COMPLETE SETS OF ORTHOGONAL, SELF-ORTHOGONAL LATIN SQUARES

George P. Graham and Charles E. Roberts
Department of Mathematics and Computer Science
Indiana State University, Terre Haute, IN 47809

Abstract

We show how to produce algebraically a complete orthogonal set of Latin squares from a left quasifield and how to generate algebraically a maximal set of self-orthogonal Latin squares from a left nearfield.

INTRODUCTION

A set $\mathcal{A} = \{A_1, A_2, \ldots, A_k\}$ of Latin squares of order n is *mutually orthogonal* provided A_i is orthogonal to A_j for each $i \neq j$. The first general results on the construction of mutually orthogonal Latin squares were given by MacNeish [4] in 1922. For n a prime, he showed how to construct a set of $n-1$ mutually orthogonal Latin squares of order n. For any n, no larger set can exist, so a set of $n-1$ mutually orthogonal Latin squares of order n is called a *complete set of mutually orthogonal Latin squares.* A Latin square which is orthogonal to its transpose is said to be a *self-orthogonal Latin square.* The term "self-orthogonal" was introduced in 1970 by R. C. Mullin and E. Nemeth [6]; however, the problem of constructing a Latin square orthogonal to its transpose seems to have been considered first by S. K. Stein [7] in 1957. In 1971, N. S. Mendelsohn [5] showed how to construct a Latin square orthogonal to its transpose for every order n such that $n \not\equiv 2 \pmod 4$, or $n \not\equiv 3 \pmod 9$, or $n \not\equiv 6 \pmod 9$. And in 1973-74 Brayton, Coppersmith, and Hoffman [1] and [2] showed that there exists a self-orthogonal Latin square of order n for $n \neq 2, 3, 6$.

We define an orthogonal set of Latin squares $\{A_1, A_2, \ldots, A_r\}$ to be *orthogonal, self-orthogonal* or *OSO*, if $\{A_1, A_1^T, A_2, A_2^T, \ldots, A_r, A_r^T\}$ is an orthogonal set. For Latin squares of order n let $N(n)$ denote the maximum number of mutually orthogonal Latin squares and let $S(n)$ denote the size of a maximal OSO set. Certainly $S(n) \leq N(n)/2$ and due to the results of Brayton, Coppersmith, and Hoffman, $S(n) \geq 1$ for $n \neq 2, 3, 6$.

This paper is an extension of G. Graham and C. Roberts [3]. Here we establish a connection between maximal sets of self-orthogonal Latin squares and nearfields.

QUASIFIELDS, NEARFIELDS, AND LATIN SQUARES

A *left quasifield* is a nonempty set of elements R and two binary operations $+$ and $*$ on R such that $(R, +)$ is an abelian group with additive identity, 0; $(R-\{0\}, *)$ is a loop with multiplicative identity, 1; for all $a \in R$, $0 * a = 0$; and the left distributive law holds—that is, for all $a, b, c \in R$, $a*(b+c) = a*b+a*c$. A *left nearfield* is a left quasifield in which $(R-\{0\}, *)$ is a group. In 1936, H. J. Zassenhaus [8] determined all finite nearfields.

It is very straightforward to show that for all $a \in R$, $a * 0 = 0$.

Lemma 1. For all $x, y \in R$ and $w \in R - \{0\}$, if $x * w = y * w$, then $x = y$

Proof: If $x \neq 0$. Then $x*w \neq 0$ since $(R-\{0\}, *)$ is a loop, hence $y*w \neq 0$. Also $y \neq 0$ since $0 * w = 0$. Then $x, y, w \in R - \{0\}$. By cancellation in $(R - \{0\}, *)$, $x = y$. If $x = 0$. Then $x * w = 0 = y * w$. Since $w \neq 0$, then necessarily $y = 0$, i.e. $x = y$.

Theorem 1. Let $(R, +, *)$ be a left quasifield with additive identity 0 and multiplicative identity 1 in which R has $n \geq 4$ elements. Order the elements of R as $\{0, 1, r_3, r_4, \ldots, r_n\}$. For each $z \in R$ such that $z \neq 0$ and $z \neq 1$ define C^z to be the Latin square with elements $c^z_{ij} = (j - i) * z + i$ for $i, j \in R$. The set

$$C = \{C^z \,|\, z \in R \text{ and } z \neq 0 \text{ and } z \neq 1\}$$

is a set of $n - 2$ mutually orthogonal Latin squares.

Proof: For each $z \neq 0, 1$ suppose $c^z_{ij} = c^z_{ik}$. Then

$$(j - i) * z + i = (k - i) * z + i$$

$$(j - i) * z = (k - i) * z$$

By Lemma 1,

$$(j - i) = (k - i)$$

Whence,

$$j = k$$

and the rows of C^z are permutations of R.

