Separability of homogeneous perfect codes from transitive [1]

Ivan Yu. Mogilnykh, Faina I. Solov'eva ivmog,sol@math.nsc.ru
Sobolev Institute of Mathematics SB RAS

Abstract. It is proved that there exist homogeneous perfect binary codes that are not transitive for any admissible code length more than 7. Therefore taking into account the previous known results it is established a hierarchical measure of linearity of binary codes: a class of linear codes is strictly contained in the class of propelinear codes, which is strictly contained in the class of all transitive codes, and the last class is strictly included in the class of homogeneous codes. We derive a transitivity criterion for perfect binary codes of rank greater by one than the rank of the Hamming code of the same length.

1 Introduction

Propelinear and transitive codes are very close to linear by some properties, especially by the structure of the automorphism groups. The question on the existence of transitive nonpropelinear codes was posed by Pujol, Rifa and Solov'eva in 2006. When the classification of perfect binary codes of length 15 was obtained, all transitive and homogeneous perfect binary codes of length 15 were enumerated, see [1, 2]. The problem of the existence of infinite series of perfect homogeneous nontransitive codes was then naturally posed. The problem of the existence of transitive nonpropelinear is solved in [3], where it is proved that the well known Best code of length 10 and code distance 4 is transitive nonpropelinear. In [4] it is shown that among 201 pairwise nonequivalent transitive perfect binary codes of length 15 there exists just one nonpropelinear perfect binary code. The infinite series of transitive nonpropelinear perfect binary codes is proposed in [4, 5]:

Theorem 1. *For any $n \geq 15$ there exist transitive nonpropelinear perfect binary codes of length n.*

Here we give a positive answer on the existence of homogeneous nontransitive perfect binary codes. It is known that there exist Z_4-linear codes which are not linear. Therefore the following holds:

$$\boldsymbol{L} \subset \boldsymbol{Prl} \subset \boldsymbol{Tr} \subset \boldsymbol{Hom},$$

where $\boldsymbol{L}$ is the class of linear codes, $\boldsymbol{Prl}$ is the class of propelinear codes, $\boldsymbol{Tr}$ is the class of transitive codes; $\boldsymbol{Hom}$ is the class of homogeneous codes.

[1] The work is supported by the Grant the Russian Scientific Fund 14-11-00555.

2 Preliminaries and notations

By F^n we denote n-dimensional metric space of all binary vectors of length n with respect to the Hamming metric. A code $C \subset F^n$ is called a *perfect binary code correcting single error* (in what follows a *perfect code*) of length n if for any vector $x \in F^n$ there exists a unique vector $y \in C$ at Hamming distance not more than one from x. In sequel for the sake of simplicity we require the all-zero vector 0^n to be always in a code. It is well known that for the automorphism group $\mathrm{Aut}(F^n)$ of F^n it is true

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

here $\leftthreetimes$ is the semidirect product and S_n is the symmetry group of all permutations of n coordinate positions of vectors in F^n. The setwise stabilizer of a code C in $\mathrm{Aut}(F^n)$ is called the *automorphism* $\mathrm{Aut}(C)$ of the code C, i.e.

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

The set $\mathrm{Sym}(C) = \{\pi \in S_n \mid \pi(C) = C\}$ is called the *symmetry group* of the code C.

A code C is called *transitive* if there is a subgroup $H < \mathrm{Aut}(C)$, 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 the subgroup H such that $h(x) = y$, then H acting on C is called a *regular group* [6] (sometimes sharply-transitive) and the code C is called *propelinear* (for the original definition see [7]). It is clear that in this case the order of H is equal to the size of C.

Recall that a *Steiner triple system* (briefly STS) is a collection of blocks (subsets) of size 3 of an n-element set such that any unordered pair of distinct elements is exactly in one block. The set of codewords of weight 3 of a perfect code C that contains the all-zero word is a Steiner triple system, which we denote by $\mathrm{STS}(C)$. The set $supp(x) = \{i : x_i = 1\}$ is called the *support* of the vector x. The set $\{supp(x + y) : x \in C, d(x, y) = 3\}$ for a codeword $y \in C$ we denote by $STS(C, y)$.

