On the numbers of *n*-ary quasigroups, Latin hypercubes and MDS codes

Vladimir N. Potapov

Sobolev Institute of Mathematics

Graphs and Groups, Spectra and Symmetries

Novosibirsk, Russia; August, 15-28, 2016

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)

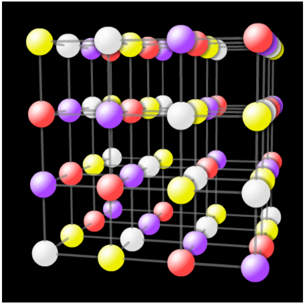
0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

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

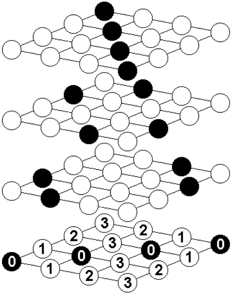
A d-dimensional array with the same property is called a latin d-cube.



A function $f : \{0, \ldots, n-1\}^d \to \{0, \ldots, n-1\}$ is called an d-ary quasigroup of order n iff $f(x) \neq f(y)$ as d-tuples x and y are differ in one position.
From the definition we can ensure that a latin d-cube is the Cayley table of a d-ary quasigroup.

Definition

A subset C of $\{0,\dots,n-1\}^{d+1}$ is called an MDS code with code distance $t+1$ and with length $d+1$ if $|C \cap \Gamma| = 1$ for each t-dimensional face Γ.
A graph $C[f] = \{(x, f(x)) \mid x \in \{0,\dots,n-1\}^d\}$ of d-ary quasigroup f is MDS code with distance 2.



If quasigroups $f_1, f_2, \dots, f_t$ define a system of MOLS then the set

$$M = \{(x_1, x_2, f_1(x_1, x_2), \dots, f_t(x_1, x_2)) \; | (x_1, x_2) \in \{0, \dots, n-1\}^2\}$$

is an MDS code with code distance $t+1$.

History

Let $N(n, d, \varrho)$ be the number of MDS codes of order n with code distance ϱ and length d.

Numbers of latin d-cubes ($d \geq 3$) for small orders are calculated by McKay and Wanless (2008).
Numbers of MDS codes (with code distance large than 2) for small orders are calculated by Kokkala, Krotov and Ostergard (2015).

An upper bound $N(n, d, 2) \leq ((1 + o(1))n/e^d)^{n^d}$ is proved by Linial and Luria (2014).

A lower bound of number of systems of MOLS (as order in a prime power) $\ln N(n, d, d-1) \geq \alpha n^2 \ln n$ as $n \to \infty$ is proved by Donovan and Grannell (2013).

Main Result

Theorem

For each prime number p and $d \leq p+1$ if $3 \leq \varrho \leq p$ or an arbitrary $d \geq 2$ if $\varrho = 2$ it holds
$\ln N(p^k, d, \varrho) \geq (k+m)p^{(k-2)m} \ln p(1+o(1))$ as $k \to \infty$,
$m = d - \varrho + 1$.

Corollary 1

The logarithm of the number of latin d-cubes of order n is $\Theta(n^d \ln n)$ as $n \to \infty$.

Corollary 2

The logarithm of the number of systems of t mutually orthogonal latin squares of order n is $\Theta(n^2 \ln n)$ as $n \to \infty$.

Sketch of proof. n is a prime power.

Let p be a prime number, d, k be integers and $n = p^k$. Then we can consider $\{0, \dots, n-1\}$ as $GF(p^k)$ or k-dimensional vector space over $GF(p)$. We will call MDS code a linear code over $GF(p)$ if it is linear (i. e. $f_i = \alpha_{1i}x_1 + \dots + \alpha_{di}x_d$) and all coefficients α_{ji} ($j = 1, \dots, d$, $i = 1, \dots, m$) are in $GF(p)$. For $a, v \in GF(p^k)$ denote by $L(a, v) = \{a + \alpha v \mid \alpha \in GF(p)\}$ an affine 1-subspace.

Proposition 1

(a) for each $\varrho \in \{2, d\}$ there exists a linear over $GF(p)$ MDS code $C \subset (GF(p^k))^d$ with code distance ϱ,
(b) for each integers $d \leq p + 1$ there exists a linear over $GF(p)$ MDS code $C \subset (GF(p^k))^d$ with code distance ϱ, $3 \leq \varrho \leq p$.

Proposition 2

Let C be a linear code over $GF(p)$, $(a_1, \dots, a_d) \in C$, $v \in GF(p^k) \setminus \{0\}$. Then $C \cap (L(a_1, v) \times \dots \times L(a_d, v))$ is a subcode of C of order p.

