PAPER Special Section on Discrete Mathematics and Its Applications

On Dimensionally Orthogonal Diagonal Hypercubes

Xiao-Nan LU[†*a)], ***Member and*** **Tomoko ADACHI**[††b)], ***Nonmember***

SUMMARY In this paper, we propose a notion for high-dimensional generalizations of mutually orthogonal Latin squares (MOLS) and mutually orthogonal diagonal Latin squares (MODLS), called mutually dimensionally orthogonal d-cubes (MOC) and mutually dimensionally orthogonal diagonal d-cubes (MODC). Systematic constructions for MOC and MODC by using polynomials over finite fields are investigated. In particular, for 3-dimensional cubes, the results for the maximum possible number of MODC are improved by adopting the proposed construction.

key words: *Latin square, Latin cube, dimensional orthogonality, transversal, finite field, permutation polynomial, irreducible polynomial*

1. Introduction

A *Latin square* of order n is an $n \times n$ array containing n distinct symbols with the property that in each row and each column, each symbol occurs exactly once. Moreover, if each symbol occurs exactly once in each diagonal, then it is said to be a *diagonal* Latin square.

Two Latin squares of order n are *orthogonal* if when superimposed, each of the n^2 ordered pairs of symbols appears exactly once. Moreover, a collection of Latin squares is said to be *mutually orthogonal* if the members are pairwise orthogonal.

Latin squares have been extensively studied in discrete mathematics, computer sciences, and statistical designs of experiments. (See the monographs [1]–[3] for details.)

Example 1.1: Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two diagonal Latin squares as follows:

$$\mathcal{L}_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{bmatrix}, \quad \mathcal{L}_2 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix}.$$

By superimposing $\mathcal{L}_1$ and $\mathcal{L}_2$, we obtain a square

$$\mathcal{L} = \begin{bmatrix} 00 & 11 & 22 & 33 \\ 23 & 32 & 01 & 10 \\ 31 & 20 & 13 & 02 \\ 12 & 03 & 30 & 21 \end{bmatrix}$$

containing all the elements in $\{0, 1, 2, 3\}^2$. Hence, $\mathcal{L}_1$ and $\mathcal{L}_2$ are orthogonal.

The problems of determining the maximum possible number of mutually orthogonal Latin squares (MOLS) and mutually orthogonal diagonal Latin squares (MODLS) have attracted much attention in the past century. The interested reader is referred to [1], [2] and references therein for more details.

However, high-dimensional generalizations of MOLS and MODLS are less studied and the related results are presented in several different notation. In this paper, we aim to give a unified notion and propose some systematic constructions by using polynomials over finite fields.

The remaining of this paper is organized as follows: In Sect. 2, we will introduce the d-dimensional generalizations of MOLS and MODLS, called mutually dimensionally orthogonal d-cubes of type $d-1$ (simply, $(d, d-1)$-MOC(n)) and mutually dimensionally orthogonal diagonal d-cubes of type $d-1$ (simply, $(d, d-1)$-MODC(n)), respectively. In Sect. 3, we will summarize the known results on $(d, d-1)$-MOC(n) and $(d, d-1)$-MODC(n). In Sect. 4, we will review the fundamental constructions of $(d, d-1)$-MOC(n) via finite fields, and then propose the finite field construction for $(d, d-1)$-MODC(n). In Sect. 5, we will concentrate on the 3-dimensional cubes and show the improvement for $(3, 2)$-MODC(n). Lastly, concluding remarks and further work will be given in Sect. 6.

2. Definitions and Notation

2.1 Hypercubes and Their Orthogonality

Let d and n be positive integers. Let t be an integer with $0 \le t \le d-1$. A *d-dimensional hypercube* (simply, d-cube) of order n and type t is an $n \times n \times \cdots \times n$ (d times) array on n distinct symbols with the property that each symbol occurs exactly n^{d-t-1} times in every $(d-t)$-dimensional subarray obtained by fixing t indices of the array. In particular, when $d = 2$ and $t = 1$, the above definition of hypercubes reduces to Latin squares. For $d = 2$ and $d = 3$, we simply say squares and cubes, respectively.

Remark 2.1: The term "Latin d-cube" is usually used

Manuscript received October 21, 2019.
Manuscript revised January 16, 2020.

[†]The author is with Department of Industrial Administration, Faculty of Science and Technology, Tokyo University of Science, Noda-shi, 278-8510 Japan.
[††]The author is with Department of Information Sciences, Toho University, Funabashi-shi, 274-8510 Japan.
[*]Presently, with Department of Computer Science and Engineering, Faculty of Engineering, University of Yamanashi.
a) E-mail: lu@rs.tus.ac.jp
b) E-mail: adachi@is.sci.toho-u.ac.jp

DOI: 10.1587/transfun.2019DMP0009

to refer to a d-cube of type 1 in literature (see [4, Remark 22.33] and [5]). Whereas, sometimes "Latin d-cube" is used to refer to a d-cube of type $d-1$ (see, for example, [6]–[8]). To avoid ambiguity, in this paper, we use "type $d-1$" rather than "Latin" for $d \geq 3$.

Two d-cubes of order n are *orthogonal* when superimposed, each of the n^2 ordered pairs of symbols appears exactly n^{d-2} times. Moreover, a collection of d ($d \geq 2$) d-cubes of order n is *dimensionally orthogonal*, or *d-orthogonal*, if when superimposed, each of the n^d ordered d-tuples appears exactly once. Furthermore, a set of j ($j \geq d$) d-cubes is *mutually d-orthogonal* if any choice of d of them preserves the d-orthogonal property (see [5]). When $d = 2$ and $t = 1$, the above definitions reduce to the orthogonality of Latin squares.

