Construction of Pairs of Orthogonal Latin Cubes

Vladimir N. Potapov

Sobolev Institute of Mathematics, Novosibirsk, Russia

26th British Combinatorial Conference

Glasgow, UK; July, 3-7, 2017

Definition

A latin square of order n is an $n \times n$ array of n symbols in which each symbol occurs exactly once in each row and in each column.

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

Definition

Two latin squares are orthogonal if, when they are superimposed, every ordered pair of symbols appears exactly once. If in a set of latin squares, any two latin squares are orthogonal then the set is called Mutually Orthogonal Latin Squares (MOLS)

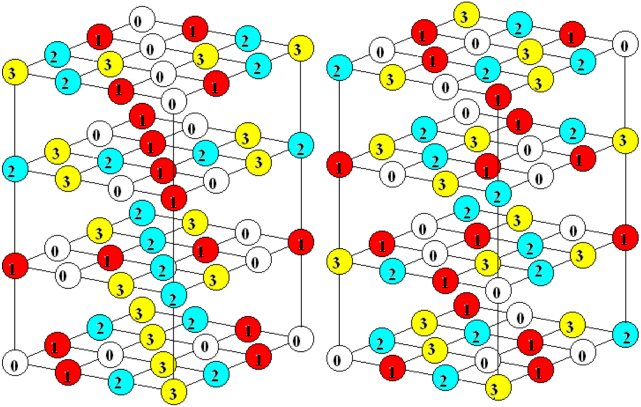
0	**2**	3	1
3	1	0	**2**
1	3	**2**	0
2	0	1	3

0	**2**	3	1
2	0	1	**3**
3	1	**0**	2
1	3	2	0

0	**2**	3	1
1	3	2	**0**
2	0	**1**	3
3	1	0	2

Definition

d-Dimensional array with the same condition is called latin *d*-cube. Two latin *d*-cubes are orthogonal if the same 2-dimensional faces in cubes contain orthogonal latin squares.



Main Result

Theorem

If $q = 16(6k \pm 1) + 4$ then there exists a pair of OLC of order q.

If $6k - 1 = 18i - 1$ or $6k - 1 = 18i + 5$ then pairs of OLC of order $q = 16(6k - 1) + 4$ was not previously known. A minimal new order is 84.

Definition

A system consist of t functions $f_1, \ldots, f_t$, $f_i : Q^s \to Q$, $(t \geq s)$ is orthogonal, if for each subsystem $f_{i_1}, \ldots, f_{i_s}$ consist of s functions hold

$$\{(f_{i_1}(\overline{x}), \ldots, f_{i_s}(\overline{x})) \mid \overline{x} \in Q^s\} = Q^s.$$

If the system keep to be orthogonal after substituting any constants for each subset of variables then it is called strong orthogonal.
A subset C of Q^{t+s} is called an MDS code with code distance $t+1$ and with length $t+s$ (denoted by $MDS_q(t+1, t+s)$, $q = |Q|$) if $|C \cap \Gamma| = 1$ for each t-dimensional face Γ.

Proposition (Ethier and Mullen 2012)

$MDS_q(t+1, t+s)$ codes are equivalent to strong orthogonal systems.

$$C = \{(x_1, \ldots, x_s, f_1(\overline{x}), \ldots f_t(\overline{x})) : x_i \in Q\}$$

Examples

(s, t, q) — strong orthogonal systems are

1. Reed–Solomon codes $[n, k, n-k+1]$, here
$n = s + t = q - 1, k = s$.

2. Hamming codes (perfect 1-error corrected) $[q+1, q-1, 3]$, here
$s = q - 1, t = 2$.

3. MOLS, here $s = 2$, t is the number of LS.

4. Finite projective planes, here $s = 2$, $t = q - 1$.

5. Pairs of OLC, here $s = 3$, $t = 2$.

Constructions

1. Solution of the system of linear equations over finite field.

2. Product construction (McNeish's theorem).

3. Wilson's construction (only for $s = 2$).

Problems

1. Is their exist finite projective planes if q is not prime power?

2. Is their exist 1-error corrected perfect codes (Hamming-like codes) if q is not prime power?

3. Does for any s and t exist an integer q_0 such that $MDS_q(t+1, t+s)$ code exists for any $q \geq q_0$?
(for $s = 2$ it is proved by Wilson R.M. (1979))

