Res. Math. **29**(2), 2021, p. 28–43
doi:10.15421/242107
ISSN (Print) 2664-4991
ISSN (Online) 2664-5009

UDK 519.688, 512.54

V. A. Olshevska*

* National University of Kyiv-Mohyla Academy,
Kyiv 04070. *E-mail: v.olshevska@ukma.edu.ua*

Permutation codes over Sylow 2-subgroups $Syl_2(S_{2^n})$ of symmetric groups S_{2^n}

Abstract. The permutation code (or the code) is well known object of research starting from 1970s. The code and its properties is used in different algorithmic domains such as error-correction, computer search, etc. It can be defined as follows: the set of permutations with the minimum distance between every pair of them. The considered distance can be different. In general, there are studied codes with Hamming, Ulam, Levensteins, etc. distances.

In the paper we considered permutations codes over 2-Sylow subgroups of symmetric groups with Hamming distance over them. For this approach representation of permutations by rooted labeled binary trees is used. This representation was introduced in the previous author's paper. We also study the property of the Hamming distance defined on permutations from Sylow 2-subgroup $Syl_2(S_{2^n})$ of symmetric group S_{2^n} and describe an algorithm for finding the Hamming distance over elements from Sylow 2-subgroup of the symmetric group with complexity $O(2^n)$.

The metric properties of the codes that are defined on permutations from Sylow 2-subgroup $Syl_2(S_{2^n})$ of symmetric group S_{2^n} are studied. The capacity and number of codes for the maximum and the minimum nontrivial distance over codes are characterized.

Key words: permutation codes, Sylow 2-subgroup, symmetric group, Hamming distance

Анотація. Починаючи із 1970-х років коди, побудовані на підстановках, та їх властивості широко досліджуються у різних сферах. Під кодом на групі підстановок розуміють множину елементів із групи S_n, де довільна пара із множини має відстань не меншу від заданої. При цьому можуть використовувати як різні підгрупи симетричної групи, так і різні метрики, наприклад, Хеммінга, Улама, Левенштейна тощо. У статті розглядаються коди підстановок із силовської 2-підгрупи $Syl_2(S_{2^n})$ симетричної групи S_{2^n} з відстанню Хеммінга d_H над ними. Для їх дослідження використано зв'язок групи $Syl_2(S_{2^n})$ із групою бінарних кореневих n-рівневих дерев з мітками $LT_{2,n}$. Також описано властивості відстані Хеммінга на підстановках із силовської 2-підгрупи $Syl_2(S_{2^n})$ симетричної групи S_{2^n} та побудовано алгоритм пошуку відстані Хеммінга для підстановок групи, що має складність $O(2^n)$. Окрім того, досліджено метричні властивості кодів на підстановках із $Syl_2(S_{2^n})$ та знайдено розміри і кількість кодів для максимальної та мінімальної ненульової відстані Хеммінга.

Ключові слова: коди на підстановках, силовська 2-підгрупа, симетрична група, відстань Хеммінга

MSC2020: 94B60, 05A05

1. Introduction

A permutation codes is studied since the 1970s (see [2], [3], [5] for examples). The permutation code of length n and with minimum distance d over metric $\mathbf{d}$ is the set of permutations $C \in S_n$ such that for every pair of different permutations $\pi, \sigma \in C$ the distance between π and σ is greater or equal to d. Usually it is considered Hamming distance between permutations.

Permutation codes are used as error-correction codes in channels with low power-line communication (see [4], [8]).

One of direction of investigations is to study properties of codes defined on algebraic substructures. Bailey in [1] gave efficient decoding algorithms in the case when the permutation codes are subgroups. In this paper, we discuss properties of codes in the case when permutation codes are defined on Sylow 2-subgroup of the symmetric group S_{2^n}.

We also study the property of the Hamming distance d_H defined on permutations from Sylow 2-subgroup $Syl_2(S_{2^n})$ of symmetric group S_{2^n} and describe an algorithm for finding the Hamming distance over elements from Sylow 2-subgroup of the symmetric group with complexity $O(2^n)$.

2. Preliminaries

A tree T is called *rooted tree* if there is one vertex v_0 that is called the *root*. A rooted tree is called *binary tree* if the degree of the root v_0 is equal 2 and the degrees of other vertices (except leaves) are equal 3. Denote by T_n a binary rooted tree with n levels. Let $V(T_n)$ be a set of all vertices of the tree T_n (see [7], [12]). We denote by $LT_{2,n}$ the set of all binary n-levels rooted trees with labels 0 or 1 on all vertices from the 0th to the $(n-1)$th levels.

Let D be a tree from the set $LT_{2,n}$. We enumerate all vertices of all levels. Let i be a number of vertex v on level j. We say that a pair (j,i) is *coordinates of the vertex* v of a tree D, $i \in \{1,\dots,2^j\}$, $j \in \{0,\dots,(n-1)\}$. Denote this $c(v) = (j,i)$.

Assume that $(j,i) < (k,r)$ if $j < k$ or $j = k$ and $i < r$. We also say that vertex v is less then vertex w $(v < w)$ if $c(v) < c(w)$ (see [10]).

Denote by $OV(D)$ *the set of vertices labeled by 1 of a tree* $D \in LT_{2,n}$ (see [10]).

Let $v_0, v, w \in V(T_n)$. We say that the vertex v *is under* the vertex w (the vertex w is above the vertex v) if w belongs to the path which connects v with the root v_0 of the tree. Denote $v \succ w$ (see [10]).

