

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

<http://semr.math.nsc.ru>

Том 16, вып. 1689–1702 (2019)

DOI 10.33048/semi.2019.16.119

УДК 519.725

MSC 94B60

A CONCATENATION CONSTRUCTION FOR PROPELINEAR
PERFECT CODES FROM REGULAR SUBGROUPS OF $GA(r, 2)$

I.YU. MOGILNYKH, F.I. SOLOV'eva

ABSTRACT. A code C is called propelinear if there is a subgroup of $\text{Aut}(C)$ of order $|C|$ acting transitively on the codewords of C . In the paper new propelinear perfect binary codes of any admissible length more than 7 are obtained by a particular case of the Solov'eva concatenation construction–1981 and the regular subgroups of the general affine group of the vector space over $\text{GF}(2)$.

Keywords: Hamming code, perfect code, concatenation construction, propelinear code, Mollard code, regular subgroup, transitive action.

1. INTRODUCTION

The vector space of dimension n over the Galois field F of two elements with respect to the Hamming metric is denoted by F^n . The *Hamming distance* between any two vectors $x, y \in F^n$ is defined as the number of coordinates in which x and y differ. The *support* of a vector x from F^n denoted by $\text{supp}(x)$ is the collection of the indices of its nonzero coordinate positions. The *Hamming weight* $\text{wt}(x)$ of a vector x is the size of its support. A *code* of length n is an arbitrary set of vectors of F^n that are called *codewords* of C . The *code distance* of a code is the minimum value of the Hamming distance between two different codewords from the code. A code C is called *perfect binary single-error-correcting* (briefly *perfect*) if for any vector x from F^n there exists exactly one vector $y \in C$ at the Hamming distance not more than 1 from the vector x . A perfect linear code is called the *Hamming code*. Adding

MOGILNYKH, I.YU., SOLOV'eva, F.I., A CONCATENATION CONSTRUCTION FOR PROPELINEAR PERFECT CODES FROM REGULAR SUBGROUPS OF $GA(r, 2)$.

© 2019 MOGILNYKH I.YU., SOLOV'eva F.I.

The work was supported by the Ministry of Education and Science of Russia (state assignment No. 1.13557.2019/13.1).

Received March, 15, 2019, published November, 21, 2019.

the overall parity check to all codewords of a code of length n we obtain the code of length $n + 1$ that is called *extended*.

Let x be a binary vector of F^n , π be a permutation of the coordinate positions of vectors in F^n . Consider the transformation (x, π) that maps a binary vector y as follows:

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

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

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

where $\pi \circ \pi'$ is the composition of permutations π and π' defined as follows:

$$\pi \circ \pi'(i) = \pi(\pi'(i))$$

for any $i \in \{1, 2, \dots, n\}$. The automorphism group $\text{Aut}(F^n)$ of F^n is the group of all such transformations (x, π) with respect to the composition. The automorphism group $\text{Aut}(C)$ of a code C is the setwise stabilizer of C in $\text{Aut}(F^n)$.

A group G acting on a set is called *regular* if the action is transitive and the order of G coincides with the size of the set. A subgroup of the automorphism group of a code is called *regular* if it acts regularly on the set of its codewords. A code C is called *propelinear* [19] if $\text{Aut}(C)$ has a regular subgroup.

It is well-known that the supports of the codewords of weight 3 in any perfect code containing the all-zero vector form a Steiner triple system. A perfect code C is called *homogeneous* if all Steiner triple systems of the codes $C + y$, $y \in C$ are isomorphic. The homogeneous perfect codes were introduced in [17]. Obviously, any propelinear code is necessarily homogeneous. Despite of the existence of nonpropelinear homogeneous Vasil'ev perfect codes for any length n , $n \geq 15$ [15], the existence of a rich construction of such codes remains to be an open problem.

Propelinear codes play an important role in the theory of optimal codes since they are close to linear codes by several properties of their automorphism groups. Nowadays there are known several classes of propelinear codes, among them are Preparata and Kerdock codes [7], [20] Z_4 -linear Reed-Muller codes [12], Z_4 -linear and Z_{2^k} -linear Hadamard codes [9] [10], etc.

Classical propelinear perfect codes are Z_4 -linear [9] and Z_2Z_4 -linear codes [5]. It is known that propelinear perfect codes can be obtained by the Plotkin and the Vasil'ev constructions [2]. In [3] all transitive codes from [21] found by a representation via the Phelps construction were proved to be propelinear. The codes from [21] were later generalized by Krotov and Potapov in [11] who utilized quadratic functions in the Vasil'ev construction. Note that the Vasil'ev construction was generalized by the Mollard construction for propelinear perfect codes [2]. The approaches of [21, 3, 11] gave exponential classes of propelinear codes (the best lower bound was obtained in [11]) but all these codes are of small rank $n - \log(n + 1) + 1$, where n is the length of the codes. Moreover, the ranks of Z_4 -linear extended perfect codes of length n do not exceed $n - \lceil \frac{\log(n+1)}{2} \rceil$, see [9] (an analogous result [19] holds for ranks of Z_2Z_4 -linear perfect codes from [5]).

The question of finding propelinear perfect codes of large ranks was considered in [6] and was based again on the Mollard construction. In this paper a solution for the rank problem for propelinear codes is given with exception of few finite open cases. Therefore the problem of finding new methods of constructing propelinear non-Mollard codes of large ranks is open. The kernel problem as far as the rank

and kernel problem is still open for propelinear perfect binary codes. Recall that the rank and kernel problem for perfect binary codes was solved in the paper [1].

In the paper we obtain a new class of propelinear perfect and extended perfect binary codes of ranks in $\{2^r - r - 1, \dots, 2^r - 2\}$ and the dimensions of the kernels in $\{2^r - 2r - 2, \dots, 2^r - r - 3\}$. The paper is organized as follows. The general construction is given in Section 2. The concatenation construction [22], see also [18], uses a partition of the even weight code into the extended perfect codes of length 2^r and a permutation on the elements of the partition. It is not difficult to show that the full rank codes can not be obtained by the construction [22]. In the paper we consider the case when the partition is into extended Hamming codes. The construction in Section 2 for propelinear codes uses the automorphisms of the regular subgroups of the general affine group of F^r as permutations. In Section 3 we investigate ranks and kernels of the version of the construction [22] with arbitrary permutations. We obtain the expressions for the ranks and the dimension of the kernels of these codes in terms of these permutations. Moreover, we show that any such code with the dimension of the kernel $2^r - 2r - 2$ is inequivalent to any Mollard propelinear code. The discussion is continued in Section 4 where we construct an infinite series of new propelinear perfect codes. For this purpose we apply the direct product construction for regular subgroups of the general affine group [14] to a regular subgroup of the general affine group constructed by Hegedus in [8].

2. A CONSTRUCTION FOR PROPELINEAR PERFECT CODES

Let the coordinates of the vector space F^{2^r} be indexed by the vectors from F^r . Below the all-zero vector $\mathbf{0}^r$ of length r is denoted by $\mathbf{0}$ and the length of the vector will be always clear from the context. Define the following code:

$$\mathcal{H} = \{c \in F^{2^r} : \sum_{a:c_a=1} a = \mathbf{0}, \text{wt}(c) \equiv 0(\text{mod } 2)\}.$$

Given a code C and a coordinate position *the punctured code* C' is defined as the code whose codewords are obtained by removing the coordinate in all codewords of C . Consider the code \mathcal{H}' obtained by puncturing \mathcal{H} in the coordinate indexed by $\mathbf{0}$. We index the coordinate positions of F^{2^r-1} by the nonzero vectors of F^r and therefore we have:

$$\mathcal{H}' = \{c \in F^{2^r-1} : \sum_{a:c_a=1} a = \mathbf{0}\}.$$

For an arbitrary vector a in F^r the code $\mathcal{H} + e_a + e_{\mathbf{0}}$ is denoted by \mathcal{H}_a , here e_a is the vector in F^n with the only one nonzero position a , $a \in F^r$. The code \mathcal{H} is an extended Hamming code and the collection of the cosets \mathcal{H}_a , where $a \in F^r$, is the partition of the set of all even weight vectors of F^{2^r} into cosets of the code \mathcal{H} .

