Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 267-272*

Existence of transitive partitions into binary codes

Faina Solov'eva sol@math.nsc.ru
Sobolev Institute of Mathematics, Novosibirsk State University
pr. ac. Koptyuga 4, Novosibirsk 630090, RUSSIA

Abstract. Some methods to construct transitive partitions of the set F_2^n of all binary vectors of length n into binary codes are presented. It is established that for any $n = 2^k - 1, k \geq 3$, there exist transitive partitions of F_2^n into perfect binary transitive codes of length n and distance 3.

1 Introduction

In this paper we continue the investigation of transitive objects beginning in [1-4]. Applying some switching constructions of partitions of the set F_2^n of all binary vectors of length n into perfect binary codes given in [5] (using Vasil'ev construction [6]) and also using Mollard construction [7] we construct transitive partitions of F_2^n into transitive binary codes. The methods permit us to construct transitive partitions of F_2^n into perfect binary codes. Mollard construction allows to get transitive partitions of F_2^n into nonparallel Hamming codes, i.e. the codes, which can not be obtained from each other using a translation by a vector of F_2^n (the method is essentially different from the method to construct partitions of F_2^n into nonparallel Hamming codes, see [8]). Transitive objects play an important role in the coding theory. Transitive codes are close to linear codes by some of their properties. Transitive partitions can be useful to construct new transitive codes.

In [2] several methods to construct transitive binary codes are given, in particular, we got a class of perfect and extended perfect transitive codes for any admissible length $n \geq 31$. The number of nonequivalent perfect transitive codes of length $n = 2^k - 1$ and distance 3 is not less than $\lfloor k/2 \rfloor^2$. An analogous estimate is true for extended perfect transitive codes. Earlier it was known $\lfloor (k+1)/2 \rfloor$ such perfect codes of length $n = 2^k - 1$, see [9]; analogous for the extended case, see [10]. Transitive codes obtained in [2] have different ranks, for example, for $n = 16^l - 1, l > 0$ the ranks vary from $n - \log(n+1)$ (the rank of the Hamming code of length n) to $n - \frac{\log(n+1)}{4}$. In [11] Potapov found the exponential number of transitive extended perfect codes of small rank. Transitive perfect binary codes of length 15 are investigated in [12]. It is easy to see that an extension of any transitive code by the parity checking

give us a transitive code. The converse is not true, in [13] Malyugin has shown that there exists the transitive perfect binary code of length 16 such that any its puncturing perfect code is not transitive. Therefore it is worthwhile to investigate independently the extended case. Many known classes of good codes are transitive, for example, all additive codes, all Z_4-linear codes. In [13] perfect transitive codes of length 15 which belong to the switching class of the Hamming code are enumerated.

Two constructions of partitions of F_2^n into perfect codes were given in [5]. For any admissible $n \geq 15$ one of these construction allowed to get not less than $2^{2^{(n-1)/2}}$ different partitions of F_2^n into perfect binary codes of length $n > 15$, see [14]. In [15] a switching construction of the partitions of F_2^n into pairwise nonequivalent perfect binary codes of length n is presented for any $n = 2^k - 1$, $k \geq 5$.

2 Necessary definitions and notions

Let F_2^n be the set of all binary vectors of length n. Any subset of F_2^n is called a *binary code* of length n. A code C is *perfect binary code correcting single error* (briefly a perfect code) if for any vector $x \in F_2^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$. It is well known that perfect binary codes with code distance 3 exist if and only if $n = 2^k - 1, k > 1$. It is known that every isometry of F_2^n is defined as

$$\mathrm{Aut}(F_2^n) = F_2^n \leftthreetimes S_n = \{(v, \pi) \mid v \in F_2^n, \pi \in S_n\},$$

where $\leftthreetimes$ denotes a semidirect product, S_n is a group of symmetry of order n. The *automorphism group* $\mathrm{Aut}(C)$ of any code C of length n consists of all the isometries of F_2^n that transform the code into itself:

