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 $f_1, \ldots, f_t$ ($t \geq s$) is orthogonal, if for each subsystem $f_{i_1}, \ldots, f_{i_s}$ consisting of $s$ functions it holds $\{(f_{i_1}(\varpi), \ldots, f_{i_s}(\varpi)) \mid \varpi \in Q^s\} = Q^s$. 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 $\Gamma$. 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 $N(n,d,g)$ be the number of MDS codes of order $n$ with code distance $g$ and length $d$. An upper bound $N(n,d,2) \leq ((1+o(1)) n/e^d)^n$ is proved in [6].

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

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