Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 240–246*

Linear coordinates and symmetry groups of perfect Mollard codes [1]

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

Abstract. For a pair of given binary perfect codes C and D of lengths t and m, the Mollard construction outputs a perfect code $M(C,D)$ of length $tm+t+m$, having subcodes C^1 and D^2, that are obtained from codewords of C and D respectively by adding appropriate number of zeros. In this work we obtain a generalization of a result for symmetry groups of Vasil'ev codes [1] and find the group $Stab_{D^2}Sym(M(C,D))$. The result is preceded by and partially relies on the discussion of "linearity" of coordinate positions (points) in a nonlinear perfect code (non-projective Steiner triple system respectively).

1 Mollard code

Let C and D be two binary codes of lengths t and m respectively. We give a representation for the Mollard construction for binary codes [4]. Consider the coordinate positions of the Mollard code $M(C,D)$ of length $tm+t+m$ to be pairs (r,s) 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 $\mathbf{F}_2^m$ of length m and $p_1(z)$ and $p_2(z)$ be the generalized parity check functions:

$$p_1(z) = (\sum_{s=0,\ldots,m} z_{1,s},\ldots,\sum_{s=0,\ldots,m} z_{t,s}),$$

$$p_2(z) = (\sum_{r=0,\ldots,t} z_{r,1},\ldots,\sum_{r=0,\ldots,t} z_{r,m}).$$

The binary code $M(C,D)=\{z\in\mathbf{F}_2^{tm+t+m} : p_1(z)\in C, p_2(z)\in f(p_1(z))+D\}$ is called the Mollard code. In the case when C and D are perfect, the code $M(C,D)$ is perfect. Throughout the paper we consider the case when f is the zero function, C and D are perfect codes, containing the all-zero words.

Recall that a *Steiner triple system* 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 in a perfect code C, that contains the all-zero word is a Steiner triple system, which we denote STS(C). With a Steiner triple system S we associate a *Steiner quasigroup* $(P(S),\cdot)$ to be the

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

point set $P(S)$ of S with a binary operation $\cdot$ such that: $i \cdot j = k$, if (i, j, k) is a triple of S and $i \cdot i = i$. A Steiner loop $(0 \cup P(S), \star)$ with a binary operation $\star$ fulfills properties $i \star j = k$, if (i, j, k) is a triple of S, $i \star i = 0$ and $i \star 0 = i$.

The Steiner triple system of the Mollard code $M(C, D)$ can be defined as follows

$$\mathrm{STS}(M(C,D)) = \bigcup_{k,p \in \{0,3\}} T_{kp}, \text{ where}$$

$$T_{00} = \{((r,0),(r,s),(0,s)) : r \in \{1,\dots,t\}, s \in \{1,\dots,m\}\};$$

$$T_{33} = \{((r,s),(r',s'),(r'',s'')) : (r,r',r'') \in \mathrm{STS}(C), (s,s',s'') \in \mathrm{STS}(D)\};$$

$$T_{30} = \{((r,0),(r',s),(r'',s)) : \{r,r',r''\} \in \mathrm{STS}(C), s \in \{0,\dots,m\}\};$$

$$T_{03} = \{((r,s),(r,s'),(0,s'')) : \{s,s',s''\} \in \mathrm{STS}(D), r \in \{0,\dots,t\}\}.$$

We see that for codes S and S' that are vector representations of Steiner triple systems S and S' of orders t and m with all-zero words the code $M(0^t \cup S, 0^m \cup S')$ is the vector representation of Steiner triple system of order $tm+t+m$ with all-zero word.

For a codeword x from C and y from D denote by x^1 (y^2 respectively) a codeword in $M(C,D)$ such that $(x^1_{1,0},\dots,\ x^1_{t,0}) = x \in C$ $((y^2_{0,1},\dots,y^2_{0,m})=$ $y \in D$ respectively) with zeros in all positions from $\{0,\dots,t\} \times \{1,\dots,m\}$ ($\{1,\dots,t\} \times \{0,\dots,m\}$ respectively). Note that $M(C,D)$ contains the codes C and D as the subcodes $C^1 = \{x^1 : x \in C\}$ and $D^2 = \{y^2 : y \in D\}$ respectively.

