q-ary propelinear perfect codes from the regular subgroups of the $GA(r, q)$ and their ranks[⋆]

Ivan Mogilnykh

Sobolev Institute of Mathematics
ivmog84@gmail.com

Abstract. We propose a new method of constructing q-ary propelinear perfect codes. The approach utilizes permutations of the fixed length q-ary vectors that arise from the automorphisms of the regular subgroups of the affine group. For any prime q it is shown that the new class contains an infinite series of q-ary propelinear perfect codes of varying ranks.

Keywords: q-ary perfect code · propelinear code · regular action · general affine group · permutations on finite vector spaces

1 Introduction

Propelinear codes were introduced by Rifà, Basart and Huguet in [15] and provide a general view on linear, additive (including Z_4-linear codes) and other classes of codes. There are instances where propelinear approach yields codes with larger size than linear ones. In particular, this holds for Preparata codes, and all known classes of these codes are shown to be propelinear [5], [3], [18].

Unlike binary codes, which are well-studied, there are rather few works devoted to q-ary propelinear codes, for $q \geq 3$. We refer to [7], [2], [8], [1] for q-ary perfect, MDS and generalized Hadamard propelinear codes.

In this work we propose a method of constructing q-ary perfect codes based on the automorphisms of the regular subgroups of the general affine group $GA(r, q)$ and a Mollard construction [12]. For $q = 2$ this approach which uses particular case of Solov'eva construction was the topic of study of works [10] and [11]. In [10] the values for the ranks and the kernels of these codes were found. A criteria for coordinate transitivity of resulting code in terms of double cosets of $GL(r, 2)$ was suggested in [11]. An infinite series of binary extended perfect codes were constructed in [11] with automorphism groups acting transitively on the code and transitively on the set of its neighbors. Codes with such exquisite algebraic properties are known as neighbor-transitive [4].

Basic definitions are given in Section 2. In Section 3.1 the general Mollard approach [12] is described in terms of work [16]. The construction involves permutations of the vectors of $\mathbb{F}_q^r$. In Section 3.2 we focus on the case when the

[⋆] This work was funded by the Russian Science Foundation under grant 22-21-00135, https://rscf.ru/en/project/22-21-00135/

permutations arise from the automorphisms of regular subgroups of $GA(r,q)$ and then the resulting perfect codes are propelinear. Section 4 is on ranks of the codes from general Mollard construction, which could be described in terms of such permutations of $\mathbb{F}_q^r$. Sections 5 and 6 are devoted to obtaining propelinear perfect codes of various ranks. The idea behind the last two Sections is a natural iterative approach for regular subgroups of $GA(r,q)$.

2 Definitions

The all-zeros and all-ones vectors of the vector space $\mathbb{F}_q^n$ are denoted as $\mathbf{0}$, $\mathbf{1}$ and their length will be clear from the context. The concatenation of vectors x and y is denoted as $x|y$. For q-ary codes C and D we use the following notation:

$$C \times D = \{(x|y) : x \in C, y \in D\}.$$

A q-ary code of length n is called *perfect* if it has minimum distance 3 and its size is $\frac{q^n}{1+(q-1)n}$. *The automorphism group* $Aut(\mathbb{F}_q^n)$ of $\mathbb{F}_q^n$ is defined as the group of all isometries of $\mathbb{F}_q^n$, i.e. the automorphism group of the corresponding Hamming graph $H(n,q)$. *The automorphism group* $Aut(C)$ of a code C is the setwise stabilizer of C in $Aut(\mathbb{F}_q^n)$. A q-ary *propelinear* code (original definition was given in [15]) is a q-ary code whose automorphism group contains a subgroup acting regularly on the codewords of C. The *rank* of a q-ary code C is is the dimension of its linear span over $\mathbb{F}_q$. We denote the latter by $< C >$. The rank is an important invariant for distinguishing inequivalence of codes. For a thorough study of ternary perfect codes of length 13 we refer to [9], where a large class of codes from construction [16] were classified, and the values of their ranks were described. The ranks of q-ary perfect codes were studied in [14]. We note that there are no results on ranks of propelinear perfect codes for $q \geq 3$ and adress their study in this paper.