Example of subcode

0	1	2	3	4	**5**	6	**7**	8
1	**2**	0	**4**	5	3	7	8	**6**
2	0	1	5	3	4	8	6	7
3	**4**	5	**6**	7	8	0	1	**2**
4	5	3	7	8	6	1	2	0
5	3	4	8	6	**7**	2	**0**	1
6	7	8	0	1	2	3	4	5
7	8	6	1	2	**0**	4	**5**	3
8	**6**	7	**2**	0	1	5	3	**4**

0	1	2	3	4	**5**	6	**7**	8
2	**0**	1	**5**	3	4	8	6	**7**
1	2	0	4	5	3	7	8	6
6	**7**	8	**0**	1	2	3	4	**5**
8	6	7	2	0	1	5	3	4
7	8	6	1	2	**0**	4	**5**	3
3	4	5	6	7	8	0	1	2
5	3	4	8	6	**7**	2	**0**	1
4	**5**	3	**7**	8	6	1	2	**0**

Example of switching

0	1	2	3	4	5	6	7	8
1	2	0	4	5	3	7	8	6
2	0	1	5	3	4	8	6	7
3	4	5	6	7	8	0	1	2
4	5	3	7	8	6	1	2	0
5	3	4	8	6	7	2	0	1
6	7	8	0	1	2	3	4	5
7	8	6	1	2	0	4	5	3
8	6	7	2	0	1	5	3	4

0	1	2	3	4	5	6	7	8
2	0	1	5	3	4	8	6	7
1	2	0	4	5	3	7	8	6
6	7	8	0	1	2	3	4	5
8	6	7	2	0	1	5	3	4
7	8	6	1	2	0	4	5	3
3	4	5	6	7	8	0	1	2
5	3	4	8	6	7	2	0	1
4	5	3	7	8	6	1	2	0

The result of switching.

0	1	2	3	4	5	6	7	8
1	2	0	4	5	3	7	8	6
2	0	1	5	3	4	8	6	7
3	4	5	6	7	8	0	1	2
4	5	3	7	8	6	1	2	0
5	3	4	8	6	7	2	0	1
6	7	8	0	1	2	3	4	5
7	8	6	1	2	0	4	5	3
8	6	7	2	0	1	5	3	4

0	1	2	3	8	5	6	7	4
2	0	1	5	3	4	8	6	7
1	2	0	4	5	3	7	8	6
6	7	8	0	1	2	3	4	5
4	6	7	2	0	1	5	3	8
7	8	6	1	2	0	4	5	3
3	4	5	6	7	8	0	1	2
5	3	4	8	6	7	2	0	1
8	5	3	7	4	6	1	2	0

Example of switching

0	1	2	3	4	5	6	7	8
1	2	0	4	5	3	7	8	6
2	0	1	5	3	4	8	6	7
3	4	5	6	7	8	0	1	2
4	5	3	7	8	6	1	2	0
5	3	4	8	6	7	2	0	1
6	7	8	0	1	2	3	4	5
7	8	6	1	2	0	4	5	3
8	6	7	2	0	1	5	3	4

0	1	2	3	4	5	6	7	8
2	0	1	5	3	4	8	6	7
1	2	0	4	5	3	7	8	6
6	7	8	0	1	2	3	4	5
8	6	7	2	0	1	5	3	4
7	8	6	1	2	0	4	5	3
3	4	5	6	7	8	0	1	2
5	3	4	8	6	7	2	0	1
4	5	3	7	8	6	1	2	0

The result of switching.

0	1	2	3	4	5	6	7	8
2	**0**	**1**	4	5	3	7	8	6
1	**2**	**0**	5	3	4	8	6	7
3	4	5	6	7	8	0	1	2
4	5	3	7	8	6	1	2	0
5	3	4	8	6	7	2	0	1
6	7	8	0	1	2	3	4	5
7	8	6	1	2	0	4	5	3
8	6	7	2	0	1	5	3	4

0	1	2	3	8	5	6	7	4
1	**2**	**0**	5	3	4	8	6	7
2	**0**	**1**	4	5	3	7	8	6
6	7	8	0	1	2	3	4	5
4	6	7	2	0	1	5	3	8
7	8	6	1	2	0	4	5	3
3	4	5	6	7	8	0	1	2
5	3	4	8	6	7	2	0	1
8	5	3	7	4	6	1	2	0

Sketch of proof. n is arbitrary.

Theorem (Krotov, P., Sokolova, 2008)

For every integers n, ℓ, d, $\ell \leq n/2$, there exists a latin d-cube of order n with a latin d-subcube of order m.

Theorem (Heinrich, Zhu, 1986)

For every integers $n, \ell \notin \{1, 2, 6\}$, $\ell \leq n/3$, there exists a pair of orthogonal latin squares of order n with orthogonal latin subsquares of order ℓ.

Theorem (van Bommel, 2015)

For large enough integers n, ℓ, $\ell \ll n$, there exists a system of t MOLS of order n with a subcode of order ℓ.

Example of subcode

8	9	3	0	5	6	7	1	2	4
9	7	0	2	3	4	8	5	6	1
4	0	6	7	1	8	9	2	3	5
0	3	4	5	8	9	1	6	7	2
7	1	2	8	9	5	0	3	4	6
5	6	8	9	2	0	4	7	1	3
3	8	9	6	0	1	2	4	5	7
1	4	7	3	6	2	5	8	9	0
6	2	5	1	4	7	3	9	0	8
2	5	1	4	7	3	6	0	8	9

1	2	8	4	0	9	7	3	6	5
5	8	7	0	9	3	4	6	2	1
8	3	0	9	6	7	1	2	5	4
6	0	9	2	3	4	8	5	1	7
0	9	5	6	7	8	2	1	4	3
9	1	2	3	8	5	0	4	7	6
4	5	6	8	1	0	9	7	3	2
2	6	3	7	4	1	5	8	9	0
7	4	1	5	2	6	3	0	8	9
3	7	4	1	5	2	6	9	0	8