If $c^z_{ij} = c^z_{kj}$, then

$$(j - i) * z + i = (j - k) * z + k$$

$$(j - i) * z + i - j = (j - k) * z + k - j$$

$$\begin{aligned}(j-i)*z-(j-i)*1 &= (j-i)*z-(j-i)\\ &= (j-k)*z-(j-k)\\ &= (j-k)*z-(j-k)*1\end{aligned}$$

By left distributivity

$$(j-i)*(z-1)=(j-k)*(z-1)$$

As above it follows that

$$i=k$$

Whence the columns of C^z are permutations of R. That is, C^z is a Latin square.

To establish orthogonality, suppose that $(c^z_{ij}, c^y_{ij}) = (c^z_{pq}, c^y_{pq})$ and $z \neq y$. Since $c^z_{ij} = c^z_{pq}$,

(1) $$(j-i)*z+i=(q-p)*z+p$$

and since $c^y_{ij} = c^y_{pq}$,

(2) $$(j-i)*y+i=(q-p)*y+p$$

Subtracting (2) from (1) and using the left distributive law, we find

$$(j-i)*(z-y)=(q-p)*(z-y).$$

Hence by Lemma 1,

(3) $$j-i=q-p$$

Substituting into (1) results in $(j-i)*z+i=(j-i)*z+p$, so $i=p$ and then from (3), $j=q$.

Theorem 2. Let R be a left quasifield as specified in Theorem 1 and let C^- be the Latin square with elements $c^-_{ij} = i-j$. The set $\mathcal{C} \cup \{C^-\}$ is a set of $n-1$ mutually orthogonal Latin squares.

Proof: Let $C^z \in \mathcal{C}$. Suppose $(c^z_{ij}, c^-_{ij}) = (c^z_{pq}, c^-_{pq})$ for some i, j, p, and q. Then since $c^z_{ij} = c^z_{pq}$,

(4) $$(j-i)*z+i=(q-p)*z+p$$

and since $c^-_{ij} = c^-_{pq}$,

$$i-j=p-q$$

or

(5) $$j-i=q-p$$

Substituting (5) into (4), we get $i=p$, and substituting this result into (5), we get $j=q$.

Lemma 2. Any set of mutually orthogonal Latin squares can contain at most one symmetric Latin square.

Proof: Suppose A and B are symmetric Latin squares and A and B are orthogonal. By symmetry $a_{12} = a_{21}$ and $b_{12} = b_{21}$, so the ordered pairs (a_{12}, b_{12}) and (a_{21}, b_{21}) are identical. Thus, A and B are not orthogonal.

Lemma 3. In each C^z the main diagonal is $(0, 1, r_3, r_4, \ldots, r_n)$.

Lemma 4. For n even, C contains no symmetric Latin square.

Proof: By Lemma 3 each element of R appears exactly once on the diagonal of each $C^z \in C$. For any Latin square in C to be symmetric, each element in R must appear the same number of times in the upper triangular part of the Latin square as in the lower triangular part. Thus, each element of R must appear $(n-1)/2$ times in the upper and lower triangular part of a symmetric Latin square. But for n even, this is impossible, since $n-1$ is odd and $(n-1)/2$ is not an integer.

In a left nearfield it is easy to see that for each $a, b \in R$, $a * (-b) = -(a * b)$.

Lemma 5. For each b in a left nearfield R, $(-1) * b = -b$.

Proof: $(-1) * (-1) = -((-1) * 1) = -(-1) = 1$. If it were the case that for some $b' \in R$, $(-1) * b' + b' \neq 0$. Then

$$\begin{aligned}
(-1) * ((-1) * b' + b') &= (-1) * ((-1) * b')) + (-1) * b' \\
&= ((-1) * (-1)) * b' + (-1) * b' \\
&= 1 * b' + (-1) * b' \\
&= (-1) * b' + b' \\
&= 1 * ((-1) * b' + b')
\end{aligned}$$

By Lemma 1 we would have $-1 = 1$. But then

$$(-1) * b' + b' = 1 * b' + b' = b' * 1 + b' = b' * (-1) + b' = 0,$$

a contradiction. It follows that for all $b \in R$, $(-1) * b = -b$.

Lemma 6. In a left nearfield $(R, +, *)$, for each $a, b, c \in R$, $(-a) * b = -(a * b)$.

Proof: If $a = 0$, then $-a = 0$ and $(-a) * b = -(a * b) = 0$. If $a \neq 0$, then

$$\begin{aligned}
a^{-1} * [(-a) * b + a * b] &= a^{-1} * ((-a) * b) + a^{-1} * (a * b) \\
&= (a^{-1} * (-a)) * b + (a^{-1} * a) * b \\
&= (-(a^{-1} * a)) * b + 1 * b \\
&= (-1) * b + b \\
&= -(1 * b) + b \qquad \text{by Lemma 5} \\
&= 0
\end{aligned}$$

Since $a^{-1} \neq 0$, then $(-a) * b + a * b = 0$, that is, $(-a) * b = -(a * b)$.