The *general affine group* $GA(r,q)$ is the group of all transformations (a, M), where $a \in \mathbb{F}_q^r$, $M \in GL(r,q)$, acting on the column-vectors $b \in \mathbb{F}_q^r$ as follows: $(a,M)(b) = a + Mb$, with respect to the composition:

$$(a,M)(b,M') = (a + Mb, MM'). \tag{1}$$

A subgroup of $GA(r,q)$ is called *regular* if it acts regularly on the vectors of $\mathbb{F}_q^r$with respect to the above defined action. Apart from the translation group $(\mathbb{F}_q^r, +)$ there are many other regular subgroups of $GA(r,q)$. In Example 1 of this paper we consider a regular subgroup of $GA(2,q)$ for a prime q, which is isomorphic to $(\mathbb{F}_q^r, +)$ but not conjugate in $GA(2,q)$.

3 The construction of q-ary propelinear perfect codes from regular subgroups of $GA(r,q)$

3.1 Concatenation construction for q-ary perfect codes

The construction for propelinear perfect codes is based on more a general method of Mollard [12]. We use the representation of this approach from work [16] by

Romanov. Let H_C be a parity check matrix of q-ary Hamming code C of length $\frac{q^r-1}{q-1}$, H' be a $r \times q^r$ matrix whose columns are all q-ary vectors of length r. A $(r+1) \times \frac{q^r-1}{q-1}$ parity check matrix of q-ary Hamming code of length $\frac{q^{r+1}-1}{q-1}$ could be taken in a block form:

$$\left(\begin{array}{c|c} \mathbf{0} & \mathbf{1} \\ \hline H_C & H' \end{array}\right). \tag{2}$$

For any column-vector $a, a \in \mathbb{F}_q^r$ we use the notation below for a coset C_a of the code C:

$$C_a = \{x : x \in \mathbb{F}_q^{\frac{q^r-1}{q-1}}, H_C x^T = a\}. \tag{3}$$

We also denote by D the linear code with the following $r+1 \times q^r$ parity check matrix:

$$H_D = \begin{pmatrix} \mathbf{1} \\ H' \end{pmatrix}. \tag{4}$$

We index the positions of D with the columns of the parity check matrix H_D and the position has index a, where a is a column-vector of $\mathbb{F}_q^r$, if $\begin{pmatrix} 1 \\ a \end{pmatrix}$ is the corresponding column of H_D. Denote by e_a the vector of length $\frac{q^r-1}{q-1}$ of weight 1 with one in the position indexed by vector a. For $a \in \mathbb{F}_q^r$ denote by D_a the coset $D + e_{\mathbf{0}} - e_a$. Note that for any a the coset D_a fulfills overall parity check, i.e. for any $y \in D_a$ we have $\sum\limits_{i=1}^{q^r} y_i = \mathbf{0}$.

Theorem 1. *[12][16] For any $q \geq 2$ and any permutation τ of the vectors of $\mathbb{F}_q^r$ the code*

$$S_\tau = \bigcup_{a \in \mathbb{F}_q^r} C_a \times D_{\tau(a)}$$

is a q-ary perfect code of length $\frac{q^{r+1}-1}{q-1}$.

Throughout the paper we assume that τ fixes the all-zero vector. We note that the Hamming code with the parity check matrix (2) coincides with $\bigcup\limits_{a \in \mathbb{F}_q^r} C_a \times D_a$.

3.2 Concatenation construction for propelinear perfect codes from the regular subgroups of $GA(r, q)$

Let G be a regular subgroup of the general affine group $GA(r, q)$. Since G acts regularly on $\mathbb{F}_q^r$, for any a in $\mathbb{F}_q^r$ there is an element of G that sends the all-zero vector $\mathbf{0}$ to a. We denote this element by g_a. Since $g_a(\mathbf{0}) = a$ we see that the translation part of g_a is a:

$$g_a = (a, M_a) \tag{5}$$

for some nonsingular matrix M_a. Thus the elements of any regular subgroup of $GA(r, q)$ are indexed by the vectors of $\mathbb{F}_q^r$.

