Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 247–252*

Existence of transitive nonpropelinear perfect codes[1]

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

Abstract. Using Magma software package we established that among 201 equivalence classes of transitive perfect codes of length 15 from [8] 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 pairwise nonequivalent such codes for any admissible length n, $n \geq 255$.

1 Introduction

Consider a transformation (x, π), where x is a binary vector of length n, and π is a permutation on coordinate positions acting on a binary vector y of length n by the following rule:

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

where $\pi(y) = (y_{\pi(1)}, \ldots, y_{\pi(n)})$.

The *automorphism group* $\mathrm{Aut}(C)$ of a binary code C of length n equipped with the Hamming metric is a collection of all transformations (x, π) fixing C setwise with respect to composition

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

In sequel for the sake of simplicity we require the all-zero vector $\mathbf{0}^n$ to be always in a code. Then we have the following representation $\mathrm{Aut}(C) = \{(x, \pi), x \in C, \pi \in S_n,\ x + \pi(C) = C\}$, here S_n denotes the group of symmetries of order n.

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* [10] (sometimes sharply-transitive) and the code C is called *propelinear* (for the original definition see [11]). 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

[1]The first author was supported by the Grants RFBR 12-01-00448 and 13-01-00463. The second author was supported by the Grant RFBR 12-01-00631-a. Both authors are supported by the Grant NSh-1939.2014.1 of President of Russia for Leading Scientific Schools.

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 $(C, *)$ 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. By the definitions a propelinear code is transitive, however both topics were studied by several different authors and were developed somewhat independently.

In [13] it was shown that the applications of the Vasil'ev, Plotkin and Mollard constructions to transitive codes give transitive codes. An analogous fact for propelinearity was proven for Vasil'ev codes earlier in [12] and later in [3] for the Plotkin and Mollard constructions. Studying 1-step switching class of the Hamming code, Malyugin in 2004 found several transitive perfect codes of length 15 (they were shown to be propelinear later in [3]). The first nonadditive propelinear codes of different ranks were found in [3]. An asymptotically exponential of length class of transitive extended perfect codes constructed in [9] were shown to be propelinear in [4]. This class was later expanded in [6]. The well known Best code of length 10 and code distance 4 was shown in [3] to be the first transitive nonpropelinear code. In the same work the question of the existence of transitive nonpropelinear perfect code was proposed.

2 Preliminaries and notations

For the definition of the Mollard code see [7]. A *Steiner triple system* is a set of n points together with a collection of blocks (subsets) of size 3 of points, such that any unordered pair of distinct points is exactly in one block. The set of codewords of weight 3 in a perfect code C, that contains the all-zero codeword defines a Steiner triple system, which we denote $\mathrm{STS}(C)$.

The *symmetry group* $\mathrm{Sym}(C)$ of a code C (sometimes being called permutational automorphism group or full automorphism group) is the collection of permutations on n elements with the operation composition, preserving the code setwise: $\mathrm{Sym}(C) = \{\pi \in S_n : \pi(C) = C\}$.

The *group of rotations*, see [1], [3], $\mathcal{R}(C)$ consists of all permutations with the operation composition, that could be embedded into the permutational part of an automorphism of C, i. e. $\mathcal{R}(C) = \{\pi \in S_n : \text{there exists } x \in C \text{ such that } (x, \pi) \in \mathrm{Aut}(C)\}$. Obviously, the symmetry group is a subgroup of the group of rotations and $\mathcal{R}(C)$ stabilizes the dual of the code and its kernel [10], [3]: $\mathcal{R}(C) \leq \mathrm{Sym}(C^{\perp})$ and

$$\mathrm{Sym}(C) \leq \mathcal{R}(C) \leq \mathrm{Sym}(\mathrm{Ker}(C)), \tag{1}$$

Finally, the constant weight subcode of the code is stabilized by symmetries of the code, so in case of weight three we have

$$\mathrm{Sym}(C) \leq \mathrm{Aut}(\mathrm{STS}(C)). \tag{2}$$

Denote by $\mathcal{R}_x(C)$ the set of elements of $\mathcal{R}(C)$ associated with a codeword x of C: $\mathcal{R}_x(C) = \{\pi : (x, \pi) \in \mathrm{Aut}(C)\}$. It is easy to see that the introduced sets are exactly cosets of $\mathcal{R}(C)$ by $\mathrm{Sym}(C)$ [3], i. e. $\mathcal{R}_x(C) = \pi\mathrm{Sym}(C)$, for any $\pi \in \mathcal{R}_x(C)$.