Recall that *the dual* $C^\perp$ of a code C is a collection of all binary vectors x such that $\sum_{i=1,\dots,n} x_i c_i = 0 (\mathrm{mod}\ 2)$ for any codeword c of C. For perfect codes C and D, the dual of the Mollard code $M(C,D)$ can be described in the following way:

$$(M(C,D))^\perp = \{z : p_1(z) \in C^\perp, p_2(z) \in D^\perp\}.$$

2 Symmetry group of a perfect code

The *symmetry group* $\mathrm{Sym}(C)$ of a code C (sometimes being called permutational automorphism group or full automorphism group [5]) is the subgroup of permutations on n elements preserving the code setwise:

$$\mathrm{Sym}(C) = \{\pi \in S_n : \pi(C) = C\},$$

where

$$\pi(x) = (x_{\pi(1)},\dots,x_{\pi(n)})$$

with respect to the composition $\circ$ of permutations.

It is well-known that the symmetry group stabilizes the dual of the code, its kernel [8] and Steiner triple system:

$$\mathrm{Sym}(C) \leq \mathrm{Sym}(\mathrm{Ker}(C)),\ \mathrm{Sym}(C) \leq \mathrm{Sym}(C^{\perp}),\ \mathrm{Sym}(C) \leq \mathrm{Aut}(\mathrm{STS}(C)).$$

Now consider the Mollard code $M(C, D)$. For a permutation π on the coordinate positions of the code C (the code D), denote by $Dub_1(\pi)$ ($Dub_2(\pi)$ respectively) a permutation of coordinates of $M(C, D)$ such that

$$Dub_1(\pi)(r, s) = (\pi(r), s) \text{ if r is nonzero, } Dub_1(\pi)(0, s) = (0, s) \text{ otherwise;}$$

$$Dub_2(\pi)(r, s) = (r, \pi(s)) \text{ if s is nonzero, } Dub_2(\pi)(r, 0) = (r, 0) \text{ otherwise}$$

(see [9], [2]). For a collection Π of permutations we agree that $Dub_i(\Pi)$ denotes $\{Dub_i(\pi) : \pi \in \Pi\}$, $i = 1, 2$. We have the following statement:

Lemma 1. *Let C and D be two perfect codes. Then*

$$Stab_{C^1} Sym(M(C, D)) \cap Stab_{D^2} Sym(M(C, D)) =$$
$$Dub_1(Sym(C)) \times Dub_2(Sym(D)).$$

3 Linear coordinates

We consider two characteristics for a coordinate of a perfect code or a point of a Steiner triple system, which we use later for describing the symmetry groups of Mollard codes or the automorphism groups of Mollard Steiner triple systems. In this section we underline some properties of these characteristics.

For a Steiner triple system S on points $\{1, \ldots, n\}$ and $i \in \{1, \ldots, n\}$, define $\nu_i(S)$ to be the number of different *Pasch configurations*, incident to i, i. e. collections of triples $\{(i, j, k), (i, j_1, k_1), (i_1 j, j_1), (i_1, k, k_1)\}$.

For a perfect code C of length n containing the all-zero word for a coordinate position i we consider $\mu_i(C)$ to be the number of code triples, containing i from $Ker(C)$:

$$\mu_i(C) = |\{x \in \mathrm{STS}(C) \cap \mathrm{Ker}(C) : i \in supp(x)\}|.$$

We say that a coordinate i is *μ-linear* for a code C of length n if $\mu_i(C)$ takes the maximal possible value, i.e. $(n-1)/2$. Obviously, two coordinate positions i, j of S or C are in different orbits by $Aut(S)$ or $Sym(C)$ respectively if $\nu_i(S) \neq \nu_j(S)$ or $\mu_i(C) \neq \mu_j(C)$ respectively. We say that a point $i \in \{1, \ldots, n\}$ is *ν-linear* for a Steiner triple system S of order n if $\nu_i(S)$ takes the maximal possible value, i.e. $(n-1)(n-3)/4$. By $Lin_\nu(S)$ and $Lin_\mu(C)$ denote the sets of ν-linear coordinates of S and μ-linear coordinates of C respectively. $Lin_\nu(S)$ and $Lin_\mu(C)$ are characteristics of a nonlinearity of a Steiner triple system S and a perfect code C respectively.