Let T be an automorphism of G. The permutation τ of the vectors of $\mathbb{F}_q^r$ such that for any $a \in \mathbb{F}_q^r$ $g_{\tau(a)} = T(g_a)$, is called the permutation *induced by the automorphism* T. As any automorphism fixes the neutral element, the permutation τ induced by any automorphism fulfills the equality $\tau(\mathbf{0}) = \mathbf{0}$. The following result was proved in [10] for $q = 2$. The ideas behind the proofs are similar and we skip the proof due to the lack of space.

Theorem 2. *Let τ be the permutation induced by an automorphism of a regular subgroup of $GA(r,q)$. Then S_τ is a q ary propelinear perfect code of length $\frac{q^{r+1}-1}{q-1}$.*

4 The ranks of the codes obtained by concatenation construction

Let τ be a permutation of the vectors of $\mathbb{F}_q^r$ that fixes $\mathbf{0}$. Since the positions of the code D are indexed by the vectors of $\mathbb{F}_q^r$, τ is also a permutation of the positions of vectors of D. We define *the defect* of a permutation τ to be $dim(D) - dim(D \cap \tau(D))$. We have the following equality

$$dim(D) - dim(D \cap \tau(D)) = rank \begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix} - dim(D^\perp), \qquad (6)$$

where $D^\perp$ is the dual code of D, i.e. the code whose generator matrix is the parity check matrix H_D for the code D.

Consider the code $S_\tau = \bigcup_{a \in \mathbb{F}_q^r} C_a \times D_{\tau(a)}$, described in Section 3.1. The main result of this section is the expression for the rank of S_τ in terms of defect of τ, which is given by exhibiting an explicit basis of the linear span $< S_\tau >$.

For any $a \in \mathbb{F}_q^r$, we choose a representative of C_a which we denote by x_a throughout this section. By definition of the coset C_a, we have $H_C(x_a)^T = a$. The leader $e_{\mathbf{0}} - e_a$ of the coset D_a is denoted by y_a and we have

$$H_D y_a^T = -\begin{pmatrix} 0 \\ a \end{pmatrix}.$$

In view of the considered numeration of cosets of C and D via the vectors of $\mathbb{F}_q^r$, we have the following natural correspondence for linear dependencies in the coset spaces of C and D.

Proposition 1. *Let τ be a permutation of $\mathbb{F}_q^r$, fixing $\mathbf{0}$. For any elements $\alpha_a \in \mathbb{F}_q$, $a \in \mathbb{F}_q^r$ we have the following*

$$\sum_{a \in \mathbb{F}_q^r} \alpha_a x_a \in C \quad \textit{if and only if} \quad \sum_{a \in \mathbb{F}_q^r} \alpha_a y_{\tau(a)} \in \tau(D).$$

Proof. The permutation τ fixes $\mathbf{0}$ and acts on the positions of $\mathbb{F}_q^r$ that are indexed by columns of H_D, i.e. the vectors of $\mathbb{F}_q^r$. Therefore we have:

$$\sum_{a \in \mathbb{F}_q^r} \alpha_a y_{\tau(a)} = \sum_{a \in \mathbb{F}_q^r} \alpha_a (e_{\mathbf{0}} - e_{\tau(a)}) = \sum_{a \in \mathbb{F}_q^r} \alpha_a (e_{\tau(\mathbf{0})} - e_{\tau(a)}) = \tau(\sum_{a \in \mathbb{F}_q^r} \alpha_a y_a).$$

It remains to show that

$$\sum_{a\in\mathbb{F}_q^r} \alpha_a y_a \in D \Leftrightarrow \sum_{a\in\mathbb{F}_q^r} \alpha_a x_a \in C.$$

Because the syndrome of $x_a \in C_a$ is $H_C x_a^T = a$, see (3), we have that

$$\sum_{a\in\mathbb{F}_q^r} \alpha_a x_a \in C \Leftrightarrow H_C(\sum_{a\in\mathbb{F}_q^r} \alpha_a x_a)^T = \sum_{a\in\mathbb{F}_q^r} \alpha_a a = \mathbf{0}. \tag{7}$$