For convenience, we use the following notation throughout this paper.

- A collection of mutually d-orthogonal d-cubes of type t and order n is abbreviated as (d, t)-MOC(n).
- The maximum possible number of d-cubes in a $(d, d-1)$-MOC(n) is denoted by $N^{(d)}(n)$.

2.2 Diagonal Hypercubes

A d-cube $\mathcal{H}$ can be represented by the indices $i_1, i_2, \ldots, i_d$ and the corresponding entry $x_{i_1,i_2,\ldots,i_d}$ as

$$\mathcal{H} = \{(i_1, i_2, \ldots, i_d; x_{i_1,i_2,\ldots,i_d}) \mid 1 \leq i_k \leq n, 1 \leq k \leq d\}.$$

Definition 2.2: Let

$$\mathscr{T} = \left\{(i_1^{(j)}, i_2^{(j)}, \ldots, i_d^{(j)}; x_{i_1^{(j)},i_2^{(j)},\ldots,i_d^{(j)}}) \mid 1 \leq j \leq n\right\}$$

be a subset of $\mathcal{H}$ with $|\mathscr{T}| = n$. If $(i_k^{(1)}, i_k^{(2)}, \ldots, i_k^{(n)})$ forms a permutation of $(1, 2, \ldots, n)$ for each $1 \leq k \leq d$, and $(x_{i_1^{(j)},i_2^{(j)},\ldots,i_d^{(j)}})_{1\leq j\leq n}$ also forms a permutation of all the symbols, then $\mathscr{T}$ is called a *transversal*.

The diagonals of a square (main diagonal and back diagonal) can be intuitively realized. For d-cubes, diagonals can be defined as follows:

Definition 2.3: Let τ be a function defined by $\tau(i) = n - i + 1$ for $1 \leq i \leq n$. Let $\tau^0(i)$ and $\tau^1(i)$ denote the identity mapping and $\tau(i)$, respectively. For each binary vector $\boldsymbol{s} = (s_1, s_2, \ldots, s_{d-1}) \in \{0, 1\}^{d-1}$, the subset

$$\mathscr{D}_{\boldsymbol{s}} = \{(i, \tau^{s_1}(i), \tau^{s_2}(i), \ldots, \tau^{s_{d-1}}(i); x_{i,\tau^{s_1}(i),\tau^{s_2}(i),\ldots,\tau^{s_{d-1}}(i)}) \mid 1 \leq i \leq n\} \subseteq \mathcal{H}$$

is called a *diagonal* of $\mathcal{H}$. Then, $\mathcal{H}$ has 2^{d-1} diagonals.

For example, for squares ($d = 2$), the main diagonal and the back diagonal can be written, respectively, as follows:

$$\mathscr{D}_0 = \{(i, i; x_{i,i}) \mid 1 \leq i \leq n\} \text{ and}$$

$$\mathscr{D}_1 = \{(i, n-i+1; x_{i,n-i+1}) \mid 1 \leq i \leq n\}.$$

Definition 2.4: A d-cube is *diagonal* if all of its diagonals are transversals.

For convenience, we use the following notation throughout this paper.

- A collection of mutually d-orthogonal diagonal d-cubes of type t and order n is abbreviated as (d, t)-MODC(n).
- The maximum possible number of d-cubes in a $(d, d-1)$-MODC(n) is denoted by $D^{(d)}(n)$.

Clearly, $D^{(d)}(n) \leq N^{(d)}(n)$ for given n and d.

3. Known Results and Constructions

3.1 Known Constructions on $(d, d-1)$-MOC(n)

Ethier et al. [5, Theorem 2.7] showed that for $d \geq 2$, the number $N^{(d)}(n)$ of d-cubes in a $(d, d-1)$-MODC(n) cannot exceed $n+d-1$. Constructions have been proposed in several different notation. A recursive construction for $(d, d-1)$-MOC(n) of size d was proposed early in 1974 by Arkin and Straus [7] by using a $(d-1, d-2)$-MOC(n) of size $d-1$. While, Trenkler used the same idea and independently introduced equivalent constructions in [9] (for $d = 3$) and [8] (for general d).

Theorem 3.1: If there exist two orthogonal Latin squares of order n, then there exist a $(3, 2)$-MOC(n) of size 4 (see [7, §2]), and $(d, d-1)$-MOC(n) of size d for each $d \geq 4$ (see [7, §2] and [8]).

Consequently, a lower bound of $N^{(d)}(n)$ can be obtained from Theorem 3.1 combining with the existence of mutually orthogonal Latin squares. We summarize the known results as follows:

Corollary 3.2: For any $n \geq 2$ and $d \geq 2$, the following hold:

(i) [5, Theorem 2.7] $N^{(d)}(n) \leq n + d - 1$;

(ii) For any $n \geq 2$ with $n \neq 6$, it holds that $N^{(d)}(n) \geq d$. Moreover, $N^{(3)}(n) \geq 4$.

3.2 Known Constructions on $(d, d-1)$-MODC(n)

When $d = 2$, the study of $(d, d-1)$-MODC(n) reduces to MODLS, which has been intensively studied. (See [10], [11], [1, §10.2], and their references.)