$$\mathrm{Aut}(C) = \{(v, \pi) \mid v + \pi(C) = C\}.$$

A code C is said to be *transitive* if its automorphism group acts transitively on all codewords. *The automorphism group of any family of codes* $\mathcal{P} = \{C_0, C_1, \ldots, C_m\}$, $\mathcal{P} \subseteq F_2^n$, $m \leq n$, is a group of isometries of F_2^n that transform the set $\mathcal{P}$ into itself such that for any $i \in M = \{0, 1, \ldots, m\}$ there exists $j \in M$, $v \in F_2^n$, $\pi \in S_n$ satisfying $v + \pi(C_i) = C_j$. Every such isometry induces a permutation τ on the index set M that permutes the codes in the partition $\mathcal{P}$:

$$\tau(\{C_0, C_1, \ldots, C_m\}) = \{C_{\tau(0)}, C_{\tau(1)}, \ldots, C_{\tau(m)}\},$$

i. e. the automorphism group of the family $\mathcal{P}$ is isomorphic to some subgroup of the group S_{m+1}. A family of codes $\mathcal{P}$ is *transitive* if its automorphism group acts transitively on the elements (the codes) of the family. Two partitions we call *equivalent* if there exists an isometry of the space F_2^n that transforms one partition into another one.

3 Constructions of transitive partitions

In this section we give two constructions of transitive partitions. As the starting point for the case of perfect codes we will take transitive Phelps partitions given in [16], where he classified all partitions of F_2^7 into Hamming codes of length 7. Regardless of the fact that the Hamming code is unique (up to equivalence) there are 11 such nonequivalent partitions. In the list of these partitions we will use one special partition $\mathcal{P}^7 = \{H_0^7, H_1^7, \ldots, H_7^7\}$, here $\mathbf{0}^7 \in H_0^7$ and $\mathbf{0}^7 \in H_i^7 + e_i$ for every $i \in \{1, \ldots, 7\}$, where e_i is the vector of length 7 with only one ith unit coordinate. For the partition it is true $|(H_i^7 + e_i) \cap (H_j^7 + e_j)| = 4$ for any $i \neq j,\ i, j \in \{1, \ldots, 7\}$, i. e. the codes in the partition are pairwise nonparallel. It is true the following known fact

Proposition 1. *The partition $\mathcal{P}^7$ is a transitive partition of F_2^7 into pairwise nonparallel Hamming codes of length 7.*

Construction A. In this section we show how the iterative construction of the partitions from [5] based on Vasil'ev codes from [6] allows to get transitive classes of codes. As a particular case we get transitive partitions of F_2^n into perfect codes for any admissible length.

Theorem 1. *Let $\mathcal{P}^n = \{C_0^n, C_1^n, \ldots, C_m^n\}$ be a transitive family of binary codes of length n; let B^n be any binary linear code of length n with odd code distance such that for any automorphism $(y, \pi) \in Aut(\mathcal{P}^n)$ it holds $\pi \in Sym(B^n)$. Then the family of the codes*
$\mathcal{P}^{2n+1} = \{C_0^{2n+1}, C_1^{2n+1}, \ldots, C_{2m+1}^{2n+1}\}$:
$C_i^{2n+1} = \{(x, |x|, x + y) : x \in B^n, y \in C_i^n\},\ \ C_{m+i+1}^{2n+1} = C_i^{2n+1} + e_{n+1}$,
where $i = 0, 1, \ldots, m$, is transitive.

Codes from Theorem (1) we call Vasil'ev codes.