Define the next operations on a set of all vertices of the tree D:
$switch(D,v)$ = "to switch two sub-trees of the tree D, for which vertex v is a

root"(see [10]).

For every vertex $v \in V(T_n)$ determine a mapping $\mathbb{ACT}_w : V(T_n) \to V(T_n)$ by the next rule (see [10]):

$$\mathbb{ACT}_w(v) = v' \text{ if and only if } v' \text{ is an image of } v \text{ after } switch(T_n, w).$$

Note that:

- if $v \succ w$ and $c(w) = (k, r), c(v) = (j, i)$, then $c(v') = (j, i')$ and

$$i' = \begin{cases} i + 2^{j-k-1}, \text{ if } i \leq (r-1) \cdot 2^{j-k} + 2^{j-k-1}, \\ \text{(i.e., } v \text{ is in the left branch of a sub-tree with a root } w); \\ i - 2^{j-k-1}, \text{ if } i \geq (r-1) \cdot 2^{j-k} + 2^{j-k-1} + 1, \\ \text{(i.e., } v \text{ is in the right branch of a sub-tree with a root } w). \end{cases}$$

- if $v \not\succ w$, then $\mathbb{ACT}_w(v) = v$.

We extend the definition of $\mathbb{ACT}$ on ordered sets of vertices in the next way.

1. For an ordered set of vertices $A = \{a_1, \ldots, a_u\}$ and some vertex b define:

$$\mathbb{ACT}_A(b) = \mathbb{ACT}_{a_u}(\mathbb{ACT}_{a_{u-1}}(\ldots(\mathbb{ACT}_{a_1}(b))\ldots)).$$

2. For ordered sets of vertices $A = \{a_1, \ldots, a_u\}$ and $B = \{b_1, \ldots, b_r\}$ define:

$$\mathbb{ACT}_A(B) = (\mathbb{ACT}_A(b_1), \ldots, \mathbb{ACT}_A(b_r))$$

Note that the result of operation $\mathbb{ACT}_A(B)$ is an odered set.

Theorem 1. *[10]. For any trees $D_1, D_2 \in LT_{2,n}$ we have:*

$$OV(D_1 \cdot D_2) = \Big(\mathbb{ACT}_{(OV(D_1),<)}\big(OV(D_2)\big)\Big)\Delta OV(D_1).$$

Lemma 1. *[10]. Let $A \subset V(T_n)$ be some an ordered set of vertices and $B, C \subset V(T_n)$. Then we have:*

$$\mathbb{ACT}_A(B\Delta C) = \mathbb{ACT}_A(B)\Delta\mathbb{ACT}_A(C),$$

where Δ is symmetric difference of the sets.

Let $D_1, D_2 \in LT_{2,n}$. Then:

- denote by $D_1\Delta D_2$ the tree from $LT_{2,n}$ which is defined by a set of vertices with labels 1 $OV(D_1)\Delta OV(D_2)$;
- by the symbol $\mathbb{ACT}_{D_1}\big(D_2\big)$ we define the set $\mathbb{ACT}_{(OV(D_1),<)}\big(OV(D_2)\big)$.

Let a vertex v be a vertex with label 1 of a tree. We call the vertex v *the main vertex* if any vertex from the way between v and v_0 has the label 0 (see [11]).

Recall that *the number of unfixed points* of permutation π is the number of indexes i where $\pi(i) \neq i$. Denote $h(\pi)$ (see [9]).

Proposition 1. [11]. The number of unfixed point $h(\pi)$ of permutation $\pi \in Syl_2(S_{2^n})$ is equal to the number of leaves under all main vertices of the corresponding tree $D \in LT_{2,n}$.

The second row $a = (a_1, a_2, \ldots, a_{2^n})$ of permutation $\pi = \begin{pmatrix} 1 & 2 & \ldots & 2^n \\ a_1 & a_2 & \ldots & a_{2^n} \end{pmatrix}$ is called *a block of elements* (see [10]).

Recall the definition of 2-separated permutation (see [10]).

Definition 1. Permutation π is called 2-*separated* if we can do the next steps.

1. At first, we divide the block a into 2 sub-blocks with the same length: $u_1 = (a_1, \ldots, a_{2^{n-1}})$ and $u_2 = (a_{2^{n-1}+1}, \ldots, a_{2^n})$.Then we check if every element of u_1 is greater (or less) than every element of u_2.

2. If step 1 holds, then we repeat process and divide blocks u_1 and u_2 into sub-blocks $u_{1,1}$, $u_{1,2}$ and $u_{2,1}$ $u_{2,2}$. After that we check the value of elements between corresponding blocks. And so on until we get sub-blocks that contain only one element.

Remark, that all permutations from the group $Syl_2(S_{2^n})$ are 2-separated (see [10]).

3. Hamming distance between two permutations from $Syl_2(S_{2^n})$

Recall that the *Hamming distance* between two permutations $\pi_1, \pi_2 \in S_k$ is the number of elements at which the corresponding images are different:

$$d_H(\pi_1, \pi_2) = \Big|\big\{x \in \{1, \ldots, k\} \mid \pi_1(k) \neq \pi_2(k)\big\}\Big|. \tag{3.1}$$

Suppose we have two isomorphic mappings:

- $\psi : LT_{2,n} \to Syl_2(S_{2^n})$ is defined by Algorithm 1 of transformation a tree into a permutation [10];

- $\tau : Syl_2(S_{2^n}) \to LT_{2,n}$ is defined by Algorithm 2 of transformation a permutation into a tree [10].

