G.R.

Department of Mathematics

Manipal Institute of Technology, Manipal University, Manipal, Karnataka-576104, India

B.R.Shankar

Department of Mathematical and Computational Sciences

National Institute of Technology, Surathkal, Karnataka, India

E-mail: vadiraja.bhatta@manipal.edu

Abstract: Orthogonal properties of Latin squares represented by permutation polynomials are discussed. Pairs of bivariate polynomials over small rings are considered.

Key Words: Bivariate polynomials, Latin squares, orthogonal Latin squares

AMS(2010): 08B15.

§1. Introduction

1.1 Latin Squares

Combinatorial theory is one of the fastest growing areas of modern mathematics. Combinatorial designs have wide applications in various fields, including coding theory and cryptography. Many examples of combinatorial designs can be listed like linked design, balanced design, one-factorization, graph etc. *Latin square* is one such combinatorial concept.

Definition 1.1 *A Latin square of order (or size) n is an $n \times n$ array based on some set S of n symbols (treatments), with the property that every row and every column contains every symbol exactly once.*

In other words, every row and every column is a permutation of S. Also it can be thought of as a two dimensional analogue of a permutation. A Latin square can be viewed as a quadruple $(R, C, S; L)$, where R, C, and S are sets of cardinality n, L is a mapping $L : R \times C \to S$ such that for any $i \in R$ and $x \in S$, the equation

$$L(i, j) = x$$

has a unique solution $j \in C$, and for any $j \in C$, $x \in S$, the same equation has a unique solution

[1]Received December 21, 2014, Accepted August 12, 2015.

$i \in R$. That is any two of $i \in R, j \in C, x \in S$ uniquely determine the third so that $L(i,j) = x$. i.e., the cell in row i and column j contains the symbol $L(i,j)$.

Using the concept of permutation functions we can define Latin squares as follows:

Definition 1.2 *A function $f : S^2 \to S$ on a finite set S of size $n > 1$ is said to be a Latin square (of order n) if for any $a \in S$ both the functions $f(a,.)$ and $f(.,a)$ are permutations of S.*

Here, $f(a,.)$ determines the rows and $f(.,a)$ determines the columns of the Latin square. Latin squares exist for all n, as an obvious example we can consider addition modulo n.

Example 1.3 A Latin square of order 5 over the set $\{a,b,c,d,e\}$ is below:

a	b	c	d	e
b	a	e	c	d
c	d	b	e	a
d	e	a	b	c
e	c	d	a	b

The terminology 'Latin square' originated with Euler who used a set of Latin letters for the set S. We discussed some results in [2] about the formation of Latin squares using bivariate permutation polynomials.

1.2 Orthogonal Latin Squares

One of the origins of the study of Latin squares is usually identified with the now famous problem of Euler concerning the arrangement of 36 officers of 6 different ranks and 6 different regiments into a 6×6 square. If there were such an officer holding each rank from each regiment, Euler's problem was to find an arrangement in which each rank and each regiment would be represented in every row and column. A solution requires two Latin squares of order 6; in one, the symbols represent the ranks and in the other regiments. Furthermore,the two Latin squares must be compatible in a very precise sense so that if one is superimposed on the other, each ordered pair occurs exactly once. Two such squares which exhibit such "compatibility" are *orthogonal Latin squares*. It is interesting to compare two Latin squares on the same set in different ways like *equivalence*, which we already saw above. *Orthogonality* is a very useful concept in the study of Latin squares, having a lot of applications in cryptography.

Definition 1.4 *Two Latin squares $L_1 : R \times C \to S$ and $L_2 : R \times C \to S$ (with the same row and column sets) are said to be orthogonal when for each ordered pair $(s,t) \in S \times T$, there is a unique cell $(x,y) \in R \times C$ so that*

$$L_1(x,y) = s \text{ and } L_2(x,y) = t.$$

That is, two Latin squares A and B of the same order n are *orthogonal*, if the n^2 ordered pairs (a_{ij}, b_{ij}), the pairs formed by superimposing one square on the other, are all different. One can say "*A is orthogonal to B*" or "*B is orthogonal to A*". So, the relation of orthogonality

is symmetric. In general, one can speak of k *mutually orthogonal* Latin squares $A_1, A_2, \cdots, A_k$ such that A_i is orthogonal to A_j whenever $i \neq j$.