Denote the *general linear group* that consists of nonsingular $r \times r$ matrices over F by $\text{GL}(r, 2)$. Consider an affine transformation (a, M) , $a \in F^r$, $M \in \text{GL}(r, 2)$. Its action on F^r is defined as

$$(1) \quad (a, M)(b) = a + Mb,$$

$b \in F^r$. The composition of any two affine transformations (a, M) and (b, M') is the transformation $(a + bM, MM')$. The *general affine group* of the space F^r with elements $\{(a, M) : a \in F^r, M \in \text{GL}(r, 2)\}$ with respect to the composition is denoted by $\text{GA}(r, 2)$.

A subgroup G of a group $\text{GA}(r, 2)$ is called *regular* if it is regular with respect to the action (1) on the vectors of F^r . The action of $\text{GA}(r, 2)$ on the vectors of F^r is equivalent to the action of the automorphism group on the codewords of the Hadamard code (the dual code to the Hamming code of length $2^r - 1$), see [14]. Therefore the regular subgroups of $\text{GA}(r, 2)$ are in a one-to-one correspondence with the regular subgroups of the automorphism group of the Hadamard code.

By definition for any regular subgroup G of the group $\text{GA}(r, 2)$ and any $a, a \in F^r$ there is a unique affine transformation that maps $\mathbf{0}$ to a . In throughout what follows we denote it by g_a . Obviously, g_a is (a, M_a) for some matrix M_a in $\text{GL}(r, 2)$. Since

$$(2) \quad g_a g_b = (g_a(b), M_a M_b)$$

we have

$$(3) \quad M_{g_a(b)} = M_a M_b.$$

Let T be an automorphism of a regular subgroup G of the group $\text{GA}(r, 2)$. By τ we denote the permutation on the vectors of F^r induced by the automorphism T , i.e.

$$T(g_a) = g_{\tau(a)}.$$

Obviously we always have $\tau(\mathbf{0}) = \mathbf{0}$. Since T is an automorphism of G then by the definition of τ and (2) we have $(\tau(g_a(b)), M_{\tau(g_a(b))}) = T(g_a g_b) = T(g_a)T(g_b) = g_{\tau(a)} g_{\tau(b)} = (g_{\tau(a)}(\tau(b)), M_{\tau(a)} M_{\tau(b)})$.

Therefore the following equalities hold:

$$(4) \quad \tau(g_a(b)) = g_{\tau(a)}(\tau(b)),$$

$$(5) \quad M_{\tau(g_a(b))} = M_{\tau(a)} M_{\tau(b)}.$$

The concatenation of two vectors $x \in F^{r'}$ and $y \in F^{r''}$ is denoted by $x|y$. For codes C and D by $C \times D$ denote the code $\{x|y : x \in C, y \in D\}$. Let π', π'' be permutations on the vectors of $F^{r'}$ and $F^{r''}$ respectively then by $\pi'|\pi''$ we denote the permutation acting on the concatenations $x|y$ of the vectors $x \in F^{r'}$ and $y \in F^{r''}$ from $F^{r'+r''}$ as follows: $(\pi'|\pi'')(x|y) = \pi'(x)|\pi''(y)$.

In particular, let π' and π'' be permutations on the coordinate positions of $F^{r'}$. A permutation on the coordinates of the vector space naturally induces the permutation on the set of vectors. So throughout Section 2, we use the same notation $\pi'|\pi''$ for the permutation of the coordinate positions of $F^{2r'}$ that acts as follows: $(\pi'|\pi'')(x|y) = \pi'(x)|\pi''(y)$, for any $x, y \in F^{r'}$.

Consider the following particular case of the concatenation construction [22] for extended perfect codes:

$$(6) \quad S_{\mathcal{H}, \tau} = \bigcup_{a \in F^r} \mathcal{H}_a \times \mathcal{H}_{\tau(a)},$$

where τ is a bijection from F^{2r} to F^{2r} .

Theorem 1. *Let G be a regular subgroup of $\text{GA}(r, 2)$ and τ be the permutation induced by an automorphism of G . Then the code $S_{\mathcal{H}, \tau}$ is a propelinear extended perfect binary code of length 2^{r+1} .*

Proof. For an element $g_a = (a, M_a)$ of a regular subgroup G of $\text{GA}(r, 2)$ by π_a we denote the permutation corresponding to the matrix M_a , i.e.

$$(7) \quad \pi_a(b) = M_a b.$$

Since M_a is in $\text{GL}(r, 2)$, it preserves linear independency, so by definition of \mathcal{H} , we have

$$(8) \quad \pi_a(\mathcal{H}) = \mathcal{H}, \pi_a(e_0) = e_0.$$

Consider the following set of automorphisms of F^{r+1} :

$$\Gamma = \bigcup_{a \in F^r} \{(x|y, \pi_a | \pi_{\tau(a)}) : x \in \mathcal{H}_a, y \in \mathcal{H}_{\tau(a)}\}.$$

Note that when $(x|y, \pi_a | \pi_{\tau(a)})$ runs through Γ , the vector $x|y$ runs through the code $S_{\mathcal{H}, \tau}$. If we prove that Γ is a group, then the orbit of the all-zero vector from $F^{2^{r+1}}$ under Γ is $S_{\mathcal{H}, \tau}$, so Γ is a regular subgroup of $\text{Aut}(S_{\mathcal{H}, \tau})$.

We now show that Γ is closed under composition. Consider two automorphisms $(x|y, \pi_a | \pi_{\tau(a)})$ and $(u|v, \pi_b | \pi_{\tau(b)})$ from Γ , by definition of Γ we have:

$$(9) \quad x \in \mathcal{H}_a, y \in \mathcal{H}_{\tau(a)},$$

$$(10) \quad u \in \mathcal{H}_b, v \in \mathcal{H}_{\tau(b)}.$$

We denote the composition of these two automorphisms by $(w|z, \pi_a \pi_b | \pi_{\tau(a)} \pi_{\tau(b)})$, where

$$\begin{aligned} w &= x + \pi_a(u), \\ z &= y + \pi_{\tau(a)}(v) \end{aligned}$$

and show that it is in Γ .