Theorem 2. *Let π_1, π_2 be permutations from $Syl_2(S_{2^n})$ and $D_1, D_2 \in LT_{2,n}$ be corresponding trees. Then :*

$$d_H(\pi_1, \pi_2) = d_H\Big(e, \psi(D_1 \Delta D_2)\Big), \tag{3.2}$$

where e is the identity element of the group $Syl_2(S_{2^n})$.

Proof. Induction on the index n.

The basis. In case $n = 1$ the statement of the theorem holds for the group $Syl_2(S_2)$.

Inductive step:. We shall show that if the statement of the theorem holds for n, then the statement also holds for $n + 1$.

1. Let v_0 be the root of $D_1 \Delta D_2$ with label 1, i.e.,

$$v_0 \in OV(D_1 \Delta D_2). \tag{3.3}$$

Without loss of generality we can say that $v_0 \in OV(D_1)$ and $v_0 \notin OV(D_2)$.

From Algorithm 2 (see [10]) follow that:

$$\pi_1(1) > \pi_1(2^n + 1) \text{ and } \pi_2(1) < \pi_2(2^n + 1).$$

These permutations are 2-separated because $\pi_1, \pi_2 \in Syl_2(S_{2^{n+1}})$. Hence,

$$\pi_1\Big(\{1, \dots, 2^n\}\Big) = \{2^n + 1, \dots 2^{n+1}\},\ \pi_1\Big(\{2^n + 1, \dots, 2^{n+1}\}\Big) = \{1, \dots 2^n\},$$

$$\pi_2\Big(\{1, \dots, 2^n\}\Big) = \{1, \dots, 2^n\},\ \pi_2\Big(\{2^n + 1, \dots, 2^{n+1}\}\Big) = \{2^n + 1, \dots, 2^{n+1}\},$$

Therefore,

$$d_H(\pi_1, \pi_2) = 2^{n+1}. \tag{3.4}$$

On the other hand, from Lemma 3.3 and Algorithm 1 (see [10]) it follows that:

$$\pi(1) > \pi(2^n + 1), \text{ for } \pi = \psi(D_1 \Delta D_2).$$

Note that π is 2-separated because $\pi \in Syl_2(S_{2^{n+1}})$. Hence,

$$\pi\Big(\{1, \dots, 2^n\}\Big) = \{2^n + 1, \dots 2^{n+1}\} \text{ and } \pi\Big(\{2^n + 1, \dots, 2^{n+1}\}\Big) = \{1, \dots 2^n\}.$$

So,

$$d_H(e, \pi) = 2^{n+1}. \tag{3.5}$$

Thus by equations (3.4) and (3.5) we have (3.2).

2. Let v_0 be a root of the tree $D_1 \Delta D_2$ with label 0, i.e.,

$$v_0 \notin OV(D_1 \Delta D_2). \tag{3.6}$$

Then $v_0 \notin OV(D_1)$ and $v_0 \notin OV(D_2)$ or $v_0 \in OV(D_1)$ and $v_0 \in OV(D_2)$.

Consider the case $v_0 \notin OV(D_1)$ and $v_0 \notin OV(D_2)$. Let $\pi_1, \pi_2 \in Syl_2(S_{2^{n+1}})$ be corresponding permutations to trees D_1, D_2.

The image of the left sub-tree will be the left sub-tree and the image of the right sub-tree will be the right sub-tree because both trees have the label 0 at the root. Then from Algorithm 2 (see [10]) implies that:

$$\pi_1(1) < \pi_1(2^n + 1) \text{ та } \pi_2(1) < \pi_2(2^n + 1).$$

As $\pi_1, \pi_2 \in Syl_2(S_{2^{n+1}})$, these permutations are 2-separated. So,

$$\pi_1\Big(\{1, \ldots, 2^n\}\Big) = \{1, \ldots, 2^n\},\ \pi_1\Big(\{2^n + 1, \ldots, 2^{n+1}\}\Big) = \{2^n + 1, \ldots, 2^{n+1}\},$$

$$\pi_2\Big(\{1, \ldots, 2^n\}\Big) = \{1, \ldots, 2^n\},\ \pi_2\Big(\{2^n + 1, \ldots, 2^{n+1}\}\Big) = \{2^n + 1, \ldots, 2^{n+1}\}.$$

Note that the part of permutation π, that corresponds to the left sub-tree, permutes elements $1, \ldots, 2^n$. And the part of permutation π, that corresponds to the right sub-tree, permutes elements $2^n + 1, \ldots, 2^{n+1}$. So, the narrowing of permutation $\pi \in Syl_2(S_{2^{n+1}})$ can be decomposed into two sub-permutations $\pi_1, \pi_2 \in Syl_2(S_{2^n})$ (see Fig. 1):