Since $H_D(y_a)^T = -\begin{pmatrix} 0 \\ a \end{pmatrix}$, we obtain that $\sum_{a\in\mathbb{F}_q^r} \alpha_a y_a$ is in D if and only if

$$H_D(\sum_{a\in\mathbb{F}_q^r} \alpha_a y_a)^T = -\begin{pmatrix} 0 \\ \sum_{a\in\mathbb{F}_q^r} \alpha_a a \end{pmatrix} = \mathbf{0}.$$

This, combined with (7), gives the required:

$$\sum_{a\in\mathbb{F}_q^r} \alpha_a x_a \in C \Leftrightarrow \sum_{a\in\mathbb{F}_q^r} \alpha_a a = \mathbf{0} \Leftrightarrow \sum_{a\in\mathbb{F}_q^r} \alpha_a y_a \in D.$$

□

In what follows we denote by $z_1 \ldots, z_{dim(C)}$ a basis of C, where $dim(C) = \frac{q^r-1}{q-1} - r$ and by $v_1 \ldots, v_l$ we denote the vectors that complete a basis of $D \cap \tau(D)$ to a basis of D. Note that here $l = dim(D) - dim(D) \cap dim(\tau(D))$ is the defect of the permutation τ.

We introduce three sets of vectors

$$B = \{(x_a|y_{\tau(a)}) : a \in \mathbb{F}_q^r \setminus \mathbf{0}\}, B' = \{(z_i|\mathbf{0}) : i \in \{1, \ldots, dim(C)\}\},$$

$$B'' = \{(\mathbf{0}|v_j) : j \in \{1, \ldots, l\}\}.$$

We see that

$$|B| + |B'| + |B''| = (q^r - 1) + (\frac{q^r - 1}{q - 1} - r) + l = \frac{q^{r+1} - 1}{q - 1} - r - 1 + l. \tag{8}$$

We will now show that $B \cup B' \cup B''$ is a basis of the linear span S_τ.

Lemma 1. *The set $B \cup B' \cup B''$ is linearly independent.*

Proof. Clearly the sets $B \cup B'$ and B'' are linearly independent. Suppose that $B \cup B' \cup B''$ is linearly dependent and consider a nonzero vector of the space $< B \cup B' > \cap < B'' >$. In view of B, B' and B'' introduced above, the vector can be represented in two ways

$$\sum_{a\in\mathbb{F}_q^r\setminus\mathbf{0}} \alpha_a(x_a|y_{\tau(a)}) + \sum_{i\in\{1,\dots,dim(C)\}} \beta_i(z_i|\mathbf{0}) = \sum_{j\in\{1,\dots,l\}} \gamma_j(\mathbf{0}|v_j)$$

for some $\alpha_a, \beta_i, \gamma_j \in \mathbb{F}_q$ and for all $i \in \{1,\dots,dim(C)\}$, $j \in \{1,\dots,l\}$, $a \in \mathbb{F}_q^r$. Equivalently, we have two equalities:

$$\sum_{a\in\mathbb{F}_q^r\setminus\mathbf{0}} \alpha_a x_a + \sum_{i\in\{1,\dots,dim(C)\}} \beta_i z_i = \mathbf{0},$$

$$\sum_{a\in\mathbb{F}_q^r\setminus\mathbf{0}} \alpha_a y_{\tau(a)} = \sum_{j\in\{1,\dots,l\}} \gamma_j v_j.$$

Since z_i's are in C, the first of these equalities implies that

$$\sum_{a\in\mathbb{F}_q^r\setminus\mathbf{0}} \alpha_a x_a \in C. \tag{9}$$

By the choice of $\{v_j\}_{j\in\{1,\dots,l\}}$ they complete a basis of $D\cap\tau(D)$ to a basis of D. Therefore their nontrivial linear combination $\sum\limits_{j\in\{1,\dots,l\}} \gamma_j v_j$ is never in $\tau(D)$. Then the second equality gives that

$$\sum_{a\in\mathbb{F}_q^r\setminus\mathbf{0}} \alpha_a y_{\tau(a)} \notin \tau(D). \tag{10}$$

Since (9) and (10) do not hold simultaneously by Proposition 1, we obtain a contradiction.

