European Journal of Combinatorics 54 (2016) 51–64

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Constructions of transitive latin hypercubes

Denis S. Krotov, Vladimir N. Potapov

Sobolev Institute of Mathematics, pr. Akademika Koptyuga 4, Novosibirsk 630090, Russia

ARTICLE INFO

Article history:
Received 28 April 2015
Accepted 2 December 2015
Available online 24 December 2015

ABSTRACT

A function $f : \{0, \dots, q-1\}^n \to \{0, \dots, q-1\}$ invertible in each argument is called a latin hypercube. A collection $(\pi_0, \pi_1, \dots, \pi_n)$ of permutations of $\{0, \dots, q-1\}$ is called an autotopism of a latin hypercube f if $\pi_0 f(x_1, \dots, x_n) = f(\pi_1 x_1, \dots, \pi_n x_n)$ for all $x_1, \dots, x_n$. We call a latin hypercube isotopically transitive (topolinear) if its group of autotopisms acts transitively (regularly) on all q^n collections of argument values. We prove that the number of nonequivalent topolinear latin hypercubes grows exponentially with respect to $\sqrt{n}$ if q is even and exponentially with respect to n^2 if q is divisible by a square. We show a connection of the class of isotopically transitive latin squares with the class of G-loops, known in noncommutative algebra, and establish the existence of a topolinear latin square that is not a group isotope. We characterize the class of isotopically transitive latin hypercubes of orders $q = 4$ and $q = 5$.

We consider the latin hypercubes such that their autotopism groups act transitively (or regularly) on their elements. We call them the isotopically transitive (topolinear, respectively) latin hypercubes. The study of highly symmetrical objects, such as the objects from the considered class, is a natural direction in the enumerative combinatorics. On the other hand, latin hypercubes are also very natural research objects, which are studied in different areas of mathematics. For example, in coding theory, equivalent objects are known as the distance-2 MDS codes; in noncommutative algebra, the n-ary quasigroups. The number of latin n-cubes, MDS codes, and related objects attracts attention of mathematicians in the last few years; different evaluations and exact values can be found in [5,8–11,15,17,18,25,24]. In this paper, we are mainly concentrated on the number of nonequivalent

E-mail address: krotov@math.nsc.ru (D.S. Krotov).

http://dx.doi.org/10.1016/j.ejc.2015.12.001
0195-6698/

isotopically transitive latin hypercubes, proving that this number is exponential with respect to the dimension, for some fixed orders. However, some additional interesting characterization results are obtained for isotopically transitive latin squares and isotopically transitive latin hypercubes of order 4.

In Section 1, we give definitions and some preliminary results. In Section 2, Theorem 1, we prove a connection (in some sense, one-to-one correspondence) between the isotopically transitive latin squares and the algebraic structures known as G-loops. In Section 3, we consider examples of G-loops, which are utilized in Section 4 to construct an exponential (in $\sqrt{n}$) number of nonequivalent topolinear latin n-cubes, for every even order ≥ 4 (Theorems 2 and 3, Corollary 2). Additionally, in Section 3 we show that there are topolinear latin squares that are not isotopic to a group operation (Corollary 1). In Section 5, we consider a direct construction, using quadratic functions, which gives an exponential (in n^2) number of nonequivalent topolinear latin n-cubes, for every order divisible by a square (Corollary 3). In Sections 6 and 7, we characterize the class of isotopically transitive latin hypercubes of orders 4 and 5 (Theorems 5 and 6, respectively). In the concluding section, we consider some open problems.