Since the code \mathcal{H} is linear and $\pi_a(\mathcal{H}) = \mathcal{H}$ (see (8)), $u \in \mathcal{H}_b$, $\mathcal{H}_b = e_b + e_0 + \mathcal{H}$ (see (10)) we have

$$w + \mathcal{H} = x + \pi_a(u) + \mathcal{H} = x + \pi_a(e_b + e_0) + \mathcal{H}.$$

Because x is in $\mathcal{H}_a = \mathcal{H} + e_a + e_0$ (see (9)), $\pi_a(e_0) = e_0$ (see (8)) we obtain $x + \pi_a(e_b + e_0) + \mathcal{H} = e_a + \pi_a(e_b) + \mathcal{H}$. By (7), i.e. $\pi_a(e_b) = e_{M_a b}$, we have $e_a + \pi_a(e_b) + \mathcal{H} = e_a + e_{M_a b} + \mathcal{H}$. The linear code \mathcal{H} contains the vector $e_a + e_{M_a b} + e_{a+M_a b} + e_0$, hence

$$(11) \quad w + \mathcal{H} = \mathcal{H}_{a+M_a b} = \mathcal{H}_{g_a(b)}.$$

Let us now show that

$$(12) \quad z + \mathcal{H} = \mathcal{H}_{\tau(g_a(b))}.$$

From $z = y + \pi_{\tau(a)}(v)$, $\pi_{\tau(a)}(\mathcal{H}) = \mathcal{H}$, $\pi_{\tau(a)}(e_0) = e_0$ (see (8)), $v \in \mathcal{H}_{\tau(b)}$, $y \in \mathcal{H}_{\tau(a)}$ (see (9) and (10)) and by (7) we have

$$z + \mathcal{H} = y + \pi_{\tau(a)}(v) + \mathcal{H} = e_{\tau(a)} + \pi_{\tau(a)}(e_{\tau(b)}) + \mathcal{H} = e_{\tau(a)} + e_{M_{\tau(a)}\tau(b)} + \mathcal{H}.$$

By definition of \mathcal{H} we have $e_{\tau(a)} + e_{M_{\tau(a)}\tau(b)} + e_{\tau(a)+M_{\tau(a)}\tau(b)} + e_0 \in \mathcal{H}$, which combined with $g_{\tau(a)}(\tau(b)) = \tau(a) + M_{\tau(a)}\tau(b)$ and the fact that \mathcal{H} is linear we obtain

$$e_{\tau(a)} + e_{M_{\tau(a)}\tau(b)} + \mathcal{H} = \mathcal{H}_{\tau(a)+M_{\tau(a)}\tau(b)} = \mathcal{H}_{g_{\tau(a)}(\tau(b))}.$$

Using (4) we have $z + \mathcal{H} = \mathcal{H}_{\tau(g_a(b))}$, i.e. (12) holds.

Note that according to the correspondence (7) the equalities $M_{g_a(b)} = M_a M_b$ and $M_{\tau(g_a(b))} = M_{\tau(a)} M_{\tau(b)}$, see (3) and (5), can be rewritten as $\pi_{g_a(b)} = \pi_a \pi_b$ and

$\pi_{\tau(g_a(b))} = \pi_{\tau(a)}\pi_{\tau(b)}$. These equalities imply that the permutation $\pi_a\pi_b|\pi_{\tau(a)}\pi_{\tau(b)}$ is equal to $\pi_{g_a(b)}|\pi_{\tau(g_a(b))}$. Therefore the considered composition of automorphisms $(x|y, \pi_a|\pi_{\tau(a)})$ and $(u|v, \pi_b|\pi_{\tau(b)})$, i.e. $(w|z, \pi_{g_a(b)}|\pi_{\tau(g_a(b))})$ belongs to Γ since by the equalities (11) and (12) the vector $w|z$ belongs to $\mathcal{H}_{g_a(b)} \times \mathcal{H}_{\tau(g_a(b))}$. Hence Γ is a regular subgroup of the automorphism group of the code $S_{\mathcal{H},\tau}$ and the code $S_{\mathcal{H},\tau}$ is propelinear. □

Proposition 1. *Let C be a propelinear code with minimum distance at least 2 whose automorphism group contains a regular subgroup G . Let i be a coordinate such that $\pi(i) = i$ for any $(x, \pi) \in G$. Then the code C' obtained from C by puncturing in the i th coordinate position is propelinear.*

Proof. For $x \in C$ let x' denote the codeword of C' obtained by deleting its i th coordinate position. Suppose the coordinates of C' are indexed by the coordinates of the code C without i th position, so $\text{supp}(x') = \text{supp}(x) \setminus \{i\}$ if $i \in \text{supp}(x)$ and $\text{supp}(x') = \text{supp}(x)$ otherwise. For a permutation π , where $(x, \pi) \in G$, by π' denote the permutation acting on the coordinate positions of C' , where $\pi'(j) = \pi(j)$, for any coordinate j of the code C different from i . Obviously, the group $G' = \{(x', \pi') : (x, \pi) \in G\}$ is isomorphic to G and G' is a regular subgroup of $\text{Aut}(C')$. □

Consider the following puncturing $S'_{\mathcal{H},\tau}$ of $S_{\mathcal{H},\tau}$:

$$(13) \quad S'_{\mathcal{H},\tau} = \bigcup_{a \in F^r} \mathcal{H}'_a \times \mathcal{H}_{\tau(a)},$$

where $\mathcal{H}'_a = e_a + \mathcal{H}'$, $\mathcal{H}'_0 = \mathcal{H}'$. The code $S'_{\mathcal{H},\tau}$ is perfect. Let τ be a permutation induced by an automorphism of a regular subgroup G of $\text{GA}(r, 2)$. In this case for every $a \in F^r$ the permutation π_a defined in (7) fixes the coordinate $\mathbf{0}$ of \mathcal{H} . Then every permutation $\pi_a|\pi_{\tau(a)}$ of any automorphism $(x|y, \pi_a|\pi_{\tau(a)})$ of the regular subgroup Γ of $\text{Aut}(S_{\mathcal{H},\tau})$ fixes the coordinate position of $S_{\mathcal{H},\tau}$ in which we puncture the code $S_{\mathcal{H},\tau}$ to obtain $S'_{\mathcal{H},\tau}$. By Proposition 1 we see that $S'_{\mathcal{H},\tau}$ is propelinear. Therefore, a class of propelinear perfect codes is obtained:

Corollary 1. *Let G be a regular subgroup of $\text{GA}(r, 2)$ and τ be the permutation induced by an automorphism of the group G . Then the code $S'_{\mathcal{H},\tau}$ is a propelinear perfect binary code of length $2^{r+1} - 1$.*

Moreover, the values for invariants (i.e. rank and kernel) which we obtain below in the paper for the extended perfect code $S_{\mathcal{H},\tau}$ are the same for the perfect code $S'_{\mathcal{H},\tau}$.

3. RANK AND KERNEL OF $S_{\mathcal{H},\tau}$

In the current section we discuss the ranks and the dimensions of the kernels for the codes $S_{\mathcal{H},\tau}$. We find the formulas for these invariants in terms of the intersection of $\tau(\mathcal{H})$ and \mathcal{H} . Note that τ is an arbitrary bijection preserving $\mathbf{0}$ in this section with exception of Example 1.

We denote the dimension of a linear code C by $\text{dim}(C)$. The linear span of a code C over F is denoted by $\langle C \rangle$. The rank of a code C , denoted by $\text{rank}(C)$, is $\text{dim}(\langle C \rangle)$. The kernel $\text{Ker}(C)$ of a code C of length n is defined as the set of all

vectors $x \in F^n$ such that $x + C = C$. Note that the all-zero vector is in C if and only if $\text{Ker}(C) \subseteq C$.

Let τ be a bijection from F^r to F^r (a permutation of the coordinate positions of \mathcal{H}) that fixes the vector $\mathbf{0}$. Define the *distension* of τ to be $2^r - r - 1 - \dim(\mathcal{H} \cap \tau(\mathcal{H}))$, where $\tau(\mathcal{H}) = \{\tau(x) : x \in \mathcal{H}\}$. Note that $2^r - r - 1$ is the dimension of the code \mathcal{H} .

