ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 16, No. 1, 2021, *pp.*064-070

A construction of special self-orthogonal Latin squares based on frequency squares

Yong Zhang, Wen Li, Xuerong Shi
School of Mathematics and Statistics, Yancheng Teachers University,
Yancheng 224002, Jiangsu, P. R. China
(Received February 21, 2021, accepted April 05, 2021)

Abstract: Let $n = p^k$, where p is a prime and $k \geq 2$. In this paper, a construction for weakly pandiagonal strongly symmetric self-orthogonal diagonal Latin squares of order n is given by using frequency squares over finite field $of\ order\ p$. It is proved that there exists a weakly pandiagonal strongly symmetric self-orthogonal diagonal Latin square of order n for $n > 4$.

Keywords: Latin square, frequency square, self-orthogonal, strongly symmetric, weakly pandiagonal.

1. Introduction

A Latin square of order n is an $n \times n$ array such that every row and every column is a permutation of an n-set S. A transversal in a Latin square is a set of positions, one per row and one per column, among which the symbols occur precisely once each. A diagonal Latin square is a Latin square with the additional property that the main diagonal and back diagonal are both transversals.

Two Latin squares of order n are orthogonal if each symbol in the first square meets each symbol in the second square exactly once when they are superposed. A Latin square of order n is self-orthogonal if it is orthogonal to its transpose.

Let $I_n = \{0,1,\cdots,n-1\}$. A Latin square of order n over I_n, $L = (l_{i,j})$ is called strongly symmetrical if $l_{i,j} + l_{n-1-i,n-1-j} = n-1$ for all $i,j \in I_n$.

The investigation of the existence of a strongly symmetrical self-orthogonal diagonal LS(n) was started by Danhof et al [2]. They show that there exists a strongly symmetrical self-orthogonal diagonal LS(n) for each $n \in \{4,5,7,8,12\}$ and a strongly symmetrical self-orthogonal diagonal LS(n) does not exist for each $n \in \{2,3,6,10\}$. Du and Cao proved that a strongly symmetrical self-orthogonal diagonal LS (n) exists for all positive integers $n \equiv 0,1,3(mod 4)$ and $n \neq 3, 15$ in 2002 [3]. Cao and Li completely solved the existence of SSSODLS (n) [4]. They proved the following.

Lemma 1.1 ([4]) There exists strongly symmetrical self-orthogonal diagonal LS (n) if and only if $n \equiv 0,1,3(mod 4)$ and $n \neq 3$.

Let $A = (a_{i,j})$ be an $n \times n$ array, we index its rows and columns by $I_n = \{0,1,\cdots,n-1\}$. For $k \in I_n$, the set $\{a_{i,k+i} | i \in I_n\}$ and $\{a_{i,k-i} | i \in I_n\}$ are called k-th right diagonal and k-th left diagonal of A respectively, where the additions of the subscripts are all taken modulo n.

If A is a Latin square with the property that every right diagonal and every left diagonal is a transversal, then A is said to be a pandiagonal Latin square or a Knut Vik design, denoted by pandiagonal LS(n). It has been used in statistical designs to eliminate sources of variation along four dimensions ([10]) and in n-queens problems ([11, 12]) etc. Hedayat proved in [16] that a pandiagonal LS(n) and orthogonal pandiagonal LS(n) exist if and only if $n \equiv 1,5(mod 6)$.

Xu introduced a weak form of Knut Vik design to construct pandiagonal magic squares ([5]). A Latin square $A = (a_{i,j})$ of order n over I_n is called weakly pandiagonal, if the sum of n elements in each right diagonal and each left diagonal is the same, i.e. for each $w \in I_n$, $\sum_{i=0}^{n-1} l_{i,i+w} = \frac{n(n-1)}{2}$ and $\sum_{i=0}^{n-1} l_{i,w-i} = \frac{n(n-1)}{2}$, where the operations in the subscripts are all taken modulo n. Clearly, a pandiagonal LS(n) is necessarily a weakly pandiagonal LS(n). Xu proved in [5] that

Lemma 1.2 ([5]) An weakly pandiagonal self-orthogonal LS(n) exists if $n \equiv 0,1,3(mod\ 4)$ and $n \equiv\!\!/\ 3,6(mod\ 9)$.

A weakly pandiagonal strongly symmetrical self-orthogonal diagonal LS (n) is denoted by *LS(n). The existence of *LS(n) is an intriguing problem itself and it is also an improvement question of Cao and Li's result.