□

Lemma 2. *Any vector of $B \cup B' \cup B''$ is in S_τ and $S_\tau \subseteq < B \cup B' \cup B'' >$.*

Proof. Any vector of B is $(x_a|y_{\tau(a)})$ for some $a \in \mathbb{F}_q^r$ and therefore it is in $S_\tau = \bigcup\limits_{a\in\mathbb{F}_q^r} C_a \times D_{\tau(a)}$, so $B \subset S_\tau$. The set B' is a basis $C \times 0$, therefore it is included in S_τ, whereas B'' completes a basis of $\mathbf{0} \times (\tau(D) \cap D)$ to a basis of $\mathbf{0} \times D$ and therefore $B'' \subset C \times D \subset S_\tau$. Since S_τ is the union of the cosets of $C \times D$ with representatives $(x_a|y_{\tau(a)})$, $a \in \mathbb{F}_q^r$, the said above implies that it remains to prove that $\mathbf{0} \times (\tau(D) \cap D)$ is contained in the span of $B \cup B'$.

Given a vector $(\mathbf{0}|w)$, $w \in \tau(D) \cap D$ we will show that it is the sum of two vectors from $< B >$ and $< B' >$. Recall that the parity check matrix H_D of D has an all-ones row, see (4). So, the code D, as well as $\tau(D)$, are subcodes of the supercode with the parity check matrix $(1,\dots,1)$. It is not hard to see that the vectors $y_{\tau(a)} = e_{\mathbf{0}} - e_{\tau(a)}$, for all $a \in \mathbb{F}_q^r \setminus \mathbf{0}$ form a basis of the supercode. We consider a basis decomposition of $w \in \tau(D) \cap D$ on $y_{\tau(a)}$'s:

$$w = \sum_{a\in\mathbb{F}_q^r\setminus\mathbf{0}} \alpha_a y_{\tau(a)}, \tag{11}$$

for some $\alpha_a \in \mathbb{F}_q$, $a \in \mathbb{F}_q^r$.

Take the vector $\sum\limits_{a\in\mathbb{F}_q^r\backslash\mathbf{0}} \alpha_a(x_a|y_{\tau(a)})$, $w \in \tau(D)\cap D$ in $< B >$, which is the linear combination of the vectors $(x_a|y_{\tau(a)})$, $a \in \mathbb{F}_q^r\backslash\mathbf{0}$ from B with the coeffcients α_a's. From the equality (11) we see that the right side of this vector is w:

$$\sum_{a\in\mathbb{F}_q^r\backslash\mathbf{0}} (\alpha_a x_a|\alpha_a y_{\tau(a)}) = (\sum_{a\in\mathbb{F}_q^r\backslash\mathbf{0}} \alpha_a x_a|w) \in < B > . \tag{12}$$

By the choice of the vector w, it is in $\tau(D)$. Because $w = \sum\limits_{a\in\mathbb{F}_q^r\backslash\mathbf{0}} \alpha_a y_{\tau(a)}$, by Proposition 1 the vector $\sum\limits_{a\in\mathbb{F}_q^r\backslash\mathbf{0}} \alpha_a x_a$ is in C. Because B' is a basis of $C\times 0$ we have that

$$\sum_{a\in\mathbb{F}_q^r\backslash\mathbf{0}} (\alpha_a x_a|\mathbf{0}) \in < B' > .$$

This, combined with (12), gives that $(\mathbf{0}|w)$ is in $< B\cup B' >$. We conclude that $C\times D$ and S_τ is a subset of the span of $B\cup B'\cup B''$.

□

From Lemmas 1 and 2 and equality (8) we obtain the following.