Lemma 1. *[13] [3] If C and D are transitive (propelinear) codes, then $M(C, D)$ is transitive (propelinear respectively).*

3 Transitive nonpropelinear perfect codes

We say that a codeword x of C has *the incorrect inverse*, if any element of $\mathcal{R}_x(C)$ is of order more than 2 and stabilizes $\mathrm{supp}(x)$.

Proposition 1. *A code C containing a codeword x with the incorrect inverse is not propelinear.*

Proof. Suppose H is a regular subgroup of the automorphism group of a code C of length n. Let $h_x = (x, \pi_x) \in H$ be the automorphism that is attached to x, i.e h_x maps $\mathbf{0}^n$ into x. Then $h_x^{-1} = (\pi_x^{-1}(x), \pi_x^{-1}) \in H$ maps $\mathbf{0}^n$ to $\pi_x^{-1}(x)$. Because H is a regular group, there is a unique element of H sending $\mathbf{0}^n$ to x. However we have that $\pi_x^{-1}(x) = x$ and therefore the automorphisms h_x and h_x^{-1} must be equal, because they both map $\mathbf{0}^n$ to x. So we get that π_x^2 is the identity permutation for some $\pi_x \in \mathcal{R}_x(C)$, which contradicts the fact that x is a codeword with the incorrect inverse. □

Corollary 1. *If C is a code containing a codeword x with the incorrect inverse, then* $\mathrm{Sym}(C)$ *is of even order and stabilizes supp(x) setwise.*

Denote by $I(C)$ the following set, associated with a code C: $I(C) = \{i : x_i = 0 \text{ for all } x \in C^{\perp}\}$, where $C^{\perp}$ is the dual code to the code C.

We make use of the empirical fact, established by Magma software package [2]:

Proposition 2. *The code C number 4918 in classification of [8] is transitive and contains a codeword x, supp$(x) = \{2, 3, 4\} \subset I(C)$ with the incorrect inverse.*

Let C be a code of length n, then for any $i \in \{1, \dots, n\}$ define $\mu_i(C)$ to be the number of triples from $\mathrm{Ker}(C)$ that contain i. From (1), (2) we see that $\mu_i(C) \neq \mu_j(C)$ implies that the coordinates i and j are in different orbits of the group action of $\mathrm{Sym}(C)$ on the coordinate positions $\{1, \dots, n\}$. We use the iterative structure of $\mathrm{STS}(M(C, D))$ and obtain formulas for those in $M(C, D)$ from $\mu_r(C)$ and $\mu_s(D)$.

Lemma 2. *Let $M(C,D)$ be a Mollard code obtained from perfect codes C and D of length t and m respectively. Then*

$$\mu_{(r,0)}(M(C,D)) = \mu_r(C)(m+1) + m;$$

$$\mu_{(0,s)}(M(C,D)) = \mu_s(D)(t+1) + t;$$

$$\mu_{(r,s)}(M(C,D)) = 1 + 2(\mu_s(D) + \mu_r(C) + \mu_r(C)\mu_s(D)).$$

Let $\mu(C)$ be the multiset collection of $\mu_i(C)$ denoted by $\mu_{k_1}^{i_1}\mu_{k_2}^{i_2}\ldots\mu_{k_p}^{i_p}$, $p \leq n$ (here the integer μ_{k_l} appears i_l, $i_l \neq 0$ times, $1 \leq l \leq p$) for any coordinate i of C. Then $\mu(C)$ could be considered as a code invariant.

Table 1: Invariants of some transitive perfect codes of length 15

Code number in [8]	Dim Rank(C)	(Ker(C))	|Sym(C)|	$\mu(C)$	|Aut(STS(C))|	Rank (STS(C))
51	13	7	8	$1^{13}3^1 5^1$	8	13
694	13	8	32	$1^8 3^5 5^2$	32	13
724	13	8	32	$1^{13}3^1 5^1$	96	13
771	13	8	96	$1^{12}3^3$	288	13
4918	14	6	4	$\mathbf{0}^{15}$	4	14

Corollary 2. *Let $\mu(C) \neq \mu(C')$ be true for perfect codes C and C'. Then the codes $M(C,D)$ and $M(C',D)$ are noneqivalent.*

Now we consider several conditions on the initial codes in order for Mollard construction to preserve the incorrect inversion property. The constructed codes $M(C,D)$ have the symmetry group fixing subcode D^2 and therefore by result [7] inherit the incorrect inverse property from C.

For a codeword x from C denote by x^1 a codeword in $M(C,D)$ such that $(x^1_{1,0},\ldots,x^1_{t,0}) = x \in C$ with zeros in all positions from $\{0,\ldots,t\}\times\{1,\ldots,m\}$. Note that $M(C,D)$ contains the code C as the subcode $C^1 = \{x^1 : x \in C\}$.

