On the Existence of k-SOLSSOMs

Sobre la Existencia de k-SOLSSOMs

A. R. Ashrafi (ashrafi@vax.ipm.ac.ir)
A. Gordji
Department of Mathematics
Faculty of Science
University of Kashan
Kashan, Iran.

Abstract

In [2] Finizio reports some new results about k-SOLSSOMs. One of these results states that there exist 2−SOLSSOM(n), for all $n > 4308$ and if $n > 135$ is an odd integer, a 2−SOLSSOM(n) exists. In addition, when $n \equiv 0 \pmod{8}$, and $n \not\in \{24, 40, 48\}$, a 2−SOLSSOM(n) exists. These results were proved by Lee in [4].

In this paper we prove that if $p \geq 5$ is the least prime factor of $n$, then a $\frac{p+3}{2}$−SOLSSOM(n) exists. In particular, if $n \in \{49, 77, 91, 119, 133\}$, a 2−SOLSSOM(n) exists, thus extending Lee’s results.

Key words and phrases: Latin square, orthogonal latin square, self-orthogonal latin square, SOLSSOM.

Resumen

En [2] Finizio reporta algunos nuevos resultados acerca de k-SOLSSOMs. Uno de estos resultados afirma que para todo $n > 4308$ existe un 2−SOLSSOM(n), y si $n > 135$ es un entero impar, existe un 2−SOLSSOM(n). Adicionalmente, cuando $n \equiv 0 \pmod{8}$ y $n \not\in \{24, 40, 48\}$, existe un 2−SOLSSOM(n). Estos resultados fueron probados por Lee en [4].

En este artículo probamos que si $p \geq 5$ es el menor factor primo de $n$, entonces existe un $\frac{p+3}{2}$−SOLSSOM(n) . En particular, si $n \in \{49, 77, 91, 119, 133\}$, existe un 2−SOLSSOM(n), extendiendo así los resultados de Lee.

Palabras y frases clave: Cuadrado latino, cuadrado latino ortogonal, cuadrado latino auto-ortogonal, SOLSSOM.
1 Introduction

In this section we describe some definitions. If \( A = [a_{ij}] \) and \( B = [b_{ij}] \) are two \( n \times n \) matrices, the join \( (A, B) \) of \( A \) and \( B \) is the \( n \times n \) matrix whose \((i, j)-th\) entry is the pair \((a_{ij}, b_{ij})\). The latin squares \( A, B \) of order \( n \) are orthogonal if all the entries in the join of \( A \) and \( B \) are distinct. Latin squares \( A_1, \ldots, A_r \) are mutually orthogonal if they are orthogonal in pairs. The abbreviation MOLS will be used for mutually orthogonal latin squares.

A self-orthogonal latin square (SOLS) is a latin square that is orthogonal to its transpose. Finally, a \( k \)-SOLSSOM is a set \( \{S_1, S_2, \ldots, S_k\} \) of self-orthogonal latin squares, together with a symmetric latin square \( M \), for which \( \{S_i, S_i^T \mid 1 \leq i \leq k\} \cup \{M\} \) is a set of \( 2k + 1 \) MOLS.

The objective of this paper is to prove:

Theorem 1. If \( p \leq 5 \) is the least prime factor of \( n \), then a \( \frac{p-3}{2} \)-SOLSSOM exists. In particular, if \( n \in \{49, 77, 91, 119, 133\} \), a \( 2 \)-SOLSSOM exists.

In this paper, as usual, \( \mathbb{Z}_n \) denotes the cyclic group of order \( n \). Our notations are standard and taken mainly from [1] and [2].

2 Proof of the Theorem

For any odd prime power \( q \) there exist \( \frac{q-3}{2} \)-SOLSSOMs and, for \( n \geq 1 \), there is a \( (2^{n-1} - 1) \)-SOLSSOM \((2^n)\) (see [2, 41.21]). In [4], Lee shows that there exist 2-SOLSSOMs for all \( n > 4308 \) and, if \( n > 135 \) is an odd integer, a 2-SOLSSOM exists. In addition, when \( n \equiv 0 \pmod{8} \), and \( n \not\in \{24, 40, 48\} \), a 2-SOLSSOM exists.