§2. Orthogonality and Bivariate Polynomials

Using the concept of permutation functions orthogonality can be defined as follows:

Definition 2.1 *A pair of functions $f_1(*,*)$, $f_2(*,*)$ is said to be* ***orthogonal*** *if the pairs $(f_1(x,y), f_2(x,y))$ are all distinct, as x and y vary.*

Shannon observed that Latin squares are useful in cryptography. Schnorr and Vaudenay applied pairs of orthogonal Latin squares(which they called *multipermutations*) to cryptography. The following theorem is due to Rivest [1]:

Theorem 2.2 *There are no two polynomials $P_1(x,y)$, $P_2(x,y)$ modulo 2^w for $w \geq 1$ that form a pair of orthogonal Latin squares.*

In fact Euler believed that no pair of orthogonal Latin squares of order 6 exist, and this was not shown until Tarry did so around 1900 by means of an almost exhaustive search. While there are other less tedious methods now available to prove this result, it is still not an easy task to prove this without the aid of a computer [3]. Euler's actual conjecture was far stronger in that he speculated that there did not exist orthogonal Latin squares for orders $n = 6, 10, 14, \cdots$. This famous conjecture, which is associated with Euler's name remained unsolved until Bose, Parker and Shrikhande showed it to be false for $n = 10, 14, \cdots$ in a series of papers in 1959 and 1960 ([4]).

If we have two orthogonal Latin squares of order 4, both over the set, $\{1,2,3,4\}$, the configuration of their superposition is as follows:

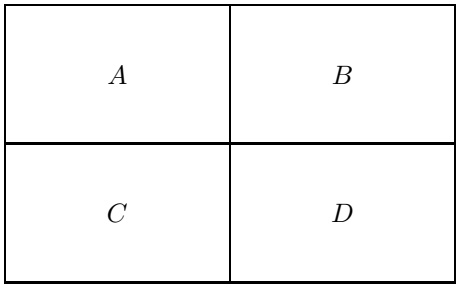
1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

The orthogonal configuration is:

(1,1)	(2,2)	(3,3)	(4,4)
(2,3)	(1,4)	(4,1)	(3,2)
(3,4)	(4,3)	(1,2)	(2,1)
(4,2)	(3,1)	(2,4)	(1,3)

Rivest [1] proved that no two bivariate polynomials modulo 2^w, for $w \geq 1$ can form a pair of orthogonal Latin squares. This is because all the bivariate polynomials over Z_n, where $n = 2^w$, will form Latin squares which can be equally divided into 4 parts as shown below, where the $n/2 \times n/2$ squares A and D are identical and $n/2 \times n/2$ squares B and C are identical.



So, no two such Latin squares can be orthogonal.

Theorem 2.3 *There are no two bivariate polynomials $P_1(x, y)$ and $P_2(x, y)$ over Z_n, where n is even, which can form orthogonal Latin squares.*

Proof Let $n = 2m$ and $Q(x)$ be any univariate polynomial over Z_n.Then, $Q(x + m) = Q(x) + m(mod\ n)$ for all $x \in Z_n$. Hence,

$$\begin{aligned} P_1(x + m, y + m) &= P_1(x, y + m) + m\ (mod\ n) \\ &= P_1(x, y) + 2m\ (mod\ n) \\ &= P_1(x, y)\ (mod\ n) \end{aligned}$$

The same holds for $P_2(x, y)$ too. Therefore,$(P_1(x, y), P_2(x, y) = P_1(x+m, y+m), P_2(x+m, y+m))$. So, the pair of Latin squares cannot be orthogonal. □

We do have examples of bivariate polynomials modulo $n \neq 2^w$ and n odd, such that the resulting Latin squares are orthogonal.

Example 2.4 The following is a pair of Latin squares over Z_9 which are orthogonal to each other.