Theorem 3.3 (see [10]): For any positive integer n with $n \notin \{2, 3, 6\}$, there exists a pair of orthogonal diagonal Latin squares, i.e., $D^{(2)}(n) \geq 2$.

Theorem 3.4 ([11, Theorem 2]): If n is even, then $D^{(2)}(n) \leq n - 2$, whereas if n is odd, then $D^{(2)}(n) \leq n - 3$. Moreover, if n is a prime power, the equality holds (see also [6, Theorems 2.1 and 2.2]).

For $d \geq 3$, using finite fields, Arkin et al. [6] proposed a construction for $(d, d-1)$-MODC(n) (see also Theorem 3.5). In Sect. 4, we will concentrate on the finite field constructions in a more detailed way.

Theorem 3.5 (see [6]): Let q be a prime power with $q \geq d > 2$. The following holds.

(i) [6, Theorem 3.1] If q is odd, then there exists a $(d, d-1)$-MOC(q) of size $q+1$, in which at least $q-(d-1)2^{d-1}$ are diagonal.

(ii) [6, Theorem 3.3] If q is a power of 2, then there exists a $(d, d-1)$-MOC(q) of size $q+1$, in which at least $q+2-d$ are diagonal.

(iii) [6, Theorem 3.2] If $q \geq 4$ is a power of 2, then there exists a $(3, 2)$-MOC(q) of size $q+2$, in which at least q are diagonal.

Example 3.6: A $(3, 2)$-MODC(4) consisting of $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$, $\mathcal{H}_\infty$ is shown as follows, where each 4×4 subarray denotes a layer of the corresponding cube.

$$\mathcal{H}_1 = \left[\begin{array}{cccc|cccc|cccc|cccc} 0&2&3&1&1&3&2&0&2&0&1&3&3&1&0&2\\ 2&0&1&3&3&1&0&2&0&2&3&1&1&3&2&0\\ 3&1&0&2&2&0&1&3&1&3&2&0&0&2&3&1\\ 1&3&2&0&0&2&3&1&3&1&0&2&2&0&1&3 \end{array}\right],$$

$$\mathcal{H}_2 = \left[\begin{array}{cccc|cccc|cccc|cccc} 0&1&2&3&1&0&3&2&2&3&0&1&3&2&1&0\\ 3&2&1&0&2&3&0&1&1&0&3&2&0&1&2&3\\ 1&0&3&2&0&1&2&3&3&2&1&0&2&3&0&1\\ 2&3&0&1&3&2&1&0&0&1&2&3&1&0&3&2 \end{array}\right],$$

$$\mathcal{H}_3 = \left[\begin{array}{cccc|cccc|cccc|cccc} 0&2&3&1&3&1&0&2&1&3&2&0&2&0&1&3\\ 3&1&0&2&0&2&3&1&2&0&1&3&1&3&2&0\\ 1&3&2&0&2&0&1&3&0&2&3&1&3&1&0&2\\ 2&0&1&3&1&3&2&0&3&1&0&2&0&2&3&1 \end{array}\right],$$

$$\mathcal{H}_\infty = \left[\begin{array}{cccc|cccc|cccc|cccc} 0&1&2&3&1&0&3&2&2&3&0&1&3&2&1&0\\ 1&0&3&2&0&1&2&3&3&2&1&0&2&3&0&1\\ 2&3&0&1&3&2&1&0&0&1&2&3&1&0&3&2\\ 3&2&1&0&2&3&0&1&1&0&3&2&0&1&2&3 \end{array}\right].$$

See also Example 5.2 for the construction of the above cubes.

Next, we restate Trenkler's construction [12] in Theorem 3.7 which can be adopted to odd n which is not a prime power (see also [8]). Then, we show the diagonal property in Theorem 3.8 when d is odd and $n > d$.

Theorem 3.7 ([12, Theorem 1]): Let n be an odd positive integer. Let

$$\mathcal{H}_t = \{(i_1, i_2, \ldots, i_d; x^{(t)}_{i_1,i_2,\ldots,i_d}) \mid 1 \leq i_k \leq n, 1 \leq k \leq d\} \quad (1)$$

with

$$x^{(t)}_{i_1,i_2,\ldots,i_d} = \sum_{\ell=1}^{t} (-1)^{\ell-1} i_\ell + (-1)^t \sum_{\ell=t+1}^{d} i_\ell + C_t \quad (2)$$

for each $0 \leq t \leq d-1$, where $C_t = -1$ if d is odd, and $C_t = (-1)^{t+1}\frac{n+1}{2} - 1$ if d is even. The arithmetic in Eq. (2) is considered modulo n as in $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$. Then, $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{d-1}$ form a $(d, d-1)$-MOC(n).

Theorem 3.8: If d is odd and $n > d$ is odd, the d-cubes $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{d-1}$ generated by Eq. (1) are diagonal. Accordingly, $D^{(d)}(n) \geq d$ for any odd d and odd $n > d$.