In this section we use a group theoretical approach to the problem of existence of \( k \)-SOLSSOMs. We first assume that \( A = [a_{ij}] \) is an arbitrary latin square of order \( n \). We define \( R_i = [a_{i1} \ldots a_{in}] \) and \( C_i = [a_{1i} \ldots a_{ni}]^T \), for all \( 1 \leq i \leq n \), then it is easy to see that \( R_i \) is the \( i \)-th row and \( C_i \) is the \( i \)-th column of the latin square \( A \) and we can write

\[
A = [C_1C_2 \ldots C_n] = [R_1R_2 \ldots R_n]^T
\]

Next we assume that \( \sigma \in S_n \), the symmetric group on \( n \) letters, then \( \sigma \) induces a permutation on rows, columns and elements of the latin square \( A \) which we denote by the same symbol. Set \( A_r(\sigma) = [R_{\sigma(1)}R_{\sigma(2)} \ldots R_{\sigma(n)}]^T \) and \( A_c(\sigma) = [C_{\sigma(1)}C_{\sigma(2)} \ldots C_{\sigma(n)}]^T \), then it is obvious that \( A_r(\sigma) \) and \( A_c(\sigma) \) are latin squares and so for all \( \sigma, \tau \in S_n \), \( A(\sigma, \tau) = (A_r(\sigma))_{c}(\tau) \) is a latin square.
Now we assume that $G$ is a group of order $n$ and $\sigma$ and $\tau$ are permutations of $G$ which can be identified with the permutations of $S_n$. It is obvious that the multiplication Cayley table $A$ of the group $G$ is a latin square and we can use the above argument to obtain the latin square $A(\sigma, \tau)$.

We begin with an elementary lemma which will be of use later.

**Lemma 1.** Let $G = \{x_1, \ldots, x_n\}$ be a group of order $n$, $A$ be the Cayley table of $G$ and $\alpha, \beta, \tau, \sigma \in S_n$. The latin squares $A(\alpha, \beta)$ and $A(\tau, \sigma)$ are orthogonal if and only if, for all $1 \leq i, j, r, s \leq n$, where $(i, j) \neq (r, s)$, the following condition is satisfied:

$$\alpha(x_i)\beta(x_j) = \alpha(x_r)\beta(x_s) \implies \tau(x_i)\sigma(x_j) \neq \tau(x_r)\sigma(x_s).$$

**Proof.** Let $A = [a_{ij}]$ be the Cayley table of $G$, $A(\alpha, \beta) = [b_{ij}]$ and $A(\tau, \sigma) = [c_{ij}]$. Then it is easy to see that $b_{ij} = a_{\alpha(i)\beta(j)} = x_{\alpha(i)}x_{\beta(j)}$ and $c_{ij} = a_{\tau(i)\sigma(j)} = x_{\tau(i)}x_{\sigma(j)}$. Suppose $A(\alpha, \beta)$ and $A(\tau, \sigma)$ are orthogonal, $(i, j) \neq (r, s)$ and $\alpha(x_i)\beta(x_j) = \alpha(x_r)\beta(x_s)$. If $\tau(x_i)\sigma(x_j) = \tau(x_r)\sigma(x_s)$ then $b_{ij} = b_{rs}$ and $c_{ij} = c_{rs}$, hence $(b_{ij}, c_{ij}) = (b_{rs}, c_{rs})$ and by orthogonality we must have $i = r$ and $j = s$, a contradiction. Therefore the above condition is satisfied. We can repeat this argument to yield the converse of the theorem. \qed

**Corollary 1.** Suppose $\alpha, \beta \in S_n$ and let $A$ be the multiplication table of the group $G$. Then the latin squares $A(i, \alpha)$ and $A(i, \beta)$, where $i$ is the identity element of $S_n$, are orthogonal if and only if the map $\alpha^{-1}\beta(i) = \alpha(x)^{-1}\beta(x)$, is bijective.

**Proof.** Suppose that $\alpha^{-1}\beta(x_j) = \alpha^{-1}\beta(x_s)$, so $\alpha(x_s)\alpha(x_j^{-1}) = \beta(x_s)\beta(x_j^{-1})$. If $\alpha(x_s)\alpha(x_j^{-1}) = x_j^{-1}x_s$, then $x_j = x_s$. Conversely, assume that $\alpha^{-1}\beta$ is bijective, $(i, j) \neq (r, s), x_i\alpha(x_j) = x_i\alpha(x_s)$ and $x_i\beta(x_j) = x_i\beta(x_s)$. Then $\alpha^{-1}\beta(x_j) = \alpha^{-1}\beta(x_s)$ and, since $\alpha^{-1}\beta$ is bijective, $x_j = x_s$. This implies that $x_i = x_r$, which is a contradiction. \qed