Theorem 3. *Let τ be a permutation of the vectors of $\mathbb{F}_q^r$ with defect l such that $\tau(\mathbf{0}) = \mathbf{0}$. Then the rank of S_τ of length $\frac{q^{r+1}-1}{q-1}$ is equal to $\frac{q^{r+1}-1}{q-1} - r - 1 + l$.*

5 The defect of the iteration of permutations

Let τ_1 and τ_2 be permutations of $\mathbb{F}_q^{r_1}$ and $\mathbb{F}_q^{r_2}$ respectively, $\tau_1(\mathbf{0}) = \mathbf{0}$, $\tau_2(\mathbf{0}) = \mathbf{0}$. We represent any column-vector of $\mathbb{F}_q^{r_1+r_2}$ as a concatenation $\binom{a}{b}$ of some column-vectors $a \in \mathbb{F}_q^{r_1}$ and $b \in \mathbb{F}_q^{r_2}$. *The iteration of permutations* τ_1 and τ_2, denoted $\tau_1|\tau_2$ acts on the vectors of $\mathbb{F}_q^{r_1+r_2}$ as follows:

$$(\tau_1|\tau_2)\tbinom{a}{b} = \tbinom{\tau_1(a)}{\tau_2(b)}, \text{ for all } a \in \mathbb{F}_q^{r_1}, b \in \mathbb{F}_q^{r_2}. \tag{13}$$

We show that the iterations of permutations that are induced by automorphisms of regular subgroups of $GA(r_1, q)$ and $GA(r_2, q)$ is a permutation induced by an automorphism of a certain regular subgroup of $GA(r_1+r_2, q)$. Let G_1 and G_2 be regular subgroups of $GA(r_1, q)$ and $GA(r_2, q)$. For elements $(a, M) \in G_1$ and $(b, M') \in G_2$ consider the following affine transformation from $GA(r_1 + r_2, q)$ which we denote by $(a, M_1) \otimes (b, M_2)$:

$$(\tbinom{a}{b}, \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}).$$

It is not hard to see that the direct product $\{(a, M_1) \otimes (b, M_2) : (a, M_1) \in G_1, (b, M_2) \in G_2\}$ of the groups G_1 and G_2 is a regular subgroup of $GA(r_1+r_2, q)$, see e.g. [13][Section 6]. Denote this group by $G_1 \otimes G_2$.

Let T_1 and T_2 be automorphisms of the groups G_1 and G_2 with induced permutations τ_1 and τ_2 respectively. We define the permutation $T_1 \otimes T_2$ on the elements of $G_1 \otimes G_2$ as follows: $(T_1 \otimes T_2)(g_1 \otimes g_2) = T_1(g_1) \otimes T_2(g_2)$. It is obvious that $T_1 \otimes T_2$ is an automorphism of the group $G_1 \otimes G_2$ and the permutation $T_1 \otimes T_2$ of $\mathbb{F}_q^{r_1+r_2}$ is $\tau_1|\tau_2$, defined earlier in (13). Thus we obtain the following.

Proposition 2. *Let τ_1 and τ_2 be permutations of $\mathbb{F}_q^{r_1}$ and $\mathbb{F}_q^{r_2}$ induced by automorphisms of regular subgroups of $GA(r_1, q)$ and $GA(r_2, q)$, $q \geq 2$. Then $\tau_1|\tau_2$ is the permutation induced by an automorphism of the regular subgroup $G_1\ G_2$ of $GA(r_1 + r_2, q)$ and the code $S_{\tau_1|\tau_2}$ is propelinear.*

We leave the following theorem without proof.

Theorem 4. *Let τ_1 and τ_2 be permutations of $\mathbb{F}_q^{r_1}$ and $\mathbb{F}_q^{r_2}$, $q \geq 2$ with defects l_1 and l_2, respectively, such that $\tau_1(\mathbf{0}) = \mathbf{0}$, $\tau_2(\mathbf{0}) = \mathbf{0}$. Then the defect of the permutation $\tau_1|\tau_2$ is $l_1 + l_2$.*

6 An infinite series of propelinear perfect codes with different ranks

We start this section with an example.

Example 1. Let q be a prime, $q \geq 3$. We will now construct a regular subgroup of $GA(2, q)$ isomorphic to Z_q^2 but not conjugate to the translation group $(\mathbb{F}_q^2, +)$ in $GA(2, q)$. We then show that there is an automorphism of this group with induced permutation of the vectors $\mathbb{F}_q^r$ having defect 2.