1. Preliminaries

1.1. Transitive and propelinear sets

Let $\Sigma = \Sigma_q$ be a finite set of cardinality q; for convenience, we choose some element of Σ and denote it 0. The set Σ^n of n-tuples from Σ^n with the Hamming distance is called a *q-ary n-dimensional Hamming space* (recall that the Hamming distance between two n-tuples is the number of positions in which they differ). An *isotopism* $\overline{\tau} = (\tau_0, \dots, \tau_{n-1})$ is a transform $\overline{x} \mapsto \overline{\tau}\overline{x}$, where $\overline{x} = (x_0, \dots, x_{n-1}) \in \Sigma^n$, $\overline{\tau}\overline{x} = (\tau_0 x_0, \dots, \tau_{n-1}x_{n-1})$, and $\tau_0, \dots, \tau_{n-1}$ are permutations of Σ. For a set $A \subseteq \Sigma^n$, denote $\overline{\tau}A = \{\overline{\tau}\overline{x} \mid \overline{x} \in A\}$. Define the *autotopism group* $\mathrm{Ist}(A) = \{\overline{\tau} \mid \overline{\tau}A = A\}$, which consists of isotopisms that map $A \subseteq \Sigma^n$ to itself. It is well known (see, e.g., [3, Theorem 9.2.1]) that every isometry of Σ^n can be represented as the composition of an isotopism and a coordinate permutation. The subgroup of the isometry group of Σ^n that maps $A \subseteq \Sigma^n$ to itself will be denoted $\mathrm{Aut}(A)$. We will say that two subsets A and B of Σ^n are *equivalent* (*isotopic*) if B is the image of A under some isometry of the space (isotopism, respectively).

A set $A \subseteq \Sigma^n$ is called *transitive* if for every two vertices $\overline{x}, \overline{y}$ from A there exists an element α of $\mathrm{Aut}(A)$ such that $\alpha(\overline{x}) = \overline{y}$; i.e., the group $\mathrm{Aut}(A)$ acts transitively on A. We call a set $A \subseteq \Sigma^n$ *isotopically transitive* if $\mathrm{Ist}(A)$ acts transitively on A. In what follows we assume that the all-zero tuple $\overline{0}$ belongs to A. Note that to make sure that $A \subseteq \Sigma^n$ is (isotopically) transitive, it is sufficient to check that the condition of the definition holds for some $\overline{x} \in A$, say $\overline{x} = \overline{0}$, and all $\overline{y}$, or for some $\overline{y}$ and all $\overline{x}$.

Remark. For $|\Sigma| = 2$, the isotopically transitive sets are exactly the affine subspaces of Σ^n, considered as a vector space over the field GF(2).

A set $A \subseteq \Sigma^n$ is called *propelinear* [26] if $\mathrm{Aut}(A)$ includes a regular subgroup, i.e., a subgroup of $\mathrm{Aut}(A)$ of cardinality $|A|$ that acts transitively on A. We call a set $A \subseteq \Sigma^n$ *topolinear* if $\mathrm{Ist}(A)$ includes a regular subgroup G_A.

Let A be a subset of Σ^n. By a *subcode* R of A, we will mean a subset of Σ^m, $m \leq n$, obtained from A by "fixing" $n - m$ coordinates. We explain this by defining a subcode recursively. Define an $(n-1)$-subcode of A as the set $\{(x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_{n-1}) \mid (x_0, \dots, x_{j-1}, a, x_{j+1}, \dots, x_{n-1}) \in A\}$ for some $j \in \{0, \dots, n-1\}$ and $a \in \Sigma$; then, for $m < n$, an m-subcode (or simply a subcode) of A is defined as $((m+1)-1)$-subcode of an $(m+1)$-subcode of A (the set A itself is an n-subcode).

Proposition 1. (1) *The subcodes of an isotopically transitive set are isotopically transitive.*
(2) *The subcodes of a topolinear set are topolinear.*

Proof. (1) Let $A \subseteq \Sigma^n$ be an isotopically transitive set, and let R be an m-subcode of A. Without loss of generality we can assume that

$$R = \{(x_0, \dots, x_{m-1}) \mid (x_0, \dots, x_{m-1}, 0, \dots, 0) \in A\} \ni (0, \dots, 0).$$