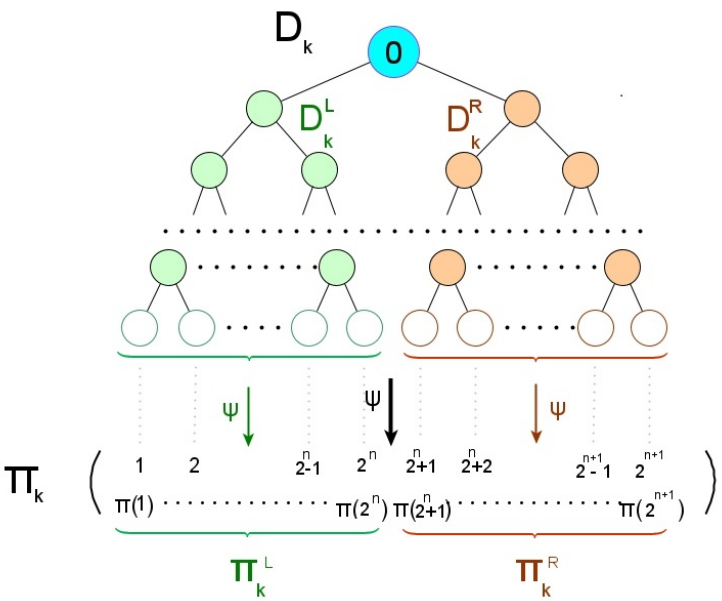

Fig. 1. Representation of tree with its sub-trees and corresponding permutation's narrowings

Denote: $\pi_k^L := \pi_k\big|_{\{1,\ldots,2^n\}}$, $\pi_k^R := \pi_k\big|_{\{2^n+1,\ldots,2^{n+1}\}}$, $k = 1, 2$.

Then we have:

$$d_H(\pi_1, \pi_2) = d_H(\pi_1^L, \pi_2^L) + d_H(\pi_1^R, \pi_2^R). \tag{3.7}$$

The permutations π_k^L and π_k^R, $k = 1, 2$, are permutations with the length 2^n. They are defined by n-levels labeled tree (by the left and the right sub-trees of trees D_1 and D_2 correspondingly). From assumption of induction we have:

$$d_H(\pi_1^L, \pi_2^L) = d_H(e^L, \psi(D_1^L \Delta D_2^L); \tag{3.8}$$

$$d_H(\pi_1^R, \pi_2^R) = d_H(e^R, \psi(D_1^R \Delta D_2^R)); \tag{3.9}$$

From equations (3.7), (3.8) and (3.9) it follows:

$$d_H(\pi_1, \pi_2) = d_H(e^L, \psi(D_1^L \Delta D_2^L) + d_H(e^R, \psi(D_1^R \Delta D_2^R)). \tag{3.10}$$

Note that the permutations π_k^L, π_k^R are defined on the disjoint union of sets. So,

$$d_H(\pi_1, \pi_2) = d_H(e^L, \psi(D_1^L \Delta D_2^L)) + d_H(e^R, \psi(D_1^R \Delta D_2^R)) = d_H(e, \psi(D_1 \Delta D_2)). \tag{3.11}$$

The case $v_0 \in OV(D_1)$ and $v_0 \in OV(D_2)$ is similar to the previous.

The proof is complete.

Proposition 2. Let $\pi \in Syl_2(S_{2^n})$, e be an identity element of the group $Syl_2(S_{2^n})$. Then:

$$d_H(e, \pi) = h(\pi).$$

Proof. The proof strictly implies from definitions of the distance d_H and the function h.

The proof is complete.

Based on Proposition 2, equation (3.2) of Theorem 2 can be represented in the following way:

$$d_H(\pi_1, \pi_2) = h\big(\psi(D_1 \Delta D_2)\big). \tag{3.12}$$

Example 1. Let $\pi_1, \pi_2 \in Syl_2(S_{2^4})$ and $D_1, D_2 \in LT_{2,4}$ be corresponding trees (see Fig. 2) Then:

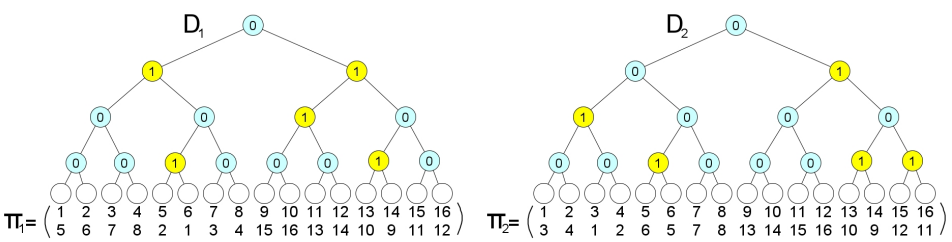

Fig. 2. Permutations π_1, π_2 and corresponding tress D_1, D_2

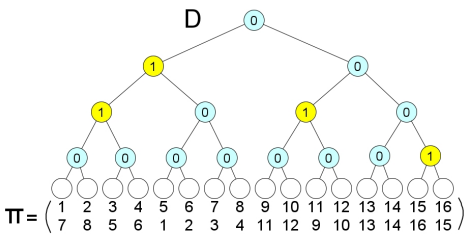

Fig. 3. Permutations π that corresponds to tree $D = D_1 \Delta D_2$

Then $D = D_1 \Delta D_2$ can be represented by the fallowing tree on Fig. 3. So, by equation (3.12) we have: $d_H(\pi_1, \pi_2) = d_H(e, \pi) = h(\pi) = 14$.

3.1. Hamming distance search algorithm

Let $\pi_1, \pi_2 \in Syl_2(S_{2^n})$. Assume that π_1, π_2 are defined by trees $D_1, D_2 \in LT_{2,n}$ correspondingly.

We introduce the next notations:
$a[k]$ be the kth coordinate of the string a;
$a[b, c]$ be a sub-string of a, which are defined from the bth to the cth coordinates of the string a;
$len(a)$ be the function, which defines the number of coordinates in the string a.

