On mutually 3-orthogonal diagonal cubes

Xiao-Nan Lu (Tokyo University of Science, Japan)
Joint work with Tomoko Adachi (Toho University, Japan)

JCCA 2018, Sendai
May 24, 2018.

Outline

Latin squares (cubes) & magic squares (cubes)

Mutually 3-orthogonal diagonal cubes of type 2

Latin squares and orthogonality

A *Latin square of order n* is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs once in each row and column.

$$L_1 = \begin{array}{|c|c|c|c|}\hline A & K & Q & J \\ \hline K & A & J & Q \\ \hline Q & J & A & K \\ \hline J & Q & K & A \\ \hline \end{array} \qquad L_2 = \begin{array}{|c|c|c|c|}\hline \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \hline \heartsuit & \clubsuit & \spadesuit & \diamondsuit \\ \hline \clubsuit & \heartsuit & \diamondsuit & \spadesuit \\ \hline \diamondsuit & \spadesuit & \clubsuit & \heartsuit \\ \hline \end{array}$$

When L_1 is superimposed on L_2, each of the 16 ordered pairs appears exactly once. L_1 and L_2 are *orthogonal*.

$$L_1 \boxplus L_2 = \begin{array}{|c|c|c|c|}\hline A\spadesuit & K\diamondsuit & Q\heartsuit & J\clubsuit \\ \hline K\heartsuit & A\clubsuit & J\spadesuit & Q\diamondsuit \\ \hline Q\clubsuit & J\heartsuit & A\diamondsuit & K\spadesuit \\ \hline J\diamondsuit & Q\spadesuit & K\clubsuit & A\heartsuit \\ \hline \end{array}$$

Diagonal Latin squares

If there are n distinct symbols on the *two main diagonals* of L, then L is called a *diagonal Latin square*.

- n: odd and $3 \nmid n$.
- a, b: positive integers s.t. a, b, $a-b$, $a+b$ are coprime to n.
- The following is a *diagonal Latin square* over $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

0	a	$2a$	$\cdots$	$(n-1)a$
b	$a+b$	$2a+b$	$\cdots$	$(n-1)a+b$
$2b$	$a+2b$	$2a+2b$	$\cdots$	$(n-1)a+2b$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(n-1)b$	$a+(n-1)b$	$2a+(n-1)b$	$\cdots$	$(n-1)a+(n-1)b$

- L and L^{T} are *orthogonal*.

- A pair of *orthogonal diagonal Latin squares* of order n exists for any positive integer n with the exception of $n \in \{2, 3, 6\}$. (Brown-Cherry-Most-Most-Parker-Wallis, 1992)

Magic squares

A *magic square of order n* is an arrangement of n^2 integers from $\{1, 2, \dots, n^2\}$ into an $n \times n$ array with the property that the sums of each row, each column, and each of the two main diagonals are the same.

2	9	4
7	5	3
6	1	8

A magic square of order 3

- Magic constant:

$$M_2(n) = \frac{1}{n} \sum_{\ell=1}^{n^2} \ell = \frac{1}{2} n(n^2 + 1).$$

Magic squares $\to$ Squares

- Reduce 1 from each cell in a magic square of order n,
- Rewrite all the integers in base n representation.

$$\begin{array}{|c|c|c|}\hline 2 & 9 & 4 \\ \hline 7 & 5 & 3 \\ \hline 6 & 1 & 8 \\ \hline \end{array} \xrightarrow{-1} \begin{array}{|c|c|c|}\hline 1 & 8 & 3 \\ \hline 6 & 4 & 2 \\ \hline 5 & 0 & 7 \\ \hline \end{array} \xrightarrow{\text{base } 3} \begin{array}{|c|c|c|}\hline 01 & 22 & 10 \\ \hline 20 & 11 & 02 \\ \hline 12 & 00 & 21 \\ \hline \end{array} =: L$$

- Split it into two squares on $\{0, 1, \ldots, n-1\}$.

$$L = L_1 \boxplus L_2$$

$$L_1 = \begin{array}{|c|c|c|}\hline 0 & 2 & 1 \\ \hline 2 & 1 & 0 \\ \hline 1 & 0 & 2 \\ \hline \end{array} \qquad L_2 = \begin{array}{|c|c|c|}\hline 1 & 2 & 0 \\ \hline 0 & 1 & 2 \\ \hline 2 & 0 & 1 \\ \hline \end{array}$$

Magic squares $\leftarrow$ (Diagonal) MOLS

- A pair of *orthogonal Latin squares* on $\{0, 1, \ldots, n-1\}$ whose trace and backtrace $= \frac{1}{2}n(n-1) \implies$ A *magic square* of order n.
- A pair of *orthogonal diagonal Latin squares* of order $n \implies$ A *magic square* of order n.