Lemma 1. *Let τ be a bijection from F^r to F^r , $\tau(\mathbf{0}) = \mathbf{0}$ and l be the distension of τ . Then the rank of $S_{\mathcal{H},\tau}$ is $(2^{r+1} - r - 2) + l$.*

Proof. Let $F_0^{2^r}$ denote the even weight code of length 2^r .

Since

$$\begin{aligned} < \bigcup_{a \in F^r} \mathcal{H}_a \times \mathcal{H}_{\tau(a)} > = < \bigcup_{a \in F^r} (\mathcal{H} + e_a + e_0) \times (\mathcal{H} + e_{\tau(a)} + e_0) > = \\ < \mathcal{H} \times \mathcal{H} \cup \{x|\tau(x) : x \in F_0^{2^r}\} >, \end{aligned}$$

we have

$$(14) \quad < S_{\mathcal{H},\tau} > = < \mathcal{H} \times \mathcal{H} \cup \{x|\tau(x) : x \in F_0^{2^r}\} > .$$

Let the vectors $\{u_i\}_{i \in \{1, \dots, 2^r - 1\}}$ be a basis of $F_0^{2^r}$ such that $u_1, \dots, u_{\dim(\mathcal{H} \cap \tau(\mathcal{H}))}$ is a basis of the subspace $\mathcal{H} \cap \tau^{-1}(\mathcal{H})$ and $u_1, \dots, u_{2^r - r - 1}$ is a basis of \mathcal{H} .

Consider the following two sets:

$$\begin{aligned} \mathcal{B} &= \{u_i|u_j, 1 \leq i, j \leq 2^r - r - 1\}, \\ \mathcal{B}' &= \{u_i|\tau(u_i) : \dim(\mathcal{H} \cap \tau(\mathcal{H})) + 1 \leq i \leq 2^r - 1\}. \end{aligned}$$

We show that $\mathcal{B} \cup \mathcal{B}'$ is a basis of $< S_{\mathcal{H},\tau} >$.

The vectors of $\mathcal{B} \cup \mathcal{B}'$ are linearly independent. Indeed, obviously, \mathcal{B} is a basis of $\mathcal{H} \times \mathcal{H}$. Suppose that a nonzero vector $x|\tau(x)$ is spanned by \mathcal{B}' . Then by the definition of \mathcal{B}' the vector x is not from $\mathcal{H} \cap \tau^{-1}(\mathcal{H})$ and therefore x and $\tau(x)$ can not be simultaneously in \mathcal{H} , i.e. $x|\tau(x) \notin \mathcal{H} \times \mathcal{H} = < \mathcal{B} >$.

We show that $< \mathcal{B} \cup \mathcal{B}' > = < S_{\mathcal{H},\tau} >$. The equality (14) and $< \mathcal{B} > = \mathcal{H} \times \mathcal{H}$ imply that it is sufficient to prove that the vectors $u_i|\tau(u_i), i \in \{1, \dots, 2^r - 1\}$ are in $< \mathcal{B} \cup \mathcal{B}' >$. By definition of $\{u_i\}_{i \in \{1, \dots, \dim(\mathcal{H} \cap \tau(\mathcal{H}))\}}$ these vectors are in $\mathcal{H} \cap \tau^{-1}(\mathcal{H})$, so $\tau(u_i)$ is in \mathcal{H} for $i \in \{1, \dots, \dim(\mathcal{H} \cap \tau(\mathcal{H}))\}$. We see that in this case the vector $u_i|\tau(u_i)$ is in $< \mathcal{B} > = \mathcal{H} \times \mathcal{H}$ for any $i \in \{1, \dots, \dim(\mathcal{H} \cap \tau(\mathcal{H}))\}$. The remaining vectors $u_i|\tau(u_i), i \in \{\dim(\mathcal{H} \cap \tau(\mathcal{H})) + 1, \dots, 2^r - 1\}$ are from \mathcal{B}' , so $\mathcal{B} \cup \mathcal{B}'$ spans $< S_{\mathcal{H},\tau} >$.

The rank of $S_{\mathcal{H},\tau}$ is $|\mathcal{B}| + |\mathcal{B}'| = 2(2^r - r - 1) + (2^r - 1 - \dim(\mathcal{H} \cap \tau(\mathcal{H}))) = (2^{r+1} - r - 2) + 2^r - r - 1 - \dim(\mathcal{H} \cap \tau(\mathcal{H}))$. Taking into account that $2^r - r - 1 - \dim(\mathcal{H} \cap \tau(\mathcal{H}))$ is the distension of τ , we obtain the required. □

For $a \in F^r$ the set of the supports of the codewords of \mathcal{H}' of weight 3 with ones in the coordinate indexed by a is called a *star* of \mathcal{H}' and denoted by $\text{Star}(a)$, i.e. we have

$$\text{Star}(a) = \{\{a, b, a + b\} : b \in F^r \setminus (\mathbf{0} \cup a)\}.$$

Let τ be a bijection from F^r to F^r such that $\tau(\mathbf{0}) = \mathbf{0}$. Since we always have $\tau(\mathbf{0}) = \mathbf{0}$, we can consider that τ acts on the coordinate positions of \mathcal{H}' which are indexed by the nonzero vectors of F^r and use notation $\tau(\mathcal{H}')$ throughout the text.

Note that $\tau(\text{Star}(a))$ is a star of \mathcal{H}' if and only if it is $\text{Star}(\tau(a))$, which is equivalent to $\tau(a + c) = \tau(a) + \tau(c)$ for all $c \in F^r$. If $\tau(a + c) = \tau(a) + \tau(c)$,

$\tau(b+c) = \tau(b) + \tau(c)$ for all $c \in F^r$, then $\tau(a+b+c) = \tau(a) + \tau(b+c) = \tau(a) + \tau(b) + \tau(c) = \tau(a+b) + \tau(c)$. We conclude that if $\tau(\text{Star}(a))$ and $\tau(\text{Star}(b))$ are stars of \mathcal{H}' , then $\tau(\text{Star}(a+b))$ is a star of \mathcal{H}' . This implies that the number of stars of \mathcal{H}' that are mapped to stars of \mathcal{H}' by τ is always a power of two but one. Define the *deficiency* of τ to be $r - \log(|\{a \in F^r : \tau(\text{Star}(a)) = \text{Star}(\tau(a))\}| + 1)$.

Lemma 2. *Let τ be a bijection from F^r to F^r such that $\tau(\mathbf{0}) = \mathbf{0}$ and the deficiency of τ be k . Then we have*

$$\dim(\text{Ker}(S_{\mathcal{H},\tau})) = 2^{r+1} - r - 2 - k.$$

Proof. It is easy to see that $\mathcal{H} \times \mathcal{H} \leq \text{Ker}(S_{\mathcal{H},\tau})$. We have that

$$(15) \quad \dim(\mathcal{H} \times \mathcal{H}) = 2^{r+1} - 2r - 2.$$

Let us consider the codeword $e_{\mathbf{0}} + e_a | e_{\mathbf{0}} + e_{\tau(a)} \in S_{\mathcal{H},\tau} \setminus \mathcal{H} \times \mathcal{H}$ for any $a \in F^r$. We show that it belongs to $\text{Ker}(S_{\mathcal{H},\tau})$ if and only if $\tau(\text{Star}(a))$ is a star of \mathcal{H}' . We have

$$\begin{aligned} & (e_{\mathbf{0}} + e_a | e_{\mathbf{0}} + e_{\tau(a)}) + S_{\mathcal{H},\tau} \\ &= \bigcup_{b \in F^r} (e_{\mathbf{0}} + e_a + \mathcal{H}_b) \times (e_{\mathbf{0}} + e_{\tau(a)} + \mathcal{H}_{\tau(b)}) \\ &= \bigcup_{b \in F^r} \mathcal{H}_{a+b} \times \mathcal{H}_{\tau(a)+\tau(b)}. \end{aligned}$$

