On the number of latin hypercubes, pairs of orthogonal latin squares and MDS codes

Article · October 2015

Source: arXiv

1 author:

Vladimir Potapov
Russian Academy of Sciences

On the number of latin hypercubes, pairs of orthogonal latin squares and MDS codes

Vladimir N. Potapov[1]

Sobolev Institute of Mathematics, 4 Acad. Koptyug Avenue, Novosibirsk, Russia

Abstract

The logarithm of the number of latin d-cubes of order n is $\Theta(n^d \ln n)$. The logarithm of the number of pairs of orthogonal latin squares of order n is $\Theta(n^2 \ln n)$. Similar estimations are obtained for systems of mutually strong orthogonal latin d-cubes.

Keywords: latin square, latin d-cube, orthogonal latin squares, MOLS, MDS code.

2010 MSC: 05B15

1. Introduction

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

From the definition we can ensure that a latin d-cube is the Cayley table of a d-ary quasigroup. Denote by Q the underlying set of the quasigroup. A system consisting of t s-ary functions $f_1,\dots,f_t$ ($t\geq s$) is *orthogonal*, if for each

Email address: vpotapov@math.nsc.ru (Vladimir N. Potapov)

[1]The work was funded by the Russian Science Foundation (grant No 14-11-00555).

subsystem $f_{i_1}, \ldots, f_{i_s}$ consisting of s functions it holds

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

If the system keeps to be orthogonal after substituting any constants for each subset of variables then it is called *strongly orthogonal* (see [4]). It is important to note that all functions in a strongly orthogonal system are multiary quasigroups. If the number of variables equals 2 ($s = 2$) then such system is equivalent to a set of MOLS. If $s > 2$, it is a set of Mutually Strong Orthogonal Latin s-Cubes (MSOLC).

The best known estimate of the number of latin squares is $((1+o(1))n/e^2)^{n^2}$ (see [10]). The lower bound obtained in [3] and the upper bound followed from Bregman's inequality for permanent. An upper bound $((1+o(1))n/e^d)^{n^d}$ of the number of latin d-cubes is proved in [9].

In this paper we find lower bounds for numbers of MOLS, latin d-cubes and MSOLC. This numbers for small orders are calculated in [11], [7].

2. MDS codes

A subset C of Q^d is called an *MDS code* (of order $|Q|$ with code distance $t+1$ and with length d) if $|C \cap \Gamma| = 1$ for each t-dimensional face Γ.

Proposition 1. [4] *A set $C \subset Q^{t+m}$ is an* MDS-*code with code distance $\varrho_C = m+1$ if and only if there exists strongly orthogonal system consisting of m t-ary quasigroups $f_1, \ldots, f_m$ such that*

$$C = \{(x_1, \ldots, x_t, f_1(\overline{x}), \ldots, f_m(\overline{x})) \mid \overline{x} \in Q^t\}.$$

Let Q be a finite field. An MDS code C is called *linear (affine)* if it is a linear (or affine) subspace of Q^d. In this case the functions $f_1, \ldots, f_m$ are linear and rank of the code is equal to $\dim(C) = t$. Let F be a subfield of a finite field Q and $|Q| = |F|^k$. Then we can consider Q as k-dimensional vector space over F. We will call $C \subset Q^d$ a linear code over F if it is linear (i. e. $f_i = \alpha_{1i}x_1 + \ldots + \alpha_{di}x_d$) and all coefficients α_{ji} ($j = 1, \ldots, d$, $i = 1, \ldots, m$) are in F. For $a, v \in Q$ denote by $L(a, v) = \{a + \alpha v \mid \alpha \in F\}$ an 1-dimensional affine subspace in Q.

The following criterion for MDS codes is well-known.

Proposition 2. *A subset $M \subset Q^d$ is an* MDS *code if and only if $|M| = |Q|^{d-\varrho+1}$, where ϱ is a code distance of M.*

By using a well-known construction of a linear MDS code ([5]) with matrix over prime subfield $GF(p)$ we can conclude that the following proposition is true.

Proposition 3. (a) *For each prime number p, integers d, k and $\varrho \in \{2, d\}$ there exists a linear over $GF(p)$* MDS *code $C \subset (GF(p^k))^d$ with code distance ϱ.*

(b) *For each prime number p and integers $d \leq p + 1$, k there exists a linear over $GF(p)$* MDS *code $C \subset (GF(p^k))^d$ with code distance ϱ, $3 \leq \varrho \leq p$.*

If $2 < \varrho < d$ and $p \neq 2$ then the length of a linear MDS code of order p^k with code distance ϱ does not exceed $p^k + 1$ or $p^k + 2$ for $p = 2$ (see [1], [2]).

3. MDS subcodes and lower bounds

A subset T of MDS code $M \subset Q^d$ is called a *subcode* or a *component* of the code if T is an MDS code in $A_1 \times \ldots \times A_d$ with the same code distance as M and $T = M \cap (A_1 \times \ldots \times A_d)$ where $A_i \subset Q$, $i \in \{1, \ldots, d\}$. Obviously $|A_1| = \ldots = |A_d|$ and $|A_1|$ is the order of the subcode T.

Let us now consider possible orders of subcodes. The following proposition is well-known for case of pairs of orthogonal latin squares (a case of MDS code with distance $\varrho = 3$).