Consider the following affine transformations

$$g = (\tbinom{1}{0}, Id), h = (\tbinom{0}{1}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}).$$

It is not hard to see that g and h commute. Moreover, the following holds:

$$g^i h^j = (\tbinom{i}{0}, Id)(\tbinom{j(j-1)}{j}, \begin{pmatrix} 1 & 2j \\ 0 & 1 \end{pmatrix}) = (\tbinom{i+j(j-1)}{j}, \begin{pmatrix} 1 & 2j \\ 0 & 1 \end{pmatrix}). \tag{14}$$

For distinct pairs (i, j) and (i', j') the vectors $\tbinom{i+j(j-1)}{j}$ and $\tbinom{i'+j'(j'-1)}{j'}$ are different. Therefore the group spanned by g and h is a regular subgroup of $GA(2, q)$, isomorphic to Z_q^2. Consider the permutation T of the elements of the subgroup spanned by g and h defined as follows:

$$T(g^i h^j) = g^j h^i$$

for all $i, j \in \{0, \ldots, q-1\}$. Since the g and h commute, the involution T is an automorphism of the group spanned by g and h. By definition, the induced permutation τ of the automorphism T is such that $\tau(a) = b$ if $T((a, M)) = (b, M')$ where (a, M) and (b, M') are elements of the considered regular subgroup. From (14) we have

$$g^i h^j = (\tbinom{i+j(j-1)}{j}, \begin{pmatrix} 1 & 2j \\ 0 & 1 \end{pmatrix})$$

and because g and h commute, we obtain

$$h^i g^j = (\binom{j+i(i-1)}{i}, \begin{pmatrix} 1 & 2i \\ 0 & 1 \end{pmatrix})$$

for all $i, j \in \{0, \ldots, q-1\}$ and therefore we have

$$\tau\binom{i+j(j-1)}{j})) = \binom{j+i(i-1)}{i}.$$

In particular if pairs (i, j) are equal to $(1, 0)$, $(0, 1)$, $(-1, -2)$ and $(0, 2)$, we obtain

$$\tau\binom{1}{0} = \binom{0}{1}, \tau\binom{0}{1} = \binom{1}{0}, \tau\binom{5}{-2} = \binom{0}{-1}, \tau\binom{2}{2} = \binom{2}{0}. \qquad (15)$$

Using (6) we find the defect of τ, i.e. $rank \begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix} - dim(D^{\perp}) = rank \begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix} - 3$. Since all-ones vectors are rows of both H_D and $\tau(H_D)$, we have that

$$rank \begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix} = 1 + rank \begin{pmatrix} \mathbf{0} & a^2 & \ldots & a^{q^2} \\ \mathbf{0} & \tau(a^2) & \ldots & \tau(a^{q^2}) \end{pmatrix},$$

where $a^2, \ldots, a^{q^2}$ are nonzero vectors of $\mathbb{F}_q^2$. We take the first four nonzero a^i's as follows:

$$a^2 = \binom{1}{0}, a^3 = \binom{0}{1}, a^4 = \binom{5}{-2}, a^5 = \binom{2}{2}.$$

From (15) applying elementary transformations to the rows of the matrix we see that

$$rank \begin{pmatrix} \mathbf{0} & a^2 & \ldots & a^{q^2} \\ \mathbf{0} & \tau(a^2) & \ldots & \tau(a^{q^2}) \end{pmatrix} = rank \begin{pmatrix} 1 & 0 & 5 & 2 & \ldots \\ 0 & 1 & -2 & 2 & \ldots \\ 0 & 1 & 0 & 2 & \ldots \\ 1 & 0 & -1 & 0 & \ldots \end{pmatrix} = rank \begin{pmatrix} 1 & 0 & 5 & 2 & \ldots \\ 0 & 1 & -2 & 2 & \ldots \\ 0 & 0 & 2 & 0 & \ldots \\ 0 & 0 & 6 & 2 & \ldots \end{pmatrix} =$$

$$= 4$$

and conclude that τ is of defect 2.