Taking into account that a translation of any transitive code by any vector of the space is again a transitive code we get from the last theorem and Theorem 1 in [2] the folowing

Corollary 1. *If every code in the family $\mathcal{P}^n$ is transitive than every code of the family $\mathcal{P}^{2n+1}$ from Theorem (1) is transitive.*

It is also true

Corollary 2. *Let $\mathcal{P}^n = \{C_0^n, C_1^n, \ldots, C_n^n\}$ be a transitive partition of F_2^n into perfect binary codes of length n. Then the family of the codes from Theorem (1) is a transitive partition of the space F_2^{2n+1} into perfect binary codes of length $2n + 1$.*

Taking into account the construction (1), Proposition 1 and corollaries 1 and 2 we can iteratively construct transitive partitions of the space F_2^n into transitive perfect codes for any admissible length $n = 2^m - 1, m \geq 3$, i. e. it is true

Theorem 2. *There exist transitive partitions of F_2^n into transitive perfect codes of length n for any $n = 2^m - 1,\ m \geq 3$.*

Corollary 3. *There exist transitive partitions of full-even binary code into extended transitive perfect codes of length n for any $n = 2^m,\ m \geq 4$.*

Construction B. Here we give another method to construct transitive partitions. The method is based on Mollard construction [7] for binary codes. It is known that Mollard construction is a generalization of Vasil'ev construction for the codes correcting single errors. The construction B given below is also a generalization of the construction A. As contrasted with the construction B the construction A gives transitive partitions into codes with big code distances. In turn the construction B allows to get partitions of F_2^n into nonparallel Hamming codes.

Further we will use the following particular case of Mollard construction [7] for binary codes. Let P^t and C^m be any two binary codes of lengths t and m respectively with code distances not less than 3. Let

$$x = (x_{11}, x_{12}, \ldots, x_{1m}, x_{21}, \ldots, x_{2m}, \ldots, x_{t1}, \ldots, x_{tm}) \in F_2^{tm}.$$

The generalized parity-check functions $p_1(x)$ and $p_2(x)$ are defined by $p_1(x) = (\sigma_1, \sigma_2, \ldots, \sigma_t) \in F_2^t$, $p_2(x) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in F_2^m$, where $\sigma_i = \sum_{j=1}^{m} x_{ij}$ and $\sigma'_j = \sum_{i=1}^{t} x_{ij}$. The set

$$C^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in F_2^{tm}, y \in P^t, z \in C^m\}$$

is a binary Mollard code of length $n = tm + t + m$ and code distance 3, see [7]. It is true the following

Theorem 3. *Let $\mathcal{P}^t = \{C_0^t, C_1^t, \ldots, C_t^t\}$ and $\mathcal{P}^m = \{D_0^m, D_1^m, \ldots, D_m^m\}$ be any transitive families of the codes of length t and m respectively correcting single errors. Then the family of the codes*

$$\mathcal{P}^n = \{C_{00}^n, C_{01}^n, \ldots, C_{tm}^n\}$$

is transitive class of codes of length $n = tm + t + m$, correcting single errors, where

$$C_{ij}^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in F_2^{tm}, y \in C_i^t, z \in D_j^m\} \qquad (1)$$

is Mollard code, $i = 0, 1, \ldots, t;\ j = 0, 1, \ldots, m$.

From this theorem and Theorem 3 of the paper [2] we get

Corollary 4. *Let $\mathcal{P}^t$ and $\mathcal{P}^m$ be any transitive partitions of F_2^t and F_2^m into perfect transitive codes of length $t = 2^r - 1$, $r \geq 3$, and $m = 2^l - 1$, $l \geq 3$, respectively. Then the construction (1) gives a transitive partition of F_2^n into perfect binary transitive codes of length $n = tm + t + m$.*

Remark. It should be noted that Theorem 3 is true to get transitive partitions into nontransitive codes. For $t = 1$ Corollary 2 can be obtain from Corollary 4 as a particular case.

Theorem 3 and Proposition 1 allow us to construct by induction transitive partitions of F_2^n into pairwise nonparallel Hamming codes.