Proof. With the notation in Definition 2.3, we can express any diagonal element of $\mathcal{H}_t$ as a sum of d terms of $\pm i$ and C_t, for any $1 \leq i \leq n$. Hence, $\mathcal{H}_t$ is diagonal if and only if the coefficient of i, that is, the difference between the numbers of $+i$'s and $-i$'s, is not zero (as in $\mathbb{Z}_n$). Since d is odd, it is impossible to have an equal number of $+i$'s and $-i$'s. Moverover, since $d < n$, even when all the terms are equal to $+i$ (or $-i$), the sum is still non-zero. Therefore, $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{d-1}$ are diagonal. □

4. Constructions for $(d, d-1)$-MODC(n)

4.1 Constructions via Finite Fields

Let $\mathbb{F}_q$ and $\mathbb{F}_q^*$ denote the finite field of order q and its multiplicative group, respectively. A polynomial $f(x_1, x_2, \ldots, x_d)$ is called a permutation polynomial (in d variables over $\mathbb{F}_q$) if the equation $f(x_1, x_2, \ldots, x_d) = a$ has q^{d-1} solutions in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$. Thus, it is natural to utilize a permutation polynomial $f(x_1, x_2, \ldots, x_d)$ for constructing a d-cube. In fact,

$$\left\{(x_1, x_2, \ldots, x_d; f(x_1, x_2, \ldots, x_d)) \mid x_1, x_2, \ldots, x_d \in \mathbb{F}_q\right\}$$

forms a d-cube.

Now we restrict on linear polynomials and summarize some essential lemmas as follows. For detailed proofs, see, for example, [1, §3.3] and [5, §4].

Lemma 4.1 ([5, Lemma 4.2]): Let $f(x_1, x_2, \ldots, x_d) = a_0 x_1 + a_1 x_2 + \cdots + a_{d-1} x_d$ be a polynomial over $\mathbb{F}_q$. If $(a_0, a_1, \ldots, a_{d-1}) \neq (0, 0, \ldots, 0)$, then $f(x_1, x_2, \ldots, x_d)$ gives a d-cube of order q. Moreover, if $a_i \neq 0$ for any $0 \leq i \leq d-1$, then the d-cube is of type $d-1$.

Lemma 4.2 ([5, Theorem 4.4]): Let $t \geq d$ be an integer. Let

$$f_i(x_1, x_2, \ldots, x_d) = a_{i,0} x_1 + a_{i,1} x_2 + \cdots + a_{i,d-1} x_d, \quad (3)$$

for $1 \leq i \leq t$, be linear polynomials over $\mathbb{F}_q$. Then, the d-cubes generated by $f_1, f_2, \ldots, f_t$ form a $(d, d-1)$-MOC(q) if and only if every d rows of the matrix $M = (a_{i,j})_{t \times d}$ are linearly independent.

Note that, in Definition 2.3, the index i_k of the kth dimension in a d-cube is assumed to be natural numbers $\{1, 2, \ldots, n\}$. In the case when the indices are the elements of finite field $\mathbb{F}_q$, for convenience of dealing with the diagonals, we arrange the indices of each dimension of the above d-cube in such a way that the sum of the $(q-i+1)$th index and the ith index is a constant $\ell \in \mathbb{F}_q$ for each $1 \leq i \leq q$.

In particular, when q is an odd prime, it is convenient to use the ordering of integers from 0 to $q-1$, and then $\ell = q-1$.

For example, when $q = 5$, the indices in any dimension are naturally $(0, 1, 2, 3, 4)$.

When $q = 8$, the indices are the elements of $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$. One can arrange them as

$$(0,\ 1,\ \alpha,\ 1+\alpha,\ \alpha^2,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2)$$

so that $0 + (1+\alpha+\alpha^2) = 1 + (\alpha+\alpha^2) = \alpha + (1+\alpha^2) = (1+\alpha) + \alpha^2 = \ell$. The arrangement is not unique. One can choose in another way as follows:

$$(0,\ \alpha,\ \alpha^2,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2,\ 1+\alpha^2,\ 1+\alpha,\ 1)$$

and then $\ell = 1$.

Lemma 4.3: Let $f(x_1, \ldots, x_d) = a_0x_1 + a_1x_2 + \cdots + a_{d-1}x_d$ be a polynomial over $\mathbb{F}_q$. The d-cube generated by $f(x_1, \ldots, x_d)$ is diagonal if and only if $f(1, \sigma_2, \sigma_3, \ldots, \sigma_d) \neq 0$ for any $(\sigma_2, \sigma_3, \ldots, \sigma_d) \in \{1, -1\}^{d-1}$.

Proof. Let τ be a permutation over $\mathbb{F}_q$ defined by $\tau(\alpha) = \ell - \alpha$. The diagonals of the d-cube generated by f can be represented by

$$\mathscr{D}_{\boldsymbol{s}} = \Big\{(i_0, \tau^{s_1}(i_0), \tau^{s_2}(i_0), \ldots, \tau^{s_{d-1}}(i_0); f(i_0, \tau^{s_1}(i_0), \ldots, \tau^{s_{d-1}}(i_0))) \mid i_0 \in \mathbb{F}_q\Big\}$$

for each $\boldsymbol{s} = (s_1, s_2, \ldots, s_{d-1}) \in \{0, 1\}^{d-1}$.

For $1 \le i \le d-1$, let $\sigma_i = 1$ if $s_i = 1$, and $\sigma_i = -1$ if $s_i = 0$. By the linearity of f, we have

$$f(i_0, \tau^{s_1}(i_0), \ldots, \tau^{s_{d-1}}(i_0)) = i_0 f(1, \sigma_2, \ldots, \sigma_d) + \ell \sum_{i=1}^{d-1} s_i.$$

Hence, $\mathscr{D}_{\boldsymbol{s}}$ forms a transversal if and only if $f(i_0, \tau^{s_1}(i_0), \ldots, \tau^{s_{d-1}}(i_0))$ is distinct from each other for every $i_0 \in \mathbb{F}_q$, which is equivalent to saying $f(1, \sigma_2, \sigma_3, \ldots, \sigma_d) \neq 0$. □

Theorem 4.4: Suppose $d \le q-1$. Let $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$ denote the distinct non-zero elements of $\mathbb{F}_q$. Let

$$f_i(x_1, x_2, \ldots, x_d) = x_1 + \alpha_i x_2 + \alpha_i^2 x_3 + \cdots + \alpha_i^{d-1} x_d \quad (4)$$

for $1 \le i \le q-1$. The set of d-cubes generated by $f_1, f_2, \ldots, f_{q-1}$ is a $(d, d-1)$-MOC(q).

