Discrete Mathematics 338 (2015) 174–182

Contents lists available at ScienceDirect

Discrete Mathematics

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

Transitive nonpropelinear perfect codes

I.Yu. Mogilnykh *, F.I. Solov'eva

Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia

ARTICLE INFO

Article history:
Received 5 May 2014
Received in revised form 2 September 2014
Accepted 3 November 2014
Available online 29 November 2014

Keywords:
Perfect code
Mollard code
Transitive action
Regular action

ABSTRACT

A code is called transitive if its automorphism group (the isometry group) of the code acts transitively on its codewords. If there is a subgroup of the automorphism group acting regularly on the code, the code is called propelinear. Using Magma software package we establish that among 201 equivalence classes of transitive perfect codes of length 15 from Östergård and Pottonen (2009) there is a unique nonpropelinear code. We solve the existence problem for transitive nonpropelinear perfect codes for any admissible length n, $n \geq 15$. Moreover we prove that there are at least 5 pairwise nonequivalent such codes for any admissible length n, $n \geq 255$.

1. Introduction

We consider codes in the Hamming space F_2^n of binary vectors of length n equipped with the Hamming metric. The Hamming distance $d(x, y)$ is the number of different coordinate positions of vectors x and y. The *code distance* of a code is the minimal value for the Hamming distance of its distinct codewords. The weight $wt(x)$ of a binary vector x of length n is defined as the Hamming distance between x and the all-zero vector 0^n. With a vector x we associate the collection of nonzero coordinates which we denote as $\mathrm{supp}(x)$. A collection C of binary vectors of length n is called a *perfect* (1-perfect) code if any binary vector is at distance 1 from exactly one codeword of C.

Let x be a binary vector, π be a permutation of the coordinate positions of x. Consider the transformation (x, π) acting on a binary vector y by the following rule:

$$(x, \pi)(y) = x + \pi(y),$$

where $\pi(y) = (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)})$. The composition of two automorphisms (x, π), (y, π') is defined as follows:

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi \circ \pi'),$$

where $\circ$ is a composition of permutations π and π'.

The automorphism group of the Hamming space F_2^n is defined as $\mathrm{Aut}(F_2^n) = \{(x, \pi) : x \in C, \pi \in S_n,\ x + \pi(F_2^n) = F_2^n\}$ with the operation composition, here S_n denotes the group of symmetries of order n.

The *automorphism group* $\mathrm{Aut}(C)$ of a code C is a collection of all transformations (x, π) fixing C setwise. In sequel for the sake of simplicity we require the all-zero vector to be always in the code. Then we have the following representation for $\mathrm{Aut}(C)$: $\{(x, \pi), x \in C, \pi \in S_n,\ x + \pi(C) = C\}$.

A code C is called *transitive* if there is a subgroup H of $\mathrm{Aut}(C)$ acting transitively on the codewords of C. If we additionally require that for a pair of distinct codewords x and y, there is a unique element h of H such that $h(x) = y$, then H acting on C is called a *regular group* [17] (sometimes called sharply-transitive) and the code C is called *propelinear* (for the original

* Corresponding author.
E-mail addresses: ivmog@math.nsc.ru (I.Yu. Mogilnykh), sol@math.nsc.ru (F.I. Solov'eva).

http://dx.doi.org/10.1016/j.disc.2014.11.001
0012-365X/

definition see [19]). In this case the order of H is equal to the size of C. If H is acting regularly on C, we can establish a one-to-one correspondence between the codewords of C and the elements of H settled by the rule $x \to h_x$, where h_x is the automorphism sending a certain prefixed codeword (in sequel the all-zero vector) to x. Each regular subgroup $H < \mathrm{Aut}(C)$ naturally induces a group operation on the codewords of C in the following way: $x * y := h_x(y)$, such that the codewords of C form a group with respect to the operation $*$, isomorphic to H: $(C, *) \cong H$. The group is called a *propelinear structure* on C. The notion of propelinearity is important in algebraic and combinatorial coding theory because it provides a general view on linear and additive codes [6].