**Corollary 2.** Let $G$ be a group and $f_i \in \text{Aut}(G), 1 \leq i \leq 4$. The latin squares $A(f_1, f_2)$ and $A(f_3, f_4)$ are orthogonal if and only if for all $x, y \in G$ with $x \neq e, y \neq e$ the following condition holds:

$$f_1(x) = f_2(y) \implies f_3(x) \neq f_4(y)$$

**Proof.** We assume that $f_1(x) = f_2(y)$, so $f_1(x)f_2(e) = f_1(e)f_2(y)$, and by Lemma 1, $f_3(x)f_4(e) \neq f_3(e)f_4(y)$, i.e. $f_3(x) \neq f_4(y)$. Conversely, suppose $f_1(x_i) = f_1(x_j)$, so $f_1(x_i^{-1}x_j) = f_2(x_i^{-1}x_j)$, which yields the required result. \qed
Corollary 3. Let \( G \) be the cyclic group of order \( n \), \( p \) the least prime factor of \( n \) and \( A \) the Cayley table of \( G \). Then for all \( 1 \leq r < p \) the latin squares \( A(i, f_r) \), where \( f_r(x) = rx \), are orthogonal.

**Proof.** It is well known that \( f_r \in Aut(Z_n) \) if and only if \( (r, n) = 1 \), hence for all \( 1 \leq i \leq p - 1 \), \( f_i \in Aut(Z_n) \). We show now that if \( 1 < i, j \leq p - 1 \), then \( f_i - f_j \) is bijective. To do this, suppose \((f_i - f_j)(x) = (f_i - f_j)(y)\). Then \((i - j)(x - y) = 0\) and since \((n, i - j) = 1\), \(x = y\). Now by Corollary 1, the proof is complete.

**Remark 1.** Let \( G \) be a group of order \( n \) and let \( A \) be the Cayley table of \( G \). It is easy to see that the latin square \( A(\alpha, \beta) \) is self-orthogonal if and only if \( A(\alpha, \beta) \) and \( A(\beta, \alpha) \) are orthogonal latin squares. Therefore by Lemma 1, the latin square \( A(\alpha, \beta) \) is self-orthogonal if and only if for any elements \( x, y, z, t \) of \( G \), the following condition holds,

\[
\alpha(x)\beta(y) = \alpha(z)\beta(t) \iff \beta(x)\alpha(y) \neq \beta(t)\alpha(z).
\]

**Remark 2.** Assume that \( f, g \in Aut(G) \). By Corollary 2, the latin square \( A(f, g) \) is self-orthogonal if and only if for any non-identity elements \( x, y \in G \), \( f(x) = g(y) \) implies that \( f(y) \neq g(x) \).

**Remark 3.** Let \( G \) be the cyclic group of order \( n \) and \( A \) be the Cayley table of \( G \). If \( p \) is the least prime factor of \( n \) then all of the latin squares \( A(i, f_r) \), \( 1 < r < p - 1 \), are mutually and self-orthogonal.

**Proof of Theorem 1.** Assume that there exists a \( 2 \times k \) matrix \( M = (a_{ij}) \) with the following conditions:

(a) For all \( i = 1, 2 \) and \( 1 \leq j \leq n \), \( a_{ij} < n \), \((a_{ij}, n) = 1 \) and \( a_{1j} \neq a_{2j} \),

(b) For all \( 1 \leq j' \leq j \leq k \), \((a_{1j}a_{1j'} - a_{2j}a_{2j'}), n) = 1 \),

(c) For all \( 1 \leq j' \leq j \leq k \), \((a_{1j}a_{2j'} - a_{2j}a_{1j'}), n) = 1 \).

We now show that with these conditions, a \( k \text{-SOLSSOM}(n) \) exists. To do this, let \( i = 1, 2, 1 \leq j \leq k \) and \( g_{ij} \) be the map \( x \mapsto a_{ij}x \). Then it is easy to see that \( g_{ij} \in Aut(Z_n) \). Set \( A_j = A(g_{1j}, g_{2j}) \), in which \( A \) is the latin square obtained from the Cayley table for \( Z_n \). Then we can see that the set \( \{A, A_j' \mid 1 \leq j \leq k\} \cup \{A\} \) form a \( k \text{-SOLSSOM}(n) \). Suppose that \( p \geq 5 \) is the least prime factor of \( n \). We now define a \( 2 \times \frac{p^2 - 3}{2} \) matrix \( M = (a_{ij}) \) as follows:

\[
a_{1j} = j \quad \text{and} \quad a_{2j} = j + 1.
\]

Now we can see that the matrix \( M \) satisfies the conditions (a), (b) and (c). Therefore a \( \frac{p^2 - 3}{2} \text{-SOLSSOM}(n) \) exists.

\( \square \)
Acknowledgements

We are pleased to thank professor G. B. Khosroshahi and Dr. R. Torabi for many helpful conversations on the subject. Also, the authors would like to thank the referees for precious observations.

References