Theorem 4. *Let $\mathcal{P}^t = \{H_0^t, H_1^t, \ldots, H_t^t\}$ and $\mathcal{P}^m = \{H_0^m, H_1^m, \ldots, H_m^m\}$ be any transitive partitions into pairwise nonparallel Hamming codes, $t = 2^r - 1$, $r \geq 3$, and $m = 2^l - 1$, $l \geq 3$. Then the family of the codes*

$$H_{ij}^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in F_2^{tm}, y \in H_i^t, z \in H_j^m\}, \qquad (2)$$

$i = 0, 1, \ldots, t$, $j = 0, 1, \ldots, m$, is a transitive partition of F_2^n into pairwise nonparallel Hamming codes of length $n = tm + t + m$.

Denote by $\bar{H}^n$ the code containing all-zero vector obtained from the code H^n of length n by a switch on some vector from F_2^n.

Remark. It holds from Theorem 4 that if we know the size of the sets $\bar{H}_i^t \cap \bar{H}_k^t$ and $\bar{H}_j^m \cap \bar{H}_s^m$ for any $i, k \in \{0, 1, \ldots, t, \}$ and $j, s \in \{0, 1, \ldots, m\}$ we can easily calculate the size of the intersection codes $\bar{H}_{ij}^n$ and $\bar{H}_{ks}^n$.

References

[1] F. I. Solov'eva, On transitive codes, it Proc. Intern. Workshop Discr. Anal. Oper. Res., Novosibirsk, Russia. 2004, 99.

[2] F. I. Solov'eva, On construction of transitive codes, *Probl. Inform. Transm.* 41, 2005, 204-211.

[3] F. I. Solov'eva, On $\mathbb{Z}_4$-linear codes with parameters of Reed-Muller codes, *Probl. Inform. Transm.* 43, 2007, 26-32.

[4] J. Pujol, J. Rifa, F. I. Solov'eva, Construction of Z_4-linear Reed-Muller codes, *IEEE Trans. Inform. Theory* submitted.

[5] F. I. Solov'eva, On binary nongroup codes, *Methody Discr. Analiza* 37, 1981, 65-76 (in Russian).

[6] Yu. L. Vasil'ev, On nongroup close-packed codes, *Probl. der Kybern.* 8, 1962, 92-95.

[7] M. Mollard, A generalized parity function and its use in the construction of perfect codes, *SIAM J. Alg. Discr. Math.* 7, 1986, 113-115.

[8] O. Heden, F. I. Solov'eva, On partitions of n-cube into nonparallel Hamming codes, submitted.

[9] J. Borges, J. K. Rifa, A characterization of 1-perfect additive codes, *IEEE Trans. Inform. Theory* 45, 1999, 1688-1697.

[10] D. S. Krotov, Z_4-linear perfect codes, *Discr. Anal. Oper. Res.* Ser. 1., 7, 2000, 78-90 (in Russian).

[11] V. N. Potapov, On lower bound on the number of transitive perfect codes, *Discr. Anal. Oper. Res.* Ser. 1, 13, 2000, 49-59 (in Russian).

[12] S. A. Malyugin, Transitive perfect codes of length 15, *Proc. Intern. Workshop Discr. Anal. Oper. Res.*, Novosibirsk, Russia, 2004, 96.

[13] S. A. Malyugin, On equivalent classes of perfect binary codes of length 15, Preprint 138. Novosibirsk: Inst. of Mathematics of SB RAS, 2004, 34.

[14] F. I. Solov'eva, On Perfect Codes and Related Topics, Com^{2}Mac Lecture Note Series 13, Pohang 2004.

[15] S. V. Avgustinovich, O. Heden, F. I. Solov'eva, On partitions of n-cube into nonequivalent perfect codes, *Probl. Inform. Transm.* 43, 2007, 45-50.

[16] K. T. Phelps, An enumeration of 1-perfect binary codes of length 15, *Australas. J. Comb.* 21, 2000, 287-298.