Lemma 2. *Let* $<\{1,\dots,n\},\cdot>$ *be a quasigroup associated with a Steiner triple system* S *of order* n. *Then the following statements are equivalent:*
1. $l \in Lin_\nu(S)$;

2. *for any distinct* $s, s' \in \{1,\dots,n\}, s, s' \neq l$ *we have that* $(l \cdot s) \cdot (l \cdot s') = s \cdot s'$;

3. *for any distinct* $s, s' \in \{1,\dots,n\}, s, s' \neq l$ *we have that* $l \cdot (s \cdot s') = (l \cdot s) \cdot s'$.

The second statement of the previous lemma implies that $0 \cup Lin_\nu(S)$ is a *nucleus* of a Steiner loop $(\{0,\dots,n\},\star)$, associated with S (see, for example [10]), which implies that $|Lin_\nu(S)| \leq (n-3)/4$ if the Steiner triple system S is nonprojective.

Theorem 1. *1. Let* C *be a perfect code. Then we have*

$$Lin_\mu(C) \subseteq Lin_\nu(STS(C)).$$

2. A subdesign of a Steiner triple system S *on the points* $Lin_\nu(S)$ *is a projective Steiner triple system.*

3. A subcode of a perfect code C *on the coordinates* $Lin_\mu(C)$ *is a Hamming code.*

4 Symmetry group of Mollard code

In this section we consider the structure of the symmetry group of a Mollard code. Recall that the Mollard construction is a generalization of the Vasil'ev construction. In [1] the structure of symmetry group of the Vasil'ev codes is investigated. In this section we obtain an extension of the result for Mollard codes.

By $Stab_C(G)$ and $Stab_{(C)}G$ of a code C we denote the setwise and codeword-wise stabilizers of the set C by the group G acting on a code C', $C \subseteq C'$. Let C be a perfect subcode of C'. Denote the set of nonzero coordinates of C by $N(C)$. Then the codeword-wise stabilizer of C and coordinate-wise stabilizer of $N(C)$ by the group $Sym(C')$ are equal, i. e. we have

$$Stab_{N(C)}Sym(C') = Stab_C Sym(C'),\ Stab_{(N(C))}Sym(C') = Stab_{(C)}Sym(C').$$

Let $\mathcal{T}$ be the subgroup formed by the collection of symmetries τ of the Mollard code $M(C,D)$ such that

$$\forall r \in \{1,\dots,t\},\ \forall s \in \{0,\dots,m\}\ \exists s' : \tau(r,s) = (r,s'),$$

$$\forall s \in \{1,\dots,m\} \text{ we have } \tau(0,s) = (0,s).$$

Proposition 1. *The group* $\mathcal{T}$ *is an elementary abelian 2-group.*

Proof. We show that $\tau \in \mathcal{T}$ is necessarily of order not more than 2. Indeed, let $\tau(r,0)=(r,s)$, then, taking into account that $\tau(0,s)=(0,s)$, we have that a triple $\tau((r,0),(0,s),(r,s))=((r,s),(0,s),(r,s'))$ for some s' must be in $STS(M(C,D))$ which is true iff $s'=0$ ($\tau((r,0),(0,s),(r,s))$ must be from T_{00}), i.e. $\tau(r,s)=(r,0)$. This implies that τ^2 fixes all coordinates $(r,0)$ and $(0,s)$ for any $r \in \{1,\dots,t\}, s \in \{1,\dots,m\}$. Therefore, τ^2 must fix (r,s) for any $r \in \{1,\dots,t\}, s \in \{1,\dots,m\}$, because τ^2 fixes elements $(r,0)$ and $(0,s)$ of the triple $((r,0),(0,s),(r,s))$. We have shown that τ^2 is an identity. □