$$L_1 \boxplus L_2 = L \equiv n \cdot L_1 + L_2$$

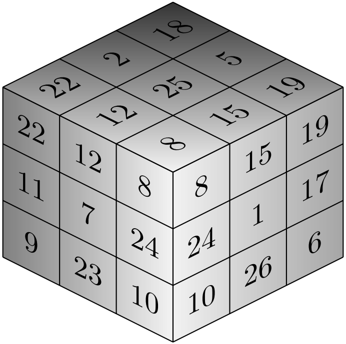
Remark

- There does not exist *orthogonal Latin squares* of order 2 and 6.
- *Magic squares* of order 6 do exist.

Magic cubes

A *magic cube* is an arrangement of $\{1, 2, \ldots, n^3\}$ into an $n \times n \times n$ array s.t. the sums along every row and every diagonal are the same.

$$M_3(n) = \frac{1}{n^2} \sum_{\ell=1}^{n^3} \ell = \frac{1}{2} n(n^3 + 1).$$



8	15	19
24	1	17
10	26	6

$(k = 1)$

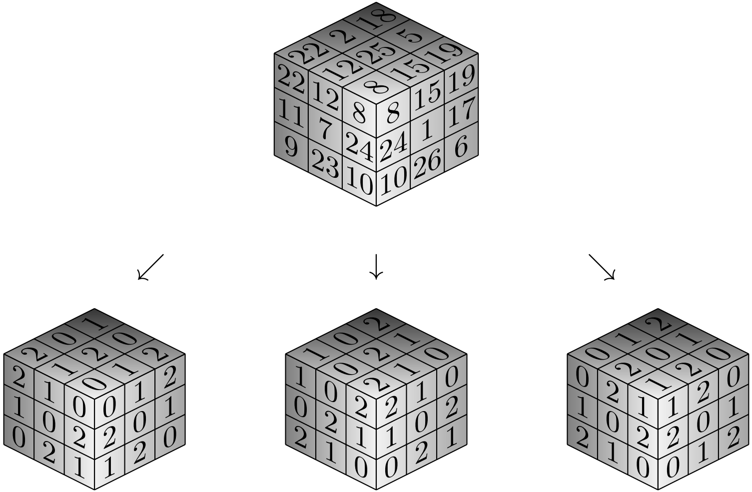
12	25	5
7	14	21
23	3	16

$(k = 2)$

22	2	18
11	27	4
9	13	20

$(k = 3)$

Magic cubes → Cubes



Magic cubes $\leftarrow$ Cubes

021	112	200
212	000	121
100	221	012

$(k = 1)$

102	220	011
020	111	202
211	002	120

$(k = 2)$

210	001	122
101	222	010
022	110	201

$(k = 3)$

A construction of orthogonal cubes (Trenkler, 2005)

- n: odd positive integer
- $L^{(1)} = (\ell^{(1)}_{i,j,k})_{1 \le i,j,k \le n}$ with $\ell^{(1)}_{i,j,k} = k - i + j - 1 \pmod n$,
- $L^{(2)} = (\ell^{(2)}_{i,j,k})_{1 \le i,j,k \le n}$ with $\ell^{(2)}_{i,j,k} = k - i - j \pmod n$,
- $L^{(3)} = (\ell^{(3)}_{i,j,k})_{1 \le i,j,k \le n}$ with $\ell^{(3)}_{i,j,k} = k + i + j - 2 \pmod n$.
- $L^{(1)}$, $L^{(2)}$, and $L^{(3)}$ are mutually orthogonal.

Outline

Latin squares (cubes) & magic squares (cubes)

Mutually 3-orthogonal diagonal cubes of type 2

Generalization of the Latin-ness

- d: dimension $d \geq 2$
- t: type $0 \leq t \leq d-1$
- n: order (also $\#$ of symbols)

Definition (d-cubes of type t)

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 symbols, s.t.

- each symbol occurs exactly n^{d-t-1} times in every $(d-t)$-dim. subarray obtained by fixing t coordinates of the array.

Remark

- If dim. $d = 2$ and type $t = 1$ $\Longrightarrow$ Latin squares.
- "Latin d-cube" is usually used to refer to a d-cube of type 1.
- I will focus on 3-cubes (simply cubes) of type 2 $(= d-1)$.