Theorem 1. *Let C be a perfect code of length t with a codeword x with the incorrect inverse. If we have*

$$\mathrm{supp}(x) \subseteq I(C), \tag{3}$$

$$\mu_r(C) < (t-1)/2 \text{ for any } r \in \{1,\ldots,t\}, \tag{4}$$

then x^1 is a codeword with the incorrect inverse in $M(C,H)$. If we have

$$\mu_r(C) = 0 \text{ for any } r \in \{1, \ldots, t\}, \tag{5}$$

$$0 < \mu_s(D) < \frac{m-1}{2} \text{ for any } s \in \{1, \ldots, m\}, m \leq t, \tag{6}$$

then x^1 *is a codeword with the incorrect inverse in* $M(C, D)$*.*

If (3), (5) hold for C *and (6) holds for* D*, then* x^1 *is a codeword with the incorrect inverse in* $M(M(C, D), H)$ *for any Hamming code* H*.*

Theorem 2. *For any* $n \geq 15$ *there is at least one transitive nonpropelinear perfect code of length* n*. For any* $n \geq 255$ *there are at least 5 inequivalent transitive nonpropelinear perfect codes of length* n*.*

Proof. If C is a unique transitive nonpropelinear perfect code of length 15, then it fulfills the incorrect inversion property for x such that $\mathrm{supp}(x) = \{2, 3, 4\}$, see Proposition 2. Show that $M(C, H)$ satisfies the condition of Theorem 1 for any Hamming code H of length at least 1. According to Proposition 2, $supp(x) = \{2, 3, 4\} \subset I(C)$, therefore (3) holds. Because there are no triples of C in $\mathrm{Ker}(C)$, the condition (4) is true. The search showed that there are just 4 of 200 propelinear perfect codes D of length 15 satisfying the condition (6): $0 < \mu_i(D) < 7$. These codes have numbers 51, 694, 724, 771 in [8], see also Table 1 above. If D is any such code then the code $M(M(C, D), H)$ is nonpropelinear.

These four codes and the code $M(C, H')$ give five infinite series of nonpropelinear codes. From Table 1 we have that the triple ($Rank(D)$, $Dim(\mathrm{Ker}(D))$, $\mu(D)$) is a complete set of invariants determining inequivalence of the codes D with numbers 51, 694, 724, 771. Since the rank of $M(C, D)$ is a sum of the ranks of C and D, we see that the code $M(C, H')$ has a smaller rank then any code of the type $M(M(C, D), H)$ of the same length. Moreover by this rank property, taking into account that $Dim(\mathrm{Ker}(M(C, D))) = Dim(\mathrm{Ker}(C)) + Dim(\mathrm{Ker}(D)) + tm$ for any code $M(C, D)$ and Corollary 2 the triple of invariants remains to be complete for the series of codes of the type $M(M(C, D), H)$. □

References

[1] S. V. Avgustinovich, F. I. Solov'eva, O. Heden, On the structure of symmetry groups of Vasil'ev codes, Probl. of Inform. Transm., **5**, 42–49, 2005.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput. **24**, 235–265, 1997.

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

[4] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, On the number of nonequivalent propelinear extended perfect codes, The Electronic J. of Combinatorics, **20** (2), 37–50, 2013.

[5] J. Doyen, X. Hubaut, M. Vandensavel, Ranks of incidence matrices of Steiner triple systems, Mathematische Zeitschrift, **163** (3), 251–259, 1978.

[6] D. S. Krotov, V. N. Potapov, Propelinear 1-perfect codes from quadratic functions, IEEE Trans. on Inform. Theory, **60**, 2065–2068, 2014.

[7] I. Yu. Mogilnykh, F. I. Solov'eva, On the structure of symmetry groups of Mollard codes, in *Proc. Int. Workshop on Alg. and Combin. Coding Theory, Svetlogorsk (Kaliningrad region), Russia*, 2014, ...–....

[8] P. R. J. Östergård, O. Pottonen, The perfect binary one-error-correcting codes of length 15: Part I – Classification. *ArXiv*, http://arxiv.org/src/0806.2513v3/anc/perfect15.

[9] V.N. Potapov, A lower bound for the number of transitive perfect codes. J. of Appl. and Industrial Math. **1** (3), 373–379, 2007.

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

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

[12] J. Rifà, J. Pujol, J. Borges, 1-Perfect Uniform and Distance Invariant Partitions. Appl. Algebra in Engeneering, Commun. and Computing, **11**, 297–311, 2001.

[13] F. I. Solov'eva, On the construction of transitive codes, Probl. of Inform. Transm., **41** (3), 204–211, 2005.