Moreover, the set of d-cubes generated by all the polynomials f_i $(1 \le i \le q-1)$ with the property that $f_i(1, \sigma_2, \sigma_3, \ldots, \sigma_d) \neq 0$ for every $(\sigma_2, \sigma_3, \ldots, \sigma_d) \in \{1, -1\}^{d-1}$ forms a $(d, d-1)$-MODC(q).

Proof. Note that all the coefficients of $f_1, f_2, \ldots, f_{q-1}$ are non-zero, and they form a Vandermonde matrix of rank d. It follows from Lemmas 4.1 and 4.2 that all these d-cubes are of type $d-1$ and mutually d-orthogonal. The latter half is straightforward by Lemma 4.3. □

Remark 4.5: The construction in Theorem 4.4 is proposed in terms of an MDS code at the end of [5, Section 4.2] (see also [13, Chapter 11 §5]).

In particular, when $d = 2$, it suffices to take

$$f_i(x_1, x_2) = x_1 + \alpha_i x_2 \in \mathbb{F}_q[x_1, x_2]$$

for each $\alpha_i \in \mathbb{F}_q \setminus \{0, \pm 1\}$. Then, the squares generated by f_i are MODLS(q), which achieve the upper bounds in Theorem 3.4 ([11, Theorem 2]).

Next, by regarding $f_i(1, \sigma_2, \sigma_3, \ldots, \sigma_d)$ as a polynomial with respect to α_i over $\mathbb{F}_q$, we propose a further result in Theorem 4.7 for even q when $d \ge 3$, which improves Theorem 3.5 (ii) ([6, Theorem 3.3]) in a variety of cases.

Lemma 4.6 ([14, Theorem 3.4.21]): The polynomial $1 + \alpha + \alpha^2 + \cdots + \alpha^{d-1} \in \mathbb{F}_q[\alpha]$ is irreducible over $\mathbb{F}_q$ if and only if d is prime and q is a primitive root modulo d.

Theorem 4.7: Let $d \ge 3$ be a prime and $q \ge d+1$ be a power of 2. If q is a primitive root modulo d, with the definition of f_i in (4), the set of d-cubes generated by $f_1, f_2, \ldots, f_{q-1}$ is a $(d, d-1)$-MODC(q).

Proof. Since $\mathbb{F}_q$ is of characteristic 2, the polynomials $f_i(1, \sigma_2, \sigma_3, \ldots, \sigma_d) \in \mathbb{F}_q[\alpha_i]$, for $1 \le i \le q-1$, are identical with $h_{d-1}(\alpha) = 1 + \alpha + \alpha^2 + \cdots + \alpha^{d-1} \in \mathbb{F}_q[\alpha]$ for any $(\sigma_2, \sigma_3, \ldots, \sigma_d) \in \{1, -1\}^{d-1}$.

By Lemma 4.6, it is clear that $h_{d-1}(\alpha)$ is irreducible and of degree greater than 2. Therefore, we have $h_{d-1}(\alpha) \neq 0$ for any $\alpha \in \mathbb{F}_q$. Then, the proof is completed by utilizing Theorem 4.4. □

4.2 Kronecker Product Construction

For any two orthogonal Latin squares $\mathcal{A}_1$, $\mathcal{A}_2$ of order m, and orthogonal Latin squares $\mathcal{B}_1$, $\mathcal{B}_2$ of order n, the Kronecker products $\mathcal{A}_1 \otimes \mathcal{B}_1$ and $\mathcal{A}_2 \otimes \mathcal{B}_2$ are also orthogonal Latin square of order mn (see [1, §2.3]). Moreover, the Kronecker products preserve the diagonal property of Latin square (see [11]).

Similarly, Kronecker products can be generalized to d-orthogonal d-cubes (see [5, Section 4.3]). It is obvious that d-dimensional Kronecker products also preserve the diagonal property (see [6]). Hence, we can immediately obtain the following theorem.

Theorem 4.8: Let $n = q_1 q_2 \ldots q_r$, where q_i is a prime power for each $1 \le i \le r$ with $q_1 < q_2 < \cdots < q_r$ and $\gcd(q_i, q_j) = 1$ for any $1 \le i < j \le r$. If $d \ge 2$, then

$$N^{(d)}(n) \ge \min\{N^{(d)}(q_i) \mid 1 \le i \le r\} \quad \text{and}$$
$$D^{(d)}(n) \ge \min\{D^{(d)}(q_i) \mid 1 \le i \le r\}.$$

5. Constructions for $(3, 2)$-MODC(n)

In this section, we focus on the constructions for $(d, d-1)$-MODC(n) with $d = 3$. Consequently, we improve the known lower bounds for the maximum possible number

$D^{(3)}(n)$ of such cubes.

First, for $\mathbb{F}_q$ of characteristic 2, we introduce the following construction by Arkin et al. [6]. (The result is previously stated in Theorem 3.5 (iii).)