Lemma 7. For R a left nearfield, $C^x, C^y \in \mathcal{C}$ are transposes if and only if $x + y = 1$.

Proof: Suppose that

$$x + y = 1.$$

Then for all $i, j \in R$ and $i \neq j$,

$$\begin{aligned} (j-i) * (x+y) &= j - i \\ (j-i) * x + (j-i) * y &= j - i \\ (j-i) * x + i &= -((j-i) * y) + j \end{aligned}$$

But by Lemma 6, $-(a * b) = (-a) * b$, so

$$\begin{aligned} (j-i) * x + i &= (i-j) * y + j \\ c^x_{ij} &= c^y_{ji} \end{aligned}$$

Hence,

$$C^x = (C^y)^T$$

On the other hand, if $C^x = (C^y)^T$, the computation above reverses to show that $x + y = 1$.

Theorem 3. For n even and R a nearfield $\mathcal{C}$ is the expansion of an OSO set.

Proof: Since $(R, +)$ is a group, for every $x \in R$ there exists a unique solution $y \in R$ to the equation $x + y = 1$. By Lemma 4 since n is even, $\mathcal{C}$ contains no symmetric Latin square. Therefore, for every $x \in R$ the unique solution y to $x + y = 1$ is not x. Furthermore, by Lemma 7, C^x and C^y are transpose Latin squares. Thus, $\mathcal{C}$ is the expansion of an OSO set.

Theorem 4. For n odd and R a nearfield, $\mathcal{C} = O \cup \{S\}$ where O is the expansion of an OSO set and S is a symmetric Latin square.

Proof: Since $(R, +)$ is a group, for every $x \in R$ there exists a unique solution $y \in R$ to the equation $x + y = 1$. Since $(R, +)$ is abelian, the solutions occur in pairs. One pair of solutions is $(0, 1)$. Since n and $n-2$ are odd and since by Lemma 2 there is at most one symmetric Latin square in a set of mutually orthogonal Latin squares, there is exactly one $x \in R - \{0, 1\}$ such that $x + x = 1$ and $C^x = S$ is symmetric. There are $(n-3)/2$ pairs (x, y) such that $x, y \in R - \{0, 1\}$, $x \neq y$ and $x + y = 1$. For these pairs (x, y), $C^x = (C^y)^T$ and consequently $O = \{C^x, C^y \mid x, y \in R - \{0, 1\},\ x \neq y \text{ and } x + y = 1\}$ is the expansion of an OSO set.

In summary, from Theorems 2, 3 and 4, when R is a nearfield of even order, the associated set C is the expansion of an OSO set and $\mathcal{C} \cup \{C^-\}$ is a complete set of mutually orthogonal Latin squares. When R is a nearfield of odd order, the associated set C consists of the expansion of an OSO set O and one symmetric Latin square S. Furthermore, $\mathcal{C} \cup \{C^-\} = \mathcal{O} \cup \{S, C^-\}$ is a complete mutually orthogonal set.

REFERENCES

1. R. K. Brayton, D. Coppersmith, and A. J. Hoffman, "Self-orthogonal Latin squares of all orders $n \neq 2, 3, 6$," Bull. Am. Math. Soc., Vol. 80, No. 1 (Jan., 1974), 116-118.
2. R. K. Brayton, D. Coppersmith, and A. J. Hoffman, "Self-orthogonal Latin squares," Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), Tomo II, 509-517. Atti dei Convegni Lincei, No. 17, Accad. Naz. Lincei, Rome, 1976.
3. G. P. Graham and C. E. Roberts, "Maximal orthogonal sets of self-orthogonal Latin squares," Congressus Numerantium, 83 (1991), 125-128.
4. H. F. MacNeish, "Euler squares," Ann. Math., 23 (1922), 221-227.
5. N. S. Mendelsohn, "Latin squares orthogonal to their transposes," J. Comb. Theory, 11 (1971), 187-189.
6. R. C. Mullin and E. Nemeth, "A construction for self-orthogonal Latin squares from certain Room squares," Proceedings of the Louisiana Conference on Combinatorics, Graph Theory and Computing (Louisiana State University, Baton Rouge, LA, 1970), 213-226.
7. S. K. Stein, "On the foundation of quasigroups," Trans. Amer. Math. Soc., 85 (1957), 228-256.
8. H. J. Zassenhaus, "Über endliche Fastkörper", Abh. Math. Sem. Hamburg, 11 (1936), 187-220.