Product construction

McNeish's theorem

If $M = \{(x_1, \ldots, x_s, f_1(x), \ldots, f_t(x)) \mid x \in Q_1^s\}$ is an MDS code and for each $x \in Q_1^s$ the set $\{(y_1, \ldots, y_s, g_1^x(y), \ldots, g_t^x(y)) \mid y \in Q_2^s\}$ is an MDS code then the set

$$\{((f_1(x), g_1^x(y)), \ldots, (f_n(x), g_n^x(y))) \mid (x, y) \in (Q_1 \times Q_2)^s\}$$

is an MDS code.

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

a	b
b	a

b	a
a	b

0a	0b	2a	2b	3a	3b	1b	1a
0b	0a	2b	2a	3b	3a	1a	1b
3b	3a	1a	1b	0a	0b	2b	2a
3a	3b	1b	1a	0b	0a	2a	2b
1b	1a	3a	3b	2a	2b	0a	0b
1a	1b	3b	3a	2b	2a	0b	0a
2a	2b	0b	0a	1a	1b	3a	3b
2b	2a	0a	0b	1b	1a	3b	3a

Wilson's construction

A	*B*	2	3	0	1
1	0	*B*	*A*	2	3
B	*A*	0	1	3	2
3	2	*A*	*B*	1	0
0	3	1	2	.	.
2	1	3	0	.	.

0	1	*B*	*A*	3	2
A	*B*	0	1	2	3
3	2	*A*	*B*	1	0
B	*A*	3	2	0	1
2	0	1	3	.	.
1	3	2	0	.	.

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

0	2	3	1
2	0	1	3
3	1	0	2
1	3	2	0

0	**2**	3	1
2	0	**1**	**3**
3	1	**0**	**2**
1	**3**	2	0

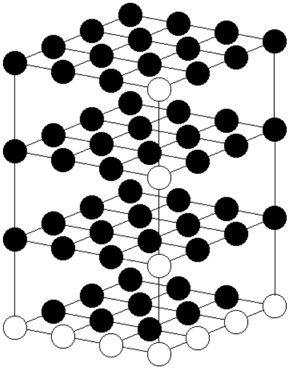
0	**2**	3	1
1	3	**2**	**0**
2	0	**1**	**3**
3	**1**	0	2

Wilson's construction

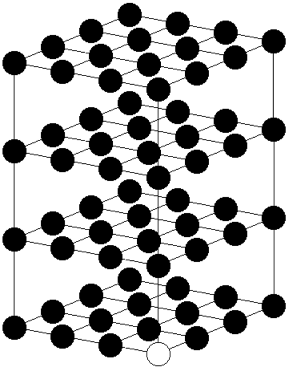
A	*B*	02	03	*C*	*D*	22	23	30	32	33	31	10	12	13	11	00	01	20	21
01	00	*B*	*A*	21	20	*D*	*C*	33	31	30	32	13	11	10	12	02	03	22	23
B	*A*	00	01	*D*	*C*	20	21	31	33	32	30	11	13	12	10	03	02	23	22
03	02	*A*	*B*	23	22	*C*	*D*	32	30	31	33	12	10	11	13	01	00	21	20
20	22	23	21	00	02	03	01	*A*	*B*	12	13	*C*	*D*	32	33	10	11	30	31
23	21	20	22	03	01	00	02	11	10	*B*	*A*	31	30	*D*	*C*	12	13	32	33
21	23	22	20	01	03	02	00	*B*	*A*	10	11	*D*	*C*	30	31	13	12	33	32
22	20	21	23	02	00	01	03	13	12	*A*	*B*	33	32	*C*	*D*	11	10	31	30
30	32	33	31	10	12	13	11	.	.	.	.	.	.	.	.	.	.	.	.
33	31	30	32	13	11	10	12	.	.	.	.	.	.	.	.	.	.	.	.
31	33	32	30	11	13	12	10	.	.	.	.	.	.	.	.	.	.	.	.
32	30	31	33	12	10	11	13	.	.	.	.	.	.	.	.	.	.	.	.
C	*D*	12	13	*A*	*B*	32	33	.	.	.	.	.	.	.	.	.	.	.	.
11	10	*D*	*C*	31	30	*B*	*A*	.	.	.	.	.	.	.	.	.	.	.	.
D	*C*	10	11	*B*	*A*	30	31	.	.	.	.	.	.	.	.	.	.	.	.
13	12	*C*	*D*	33	32	*A*	*B*	.	.	.	.	.	.	.	.	.	.	.	.
00	03	01	02	30	33	31	32	.	.	.	.	.	.	.	.	*A*	*B*	*C*	*D*
02	01	03	00	32	31	33	30	.	.	.	.	.	.	.	.	*B*	*A*	*D*	*C*
10	13	11	12	20	23	21	22	.	.	.	.	.	.	.	.	*C*	*D*	*A*	*B*
12	11	13	10	22	21	23	20	.	.	.	.	.	.	.	.	*D*	*C*	*B*	*A*