Theorem 5.1 (see [6]): Let $h(\alpha) = \alpha^2 + a\alpha + b$ be an irreducible polynomial in $\mathbb{F}_q[\alpha]$ with $ab \neq 0$. Let y_1, y_2, y_3 be three distinct elements in $\mathbb{F}_q^*$ and let $h_i(\alpha) = y_i^{-2}h(y_i\alpha) \in \mathbb{F}_q[\alpha]$ for $i \in \{1,2,3\}$. Moreover, define $q+2$ polynomials in $\mathbb{F}_q[x_1,x_2,x_3]$ as follows:

$$f_{\alpha_j}(x_1,x_2,x_3) = h_1(\alpha_j)x_1 + h_2(\alpha_j)x_2 + h_3(\alpha_j)x_3 \quad \text{with } \alpha_j \in \mathbb{F}_q,$$
$$f_\infty(x_1,x_2,x_3) = x_1 + x_2 + x_3,$$
$$f'(x_1,x_2,x_3) = y_1^{-1}x_1 + y_2^{-1}x_2 + y_3^{-1}x_3.$$

Then, the cubes generated by $\{f_{\alpha_j} \mid \alpha_j \in \mathbb{F}_q\} \cup \{f_\infty, f'\}$ are mutually 3-orthogonal. Moreover, at least q of these cubes are diagonal.

Example 5.2: Consider $\mathbb{F}_4 := \mathbb{F}_2[\beta]/(\beta^2+\beta+1)$ and let $h(\alpha) = 1 + \beta\alpha + \alpha^2 \in \mathbb{F}_4[\alpha]$. It is easy to check that $h(\alpha)$ is irreducible over $\mathbb{F}_4$. Take $(y_1,y_2,y_3) = (1,\beta,\beta^2)$. Then, $h_i(\alpha) = \beta^{i-1} + \beta^{2-i}\alpha + \alpha^2$ for $i \in \{1,2,3\}$. We have

$$\begin{pmatrix} f_0(x_1,x_2,x_3) \\ f_1(x_1,x_2,x_3) \\ f_\beta(x_1,x_2,x_3) \\ f_{\beta^2}(x_1,x_2,x_3) \\ f_\infty(x_1,x_2,x_3) \\ f'(x_1,x_2,x_3) \end{pmatrix} = \begin{pmatrix} 1 & \beta & \beta^2 \\ \beta & \beta & 1 \\ 1 & \beta^2 & 1 \\ \beta & \beta^2 & \beta^2 \\ 1 & 1 & 1 \\ 1 & \beta^2 & \beta \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

where $f_0(1,1,1) = f'(1,1,1) = 0$ and hence the corresponding cubes are not diagonal. While, it can be verified that the remaining four cubes are diagonal. Moreover, since the coefficient matrix is of rank 3 over $\mathbb{F}_4$, it follows from Lemma 4.2 that these six cubes are mutually 3-orthogonal.

More precisely, we can obtain the corresponding $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$, $\mathcal{H}_\infty$ as shown in Example 3.6, where β and β^2 are replaced by 2 and 3, respectively.

Remark 5.3: Let $q = 2^r$. There is an irreducible trinomial of the form $x^2 + ax + b \in \mathbb{F}_q[x]$ with $ab \neq 0$ if and only if the absolute trace $\mathrm{Tr}_{\mathbb{F}_q}(a^{-1}) = a^{-1} + a^{-2} + a^{-4} + \cdots + a^{-q/2} = 1$. (This is a straightforward conclusion by taking the characteristic 2 in [14, Corollary 3.4.12].) In addition, there are $q/2$ elements in $\mathbb{F}_q$ whose absolute trace equals to 1, which guarantees the existence of such an irreducible trinomial.

Next, we suppose q is a power of an odd prime p. Denote by $\left(\frac{x}{q}\right)$ the Legendre symbol of $x \in \mathbb{F}_q$, so that $\left(\frac{x}{q}\right)$ is 0, 1 or -1 according to whether x is respectively zero, a square or a non-square in $\mathbb{F}_q$. By the following Lemma 5.4, we obtain Theorem 5.5 on the existence of specific irreducible polynomials.

Lemma 5.4 ([15, Corollary 1.12]): For every ordered triple $(\epsilon_1,\epsilon_2,\epsilon_3) \in \{1,-1\}^3$, there exists $x \in \mathbb{F}_q$ such that $\left(\frac{x+i}{q}\right) = \epsilon_i$ for each $i \in \{1,2,3\}$, whenever $q \geq 19$.

Theorem 5.5: For any odd prime power $q \geq 7$, there exists $c_1, c_2 \in \mathbb{F}_q^*$, such that the trinomials $1 \pm c_1\alpha \pm c_2\alpha^2 \in \mathbb{F}_q[\alpha]$ are irreducible over $\mathbb{F}_q$.

Proof. It is easily seen that the trinomial $f(\alpha) = 1 + c_1\alpha + c_2\alpha^2 \in \mathbb{F}_q[\alpha]$ is irreducible if and only if $f(\alpha) = 0$ has no solution in $\mathbb{F}_q$, i.e., $c_1^2 - 4c_2$ is not a square in $\mathbb{F}_q$.

Firstly, we set $c_2 = 4^{-1}$, and then the trinomials $1 \pm c_1\alpha \pm 4^{-1}\alpha^2 \in \mathbb{F}_q[\alpha]$ are irreducible if and only if both c_1^2+1 and c_1^2-1 are non-squares.

