Isotopically transitive pairs of MOLS

V. N. Potapov

Sobolev Institute of Mathematics, Novosibirsk, Russia

Mal'tsev Meeting, Novosibirsk, May 3-7, 2015

Let F_q be the Galois field of order q. A subset M of F_q^n is called an MDS code (with code distance $k+1$) if $|M \cap \Gamma| = 1$ for each k-dimensional face Γ. For $k = n-2$, an MDS code is equivalent to a set of $(n-2)$ mutually orthogonal latin squares (MOLS).

f_1

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

f_2

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

f_3

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

$$M = \{(x, y, f_1(x,y), f_2(x,y), f_3(x,y)) \;|(x,y) \in F_4^2\}$$

Proposition 1

Let $M \subset F_q^m$ be an MDS code and let for each $x \in M$ a set $L(x) \subset F_{q'}^m$ be an MDS code (these codes have the same distance). Then the set $C = \{(x, y) \mid x \in M, y \in L(x)\} \subset F_{q \times q'}^m$ is an MDS code.

If the code $L(x)$ doesn't depend on x then the MDS code C is obtained as Cartesian product.

0	1	3	2	4	5
1	0	2	3	5	4
3	2	5	4	1	0
2	3	4	5	0	1
4	5	0	1	3	2
5	4	1	0	2	3

0	1	2	3	4	5
1	0	3	2	5	4
2	3	4	5	0	1
3	2	5	4	1	0
4	5	0	1	2	3
5	4	1	0	3	2

A subset T of MDS code $C \subset F_q^n$ is called a subcode if T is an MDS code in $A_1 \times \cdots \times A_n$ and $T = C \cap (A_1 \times \cdots \times A_n)$ where $A_i \subset F_q$.

An isotopism is a transform $\overline{\tau} : \overline{x} \mapsto \overline{\tau}\overline{x}$ where $\overline{x} = (x_1, \ldots, x_n) \in F_q^n$, $\overline{\tau}\overline{x} = (\tau_1 x_1, \ldots, \tau_n x_n)$, $\tau_i \in S_q$. Define the group of autotopisms $\mathrm{Ist}(A) = \{\overline{\tau} \mid \overline{\tau}A = A\}$, which map $A \subseteq F_q^n$ to itself. A set $A \subseteq F_q^n$ is called isotopically transitive if for every two vertices $\overline{x}, \overline{y}$ from A there exists an isotopism $\overline{\tau}$ such that $\overline{\tau}(\overline{x}) = \overline{y}$ and $\overline{\tau}(A) = A$; i.e., the group $\mathrm{Ist}(A)$ acts transitively on A.

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

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

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

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

Proposition 2

If a code C is obtained as the Cartesian product of two isotopically transitive codes, then C is isotopically transitive.

A code is called linear if it is a linear subspace.

Proposition 3

a) Any vertex of an MDS code obtained as the Cartesian product lies in two proper subcodes (at least).
b) A linear pair of MOLS over $GF(q^2)$ (q is prime, $d = 3$) either hasn't subcodes or any vertex of the code lies in two proper subcodes.

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

Consider the code $C_0 \subset (F_{q\times q})^4$, $(x_i, y_i) \in F_q \times F_q \simeq F_{q\times q}$, determined by the equations

$$\begin{cases} x_3 = l_{11}x_1 + l_{12}x_2; \\ x_4 = l_{21}x_1 + l_{22}x_2; \\ y_3 = m_{11}y_1 + m_{12}y_2 + \xi_1(x_1, x_2); \\ y_4 = m_{21}y_1 + m_{22}y_2 + \xi_2(x_1, x_2), \end{cases}$$

where ξ_1 and ξ_2 are quadratic functions and the pairs of vectors (l_{11}, l_{12}), (l_{21}, l_{22}) and (m_{11}, m_{12}), (m_{21}, m_{22}) are not collinear.

Theorem 1

If the pairs of vectors (l_{11}, l_{12}), (m_{11}, m_{12}) and (l_{21}, l_{22}), (m_{21}, m_{22}) are not collinear, then C_0 is an isotopically transitive MDS code.

Theorem 2

If $\xi_2(x_1, x_2) = x_1 x_2$ and $\xi_1(x_1, x_2) \equiv 0$ then C_0 isn't isotopic to a linear code or to a code obtained as the Cartesian product.

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
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
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

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

$$\begin{cases} x_3 = x_1 + x_2; \\ x_4 = x_1 + 2x_2; \\ y_3 = y_1 + 2y_2; \\ y_4 = y_1 + y_2 + x_1 x_2. \end{cases}$$

Wilson R. L. Jr. Isotopy-isomorphy loops of prime order // J. Algebra — 1974. — V. 31. P. 117–119.

Goodaire E. G., Robinson D. A. A class of loops which are isomorphic to all loop isotopes // Canadian J. Math. — 1982. — V. 34. — P. 662–672.

Kunen K. *G*-loops and permutation groups // J. Algebra — 1999. — V. 220, N 2. — P. 694–708.

Krotov D.S., Potapov V.N. Propelinear 1-perfect codes from quadratic functions // IEEE Trans. Inform. Theory. 2014. V. 60, N 4. P. 2065–2068.

Krotov D.S., Potapov V.N. Constructions of transitive latin hupercubes // arXiv.org eprint math., math.CO/1303.0004