The only known result of *LS(n) attributes to Zhang et al [6]. Although they proved that there exists a weakly pandiagonal strongly symmetrical self-orthogonal LS(n) provided $n \equiv 1,5(mod6), n \geq 5$, it is easy to verify that their result is also true for diagonal cases. So we have

Lemma 1.3 ([6]) There exists a *LS(n) provided $n \equiv 1,5(mod\ 6), n \geq 5$.

In this paper, we shall further investigate *LS(n) especially when n is a prime power. We shall use frequency squares to give a construction and prove the following.

Theorem 1.4 There exists a *LS(n) for $n > 4$ and n is a prime power.

A construction based on frequency squares will be discussed in section 2, and the proof of Theorem 1.4 will be given in section 3.

2. A construction for *LS(n) based on frequency squares

Frequency square will be used in our construction for *LS(n)s. Let $n = m\lambda$. An F$(n;\lambda)$ frequency square is an $n \times n$ array in which each of m distinct symbols occurs exactly λ times in each row and column. Moreover, two such squares are orthogonal if when superimposed, each of the m^2 possible ordered pairs occurs λ^2 times.

For $n = m\lambda$, it is known that the maximum number of mutually orthogonal frequency squares of the form F$(n;\lambda)$ is bounded above by $(n-1)^2/(m-1)$. Further, if q is any prime power and $i \geq 1$ is a positive integer, then using linear polynomials in $2i$ variables over the finite field F_q, a complete set of $F(q^i, q^{i-1})$ mutually orthogonal frequency squares can be constructed. Specifically, take the polynomials $a_1x_1 + \cdots + a_{2i}x_{2i}$ where neither $(a_1, \cdots, a_i)$ nor $(a_{i+1}, \cdots, a_{2i})$ is the zero vector $(0, \cdots, 0)$ and no two of the vectors are nonzero F_q multiples of each other, i.e. $(a'_1, \cdots, a'_i) \neq e(a_1, \cdots, a_i)$ for any nonzero $e \in F_q$. Further details may be found in Chapter 4 of [8].

Let $V = V_k(GF(p))$, $n = p^k$. Take

$$A_h = (a_{h,0}, a_{h,1}, \cdots, a_{h,k-1}), B_h = (b_{h,0}, b_{h,1}, \cdots, b_{h,k-1}),$$

$$X = (x_0, x_1, \cdots, x_{k-1}), Y = (y_0, y_1, \cdots, y_{k-1}),$$

where A_h, B_h are constant vectors in V, $h = 0,1, \cdots, k-1$, X, Y are variable vectors in V.

For any $i \in Z_n$, there exist a vector $R_i = (r_{i,0}, r_{i,1}, \cdots, r_{i,k-1})$ such that

$$i = r_{i,0}p^{k-1} + r_{i,1}p^{k-2} + \cdots + r_{i,k-1}.$$

Let $V(1) = \{R_0, R_1, \cdots, R_{n-1}\}$, $V(2) = \{C_0, C_2, \cdots, C_{n-1}\}$, where $C_i = R_i$. Index the rows of an $n \times n$ array by $V(1)$ and the columns by $V(2)$.

Note that there are strongly symmetric property,

$$n - 1 - i = r_{n-1-i,0}p^{k-1} + r_{n-1-i,1}p^{k-2} + \cdots + r_{n-1-i,k-1},$$

$$n - 1 = (p-1)(p^{k-1} + p^{k-2} + \cdots + p + 1),$$

$$i + n - 1 - i = (r_{i,0}p^{k-1} + r_{i,1}p^{k-2} + \cdots + r_{i,k-1})$$

$$+(r_{n-1-i,0}p^{k-1} + r_{n-1-i,1}p^{k-2} + \cdots + r_{n-1-i,k-1})$$

$$= (r_{i,0} + r_{n-1-i,0})p^{k-1} + \cdots + (r_{i,k-1} + r_{n-1-i,k-1}),$$

which forces $r_{i,0} + r_{n-1-i,0} = p - 1$ for any $i \in I_n$. Therefore

$$R_i + R_{n-1-i} = (r_{i,0}, r_{i,1}, \cdots, r_{i,k-1}) + (r_{n-1-i,0}, r_{n-1-i,1}, \cdots, r_{n-1-i,k-1})$$

$$=(p-1, p-1, \cdots, p-1).$$

Let a, n be integers, $< a >_p$ be the smallest nonnegative integer such that $a \equiv < a >_p (mod\ n)$, i.e, $< a >_p = r$ if $a = pn + r$, where p, r are integers and $0 \leq r < n$.

We use $\cdot$ to denote the inner product in V. Define a linear function from $V(1) \times V(2)$ to $GF(p)$.

Let $F_h = \left(F_h(R_i, C_j)\right)_{n\times n}$, where