By Lemma 5.4, for any $q \geq 19$, there exists $x \in \mathbb{F}_q^*$, such that $x-1$, x, $x+1$ are respectively a non-square, a square, a non-square. Let c_1 be a square root of such x. Then both c_1^2+1 and c_1^2-1 are non-squares.

It remains to consider $q \in \{7,9,11,13,17\}$.

For $q = 7$ or 17, we can take $c_1 = 2$, so that $\left(\frac{3}{q}\right) = \left(\frac{5}{q}\right) = -1$. For $q = 11$, we can take $c_1 = 3$, so that $\left(\frac{8}{q}\right) = \left(\frac{10}{q}\right) = -1$. For $q = 9$, we consider $\mathbb{F}_9 := \mathbb{F}_3[\beta]/(\beta^2+1)$. Then, $\pm 1, \pm\beta$ are squares. We take $c_1 = 1-\beta$, so that $c_1^2 = \beta$ and $\left(\frac{\beta-1}{q}\right) = \left(\frac{\beta+1}{q}\right) = -1$.

For $q = 13$, we set $c_2 = 2^{-1}$ and consider the trinomials $1 \pm c_1\alpha \pm 2^{-1}\alpha^2 \in \mathbb{F}_q[\alpha]$, which are all irreducible if and only if $c_1^2 \pm 2$ are non-squares. We take $c_1 = 2$ and then $\left(\frac{2}{q}\right) = \left(\frac{6}{q}\right) = -1$. □

Theorem 5.6: If $q \geq 7$ is an odd prime power, then $D^{(3)}(q) \geq q-1$.

Proof. Let $f_i(x_1,x_2,x_3) = x_1 + c_1\alpha_i x_2 + c_2\alpha_i^2 x_3$ with $\alpha_i \in \mathbb{F}_q^*$ for $1 \leq i \leq q-1$, such that $1 \pm c_1\alpha \pm c_2\alpha^2 \in \mathbb{F}_q[\alpha]$ are all irreducible, whose existence is guaranteed by Theorem 5.5. Then, by Lemmas 4.1, 4.2, and 4.3, we can conclude that $D^{(3)}(q) \geq q-1$ for odd $q \geq 7$. □

There does not exist $c_1, c_2 \in \mathbb{F}_5^*$, such that $1 \pm c_1\alpha \pm c_2\alpha^2 \in \mathbb{F}_5[\alpha]$ are all irreducible over $\mathbb{F}_5$. However, we can explicitly construct four 3-orthogonal diagonal cubes of type 2 as follows.

Example 5.7: Let f_1, f_2, f_3, f_4 be the polynomials over $\mathbb{F}_5$ defined as follows:

$$\begin{pmatrix} f_1(x_1,x_2,x_3) \\ f_2(x_1,x_2,x_3) \\ f_3(x_1,x_2,x_3) \\ f_4(x_1,x_2,x_3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

By Lemmas 4.1 and 4.3, the cubes generated by f_1, f_2, f_3, f_4 are of type 2 and diagonal. Moreover, it can be easily checked that the coefficient matrix is of rank 3 over $\mathbb{F}_5$. Thus, it follows from Lemma 4.2 that the resulting cubes are mutually 3-orthogonal. Hence, we have $D^{(3)}(5) \geq 4$.

Combining Theorem 3.5 (iii), Theorem 5.6, and Example 5.7, we obtain Theorem 5.8.

Theorem 5.8: For any prime power $q \geq 4$, the following holds:

$$D^{(3)}(q) \geq \begin{cases} q, & \text{if } q \text{ is even,} \\ q-1, & \text{if } q \text{ is odd.} \end{cases}$$

The bound in Theorem 5.8 improves Theorem 3.5 (i), which claims that $D^{(3)}(q) \geq q - 8$ for $d = 3$ and odd prime power q.

By considering Trenkler's construction (Theorem 3.8) and the Kronecker products (Theorem 4.8), we conclude this section by providing the following.

Theorem 5.9: Let $n = q_1 q_2 \dots q_r$, where q_i is a prime power for each $1 \leq i \leq r$ with $q_1 < q_2 < \cdots < q_r$ and $\gcd(q_i, q_j) = 1$ for any $1 \leq i < j \leq r$. Then,

$$D^{(3)}(n) \geq \begin{cases} 3, & \text{if } q_1 = 3 \text{ and } n \neq 3, \\ q_1, & \text{if } q_1 \geq 4 \text{ is even,} \\ q_1 - 1, & \text{if } q_1 \geq 5 \text{ is odd.} \end{cases}$$

6. Concluding Remarks and Further Work

The notion of mutually dimensionally orthogonal d-cubes of type $d-1$ (simply, $(d, d-1)$-MOC(n)) and mutually dimensionally orthogonal diagonal d-cubes of type $d-1$ (simply, $(d, d-1)$-MODC(n)), are d-dimensional generalization of MOLS and MODLS, respectively.

In Sects. 3 and 4, we summarized and characterized the known results on $N^{(d)}(n)$ and $D^{(d)}(n)$ and the constructions on $(d, d-1)$-MOC(n) and $(d, d-1)$-MODC(n). We also proposed a finite field construction for $(d, d-1)$-MODC(n). By using these constructions, we proved the following main theorems.

Theorem 3.8: If d is odd and $n > d$ is odd, then $D^{(d)}(n) \geq d$ for any odd d and odd $n > d$.

