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

Vladimir N. Potapov
Sobolev Institute of Mathematics SB RAS, Novosibirsk, Russia
vpotapov@math.nsc.ru

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 subsystem $f_{i_1}, \dots, f_{i_s}$ consisting of s functions it holds $\{(f_{i_1}(\overline{x}), \dots, f_{i_s}(\overline{x})) \mid \overline{x} \in Q^s\} = Q^s$. If the system keeps to be orthogonal after substituting any constants for each subset of variables then it is called *strongly orthogonal* (see [2]). 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). 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. A system of t MSOLC is equivalent to MDS code with distance $t + 1$ (see [2]). Numbers of MOLS, latin d-cubes and MDS codes for small orders are calculated in [4], [7].

Let $N(n, d, \varrho)$ be the number of MDS codes of order n with code distance ϱ and length d. An upper bound $N(n, d, 2) \leq ((1 + o(1))n/e^d)^{n^d}$ is proved in [6].

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

We use results of [5] to obtain (a) and results of [3] to obtain (b). Item (b) for a subsequence of integers was proved in [1]. Complete text of the report is available in [8].

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

References

[1] D. M. Donovan, M. J. Grannell, On the number of transversal designs. *J. Comb. Theory, Ser. A* **120(7)** (2013) 1562–1574.

[2] J. T. Ethier, G. L. Mullen, Strong forms of orthogonality for sets of hypercubes. *Discrete Math.* **312(12-13)** (2012) 2050–2061.

[3] K. Heinrich, L. Zhu, Existence of orthogonal Latin squares with aligned subsquares. *Discrete Math.* **59(1-2)** (1986) 69-78.

[4] J. I. Kokkala, D. S. Krotov, P. R. J. Ostergard, On the classification of MDS codes. *IEEE Trans. Inform. Theory* **61(12)** (2015) 6485–6492.

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

[6] N. Linial, Z. Luria, An upper bound on the number of high-dimensional permutations. *Combinatorica* **34(4)** (2014) 471–486.

[7] B. D. McKay, I. M. Wanless, A census of small Latin hypercubes. *SIAM J. Discrete Math.* **22(2)** (2008) 719–736.

[8] V. N. Potapov, On the number of latin hypercubes, pairs of orthogonal latin squares and MDS codes. *arXiv:1510.06212* (2015)