The equality

$$\bigcup_{b \in F^r} \mathcal{H}_{a+b} \times \mathcal{H}_{\tau(a)+\tau(b)} = \bigcup_{c \in F^r} \mathcal{H}_c \times \mathcal{H}_{\tau(c)} = S_{\mathcal{H},\tau}$$

holds if and only if $\tau(a) + \tau(b) = \tau(a+b)$ for any $b \in F^r$, i.e. $\tau(\text{Star}(a))$ is a star of \mathcal{H}' . Taking into account (15) we have

$$\begin{aligned} \dim(\text{Ker}(S_{\mathcal{H},\tau})) &= \dim(\mathcal{H} \times \mathcal{H}) + \log(|\{a : \tau(\text{Star}(a)) = \text{Star}(\tau(a))\}| + 1) = \\ &= (2^{r+1} - 2r - 2) + (r - k) = 2^{r+1} - r - 2 - k. \end{aligned}$$

□

From Lemma 2 we see that the dimension of the kernel of a code $S_{\mathcal{H},\tau}$ of length $2^{r+1} - r - 2$ is at least $2^{r+1} - 2r - 2$. If the dimension of the kernel of $S_{\mathcal{H},\tau}$ is $2^{r+1} - 2r - 2$ then the code $S_{\mathcal{H},\tau}$ could not be obtained by the Mollard construction for propelinear codes with large ranks, see [2]. Recall that two codes of length n are called *equivalent* if there is an automorphism of F^n that maps one code to another.

Theorem 2. *Let τ be a bijection from F^r to F^r such that $\tau(\mathbf{0}) = \mathbf{0}$ and r be the deficiency of τ . Then the codes $S_{\mathcal{H},\tau}$ and $S'_{\mathcal{H},\tau}$ are not equivalent to any extended perfect Mollard code and perfect Mollard code respectively.*

Proof. By the condition of the theorem the deficiency of the bijection τ from F^r to F^r is r so by Lemma 2 the dimension of $\text{Ker}(S_{\mathcal{H},\tau})$ is $2(2^r - r - 1)$. Since $\dim(\mathcal{H}) = 2^r - r - 1$, from the proof of Lemma 2 we have $\mathcal{H} \times \mathcal{H} \leq \text{Ker}(S_{\mathcal{H},\tau})$, so $\text{Ker}(S_{\mathcal{H},\tau}) = \mathcal{H} \times \mathcal{H}$. We see that the codewords of $\text{Ker}(S_{\mathcal{H},\tau}) = \mathcal{H} \times \mathcal{H}$ of weight 4 are either $c|\mathbf{0}$ or $\mathbf{0}|c$ for all codewords c of \mathcal{H} of weight 4. In particular, for any fixed coordinate there are 2^r coordinates such that there are no codewords from $\text{Ker}(S_{\mathcal{H},\tau})$ of weight 4 with ones in any of these positions and the fixed coordinate simultaneously.

Consider the construction for Mollard codes. Let C and D be any two perfect codes of lengths t and m , respectively, containing all-zero vectors. We index the coordinates of F^t by pairs $(i, 0)$, $i \in \{1, \dots, t\}$, the coordinates of F^m by pairs $(0, j)$, $j \in \{1, \dots, m\}$, the coordinates of F^{tm} by pairs (i, j) , $i \in \{1, \dots, t\}$, $j \in \{1, \dots, m\}$ and the coordinates of the Mollard code are indexed by pairs (i, j) , $i \in \{0, \dots, t\}$ $j \in \{0, \dots, m\}$, where i and j are not 0 simultaneously.

Let $x = (x_{(1,1)}, x_{(1,2)}, \dots, x_{(1,m)}, x_{(2,1)}, \dots, x_{(2,m)}, \dots, x_{(t,1)}, \dots, x_{(t,m)})$ be a vector from F^{tm} . The generalized parity check functions $p_1(x) : F^{tm} \rightarrow F^t$ and $p_2(x) : F^{tm} \rightarrow F^m$ are defined as

$$(p_1(x))_{(i,0)} = \sum_{j=1}^m x_{(i,j)}, \quad (p_2(x))_{(0,j)} = \sum_{i=1}^t x_{(i,j)}.$$

Let f be any function from C to F^m . Denote by Z the following set

$$\{(x, p_1(x), p_2(x)) : x \in F^{tm}\}.$$

The perfect binary Mollard code of length $tm + t + m$, see [16] consists of cosets of Z

$$M(C, D) = \{(\mathbf{0}|y|z + f(y)) : y \in C, z \in D\} + Z.$$

Obviously, Z is a subspace of $\text{Ker}(M(C, D))$. Moreover, the kernel of the extended Mollard code contains the extension \bar{Z} of Z :

$$\bar{Z} = \{(x|p_1(x)|p_2(x)|\text{wt}(x) \bmod 2) : x \in F^{tm}\}.$$

We index the last coordinate position of \bar{Z} by $(0, 0)$.

It is easy to see that for any two coordinates \bar{Z} contains a unique codeword of weight 4 with ones in these coordinates. Indeed, the set of supports of the codewords of weight 4 from \bar{Z} is

$$\{(i_1, j_1), (i_2, j_2), (i_2, j_1), (i_1, j_2) : i_1, i_2 \in \{0, \dots, m\}, j_1, j_2 \in \{0, \dots, t\}, i_1 \neq i_2, j_1 \neq j_2\}.$$

Suppose that the code $S_{\mathcal{H},\tau}$ is equivalent to the extended perfect Mollard code $\bar{M}(C, D)$ via an automorphism of the Hamming space. Then $\text{Ker}(S_{\mathcal{H},\tau})$ is necessarily equivalent to $\text{Ker}(\bar{M}(C, D))$. For any two coordinates of \bar{Z} there is at least one codeword of weight 4 in $\bar{Z}, \bar{Z} \leq \text{Ker}(\bar{M}(C, D))$ with ones in these coordinates. On the other hand the considerations in the beginning of the proof of the theorem imply that there are pairs of coordinate with no vectors from $\text{Ker}(S_{\mathcal{H},\tau})$ of weight 4 with ones in these coordinates. So, $S_{\mathcal{H},\tau}$ is not a Mollard code.

We now turn to the case of punctured codes. Consider the puncturing $S'_{\mathcal{H},\tau}$ of $S_{\mathcal{H},\tau}$ defined by (13).

The codewords of $\text{Ker}(S'_{\mathcal{H},\tau})$ are obtained from the codewords of $\text{Ker}(S_{\mathcal{H},\tau}) = \mathcal{H} \times \mathcal{H}$ by puncturing, so the codewords from $\text{Ker}(S'_{\mathcal{H},\tau})$ of weight 3 are $\{c|\mathbf{0} : c \in \mathcal{H}'\}$, $\text{wt}(c) = 3$. Therefore there are at least 2^r coordinates of $S'_{\mathcal{H},\tau}$ that are zeros for all codewords of weight 3 in $\text{Ker}(S_{\mathcal{H},\tau})$. On the other hand, the kernel of the Mollard code $M(C, D)$ contains $Z = \{(x|p_1(x)|p_2(x)) : x \in F^{tm}\}$. Then, $\{(i, j), (i, 0), (0, j) : i \in \{1, \dots, t\}, j \in \{1, \dots, m\}\}$ are supports of some codewords of weight 3 from $\text{Ker}(M(C, D))$. We see that for every coordinate of $M(C, D)$ there is at least one codeword of weight 3 from $\text{Ker}(M(C, D))$ with one in this coordinate. Since this property does not hold for $\text{Ker}(S'_{\mathcal{H},\tau})$, we conclude that $\text{Ker}(S'_{\mathcal{H},\tau})$ is not the kernel of any Mollard code.