A code C is called *homogeneous* if for any codeword $y \in C$ the system $\mathrm{STS}(C, y)$ is isomorphic to $\mathrm{STS}(C, 0^n)$, i.e. there exists a permutation $\pi \in S_n$ such that $\pi(STS(C, y)) = STS(C, 0^n)$. It is easy to see that any transitive code is homogeneous.

3 Infinite series of homogeneous nontransitive codes

Let us consider additional definitions. The dimension of the linear span of a code C is called its *rank*. Define the *translator* *Tr*(C) of a code C:

$$\mathrm{Tr}(C) = \{y \in C \mid \exists \pi \in S_n : (y, \pi) \in \mathrm{Aut}(C)\}.$$

The linear span over codewords of weight 3 of a code C of length n containing i, $i \in \{1, 2, \ldots, n\}$ is called the *linear i-component* (in what follows *i-component*) and denoted R_i^n. If C is the Hamming code of length n than R_i^n is its linear subcode.

Let C be any perfect code of length n, $n = 2^k - 1$, $\lambda : C \to \{0, 1\}$ be any function satisfying $\lambda(0^n) = 0$. Consider the codes $C_\lambda = \{(y, \lambda(y), 0^n) \mid y \in C\}$ and $R_{n+1}^{2n+1} = \{(x, |x|, x) \mid x \in F^n\}$, where $|x| = x_1 + \ldots + x_n (\mathrm{mod}\, 2)$. Both codes have length $2n + 1$ and the code R_{n+1}^{2n+1} is an $(n + 1)$-component. Using the codes C_λ and R_{n+1}^{2n+1} we define a perfect binary code of length $2n + 1$ called the *Vasil'ev code* [8] as follows:

$$V_C^\lambda = C_\lambda + R_n^{2n+1} = \{(x + y, |x| + \lambda(y), x) \mid x \in F^n, y \in C\}. \qquad (1)$$

Next theorem gives us a transitivity criterion for perfect binary codes of rank greater by one than the rank of the Hamming code of the same length (it is known that the class of such codes are Vasil'ev codes (1) constructed from the Hamming code with any nonlinear function λ).

Theorem 2. *Let λ be a nonlinear Boolean function on the Hamming code H of length n.Then the vector $(y' + x, \lambda(y') + |x|, x)$ belongs to $Tr(V_H^\lambda)$ of the Vasil'ev code V_H^λ of length $2n+1$ for any $x \in F^n$ if and only if there exist $\pi_{y'} \in Sym(H)$ and $u \in F^n$ such that for all $y \in H$ we have*

$$\lambda(y') + \lambda(y) + \lambda(y' + \pi_{y'}(y)) = u \cdot y, \qquad (2)$$

where $u \cdot y$ is a scalar product of the vectors u and y in F^n.

We note that the authors of [9] suggested that transitive codes of rank $n - log(n + 1) + 1$ should be sought for in the class of Vasil'ev codes with a function satisfying an equality equivalent to (2) but gave no explanation for this. Also, validity of equality (2) with $\pi_{y'} = id$ for all y, y' is equivalent to the definition of the quadratic function considered in the same paper.

We investigated all perfect codes of length 15 of rank 12. It turned out that among them only two perfect codes are homogeneous nontransitive. These are the codes denoted by $V22^1$ and $V3^11$ according to the classification of Malyugin [10].

Let H be the Hamming code of length 7 generated by the vectors

$$\{1, 2, 3\}, \ \{1, 4, 5\}, \ \{1, 6, 7\}, \ \{2, 4, 6\}.$$

The code $V22^1$ is the Vasil'ev code V_H^λ such that

$$\lambda(0^7) = \lambda(\{1, 6, 7\}) = \lambda(\{1, 3, 5, 7\}) = \lambda(1^7) = 0,$$

for other codewords in H the value of λ is 1. Here 1^7 is the all-one vector of length 7.