Proposition 4. *If an* MDS *code $M \subset Q^d$ with code distance ϱ contains a proper subcode of order m then $\varrho \leq m \leq |Q|/\varrho$.*

Proof. By definition every strongly orthogonal system consisting of $t = \varrho - 1$ functions includes a system $f_1, \ldots, f_t$ of t MOLS. A system of MOLS of order

m consists of not more than $m-1$ latin squares. Therefore $t \leq m-1$. Without loss of generality we can assume that the subcode includes a system of t MOLS of order m over the alphabet B. Denote by b the symbols of B and by a the other symbols. By the definition of orthogonal system, for any pair a, b and any $i, j \in \{1, \dots, t\}$, there exists $(u_1, u_2) \in (Q \setminus B)^2$ such that $f_i(u_1) = a$ and $f_j(u_2) = b$. Thus $|(Q \setminus B)^2| = (|Q| - m)^2 \geq tm(|Q| - m)$. ▲

From the definition of an MDS code and Proposition 5 we obtain:

Proposition 5. *Let $C \subset Q^d$ be a linear code over F, $(a_1, \dots, a_d) \in C$, $v \in Q \setminus \{0\}$. Then $C \cap (L(a_1, v) \times \ldots \times L(a_d, v))$ is a subcode of C of order $|F|$.*

Proposition 6. *Assume C is a code with a subcode C_1 of order m and a code C_2 has the same parameters as C_1. Then it is possible to exchange C_1 by C_2 in C and to obtain the code C' with the same parameters as C.*

It is said the codes C and C' obtained from each other by switching [12]. If a code has nonintersecting subcodes then it is possible to apply switching independently to each of the subcodes.

For example consider a pair of orthogonal latin squares of order 9 below. A subcode (orthogonal subsquares) is marked by boldface.

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**

Below we can see a 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**

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

Theorem 1. *For each prime number p and*
(a) *$d \leq p + 1$ if $3 \leq \varrho \leq p$ or*
(b) *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 $k \to \infty$, $m = d - \varrho + 1$.

Proof. Consider a linear MDS code C over a prime field with rank m and length d (see Proposition 3). The number of its subcodes determined in Proposition 5 is equal to $p^{k(1+m)}/p^m$ where p^m is the cardinality of subcodes. Each vertex of the code lies in $p^k - 1$ subcodes. Consequently, each subcode intersects with not more than p^{m+k} other subcodes. Thus we can choose $t = (1 - \varepsilon(k))(p^{k(1+m)}/p^{2m+k})$ times one of subcodes so that a new subcode is not intersected with subcodes choosing early. For each subcode we have more than $w = \varepsilon(k)(p^{k(1+m)}/p^m)$ alternatives, where $\varepsilon(k) = o(1)$ and $\ln \varepsilon(k) = o(k)$. By Proposition 6 the code obtained by switchings of this mutually disjoint subcodes has the same parameters as the origin code C. Then $N(p^k, d, \varrho)$ is greater than $w^t/t!$. Applying Stirling's formula, we get the lower bound on $N(p^k, d, \varrho)$. ▲

Proposition 7. [8] *For every integers n, m, d, $m \le n/2$, there exists a latin d-cube of order n with a latin d-subcube of order m.*

Corollary 1. *The logarithm of the number of latin d-cubes of order n is $\Theta(n^d \ln n)$ as $n \to \infty$.*

The lower bound comes from Theorem and Proposition 7, the upper bound is trivial.

Proposition 8. [6] *For every integers $n, \ell \notin \{1, 2, 6\}$, $\ell \le n/3$, there exists a pair of orthogonal latin squares of order n with orthogonal latin subsquares of order ℓ.*

Corollary 2. *The logarithm of the number of pairs of orthogonal latin squares of order n is $\Theta(n^2 \ln n)$ as $n \to \infty$.*

The lower bound follows from Theorem and Proposition 8, the upper bound is trivial.

References

[1] Ball S. On sets of vectors of a finite vector space in which every subset of basis size is a basis, J. Eur. Math. Soc. 2012. V. 14, N. 3. P. 733–748.

[2] Ball S., De Beule J. On sets of vectors of a finite vector space in which every subset of basis size is a basis II, Des. Codes Cryptogrophy. 2012. V. 65, N. 1-2. P. 5–14.

[3] Egorichev G. P. Proof of the van der Waerden conjecture for permanents, Siberian Math. J. 22 (1981), 854-859.

[4] Ethier J. T., Mullen G. L. Strong forms of orthogonality for sets of hypercubes, Discrete Math. 2012. V. 312, N 12-13. P. 2050–2061.

[5] Handbook of combinatorial designs. Edited by Charles J. Colbourn and Jeffrey H. Dinitz. Second edition. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007. xxii+984 pp.

[6] Heinrich K., Zhu L. Existence of orthogonal Latin squares with aligned subsquares, Discrete Math. 59 (1986), no. 1-2, 69-78.

[7] Kokkala J. I., Krotov D. S., Ostergard P. R. J. On the Classification of MDS Codes, IEEE Transactions on Information Theory, 2015 (Published online)

[8] Krotov D. S., Potapov V. N., Sokolova P. V. On reconstructing reducible n-ary quasigroups and switching subquasigroups, Quasigroups and Related Systems. 2008. V. 16. P. 55–67.

[9] Linial N., Luria Z. An upper bound on the number of high-dimensional permutations, Combinatorica. 2014. V. 34, N 4. P. 471–486.

[10] van Lint J. H., Wilson R. M. A Course in Combinatorics, Cambridge U.P., 1992.

[11] McKay B. D., Wanless I. M. A census of small Latin hypercubes, SIAM J. Discrete Math. 2008. V. 22, N 2. P. 719–736.

[12] Ostergard P. R. J. Switching codes and designs, Discrete Math. 2012. V. 312, N 3. P. 621–632.