□

Example 1. Recall that the dihedral group D_m is the group formed by the symmetries of m -sized polygon.

Consider a group that is generated by an element α of order m and β of order 2 that satisfy the relation $\beta\alpha\beta = \alpha^{-1}$. It is well-known that the group is isomorphic to the dihedral group D_m . Consider the mapping T that fixes any element of the subgroup generated by α and sends $\beta\alpha^i$ to $\beta\alpha^{i+1}$, $i \in \{0, \dots, m-1\}$. We show that T is an automorphism of the group. Indeed, using the generator relation we see that $(\beta\alpha)^2 = \beta\alpha\beta\alpha = \alpha\alpha^{-1} = 1$, so $\beta\alpha$ has order two. Moreover, we have $(\beta\alpha)\alpha(\beta\alpha) = (\beta\alpha^2\beta)\alpha = \alpha^{-2}\alpha = \alpha^{-1}$. We conclude that T is an automorphism because the generator relation for the dihedral group for α and involution $\beta\alpha$ is fulfilled.

We now consider the regular subgroup of $\text{GA}(r, 2)$ from [8]. Let α be $((101), A)$ and β be $((001), B)$, where $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

We see that the orders of α and β are 4 and 2 respectively. Moreover $\beta\alpha = ((010), BA)$, where $BA = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ has order two, so $\beta\alpha\beta = \alpha^{-1}$ and the group generated by α and β is isomorphic to D_4 . We have the following: $\beta\alpha^2 = ((110), BA^2)$ and $\beta\alpha^3 = ((100), BA^3)$. Consider the automorphism T for dihedral groups described above: T fixes α^i and sends $\beta\alpha^i$ to $\beta\alpha^{i+1}$, $i \in \{0, 1, 2, 3\}$. Let τ be the permutation induced by the automorphism T . Since $\beta = ((001), B)$, $\beta\alpha = ((010), BA)$, $\beta\alpha^2 = ((110), BA^2)$, $\beta\alpha^3 = ((100), BA^3)$ the bijection τ shifts the following vectors in the cyclic order (001) , (010) , (110) , (100) and fixes any other vector from F^3 .

Let \mathcal{H} be the code with coordinates indexed by vectors of F^3 in the lexicographical order and numbers $\{0, \dots, 7\}$ in the ascending order. Then τ is the permutation $(4, 3, 2, 1)$. We have the following supports of the codewords in \mathcal{H} containing 0:

$$\{0, 1, 2, 3\}, \{0, 1, 4, 5\}, \{0, 1, 6, 7\}, \{0, 2, 4, 6\}, \{0, 2, 5, 7\}, \{0, 3, 4, 7\}, \{0, 3, 5, 6\}, \{0, \dots, 7\}.$$

Since $\tau = (4, 2, 3, 1)$, we have the following supports of codewords of $\tau(\mathcal{H})$ containing 0:

$$\{0, 1, 3, 4\}, \{0, 2, 4, 5\}, \{0, 4, 6, 7\}, \{0, 2, 3, 6\}, \{0, 3, 5, 7\}, \{0, 1, 2, 7\}, \{0, 1, 5, 6\}, \{0, \dots, 7\}.$$

The supports of the codewords of \mathcal{H} and $\tau(\mathcal{H})$ not containing 0 are the complements of those that contain 0 to $\{0, \dots, 7\}$. Then $\tau(\mathcal{H}) \cap \mathcal{H}$ consists of the all-zero and the all-one vectors, so τ has the distension 3. The deficiency of τ is 3 because the codes $\tau(\mathcal{H})$ and \mathcal{H} do not have common codewords of weight 3. By Lemmas 1 and 2 the code $S_{\mathcal{H}, \tau}$ is a propelinear extended perfect code of length 16, rank 14 and the kernel dimension 8.

4. INFINITE SERIES OF NEW PROPELINEAR PERFECT CODES

In this section we construct an infinite series of propelinear codes $S_{\mathcal{H},\tau}$ of prefull rank and the dimension of the kernel $2^{r+1} - 2r - 2$, i.e. the maximum rank and the minimum dimension of kernel that we can obtain by the considered construction. In view of Theorem 2 these codes are new propelinear codes.

Lemma 3. *Let τ be a bijection from F^{r_1} to F^{r_1} such that $\tau(\mathbf{0}) = \mathbf{0}$ and σ be a bijection from F^{r_2} to F^{r_2} , $\sigma(\mathbf{0}) = \mathbf{0}$ with the distensions l_1 and l_2 and the deficiencies k_1 and k_2 respectively. Then the bijection $\tau|\sigma$ from $F^{r_1+r_2}$ to $F^{r_1+r_2}$ has the distension $l_1 + l_2$ and the deficiency $k_1 + k_2$.*

Proof. Consider a codeword x of the extended Hamming code \mathcal{H} of length $2^{r_1+r_2}$, whose coordinates are indexed by the vectors $a|b$, $a \in F^{r_1}$, $b \in F^{r_2}$. The bijection $\tau|\sigma$ acts on the vectors of $F^{r_1+r_2}$, so it could be treated as a permutation on the coordinate positions of \mathcal{H} .

A vector $x \in F^{2^{r_1+r_2}}$ is in \mathcal{H} if and only if

$$\text{supp}(x) = \{a_i|b_i : i \in \{1, \dots, \text{wt}(x)\}\} \text{ is such that } \sum_{i \in \{1, \dots, \text{wt}(x)\}} a_i|b_i = \mathbf{0}.$$

The vector $(\tau|\sigma)(x)$ with the support $\{\tau(a_i)|\sigma(b_i) : i \in \{1, \dots, \text{wt}(x)\}\}$ is in \mathcal{H} if and only if

$$\sum_{i \in \{1, \dots, \text{wt}(x)\}} \tau(a_i) = \mathbf{0} \text{ and } \sum_{i \in \{1, \dots, \text{wt}(x)\}} \sigma(b_i) = \mathbf{0}.$$

In other words, $(\tau|\sigma)(x)$ is in \mathcal{H} if and only if the vectors with the supports $\{\tau(a_i) : i \in \{1, \dots, \text{wt}(x)\}\}$ and $\{\sigma(b_i) : i \in \{1, \dots, \text{wt}(x)\}\}$ are codewords of \mathcal{H}^{r_1} and \mathcal{H}^{r_2} respectively. We conclude that $\dim((\tau|\sigma)(\mathcal{H}) \cap \mathcal{H}) = \dim(\tau(\mathcal{H}^{r_1}) \cap \mathcal{H}^{r_1}) + \dim(\sigma(\mathcal{H}^{r_2}) \cap \mathcal{H}^{r_2})$, so the distension of $\tau|\sigma$ is $l_1 + l_2$.