The code $V3^11$ is the Vasil'ev code V_H^λ where

$$\lambda(0^7) = \lambda(\{1,6,7\}) = \lambda(\{2,4,6\}) = \lambda(\{4,5,6,7\}) = 0,$$

and λ is equal to 1 for other codewords from H.

Using Theorem 2 we prove

Lemma. *The codes $V22^1$ and $V3^11$ are homogeneous nontransitive.*

Exploiting the Vasil'ev's construction we obtain

Theorem 3. *If C is any homogeneous perfect code than the Vasil'ev code V_C^λ with $\lambda \equiv 0$ is homogeneous.*

In order to separate the class of homogeneous perfect codes from transitive for any lengthy $n > 15$ we iteratively apply appropriate times the Vasil'ev's construction with the Boolean function $\lambda \equiv 0$ to the gomogenious nontransitive Vasil'ev codes $V22^1$ and $V3^11$ of length 15. We would emphasize that $Tr(V_C^\lambda)$ the Vasil'ev code V_C^λ of length n obtained from the perfect code C with $\lambda \equiv 0$ preserves the properties of $Tr(C)$. As the result we get

Theorem 4. *For any $n \geq 15$ there exist perfect binary homogeneous nontransitive codes for any admissible length $n > 7$.*

Remark. Perfect binary homogeneous nontransitive codes could be constructed by the Mollard's construction [11], but technically it would be much more complicated than exploiting the Vasil'ev's construction. All the details and proofs can be found in [12].

References

[1] P. R. J. Östergård, O. Pottonen, The perfect binary one-error-correcting codes of length 15: Part I-Classification, IEEE Trans. Inform. Theory. 2009. V. 55. 4657–4660.

[2] P. R. J. Östergård, K. T. Phelps, O. Pottonen, The perfect binary one-error-correcting codes of length 15: Part II-properties, IEEE Trans. Inform. Theory. 2010. V. 56. P. 2571–2582.

[3] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, Structural properties of binary propelinear codes, Advances in Math. of Commun. 2012. V. 6. N 3. P. 329–346.

[4] I. Yu. Mogilnykh, F. I. Solov'eva, Existence of transitive nonpropelinear perfect codes, Discrete Math. 2015. V. 338. P. 174–182.

[5] I. Yu. Mogilnykh, F. I. Solov'eva, Existence of transitive nonpropelinear perfect codes, in *Proc. Int. Workshop on Alg. and Combin. Coding Theory, Svetlogorsk (Kaliningrad region), Russia*, 2014, P. 247–252.

[6] K. T. Phelps, J. Rifà, On binary 1-perfect additive codes: some structural properties, IEEE Trans. Inform. Theory. 2002. V. 48. P. 2587–2592.

[7] J. Rifà, J. M. Basart, L. Huguet, On completely regular propelinear codes, Proc. 6th Int. Conference, AAECC-6. LNCS. 1989. V. 357. P. 341–355.

[8] Y. L. Vasil'ev, On nongroup close-packed codes, Problems of Cybernetics. 1962. V. 8. P. 375–378.

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

[10] S. A. Malyugin, On equivalent classes of perfect binary codes of length 15, Preprint N 138. – Novosibirsk: Sobolev Institute of Mathematics SB RAS. 2004. P. 34.

[11] M. Mollard, A generalized parity function and its use in the construction of perfect codes, SIAM J. Alg. Disc. Meth. 1986. V. 7. N 1. P. 113–115.

[12] I. Yu. Mogilnykh, F. I. Solov'eva, On separability of gomogenious class of perfect codes from transitive, Probl. Inform. Transm. V. 51. N 2. 2015. P. 139–147.