Algorithm 1. *Hamming distance search algorithm.*

Input: $a \leftarrow (a[1], \ldots, a[2^n]), b \leftarrow (b[1], \ldots, b[2^n])$, *#a and b be the second strings of permutations* π_1 *and* π_2 *correspondingly.*

Output: *Hamming distance between permutations* π_1, π_2.

 # Define the recursive sub-program with arguments a, b*:*
function HEM(a, b)
  # Check if labels of vertices with the same coordinates are different:
  if $\Big(a[1] > a[\frac{len(a)}{2} + 1]$ *xor* $b[1] > b[\frac{len(b)}{2} + 1]\Big)$ ***then***
    return $len(a)$
  end if
  if $len(a) = 2$ ***then***
    return *0*
  end if
  return $Hem\Big(a[1, \frac{len(a)}{2}]; b[1, \frac{len(b)}{2}]\Big) +$
$+Hem\Big(a[\frac{len(a)}{2} + 1\ ,\ len(a)]; b[\frac{len(b)}{2} + 1\ ,\ len(b)]\Big)$
end function
HEM(a, b)

Theorem 3. *Hamming distance search algorithm is correct.*

Proof. First we note that:

1. in step 4, the value

$$\Big(a[1] > a[2^{n-1}+1] \text{ xor } b[1] > b[2^{n-1}+1]\Big) \tag{3.13}$$

   is true if and only if corresponding vertices with the same coordinates from trees D_1, D_2 will have different labels. The last means that the vertex with the same coordinates of tree $D_1 \Delta D_2$ will be labeled by 1.

2. step 7, $len(a) = 2$, will be achieved if and only if permutations act in the same way on the corresponding points;

3. the recursive call of sub-program (step 10) means the jump from the vertex to its children in trees D_1, D_2.

As the result, condition (3.13) in the algorithm will be achieved for the main vertices of tree $D_1 \Delta D_2$. Proposition 1 claims that the number of unfixed points of permutations is equal to the number of leaves under all its main vertices. But the number of leaves under some main vertex is equal to the length of corresponding string a in recursive sub-program.

So, the algorithm calculates distance $h(\psi(D_1 \Delta D_2))$. From equation (3.12) we have:

$$h(\psi(D_1 \Delta D_2)) = d_H(\pi_1, \pi_2).$$

The proof is complete.

Proposition 3. The complexity of Algorithm 1 for any permutations $\pi_1, \pi_2 \in Syl_2(S_{2^n})$ equals $O(2^n)$.

Proof. The maximum number of operations will be achieved when the maximum number of calls to sub-program will be done because of recursiveness of the algorithm. This will be if and only if the trees D_1 and D_2 will have the same labels on vertices with the same coordinates. In this case, all vertices of tree $D_1 \Delta D_2$ will be labeled by 0. So, the Algorithm 1 needs to make 2 compares on the step 4 for every labeled vertex. The number of vertices is 2^{n-1}. So, $O(2 * 2^{n-1}) = O(2^n)$.

The proof is complete.

Theorem 4. *The average-case complexity of Algorithm 1 is* $O(n)$.

Proof. Let $\pi_1, \pi_2 \in Syl_2(S_{2^n})$. By symbol $N(\pi_1, \pi_2)$ we denote the number of calls of sub-program Hem by Algorithm 1 during the calculation of $d_H(\pi_1, \pi_2)$. Let $\Sigma(n) = \sum\limits_{\pi_1, \pi_2 \in Syl_2(S_{2^n})} N(\pi_1, \pi_2)$.

Denote by $K(n)$ the average number of these calls for all pairs of permutations from $Syl_2(S_{2^n})$. Then

$$K(n) = \frac{\Sigma(n)}{\left|Syl_2(S_{2^n})\right|^2}, \text{ where } \left|Syl_2(S_{2^n})\right| = 2^{2^n-1}.$$

We shall show, that:

$$\Sigma(n) = n \cdot (2^{2^n-1})^2 \text{ and } K(n) = n \tag{3.14}$$

by induction over index n.

The basis. Let $n = 1$. The group $Syl_2(S_{2^1})$ has the order 2 and permutations of this group are completely defined by label on the root of the tree from $LT_{2,1}$. Then the total number of all pairs of permutations is 4. As the result, $\Sigma(1) = 4$, $K(1) = 1$.

Induction step: case $n+1$ under assumption that for $l \leq n$ equation (3.14) holds.

- *Case 1.* Let corresponding trees have different labels on roots: 0 and 1 or 1 and 0. The total number of such options is 2. Then Algorithm 1 stops at the first entrance into sub-program, because of step 4. The number of trees from $LT_{2,n+1}$, which have a fixed label on root, is equal to $2^{2^{n+1}-2}$. Then the total number of calls for such pairs equals

$$1 \cdot 2 \cdot (2^{2^{n+1}-2})^2. \tag{3.15}$$

- *Case 2.* Let corresponding trees have the same labels on roots: 0 and 0 or 1 and 1. The total number of such options is 2. Then the condition at step 4 is satisfied when Algorithm 1 runs for the first time. So, the algorithm will call sub-program recursively for both sub-trees. Note, that their sub-trees belong to $LT_{2,n}$. Based on the induction assumption, it is required to make $K(n) = 2n$ average calls of Hem by the algorithm for every pair of sub-trees. As the result, we have the following number of calls of such pairs equals

$$(1 + 2K(n)) \cdot 2 \cdot (2^{2^{n+1}-2})^2. \tag{3.16}$$

From equations (3.15) and (3.16) imply the total number of calls equals:

$$\Sigma(n+1) = 2 \cdot (2^{2^{n+1}-2})^2 + (1 + 2K(n)) \cdot 2 \cdot (2^{2^{n+1}-2})^2 =$$

$$= (2 + 2n) \cdot 2 \cdot \frac{1}{4} \cdot (2^{2^{n+1}-1})^2 = (n+1) \cdot (2^{2^{n+1}-1})^2.$$

$$\text{So, } K(n+1) = \frac{\Sigma(n+1)}{\left|Syl_2(S_{2^{n+1}})\right|^2} = \frac{(n+1) \cdot (2^{2^{n+1}-1})^2}{(2^{2^{n+1}-1})^2} = n+1$$