For a nonzero vector $a|b \in F^{r_1+r_2}$ consider $\text{Star}(a|b)$:

$$\{\{a|b, c'|c'', a + c'|b + c''\} : (c', c'') \in F^{r_1+r_2} \setminus (a|b \cup \mathbf{0})\}.$$

So, $(\tau|\sigma)(\text{Star}(a|b))$ is

$$\{\{\tau(a)|\sigma(b), \tau(c')|\sigma(c''), \tau(a + c')|\sigma(b + c'')\} : (c', c'') \in F^{r_1+r_2} \setminus (a|b \cup \mathbf{0})\}.$$

From this expression we see that the set $(\tau|\sigma)(\text{Star}(a|b))$ is a star of \mathcal{H}' if and only if $\tau(a) + \tau(c') + \tau(a + c') = \mathbf{0}$ and $\sigma(b) + \sigma(c'') + \sigma(b + c'') = \mathbf{0}$ for $c' \in F^{r_1}$, $c'' \in F^{r_2}$. In other words, we have $(\tau|\sigma)(\text{Star}(a|b)) \subset \mathcal{H}'$ if and only if

$$a, b \neq \mathbf{0} \text{ and } \tau(\text{Star}(a)) \subset (\mathcal{H}^{r_1})' \text{ and } \sigma(\text{Star}(b)) \subset (\mathcal{H}^{r_2})' \text{ or}$$

$$a = \mathbf{0}, b \neq \mathbf{0} \text{ and } \sigma(\text{Star}(b)) \subset (\mathcal{H}^{r_2})' \text{ or}$$

$$b = \mathbf{0}, a \neq \mathbf{0} \text{ and } \tau(\text{Star}(a)) \subset (\mathcal{H}^{r_1})'.$$

We conclude that there are total $(2^{r_1-k_1}-1)(2^{r_2-k_2}-1) + 2^{r_1-k_1}-1 + 2^{r_2-k_2}-1 = 2^{r_1+r_2-k_1-k_2}-1$ stars in \mathcal{H}' that are mapped to stars in \mathcal{H}' by $\tau|\sigma$. So, the deficiency of $\tau|\sigma$ is $k_1 + k_2$. □

Direct product construction for regular subgroups of the general affine group [14]. Let G_1 and G_2 be regular subgroups of $\text{GA}(r_1, 2)$ and $\text{GA}(r_2, 2)$

respectively. Given two elements $g_1 = (a, A) \in G_1$ and $g_2 = (b, B) \in G_2$ consider the following element of $\text{GA}(r_1 + r_2, 2)$, which we denote by $g_1|g_2$:

$$(a|b, \begin{pmatrix} A & \mathbf{0}_{r_1, r_2} \\ \mathbf{0}_{r_2, r_1} & B \end{pmatrix}),$$

here $\mathbf{0}_{r_1, r_2}$ and $\mathbf{0}_{r_2, r_1}$ are the all-zero $r_1 \times r_2$ and $r_2 \times r_1$ matrices respectively. It is easy to see that $\{g_1|g_2 : g_1 \in G_1, g_2 \in G_2\}$ is a regular subgroup of $\text{GA}(r_1 + r_2, 2)$. We denote this group by $G_1 \otimes G_2$.

Consider automorphisms T and S of G_1 and G_2 respectively with the induced permutations τ and σ respectively. Define the following permutation $T|S$ of the elements of $G_1 \otimes G_2$: $(T|S)(g_1|g_2) = T(g_1)|S(g_2)$. Obviously, $T|S$ is an automorphism of the group $G_1 \otimes G_2$ and the permutation induced by $T|S$ is $\tau|\sigma$.

Theorem 3. *Let T and S be automorphisms of regular subgroups G_1 and G_2 of $\text{GA}(r_1, 2)$ and $\text{GA}(r_2, 2)$ respectively. Let τ and σ be the permutations induced by T and S with the distensions l_1 and l_2 and the deficiencies k_1 and k_2 respectively. Then $S_{\mathcal{H}, \tau|\sigma}$ is a propelinear extended perfect code of length $2^{r_1+r_2+1}$ with $\text{rank}(S_{\mathcal{H}, \tau|\sigma}) = 2^{r_1+r_2+1} - r_1 - r_2 - 2 + l_1 + l_2$ and $\dim(\text{Ker}(S_{\mathcal{H}, \tau})) = 2^{r_1+r_2+1} - r_1 - r_2 - 2 - k_1 - k_2$.*

Proof. The regular subgroup $G_1 \otimes G_2$ of $\text{GA}(r_1 + r_2, 2)$ obtained by direct product construction has the automorphism $T|S$ with the induced permutation $\tau|\sigma$, so $S_{\mathcal{H}, \tau|\sigma}$ is a propelinear extended perfect code. The desired values for the rank and the dimension of the kernel of the code $S_{\mathcal{H}, \tau|\sigma}$ follow from Lemmas 1, 2 and 3. □

Table 1 contains the values for the distension and the deficiency for the permutations induced by the automorphisms of the regular subgroups of $\text{GA}(r, 2)$ for $3 \leq r \leq 5$. This result was obtained by computer. For any length n , $n \geq 16$ Theorem

	The values for (l, k) , where l is the distension and k is the deficiency of the permutations induced by the automorphisms of the regular subgroups of $\text{GA}(r, 2)$
$r = 3$	$(0,0), (1,2), (2,3), (3,3)$
$r = 4$	$(0,0), (1,2), (2,3), (2,4), (3,3), (3,4), (4,3)$
$r = 5$	$(0,0), (1,2), (1,4), (2,3), (2,4), (2,5), (3,3), (3,4), (3,5), (4,3), (4,4), (4,5), (5,4), (5,5)$

TABLE 1

3 and the data from Table 1 imply the existence of propelinear extended perfect codes of length n of varying rank and kernel and, in particular, codes of prefull rank $n - 1$ and codes with the dimension of the kernel $n - 2 \log n - 2$.

Corollary 2. *For any $r \equiv 0, 2 \pmod{3}$, $r \geq 3$ there is a propelinear extended perfect code $S_{\mathcal{H}, \tau}$ of length 2^{r+1} , $\text{rank}(S_{\mathcal{H}, \tau}) = 2^{r+1} - 2$ and $\dim(\text{Ker}(S_{\mathcal{H}, \tau})) = 2^{r+1} - 2r - 2$. For any $r \equiv 1 \pmod{3}$, $r \geq 3$ there is a propelinear extended perfect code $S_{\mathcal{H}, \tau}$ of length 2^{r+1} , $\text{rank}(S_{\mathcal{H}, \tau}) = 2^{r+1} - 2$ with $\dim(\text{Ker}(S_{\mathcal{H}, \tau})) = 2^{r+1} - 2r - 1$ and there is a propelinear extended perfect code $S_{\mathcal{H}, \tau}$ of rank $(S_{\mathcal{H}, \tau}) = 2^{r+1} - 3$ and $\dim(\text{Ker}(S_{\mathcal{H}, \tau})) = 2^{r+1} - 2r - 2$.*

Proof. We fix $\tau : F^3 \rightarrow F^3$ to be the permutation induced by the automorphism of the regular subgroup G_1 considered in the Example 1. The permutation τ has the distension and the deficiency 3. We vary the permutation σ among the permutations

that are induced by the automorphisms of the regular subgroups G_2 of $\text{GA}(r_2, 2)$ for $r_2 : 3 \leq r_2 \leq 5$ with the maximum distensions and deficiencies. According to Example 1 and Table 1, for $r_2 = 3$ or 5 there are permutations with both the distension and the deficiency equal 3 or 5 respectively. For $r_2 = 4$ there are permutations with the distension 4 and the deficiency 3 and the distension 3 and the deficiency 4.