Generalization of the orthogonality

- d: dimension $d \geq 2$
- n: order (also $\#$ of symbols)

- Two d-cubes are *orthogonal* if when superimposed, each of the n^2 *ordered pairs* of symbols appears exactly n^{d-2} *times*.
- A set of d d-cubes is *dimensionally orthogonal* (d*-orthogonal*), if when superimposed, each of the n^d *ordered d-tuples* appears exactly *once*.
- A set of j ($j \geq d$) d-cubes is *mutually d-orthogonal* if any choice of d of them preserves the d-orthogonality.

Generalization of the orthogonality

- d: dimension $d \geq 2$
- n: order (also # of symbols)

- Two d-cubes are *orthogonal* if when superimposed, each of the n^2 *ordered pairs* of symbols appears exactly n^{d-2} *times*.
- A set of d d-cubes is *dimensionally orthogonal* (*d-orthogonal*), if when superimposed, each of the n^d *ordered d-tuples* appears exactly *once*.
- A set of j ($j \geq d$) d-cubes is *mutually d-orthogonal* if any choice of d of them preserves the d-orthogonality.

Generalization of the orthogonality

- d: dimension $d \geq 2$
- n: order (also $\#$ of symbols)

- Two d-cubes are *orthogonal* if when superimposed, each of the n^2 *ordered pairs* of symbols appears exactly n^{d-2} *times*.
- A set of d d-cubes is *dimensionally orthogonal* (*d-orthogonal*), if when superimposed, each of the n^d *ordered d-tuples* appears exactly *once*.
- A set of j ($j \geq d$) d-cubes is *mutually d-orthogonal* if any choice of d of them preserves the d-orthogonality.

d-orth. d-cubes

- $N^{(d)}(n)$: max. # of d-orth. d-cubes of type $d-1$ and order n.

Upper bound (Ethier-Mullen, 2012)

For $d \geq 2$,

$$N^{(d)}(n) \leq n + d - 1.$$

Construction and lower bound (Arkin-Straus, 1974)

A set of d d-orth. d-cubes of type $d-1$ $\Longleftarrow$ A set of $d-1$, $(d-1)$-orth. $(d-1)$-cubes of type $d-2$.

$$N^{(2)}(n) \geq 2 \implies N^{(3)}(n) \geq 3 \implies \cdots \implies N^{(d)}(n) \geq d$$
$$\implies N^{(3)}(n) \geq 4$$

d-orth. diagonal d-cubes

A *transversal* of a d-cube is a set of n entries s.t. no two entries share the same row or symbol.
A d-cube is *diagonal* if all 2^{d-1} diagonals are transversals.

- $D^{(d)}(n)$: max. $\#$ of d-orth. diagonal d-cubes of type $d-1$.

Basic facts

- $D^{(d)}(n) \leq N^{(d)}(n)$ (= max. $\#$ without the diag. restriction)
- $D^{(2)}(n) \geq 2$ for $n \notin \{2, 3, 6\}$ (existence of diag. MOLS)

Upper bound for diag. Latin squares (Gergely, 1974)

If n is even, $D^{(2)}(n) \leq n-2$, whereas if n is odd, $D^{(2)}(n) \leq n-3$.
If n is a prime power, the equality holds.

A fundamental construction using finite fields

Fundamental construction of a d-cube over $\mathbb{F}_q$

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 $d-1$*.

Fundamental construction of a set of d-orth. d-cube over $\mathbb{F}_q$ (Ethier-Mullen, 2012)

Define a set of t linear polynomials over $\mathbb{F}_q$:

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

The d-cubes generated by $f_1, f_2, \ldots, f_t$ form *a set of d-orthogonal d-cubes of order q* iff any d rows of the matrix $M = (a_{i,j})_{t \times d}$ are linearly independent.

3-orth. diagonal cubes

Example ($D^{(3)}(4) \geq 4$, by Arkin-Hoggatt-Straus, 1976)

Let $\mathbb{F}_4 := \mathbb{F}_2[\beta]/(\beta^2+\beta+1)$ and $h(\alpha) = 1 + \beta\alpha + \alpha^2 \in \mathbb{F}_4[\alpha]$. Here, $h(\alpha)$ is irreducible over $\mathbb{F}_4$. Now we 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

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

where $f_0(1,1,1) = f'(1,1,1) = 0$ and hence the corresponding cubes are not diagonal. While, the remaining *four cubes are diagonal*. Moreover, $\mathrm{rank}_{\mathbb{F}_4}(\text{coefficient matrix}) = 3$, these *six cubes are 3-orth*.

Lower bounds for diagonal d-cubes

Theorem (Arkin-Hoggatt-Straus, 1976)

Let q be a prime power with $q \geq d > 2$. Then the following holds.

