Construction of pairs of orthogonal latin cubes based on combinatorial designs

Vladimir N. Potapov

Sobolev Institute of Mathematics, Novosibirsk, Russia

G2R2, Novosibirsk; August 15, 2018

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).

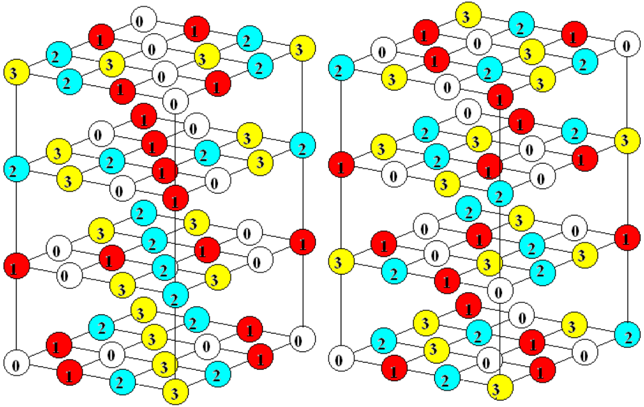
0	**2**	3	1
3	1	0	**2**
1	3	**2**	0
2	0	1	3

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

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



Definitions

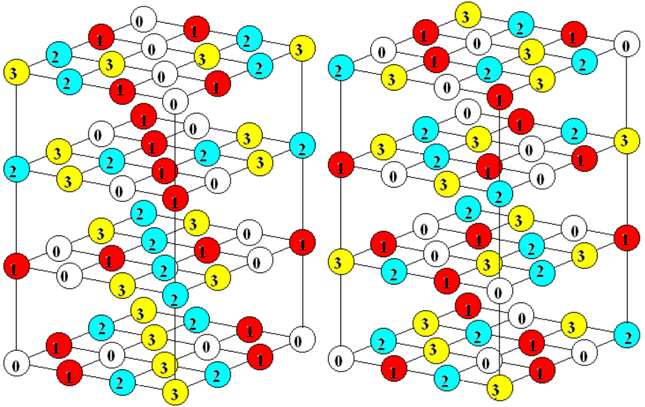
A Steiner system with parameters t, k, n, written $S(t, k, n)$, is a set of k-element unordered subsets of $[n] = \{0, \ldots, n-1\}$ (called blocks) with the property that each t-element subset of $[n]$ is contained in exactly one block. In an alternate notation for block designs, an $S(t, k, n)$ would be a $t-(n, k, 1)$ design.

An MDS code with parameters t, k, n, written $M(t, k, n)$, is a set of k-tuples from $[n]^k$ with the property that each t-tuple occupies any t positions exactly ones.

An n-ary MDS code M is a subset of $[n]^k$ with cardinality n^t such that the Hamming distance between two codewords is not less than $k - t + 1$.

A pair of OLC of order n is equivalent to $M(3,5,n)$. If a pair of orthogonal latin cubes are defined by functions $f_i : [n]^3 \to [n]$, $i = 1, 2$ then the set $M = \{(x_1, x_2, x_3, f_1(x_1, x_2, x_3), f_2(x_1, x_2, x_3)) \mid (x_1, x_2, x_3) \in [n]^3\}$ is an MDS code.

$M = \{(00000), (10011), \ldots, (33330)\}$.



Theorem (1959, Parker, Bose, and Shrikhande)

For $n \neq 2, 3, 6$ there exists a pair of orthogonal latin squares of order n.

Problem

For which n does there exist a pair of orthogonal latin cubes of order n?

Theorem (P.Keevash,14)

The natural divisibility conditions are sufficient for existence of Steiner system $S(t, k, n)$ apart from a finite number of exceptional n given fixed t and k.

Theorem (P.Keevash,18)

There exist MDS codes $M(t, k, n)$ apart from a finite number of exceptional n given fixed t and k.

Constructions

1. Solutions of systems of linear equations over finite fields (for n prime power).

2. Cartesian product construction (McNeish's theorem, for $n \neq 2q$, $n \neq 3q$).

3. Generalization of Wilson's construction (for $n = 16(6m \pm 1) + 4$).

Proposition

If designs D_2 of type $S(2,5,n)$ and D_3 of type $S(3,5,n)$ exist and $D_2 \subset D_3$, then there exits a pair of orthogonal latin cubes of order n.

The natural divisibility condition for existence of Steiner systems $S(2,5,n)$ and $S(3,5,n)$ simultaneously is that $n = 5 \text{ or } 41 \mod 60$.

Sketch of proof

$X = \{x_1, x_2, x_3, x_4, x_5\} \in D_3 \setminus D_2 \Rightarrow$
$M_X = \{(x_{\tau 1}, x_{\tau 2}, x_{\tau 3}, x_{\tau 4}, x_{\tau 5}) \mid \tau \in A_5\}$.

$X = \{x_1, x_2, x_3, x_4, x_5\} \in D_2 \Rightarrow$ define an MDS code M_X over alphabet X of type $M(3, 5, 5)$ such that M_X contains $(x_i, x_i, x_i, x_i, x_i)$ for $i = 1, \ldots, 5$.

Then $M = \bigcup_{X \in D_3} M_X$ is an MDS code of type $M(3, 5, n)$.