Let r be $3m + r_2$ for some $m \geq 0$ and $3 \leq r_2 \leq 5$. There is a regular subgroup of $\text{GA}(3m, 2)$ which is the direct product of the m copies of $G_1: G_1 \otimes \dots \otimes G_1$ with the permutation $\tau | \dots | \tau$ induced by the automorphism $T | \dots | T$, where T is the automorphism from Example 1. Using the direct product construction again we obtain a regular subgroup $G_1 \otimes \dots \otimes G_1 \otimes G_2$ of $\text{GA}(3m + r_2, 2)$ that has an automorphism with the induced permutation $\tau | \dots | \tau | \sigma$. By Theorem 3 for $r \equiv 0, 2 \pmod{3}$ the code $S_{\mathcal{H}, \tau | \dots | \tau | \sigma}$ of length 2^{r+1} has rank $2^{r+1} - 1$ and $\dim(\text{Ker}(S_{\mathcal{H}, \tau | \dots | \tau | \sigma})) = 2^{r+1} - 2r - 2$ and for $r \equiv 1 \pmod{3}$ the code $S_{\mathcal{H}, \tau | \dots | \tau | \sigma}$ has rank $2^{r+1} - 2$ and $\dim(\text{Ker}(S_{\mathcal{H}, \tau | \dots | \tau | \sigma})) = 2^{r+1} - 2r - 1$ or rank $2^{r+1} - 3$ and $\dim(\text{Ker}(S_{\mathcal{H}, \tau | \dots | \tau | \sigma})) = 2^{r+1} - 2r - 2$. \square

Remark 2. By Corollary 2 there are the propelinear codes of length $2^{r+1} - 1$ with the dimension of the kernel $2^{r+1} - 2r - 2$. Taking into account Theorem 2 and Lemma 2, for any $r \geq 3$ there are propelinear perfect codes of length $2^{r+1} - 1$ that could not be obtained by Mollard construction.

Remark 3. Applying Theorem 3 iteratively we obtain a relatively large class of nonequivalent propelinear perfect codes of any admissible length more than 7. For example, using data from Table 1, we obtained propelinear perfect codes of length 511 with the size of kernels more than 497 of all possible ranks with the only exception of the full rank. Among these codes at least 32 codes are pairwise nonequivalent as the calculated values for the pairs of rank and the dimension of the kernel are different. Note that there are 51 different pairs of the rank and the dimension of kernel for the perfect codes of length 511 with the dimension of the kernel at least 497, see [1].

REFERENCES

- [1] S. V. Avgustinovich, O. Heden, F. I. Solov'eva, Perfect codes of full rank with big kernels, *Discrete Analysis and Oper. Research*, **1** 8(4) (2001), 3–8 (in Russian). Zbl 1003.94037
- [2] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, Structural properties of binary propelinear codes, *Advances in Mathematics of Communication*, **6** (2012), 329–346. Zbl 1260.94089
- [3] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, On the number of nonequivalent propelinear extended perfect codes. *The Electronic Journal of Combinatorics*, **20**(2) (2013), 37–50. Zbl 1264.94117
- [4] J. Borges, K. T. Phelps, J. Rifà, The rank and kernel of extended 1-perfect Z4-linear and additive non-Z4-linear codes, *IEEE Transactions on Information Theory*, **49** (2003), 2028–2034. Zbl 1282.94085
- [5] J. Borges, J. Rifà, A characterization of 1-perfect additive codes, *IEEE Transactions on Information Theory*, **45** (1999), 1688–1697. Zbl 0957.94032
- [6] G. K. Guskov, I. Yu. Mogilnykh, F. I. Solov'eva, Ranks of propelinear perfect binary codes, *Siberian Electronic Mathematical Reports*, **10** (2013), 443–449. Zbl 1330.94062
- [7] A. R. Hammons, Jr, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The Z4-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Transactions on Information Theory*, **40**(2) (1994), 301–319. Zbl 0811.94039
- [8] P. Hegedus, Regular subgroups of the Affine group, *Journal of Algebra*, **225** (2000), 740–742. Zbl 0953.20040

- [9] D. S. Krotov, Z4-linear Hadamard and extended perfect codes, WCC2001, International Workshop on Coding and Cryptography, *Electronic Notes in Discrete Mathematics*, **6** (2001), 107–112. Zbl 0987.94513
- [10] D. S. Krotov, Z2k-Dual Binary Codes, *IEEE Transactions on Information Theory*, **53** (2007), 1532–1537. Zbl 1205.94121
- [11] D. S. Krotov, V. N. Potapov, Propelinear 1-perfect codes from quadratic functions, *IEEE Transactions on Information Theory*, **60** (2014), 2065–2068. Zbl 1360.94416
- [12] J. Pujol, J. Rifà, F. I. Solov'eva, Construction of Z4-Linear Reed-Muller Codes. *IEEE Transactions on Information Theory*, **55**(1) (2009), 99–104. Zbl 1367.94378
- [13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977. Zbl 0369.94008
- [14] I. Yu. Mogilnykh, A note on regular subgroups of the automorphism group of the linear Hadamard code, *Siberian Electronic Mathematical Reports*, **15** (2018), 1455–1462. Zbl 07052522
- [15] I. Yu. Mogilnykh, F. I. Solov'eva, On separability of the classes of homogeneous and transitive perfect binary codes, *Problems of Information Transmission*, **51** (2015), 139–147. Zbl 1339.94096
- [16] M. Mollard, A generalized parity function and its use in the construction of perfect codes, *SIAM J. Alg. Discrete Math.*, **7**(1) (1986), 113–115. Zbl 0585.94015
- [17] P. R. J. Östergård, K. T. Phelps, O. Pottonen, The perfect binary one-error-correcting codes of length 15: Part II-properties, *IEEE Transactions on Information Theory* **56** (2010), 2571–2582. Zbl 1366.94606
- [18] K. T. Phelps, A combinatorial construction of perfect codes, *SIAM J. Alg. Disc. Meth.*, **4** (1983), 398–403. Zbl 0549.94029
- [19] K. T. Phelps, J. Rifà, On binary 1-perfect additive codes: some structural properties, *IEEE Transactions on Information Theory*, **48** (2002), 2587–2592. Zbl 1062.94048
- [20] J. Rifà, J. Pujol, Translation-invariant propelinear codes, *IEEE Transactions on Information Theory*, **43** (1997), 590–598. Zbl 0876.94040
- [21] V. N. Potapov, A lower bound for the number of transitive perfect codes, *Journal of Application and Industrial Mathematics*, **1**(3) (2007), 373–379. Zbl 1249.94061
- [22] F. I. Solov'eva, On binary nongroup codes, *Methody Discretnogo Analiza*, **37** (1981), 65–75 (in Russian). Zbl 0524.94014

IVAN YUREVICH MOGILNYKH
 TOMSK STATE UNIVERSITY,
 REGIONAL SCIENTIFIC AND EDUCATIONAL MATHEMATICAL CENTER,
 36, LENINA AVE.,
 TOMSK, 634050, RUSSIA,
 SOBOLEV INSTITUTE OF MATHEMATICS,
 4, KOPTYUGA AVE.,
 NOVOSIBIRSK, 630090, RUSSIA
E-mail address: `ivmog@math.nsc.ru`

FAINA I. SOLOV'eva
 SOBOLEV INSTITUTE OF MATHEMATICS,
 4, KOPTYUGA AVE.,
 NOVOSIBIRSK, 630090, RUSSIA
E-mail address: `sol@math.nsc.ru`