(i) *If q is odd, then there exists a set of $q+1$, d-orthogonal magic-associated d-cubes of order q and type $d-1$, of which at least $q-(d-1)2^{d-1}$ are diagonal.* $D^{(d)}(q) \geq q-(d-1)2^{d-1}$.

(ii) *If q is a power of 2, then there exists a set of $q+1$, d-orthogonal d-cubes of order q and type $d-1$, of which at least $q+2-d$ are diagonal.* $D^{(d)}(q) \geq q+2-d$.

(iii) *If $q \geq 4$ is a power of 2, then there exists a set of $q+2$, 3-orthogonal cubes ($d=3$) of order q and type 2, of which at least q are diagonal.* $D^{(3)}(q) \geq q$.

Our fundamental constructions for diagonal d-cubes

Lemma 1 (iff-condition for diag. d-cubes)

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 is diagonal iff $f(1, \sigma_2, \sigma_3, \ldots, \sigma_d) \neq 0$ for any $(\sigma_2, \sigma_3, \ldots, \sigma_d) \in \{1, -1\}^{d-1}$.

Theorem 2 (a corollary of the fundamental construction)

Let $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$ be distinct non-zero elements of $\mathbb{F}_q$. Let

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

The d-cubes generated by $f_1, f_2, \ldots, f_{q-1}$ form a set of d-orth. d-cubes of order q and type $d-1$.
Moreover, if $f_i(1, \sigma_2, \sigma_3, \ldots, \sigma_d) \neq 0$, $\forall (\sigma_2, \ldots, \sigma_d) \in \{1, -1\}^{d-1}$, $\forall i$, we have a set of d-orth. diagonal d-cubes.

This construction was also proposed in terms of an MDS code.

3-orth. diagonal cubes

Lemma 2

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. *Set* $c_2 = 4^{-1}$. *Then* $1 \pm c_1\alpha \pm 4^{-1}\alpha^2 \in \mathbb{F}_q[\alpha]$ *are irreducible iff both* $c_1^2 + 1$ *and* $c_1^2 - 1$ *are non-squares. We could show that for every* $(\epsilon_1, \epsilon_2, \epsilon_3) \in \{1, -1\}^3$, *there exists* $c_1^2 = x \in \mathbb{F}_q$ *s.t.* $\left(\frac{x+i}{q}\right) = \epsilon_i$ *(quadratic residue) for* $i \in \{1, 2, 3\}$, *whenever* $q \geq 19$. $\square$

Theorem

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 irreducible (existence is guaranteed by Lemma 2). Then, using the fundamental constructions, we reach the conclusion.* $\square$

Conclusions and Future Work

Theorem

For any prime power $q \geq 4$, $D^{(3)}(q) \geq \begin{cases} q-1 & \text{if } q \text{ is odd,} \\ q & \text{if } q \text{ is even.} \end{cases}$

Theorem by combining with Kronecker product construction

Let $n = q_1 q_2 \ldots q_r$, 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 $1 \leq i < j \leq r$.

- If $q_1 = 3$ and $n \neq 3$, then $D^{(3)}(n) \geq 3$.
- If $q_1 \geq 4$ is even, then $D^{(3)}(n) \geq q_1$.
- If $q_1 \geq 5$ is odd, then $D^{(3)}(n) \geq q_1 - 1$.

Conjecture. $D^{(3)}(n) \leq n-1$ *if n is odd.* $D^{(3)}(n) \leq n$ *if n is even.*
Conjecture. $D^{(d)}(n) \geq d$ *for any positive integer* $n \notin \{2, 3, 6\}$.

Thank you very much for your attention.

Conclusions and Future Work

Theorem

For any prime power $q \geq 4$, $D^{(3)}(q) \geq \begin{cases} q-1 & \text{if } q \text{ is odd,} \\ q & \text{if } q \text{ is even.} \end{cases}$

Theorem by combining with Kronecker product construction

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 $1 \leq i < j \leq r$.

- If $q_1 = 3$ and $n \neq 3$, then $D^{(3)}(n) \geq 3$.
- If $q_1 \geq 4$ is even, then $D^{(3)}(n) \geq q_1$.
- If $q_1 \geq 5$ is odd, then $D^{(3)}(n) \geq q_1 - 1$.

Conjecture. $D^{(3)}(n) \leq n - 1$ *if* n *is odd.* $D^{(3)}(n) \leq n$ *if* n *is even.*
Conjecture. $D^{(d)}(n) \geq d$ *for any positive integer* $n \notin \{2, 3, 6\}$.

Thank you very much for your attention.