Two codes C and D are called *equivalent* if there is an automorphism ϕ of the Hamming space such that $\phi(C) = D$. Equivalence or permutational equivalence (i.e. when $\phi = (0^n, \pi)$) reduction is also often considered in problems of classification and existence for codes.

For length 7, there is just one equivalence class of perfect codes, containing the Hamming code (a unique linear perfect code). A significant empirical boost of the study of perfect codes theory was made by Östergård and Pottonen who enumerated all equivalence classes of perfect codes of length 15 (see [15] for the database of the codes). In [16] it was established that 201 of 5983 such classes are transitive.

Papers of Avgustinovich [1,2] provide a graphic point of view on the problem of equivalence of perfect codes by showing that two codes with isomorphic minimum distance graphs are equivalent. In light of this result, transitive and propelinear perfect codes have transitive and Cayley minimum distance graphs respectively [17]. This fact relates the topic of our work to a well known problem of the existence of transitive non-Cayley graphs.

Note the definitions imply that a propelinear code is necessarily transitive, however both topics were studied by several different authors and were developed somewhat independently.

In [21,22] Solov'eva showed that the application of the Vasil'ev, Plotkin and Mollard constructions to transitive codes gives transitive codes. An analogous fact for propelinearity was shown for Vasil'ev codes earlier in [20] and later in [4] for the Plotkin and Mollard constructions. Studying 1-step switching class of the Hamming code, Malyugin [13] found several transitive perfect codes of length 15 (they were shown to be propelinear later in [4]).

The first nonadditive propelinear codes of different ranks were found in [4]. An asymptotically exponential of length class of transitive extended perfect codes constructed in [18] was shown to be propelinear in [5]. In [11] Potapov and Krotov utilized quadratic functions in the Vasil'ev construction to obtain propelinear perfect codes. Because these codes are only of small rank the question of the existence of a big (e.g. exponential of n) class of large rank propelinear perfect codes is still open.

The first transitive code that was shown not to have a propelinear representation was the well known Best code of length 10 and code distance 4 [4]. In the same work the question of the existence of transitive nonpropelinear perfect code was proposed.

The aim of this work is to separate the classes of transitive and propelinear perfect codes for any admissible length n. Using Magma software package, we found that only one of 201 transitive perfect codes of length 15 is nonpropelinear. The code is characterized in the class of transitive codes of length 15 by a unique property of having no triples from the kernel. The extension of this code by parity check gives a propelinear code. Since adding parity check preserves propelinearity of a code, we conclude that all extended perfect codes of length 16 are propelinear. In the paper we present the solution of the problem of the existence of transitive nonpropelinear perfect code for any admissible length n, $n \geq 15$. Moreover we show that there exist nonequivalent transitive nonpropelinear perfect codes for any admissible length more than 127.

The current paper is organized as follows. Definitions and basic theoretical facts are given in the second section. The case $n = 15$ is considered in Section 3, where we give some information on the transitive nonpropelinear code and describe the way the search was carried out. A treatment of nonpropelinearity of the transitive nonpropelinear code C of length 15 is in Section 4 as well as a sufficient condition for an extension of this property for the Mollard codes $M(C, D)$ for the appropriately chosen code D. The condition is essentially a restriction on the orbits of action of the symmetry groups of the Mollard codes. The condition holds if the Mollard code has certain metrical properties which we formulate by means of a numerical invariant $\mu_i(C)$ (the number of the triples from the kernel of the code incident to coordinate i). The main result of the paper is given in Section 5.

2. Preliminaries and notations

2.1. Mollard code

First give a representation for the Mollard construction [14]. Let C and D be two codes of lengths t and m. Consider the coordinate positions of the Mollard code $M(C, D)$ of length $tm + t + m$ to be pairs (i, j) from the set $\{0, \ldots, t\} \times \{0, \ldots, m\} \setminus (0, 0)$.

Let f be an arbitrary function from C to the set of binary vectors Z_2^m of length m and let $p_1(z)$ and $p_2(z)$ be the generalized parity check functions:

$$p_1(z) = \left(\sum_{j=0}^{m} z_{1,j}, \ldots, \sum_{j=0}^{m} z_{t,j} \right),$$