Theorem 4.7: Let $d \geq 3$ be a prime and $q \geq d+1$ be a power of 2. Let f_i be the polynomials defined in Theorem 4.4. If q is a primitive root modulo d, the set of d-cubes generated by $f_1, f_2, \dots, f_{q-1}$ is a $(d, d-1)$-MODC(q).

In Sect. 5, we focused on the 3-dimensional cubes and showed the following results by investigating the existence of irreducible polynomials over finite fields.

Theorem 5.8: For any prime power $q \geq 4$, the following holds:

$$D^{(3)}(q) \geq \begin{cases} q, & \text{if } q \text{ is even,} \\ q-1, & \text{if } q \text{ is odd.} \end{cases}$$

Following our previous results and observations, we propose the following conjectures.

Conjecture 6.1: (i) $D^{(3)}(n) \leq n-1$ if n is odd.

(ii) $D^{(3)}(n) \leq n$ if n is even.

(iii) $D^{(d)}(n) \geq d$ for any positive integer $n \notin \{2, 3, 6\}$.

In particular, for $d = 3$, it remains to study the constructions of 3-orthogonal diagonal cubes of type 2 with order $n \equiv 2 \pmod 4$.

It is remarkable that Trenkler [12], [16] proposed elementary approaches for mutually d-orthogonal d-cubes. However, his constructions cannot give d-cubes of type $d-1$ in general.

More generally, when the number of symbols does not equal to the order, the notions of frequency hypercubes (see [4]) and hypercubes of class r (see [17]) are proposed. It is also interesting to study the "diagonal property" for these generalized hypercubes.

Acknowledgments

The authors express their gratitude to the two anonymous reviewers for their comments which are very helpful to the improvement of the final manuscript. This work was supported in part by JSPS KAKENHI Grant Numbers 15H03636, 18H01133, and 19K14585. X.-N. Lu was supported by Leading Initiative for Excellent Young Researchers, MEXT, Japan.

References

[1] C.F. Laywine and G.L. Mullen, Discrete Mathematics Using Latin Squares, John Wiley & Sons, 1998.
[2] A.D. Keedwell and J. Dénes, Latin Squares and Their Applications, 2nd ed., Elsevier, 2015.
[3] J. Dénes and A.D. Keedwell, eds., Latin Squares: New Developments in the Theory and Applications, Ann. Discrete Math., vol.46, North-Holland, 1991.
[4] C.F. Laywine and G.L. Mullen, "Frequency squares and hypercubes," Handbook of Combinatorial Designs, C.J. Colbourn and J.H. Dinitz, eds., ch. 22, pp.465–471, CRC Press, 2006.
[5] J.T. Ethier and G.L. Mullen, "Strong forms of orthogonality for sets of hypercubes," Discrete Math., vol.312, no.12, pp.2050–2061, 2012.
[6] J. Arkin, V.E. Hoggatt, Jr., and E.G. Straus, "Systems of magic Latin k-cubes," Can. J. Math., vol.29, no.6, pp.1153–1161, 1976.
[7] J. Arkin and E.G. Straus, "Latin k-cubes," Fibonacci Quart, vol.12, no.3, pp.288–292, 1974.
[8] M. Trenkler, "On orthogonal Latin p-dimensional cubes," Czech. Math. J., vol.55, no.3, pp.725–728, 2005.
[9] M. Trenkler, "Magic cubes," Math. Gaz., vol.82, no.493, pp.56–61, 1998.
[10] J.W. Brown, F. Cherry, L. Most, M. Most, E.T. Parker, and W.D. Wallis, "Completion of the spectrum of orthogonal diagonal Latin squares," Graphs, Matrices, and Designs, R.S. Rees, eds., Lect. Notes Pure Appl. Math., vol.139, ch. 4, pp.43–49, CRC Press, 1992.
[11] E. Gergely, "A remark on doubly diagonalized orthogonal Latin squares," Discrete Math., vol.10, no.1, pp.185–188, 1974.
[12] M. Trenkler, "Magic p-dimensional cubes of order $n \not\equiv 2 \pmod 4$," Acta Arith., vol.92, no.2, pp.189–194, 2000.
[13] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.
[14] O. Ahmadi, "Weights of irreducible polynomials," Handbook of Finite Fields, G.L. Mullen and D. Panario, eds., ch. 3.4, pp.70–73, CRC Press, 2013.
[15] L. Guerra and E. Ughi, "On the distribution of Legendre symbols in Galois fields," Discrete Math., vol.42, no.2-3, pp.197–208, 1982.
[16] M. Trenkler, "Magic p-dimensional cubes," Acta Arith., vol.96, no.4, pp.361–364, 2001.
[17] J.T. Ethier, G.L. Mullen, D. Panario, B. Stevens, and D. Thomson, "Sets of orthogonal hypercubes of class r," J. Combin. Theory Ser. A, vol.119, no.2, pp.430–439, 2012.

Xiao-Nan Lu received his M.S. degree and Ph.D. from Nagoya University in 2014 and 2017, respectively. From May 2017 to November 2019, he was an assistant professor at Tokyo University of Science. He is currently an assistant professor at University of Yamanashi. His research interests include discrete mathematics and its applications to information sciences, computer sciences, and statistics.

Tomoko Adachi received her M.S. degree from Osaka University in 1995 and Ph.D. from Keio University in 2003. She was an assistant professor at Toho University from 2003, promoted to an associate professor at Toho University in 2007, and a professor at Toho University in 2015. Her current research interests include applied mathematics, cryptography, discrete mathematics, and RAID systems.