The proof is complete.

4. Permutation codes over Sylow 2-subgroup of symmetric group

In the code theory the codes over symmetric group of permutations S_n and its subgroups are considered. With it, there are used different metrics over codes, like, Hamming, Ulam, Levenstein, etc. We will study codes, which are defined over $Syl_2(S_{2^n})$ and their properties according to Hamming distance.

4.1. Hamming distance properties

Lemma 2. *For any $\pi_1, \pi_2 \in Syl_2(S_{2^n})$ $d_H(\pi_1, \pi_2)$ is even number.*

Proof. Let π_1, π_2 be 2-separated permutations from $Syl_2(S_{2^n})$ and $D_1, D_2 \in LT_{2,n}$ be corresponding trees. From equation (3.12) we haves:

$$d_H(\pi_1, \pi_2) = h(\psi(D_1 \Delta D_2)).$$

But $h(\psi(D_1 \Delta D_2))$ is equal to the number of leaves, which are under main vertices of tree $D_1 \Delta D_2$. This number is always even (degree of 2).

The proof of Lemma 2 is complete.

Lemma 3. *Let m be an even number, $2 \leq m \leq 2^n$. Then there exist permutations $\pi, \sigma \in Syl_2(S_{2^n})$ such that*

$$d_H(\pi, \sigma) = m.$$

Proof. From Theorem 2 we have $d_H(\pi_1, \pi_2) = d_H\Big(e, \psi(D_1 \Delta D_2)\Big)$. So, we can assume that $\pi = e$. Note, that the vertices of tree D_1, that corresponds to π have labels 0.

Let D_2 be a corresponding tree to the permutation σ.

Case 1. Let $m = 2^n$. Then the root of the tree D_2 has the label 1. So, we have:

$$d_H(e, \sigma) = h(\psi(D_1 \Delta D_2)) = h(\psi(D_2)) = 2^n.$$

Case 2. Let $m \neq 2^n$. Then the root of tree D_2 is labeled by 0.

Consider expression of even number m as a base-2:

$$m = m_1 \cdot 2^1 + \ldots + m_{n-1} \cdot 2^{n-1}, \text{ where } m_k \in \{0, 1\}, \ k \in \{1, n-1\}.$$

We will label vertices of tree D_2 by 1 based on values m_k, where k decrease from $n-1$ to 1, in the following way:

- the level j is changing by the rule: $j = n - k$;
- if $m_k = 0$, then we skip the level $j = n - k$ with corresponding value k;
- if $m_k = 1$, then on the level $j = n - k$ we choose a vertex v such that the path from v to v_0 doesn't contain any vertex with label 1. We label by 1 the vertex v. So, it becomes a main vertex.

Note that the tree D_2 has at most one vertex with label 1 on every level j, where $1 \leq j \leq 2^{n-1}$.

The number of leaves, that are under main vertex of level $j = n - k$, is $2^{n-j} = 2^k$, $k \in \{1, n-1\}$. Hence, the permutation σ has exactly m unfixed points. So,

$$d_H(e, \sigma) = h(\psi(D_1 \Delta D_2)) = h(\psi(D_2)) = m.$$

The proof is complete.

Lemma 4. *Let π be a permutation from $Syl_2(S_{2^n})$, d be an even number, $0 \leq d \leq 2^n$. Then*

$$|\{\sigma \in Syl_2(S_{2^n}) | d_H(\pi, \sigma) = d\}| = |\{Q \in LT_{2,n} | h(\psi(Q)) = d\}|.$$

Proof. Let $D \in LT_{2,n}$ be the corresponding tree to the permutation $\pi \in Syl_2(2_{2^n})$. Let $D' = \tau(\sigma) \in LT_{2,n}$. Then Hamming distance between σ and π equals d if and only if the following condition holds:

$$d = d_H(\pi, \sigma) = h\Big(\psi\big(D \Delta D'\big)\Big). \tag{4.1}$$

The capacity of the set $\{\sigma \in Syl_2(S_{2^n}) | d_H(\pi, \sigma) = d\}$ equals the number of permutations σ, which are satisfying the condition (4.1).

The last equality is hold for every tree $D' \in \{D \Delta Q \big| Q \in LT_{2,n}, h(\psi(Q)) = d\}$, because:

$$d = h\big(\psi(D \Delta D')\big) = h\big(\psi(D \Delta (D \Delta Q))\big) = h\big(\psi(D \Delta D \Delta Q)\big) = h\big(\psi(Q)\big).$$

Hence,

$$\Big|\big\{D \Delta Q \mid Q \in LT_{2,n}, h(\psi(Q)) = d\big\}\Big| = \Big|\big\{Q \in LT_{2,n} \mid h(\psi(Q)) = d\big\}\Big|. \tag{4.2}$$

From (4.2) implies that the number of permutations σ, for wich $d_H(\pi, \sigma) = d$, equals the number of trees $Q \in LT_{2,n}$ such that $h(\psi(Q)) = d$.