We consider the setwise stabilizer $Stab_{D^2}Sym(STS(M(C,D)))$ of the subcode D^2 in $Sym(M(C,D))$. We show that any element of the group could be represented as a composition of the following three symmetries: $Dub_2(\pi')$, for $\pi' \in Sym(D)$, $Dub_1(\pi)$, for $\pi \in Sym(C)$ and a symmetry $\tau \in \mathcal{T}$. Here $\pi' \in Sym(D)$ is a permutation realizing σ on nonzero positions of the subcode D^2, $\pi \in Sym(C)$ is a permutation, induced by action of $\sigma Dub_2(\pi'^{-1})$ on the subsets $r \times \{0,\dots,m\}, r=1,\dots,t$. In the case of the Vasil'ev code, i.e. m=1, the following result was obtained in [1]:

$$Stab_{D^2}Sym(STS(M(C,D))) = Dub_1(Sym(C)) \leftthreetimes \mathcal{T}.$$

Lemma 3. *Let G be $Stab_{D^2}Sym(STS(M(C,D)))$. Then it is true that*

$$Stab_{(C^1)}G = Dub_2(Sym(D)) \lhd G;$$

$$Stab_{(D^2)}G = \{Dub_1(\pi)\tau : \pi \in Sym(C), \tau \in \mathcal{T}\} \lhd G;$$

$$G = Dub_2(Sym(D)) \times \{Dub_1(\pi)\tau : \pi \in Sym(C), \tau \in \mathcal{T}\}.$$

By Lemma 3 we are now focused on the description of $\mathcal{T}$.

For a codeword $u \in C$ and an element $l \in Lin_\mu(D)$, denote by $Ort_l(u)$ the permutation on the coordinates of $M(C,D)$ defined in the following way:

$$Ort_l(u)(r,s) = (r, \alpha \star s), \text{ for } \text{ r} \in supp(u), s \in \{0,\dots,m\};$$

$$Ort_l(u)(r,s) = (r,s), \text{ otherwise},$$

where $\star$ is a binary operation in $LSTS(D)$. We agree that $Ort_A(U)$ denotes the collection of permutations $\{Ort_l(u) : l \in A, u \in U\}$. In the next lemma we use an idea similar to that of work [3]. Below by $< Ort_{Lin_\mu(D)}(C^\perp) >$ we mean the subgroup generated by symmetries from the set $Ort_{Lin_\mu(D)}(C^\perp)$.

Lemma 4. *It is true that $\mathcal{T} =< Ort_{Lin_\mu(D)}(C^\perp) > \cong Z_2^{(log_2(1+|Lin_\mu(D)|))^{n-r(C)}}$, where $r(C)$ is the rank of C over $\mathbf{F}_2$.*

From Lemmas 3 and 4 we obtain

Theorem 2. *Let C and D be two perfect codes. Then*

$$Stab_{D^2}Sym(STS(M(C,D))) =$$
$$(Dub_1(Sym(C))\leftthreetimes < Ort_{Lin_\mu(D)}(C^\perp)) > \times Dub_2(Sym(D)).$$

An analogous result holds for Steiner triple systems:

Theorem 3. *Let S_1 and S_2 be arbitrary two Steiner triple systems, $M(S_1,S_2)$ be a Steiner triple system obtained from S_1 and S_2 by applying the Mollard construction. Then*
$Stab_{S_2^2}Aut(M(S_1,S_2)) = (Dub_1(Aut(S_1)) \leftthreetimes (< Ort_{Lin_\nu(S_2)}(S_1^\perp) >, \circ))\times$
$\times Dub_2(Aut(S_2))$.

In work [7] (see also [6]) a class of Mollard codes with symmetry groups, fixing D^2 fulfilling special algebraic properties was obtained. By Theorem 2 we have a description for the symmetry groups of this class.

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] 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.

[3] O. Heden, On the size of the symmetry group of a perfect code, Discrete Math., **311** (17), 1879–1885, 2011.

[4] M. Mollard, A generalized parity function and its use in the construction of perfect codes, SIAM J. Alg. Disc. Meth., **7**(1), 113–115, 1986.

[5] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North Holland, 1977.

[6] 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, ...–....

[7] I. Yu. Mogilnykh, F. I. Solov'eva, Transitive propelinear perfect codes, submitted to *Discrete Mathematics.*

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

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

[10] J. D. Phillips, P. Vojtechovsky: C-Loops: an introduction. http://arxiv.org/abs/math/0701711.