0	8	4	6	5	1	3	2	7
7	0	8	4	6	5	1	3	2
8	4	6	5	1	3	2	7	0
3	2	7	0	8	4	6	5	1
1	3	2	7	0	8	4	6	5
2	7	0	8	4	6	5	1	3
6	5	1	3	2	7	0	8	4
4	6	5	1	3	2	7	0	8
5	1	3	2	7	0	8	4	6

Latin square formed by
$5x + y + 3xy + 3x^2 + 6y^2$

0	5	7	6	2	4	3	8	1
2	4	3	8	1	0	5	7	6
7	6	2	4	3	8	1	0	5
6	2	4	3	8	1	0	5	7
8	1	0	5	7	6	2	4	3
4	3	8	1	0	5	7	6	2
3	8	1	0	5	7	6	2	4
5	7	6	2	4	3	8	1	0
1	0	5	7	6	2	4	3	8

Latin square formed by
$2x + 5y + 6xy + 3x^2 + 6y^2$

The two bivariate quadratic polynomials $x+5y+3xy+6x^2+3y^2$ and $4x+7y+6xy+3x^2+6y^2$ give two orthogonal Latin squares over Z_9. Also, $x + 4y + 3xy$ is a quadratic bivariate which gives a Latin square orthogonal to Latin square formed by $x + 5y + 3xy + 6x^2 + 3y^2$ over Z_9, but not to that of $4x + 7y + 6xy + 3x^2 + 6y^2$.

Remark 2.5 We have found many examples in which the rows or columns of the Latin square formed by quadratic bivariates over Z_n are cyclic shifts of a single permutation of $\{0, 1, 2, \cdots, n-1\}$. If two bivariates give such Latin squares, then corresponding to any one entry in one Latin square, if there are n different entries in n rows of the other Latin square, then those two Latin squares will be orthogonal.For instance, in the example below, the entries in the second square corresponding to the entry 0 in the first square are 0, 8, 7, 6, 5, 4, 3, 2, 1. The rows of the first square are all cyclic shifts of the permutation (0, 8, 4, 6, 5, 1, 3, 2, 7), not in order. Also the columns of the second square are the cyclic shifts of the permutation (0, 7, 2, 3, 1, 5, 6, 4, 8), not in order.

Example 2.6

0	8	4	6	5	1	3	2	7
7	0	8	4	6	5	1	3	2
8	4	6	5	1	3	2	7	0
3	2	7	0	8	4	6	5	1
1	3	2	7	0	8	4	6	5
2	7	0	8	4	6	5	1	3
6	5	1	3	2	7	0	8	4
4	6	5	1	3	2	7	0	8
5	1	3	2	7	0	8	4	6

Latin square formed by
$5x + y + 3xy + 3x^2 + 6y^2$

0	4	2	3	7	5	6	1	8
7	8	3	1	2	6	4	5	0
2	0	1	5	3	4	8	6	7
3	7	5	6	1	8	0	4	2
1	2	6	4	5	0	7	8	3
5	3	4	8	6	7	2	0	1
6	1	8	0	4	2	3	7	5
4	5	0	7	8	3	1	2	6
8	6	7	2	0	1	5	3	4

Latin square formed by
$7x + 4y + 6xy + 6x^2 + 3y^2$

Instead of looking for an orthogonal mate of Latin square formed by some other polynomial we looked at the mirror image of the square itself.

Example 2.7 The Latin square formed by the polynomial $4x + 7y + 6xy + 6x^2 + 3y^2$ over Z_9 and its mirror image are given below:

0	1	5	3	4	8	6	7	2
1	8	0	4	2	3	7	5	6
8	3	1	2	6	4	5	0	7
3	4	8	6	7	2	0	1	5
4	2	3	7	5	6	1	8	0
2	6	4	5	0	7	8	3	1
6	7	2	0	1	5	3	4	8
7	5	6	1	8	0	4	2	3
5	0	7	8	3	1	2	6	4

2	7	6	8	4	3	5	1	0
6	5	7	3	2	4	0	8	1
7	0	5	4	6	2	1	3	8
5	1	0	2	7	6	8	4	3
0	8	1	6	5	7	3	2	4
1	3	8	7	0	5	4	6	2
8	4	3	5	1	0	2	7	6
3	2	4	0	8	1	6	5	7
4	6	2	1	3	8	7	0	5