The proof is complete.

4.2. Permutation codes over $Syl_2(S_{2^n})$

Recall denotation $A_0(n, d)$ as the *maximum capacity of permutation code* with the length n and the minimum distance d (see [6]).

Let $C_H(2^n, d)$ be a *code*, which is defined on permutations from $Syl_2(S_{2^n})$ with Hamming distance d such that for every permutations $\pi, \sigma \in Syl_2(S_{2^n})$ we have:

$$\pi, \sigma \in C_H(2^n, d) \text{ if and only if } d_H(\pi, \sigma) \geq d.$$

Define $A_H(2^n, d)$ as the *maximum possible capacity of code*, which is consisted of permutations from $Syl_2(S_{2^n})$ of length 2^n and Hamming distance at most d.

We represent the code $C_H(2^n, D)$ in the matrix form. The rows of corresponding matrix are the second rows of permutations from $C_H(2^n, d)$.

Example 2. Consider the group

$$Syl_2(S_{2^2}) = \Big\{ \left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\1&2&4&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\2&1&3&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\3&4&2&1\end{smallmatrix}\right),$$

$$\left(\begin{smallmatrix}1&2&3&4\\4&3&1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right) \Big\}.$$

Define code $C_H(2^2, 4)$ as a set of permutations:

$$\Big\{ \left(\begin{smallmatrix}1&2&3&4\\1&2&4&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\2&1&3&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right) \Big\}.$$

Then we represent code by the next matrix:

$$M = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Also, $A_H(2^2, 4) = 4$.

Proposition 4. $A_H(2^n, 2^n) = 2^n$.

Proof. Suppose, that the code $C_H(2^n, 2^n)$ consists of $2^n + k$ permutations from $Syl_2(S_{2^n})$, $k \geq 1$. Then the matrix of this code has $(2^n + k)$ rows and 2^n columns. There are at least 2 rows, which have the same elements on the same positions because the elements of matrix are the numbers from the set $\{1, \ldots, 2^n\}$. In this case, Hamming distance between permutations, which are correspond to the current 2 rows, will be less than 2^n. It is a contradiction to the proposition's statement. So, the number of permutations in the code $C_H(2^n, 2^n)$ cannot be greater than 2^n.

Let us show that there is the code with capacity 2^n. Let $m = (m_0, \ldots, m_{n-1})$ be a sequence over set $\{0, 1\}$. For any such sequence we construct the tree $D(m)$ by the next way: if $m_j = 1$, then every vertice of the jth level of tree $D(m)$ will be labeled as 1, $j \in \{0, n-1\}$.

Any of such finite sequence defines the unique tree $D(m)$. Let m, t be two different finite sequences. Then there exists the minimum number j such that $m_j \neq t_j$. So, every vertex in the jth level of the corresponding tree $D = D(m) \Delta D(t)$ will have label 1. Every vertex of the jth level will be main vertex because j is the minimum such number. Then:

$$d_H(\psi(D(m)), \psi(D(t))) = h(\psi(D(m) \Delta D(t))) = 2^n.$$

As the number of these different finite sequences m is 2^n, we have 2^n permutations, which are obtained by $\psi(D(m))$. So, the code $C_H(2^n, 2^n)$ consists of 2^n permutations.

The proof is complete.

Remark 1. The last proof implies that every code $C_H(2^n, 2^n)$ can be defined by the square matrix M $2^n \times 2^n$ with the next conditions:

1. every element $a_{r,c}$ of the matrix M is from the range $\{1, \ldots, 2^n\}$, $1 \leq r, c \leq 2^n$;
2. in every column all elements are different;
3. every row of such matrix is a second row of some 2-separated permutation.

Note, that the switching operation over rows of the matrix M doesn't change the code. Without loss of generality, we may assume that all diagonal elements of matrix M of the code are equal to 1.

Note that every permutation from $Syl_2(S_{2^n})$ is 2-separated. So, the numbers 1 and 2 are always present in the same block of the length 2. Hence, we have the next representation for the element 2:

$$2 = \begin{cases} a_{r,r+1}, & \text{if } r \text{ is odd;} \\ a_{r,r-1}, & \text{if } r \text{ is even.} \end{cases}$$

As the result, the main diagonal will consist of the following blocks $\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}$ (see Fig. 4):

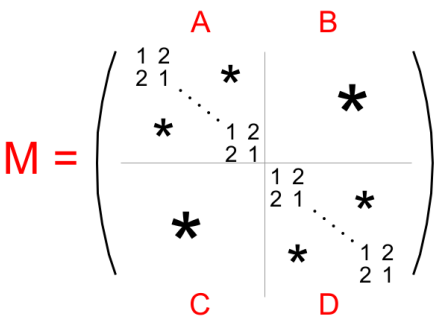

Fig. 4. Matrix M of code $C_H(2^n, 2^n)$

Theorem 5. *The number of permutation codes $C_H(2^n, 2^n)$ with the maximum Hamming distance can be defined recursively by the following way:*

$$f(n) = \begin{cases} 4, & \text{if } n = 2; \\ f^4(n-1) \cdot (2^{n-1}!)^2, & \text{if } n > 2. \end{cases}$$

Proof. From Remark 1 it follows that the number of permutation codes $C_H(2^n, 2^n)$ equals to the number of the matrices M (see Fig. 4).