Theorem 5. *For all prime $q, q \geq 3$, $r \geq 2$ and $i \in \{0, \ldots, \lfloor r/2 \rfloor\}$ there is a propelinear q-ary perfect code S_τ of length $\frac{q^{r+1}-1}{q-1}$ and rank $\frac{q^{r+1}-1}{q-1} - r - 1 + 2i$.*

Proof. Let τ be an induced permutation of $\mathbb{F}_q^2$ with defect 2 from Example 1. The permutation $\tau|\ldots|\tau|id|\ldots|id$ of $\mathbb{F}_q^r$, where τ is taken i times, and identity is taken $r-2i$ times. From Proposition 2 the code $S_{\tau|\ldots|\tau|id|\ldots|id}$ is propelinear. In view of Theorem 4 the defect of $\tau|\ldots|\tau|id|\ldots|id$ is $2i$, so from Theorem 3 we obtain the desired value for rank.

□

References

1. Armario J., Bailera I., Egan R., Generalized Hadamard full propelinear codes, Designs, Codes and Cryptography, 2021, V. 89, P. 599–615.
2. Borges J., Mogilnykh I.Y., Rifà J., Solov'eva F. I., On the number of nonequivalent propelinear extended perfect codes, Electr. J. Combin., 2013, V. 20, N. 2, P. 1–14.
3. Borges J., Phelps K. P., Rifà J., Zinoviev V. A., On Z_4 -linear Preparata- like and Kerdock-like codes, IEEE Trans. On Information Theory, 2003, V. 49, N. 11, P. 2834–2843.
4. Gillespie N. I., Praeger C. E., New characterisations of the Nordstrom–Robinson codes, Bulletin of the London Mathematical Society, 2017, V. 58, P. 320–330.
5. Hammons A. R., Jr, Kumar P. V., Calderbank A. R., Sloane N. J. A. , Sole P., The Z_4-Linearity of Kerdock, Preparata, Goethals and Related Codes, IEEE Trans. on Information Theory, 1994, V. 13, N. 2, P. 301–319.
6. Pellegrini M.A., Tamburini Bellani M.C., More on regular subgroups of the affine group, Linear Algebra and its Applications, 2016, V. 505. P. 126–151.
7. Krotov D. S., Potapov V. N., Propelinear 1-perfect codes from quadratic functions, IEEE Trans. Inform. Theory, 2014, V. 60, N. 4, P. 2065–2068.
8. Krotov D. S., Potapov V. N., Constructions of transitive latin hypercubes, European Journal of Combinatorics, 2016, V. 54, P. 51–64.
9. Krotov D. S., Shi M., An enumeration of 1-perfect ternary codes, arxiv.org/abs/2110.06305.
10. Mogilnykh I. Yu., Solov'eva F. I., A concatenation construction for propelinear perfect codes from regular subgroups of GA(r,2), Siberian Electronic Mathematical Reports, 2019, V. 16, P. 1689–1702.
11. Mogilnykh I. Yu., Solov'eva F. I., Coordinate transitivity of a class of extended perfect codes and their SQS, Siberian Electronic Mathematical Reports, 2020, V. 17, P. 1451–1462.
12. Mollard M. Une novelle famille de 3-codes parfaits sur GF(q), Discrete Mathematics, 1984, V. 49, P. 209–212.
13. Pellegrini M.A., Tamburini Bellani M.C., More on regular subgroups of the affine group Linear Algebra and its Applications, 2016, V. 505, P. 126–151.
14. Phelps K. T., Villanueva M., Ranks of q-Ary 1-Perfect Codes, Designs, Codes and Cryptography, 2002, V. 27, P. 139–144.
15. Rifà J., Basart J. M., Huguet L., On completely regular propelinear codes, Proc. 6th Int. Conference, AAECC-6, 1989, LNCS, V. 357, P. 341–355.
16. A. M. Romanov, On non-full-rank perfect codes over finite fields, Designs, Codes and Cryptography, 2019, V. 87, N. 5, P. 995–1003.
17. Solov'eva F. I., On binary nongroup codes, Methody Discretnogo Analiza, 1981, V. 37, P. 65–75 (in Russian).
18. Zinoviev V. A. , Zinoviev D. V., Generalized Preparata codes and 2-resolvable Steiner quadruple systems, Problems Inform. Transmission, 2016, V. 52, N. 2, 114–133