These two are orthogonal to each other. Over the ring Z_7, here is a Latin square formed by the polynomial $3x + 4y$, with its mirror image, which are orthogonal to each other:

0	3	6	2	5	1	4
4	0	3	6	2	5	1
1	4	0	3	6	2	5
5	1	4	0	3	6	2
2	5	1	4	0	3	6
6	2	5	1	4	0	3
3	6	2	5	1	4	0

4	1	5	2	6	3	0
1	5	2	6	3	0	4
5	2	6	3	0	4	1
2	6	3	0	4	1	5
6	3	0	4	1	5	2
3	0	4	1	5	2	6
0	4	1	5	2	6	3

But this is not always true. We have the example below 2.8: in the ring Z_8, the Latin square formed by the polynomial $x + 5y + 4xy + 2x^2 + 6y^2$ is not orthogonal with its mirror image.

Example 2.8

0	3	2	5	4	7	6	1
3	2	5	4	7	6	1	0
2	5	4	7	6	1	0	3
5	4	7	6	1	0	3	2
4	7	6	1	0	3	2	5
7	6	1	0	3	2	5	4
6	1	0	3	2	5	4	7
1	0	3	2	5	4	7	6

1	6	7	4	5	2	3	0
0	1	6	7	4	5	2	3
3	0	1	6	7	4	5	2
2	3	0	1	6	7	4	5
5	2	3	0	1	6	7	4
4	5	2	3	0	1	6	7
7	4	5	2	3	0	1	6
6	7	4	5	2	3	0	1

Here there are 32 distinct pairs, each appearing twice. Also all the pairs of the form (a, b), where one of a and b is odd and the other is even are appearing and all pairs that appear are of this form.

Theorem 2.9 *For odd n, Latin square over Z_n formed by a bivariate permutation polynomial $P(x, y)$ is orthogonal with its mirror image.*

Proof If $P(x, y)$ is a bivariate linear polynomial, then clearly the rows (columns) are simply cyclic shifts of a *single* row (column). Hence the Latin Squares got by $P(x, y)$ and its mirror image are orthogonal. In the general case, corresponding to the cell index (x, y), the index in the mirror image is $(n-1-x, y)$. Thus if L denotes the Latin square formed by $P(x, y)$ and L' is its mirror image, on superimposing L and L' the entry in cell index (x, y) will be $(P(x, y), P(n-1-x, y))$. Since P is a permutation polynomial, these pairs will all be distinct as x and y vary in Z_n. Hence they are orthogonal. □

Remark 2.10 In case of rings Z_n, where n is even, we know from Theorem 2.3, the Latin squares formed by bivariate permutation polynomials have four parts with diagonally opposite pair of parts being same. Mirror images of such squares are also of the same kind. So, in the

first $n/2$ rows we can get $n/2$ distinct pairs of corresponding entries. In the last $n/2$ rows, these pairs will repeat in the same order. So, these two pair of squares are not orthogonal.

§3. Conclusion

Identifying a pair of bivariate polynomials modulo n which represent a pair of orthogonal Latin squares is not obvious. But for odd n, a Latin square formed by a bivariate polynomial is orthogonal to its mirror image. Moreover, no two bivariate polynomials over Z_n, when n is even can form orthogonal Latin squares.

References

[1] Rivest R. L., Permutation Polynomials modulo 2^w, *Finite Fields and Their applications*, 7 (2001) 287-292.

[2] Vadiraja Bhatta and Shankar B. R., Permutation Polynomials modulo n, $n \neq 2^w$ and Latin Squares, *International Journal Of Mathematical Combinatorics,* Vol. 2 (2009) 58-65.

[3] Laywine, C.F. and Mullen, G.L., Discrete Mathematics using Latin squares, *John Wiley and Sons, Inc.* (1998).

[4] Lint J.V., and Wilson R. M., *A Course in Combinatorics*, Cambridge University Press, Cambridge, second edition, 2001.