Induction over the index n.

The basis. Let $n = 2$.

There are the following permutation codes over $Syl_2(S_{2^n})$ and Hamming distance $d_H(\pi,\sigma)=4$ for every $\pi,\sigma\in Syl_2(S_{2^2})$:

$$\begin{pmatrix}1&2&4&3\\2&1&4&3\\3&4&1&2\\4&3&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\\4&3&1&2\\3&4&2&1\end{pmatrix},\begin{pmatrix}1&2&4&3\\2&1&3&4\\3&4&1&2\\4&3&2&1\end{pmatrix},\begin{pmatrix}1&2&4&3\\2&1&3&4\\3&3&1&2\\3&4&2&1\end{pmatrix}.$$

From the direct calculations, there are no other permutation codes with the same distance.

So, $f(2)=4$.

Induction step: case n under assumption that for $l<n$ the statement holds.

Let $M=\left(\begin{smallmatrix}A&B\\C&D\end{smallmatrix}\right)$ (see Fig. 4).

- The induction assumption for matrices A and D holds. So, we have the next number of variants of them:

$$f^2(n-1). \tag{4.3}$$

- 2-separated property of permutations implies that the elements of matrices B and C are the numbers $\{2^{n-1}+1,2^{n-1}+2,\dots,2^n\}$.

  The matrix B can be transformed into the matrix B' with blocks of numbers $2^{n-1}+1$ and $2^{n-1}+2$ on the main diagonal, similar to general construction of the matrix M. The number of such different matrices B' is $f(n-1)$, as for matrices A and D. The number of different row transformations of matrix B' is $2^{n-1}!$. The rule of product implies that the total number of different matrices B equals

$$f(n-1)\cdot 2^{n-1}! \tag{4.4}$$

  We have the same for the matrix C:

$$f(n-1)\cdot 2^{n-1}! \tag{4.5}$$

(4.3)–(4.5) implies that the number of different matrices M equals

$$f(n)=f^2(n-1)\cdot f(n-1)\cdot 2^{n-1}!\cdot f(n-1)\cdot 2^{n-1}!=f^4(n-1)\cdot(2^{n-1}!)^2.$$

The proof is complete.

Proposition 5. $A_H(2^n,2)=2^{2^n-1}$.

Proof. The proof is implied by the fact that for every pair of permutations $\pi,\sigma\in Syl_2(S_{2^n})$ the following conditions hold:

- $d_H(\pi,\sigma)$ is always even number. It is based on Lemma 2;

- $d_H(\pi, \sigma) \geq 2$, if $\pi \neq \sigma$.

Therefore, the code will consist of all elements of the group. So,

$$A_H(2^n, 2) = \left|Syl_2(S_{2^n})\right| = 2^{2^n-1}.$$

The proof is complete.

Remark 2. There is the only one code $C_H(2^n, 2)$ over group $Syl_2(S_{2^n})$.

References

1. *Bailey R.F.*: Error-correcting codes from permutation groups. Discrete Math. **309** (2009), 4253—4265.
2. *Blake I.F., Cohen G., Deza M.*: Coding with permutations. Inf. Control, 43. Academic Press, New York etc., (1979), 1–19. doi:10.1016/S0019-9958(79)90076-7
3. *Cameron P.J.*: Permutation codes. European Journal of Combinatorics **31(2)** (2010), 482–490.
4. *Chee Y.M., Purkayastha P.*: Efficient decoding of permutation codes obtained from distance preserving maps. 2012 IEEE International Symposium on Information Theory Proceedings (2012), 636–640. doi:10.1109/ISIT.2012.6284273
5. *Dénes J.*: On some connections between permutations and coding. Discrete Math. **56** (1985), 141–146. doi:10.1016/0012-365X(85)90022-6
6. *Farnoud F., Skachek V., Milenkovic O.*: Error-correction in flash memories via codes in the Ulam metric. IEEE Trans. Inf. Theory **59(5)** (2013), 3003–3020. doi:10.1109/TIT.2013.2239700
7. *Grigorchuk R.I., Nekrashevich V.V., Sushchanskii V.I.*: Automata, dynamical systems, and groups. Dynamical systems, automata, and infinite groups. Transl. from the Russian. Moscow: MAIK Nauka/Interperiodica Publishing (2000), 128–203.
8. *Huczynska S.*: Powerline communication and the 36 officers problem. Phil. Trans. R. Soc. A **364** (2006), 3199–3214.
9. *Irurozki E., Calvo B., Lozano J.A.*: Sampling and learning the Mallows and Weighted Mallows models under the Hamming distance [http://hdl.handle.net/10810/11240]. Technical Report, University of the Basque Country, 2014.
10. *Olshevska V.A.*: Algorithms for computations with Sylow 2-subgroups of symmetric groups. Silesian Journal of Pure and Applied Mathematics **10** (2020), 103–120.
11. *Olshevska V.A.*: Algorithm for finding the number of unfixed points for permutations of Sylow 2-subgroups $Syl_2(S_{2^n})$ of symmetric groups S_{2^n}. Accepted in Mohyla Mathematical Journal.
12. *Diestel R.*: Graph theory. 5th ed. Grad. Texts Math. Berlin: Springer **173** (2017), xviii + 428.

Received: 06.12.2021. *Accepted:* 27.12.2021