Proposed construction

Pairs of OLC with a hole (parameters $(n+m, m)$)



Type I



Type II

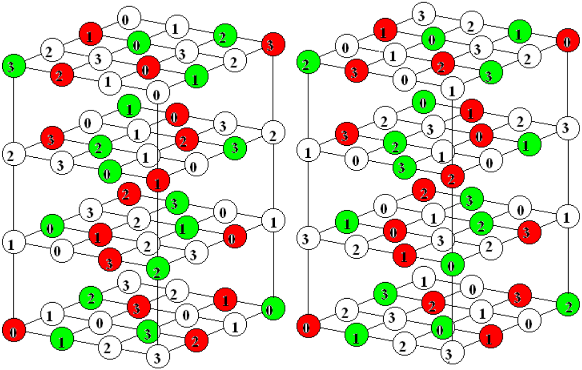
Proposed construction

POLC with a hole of Type I (parameters $(6, 2)$)

$ab2301$	$10ab32$	$23ba10$	$ba1023$	$0231..$	$3102..$
$10ba23$	$ba2310$	$ab1032$	$23ab01$	$3102..$	$0231..$
$ba0132$	$32ba01$	$01ab23$	$ab3210$	$1320..$	$2013..$
$32ab10$	$ab0123$	$ba3201$	$01ba32$	$2013..$	$1320..$
$0312..$	$2130..$	$3021..$	$1203..$	$......$	$......$
$2130..$	$0312..$	$1203..$	$3021..$	$......$	$......$

$01ba32$	$ba1023$	$ab3210$	$23ab01$	$1203..$	$3021..$
$ab0123$	$10ab32$	$32ba01$	$ba2310$	$2130..$	$0312..$
$32ab10$	$ab2301$	$ba0132$	$10ba23$	$0312..$	$2130..$
$ba3201$	$23ba10$	$01ab23$	$ab1032$	$3021..$	$1203..$
$2013..$	$0231..$	$1320..$	$3102..$	$......$	$......$
$1320..$	$3102..$	$2013..$	$0231..$	$......$	$......$

Proposed construction



By substitution into red elements of POLC with hole of Type I (6,2) with addition letters A and B, into green elements of POLC with hole of Type I (6,2) with addition letters C and D and into other elements of POLC of order 4, we obtain POLC with hole of Type I (20,4).

Proposed construction

A POLC with hole of Type II (20,4) it is easy to construct by deleting a subcube from POLC of order 20 (if it is obtained by product construction).

Using Vandermonde matrix we can obtain linear M_1 $MDS_5(5,5)$ code, M_2 $MDS_5(4,5)$ code, M_3 $MDS_5(3,5)$ code, such that $M_1 \subset M_2 \subset M_3$. $MDS_5(3,5)$ code is equivalent of POLC of order 5.

By substitution into $M_3 \setminus M_2$ a POLC of order 16 ($MDS_{16}(3,5)$); into $M_2 \setminus M_1$ a POLC with hole of Type I (20,4); into M_1 a POLC with hole of Type II (20,4) we obtain a POLC with hole of Type II (84,4).

By substitution into a hole a POLC of order 4 we obtain a POLC of order $84 = 2^2 \cdot 3 \cdot 7$.