Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 134-139*

The least known length of ordered basis of symmetric group

S. A. Kalinchuk
Yu. L. Sagalovich sagal@iitp.ru
Institute for Information Transmission Problems,
Russian Academy of Sciences, Moscow, RUSSIA

Abstract. The recurrent algorithm for construction of ordered basis of symmetric group with degree $n = 2^k$ is given. It is shown that the number of transpositions constituting such basis is equal to $O(n \log_2^2 n)$. This value exceeds the order of lower bound estimation only in coefficient $\log_2 n$.

1 Introduction

Let S_X be a symmetric group with degree $|X|$ on a set of numbers X. By S_n denote group S_X if $X = \{1, \dots, n\}$.

Let $\mathcal{T}_1, \mathcal{T}_2, \dots, \mathcal{T}_r$ be an ordered set of transpositions of S_X, where $r \leqslant C^2_{|X|}$. We shall denote such *ordered system of transpositions* by Ψ and represent as:

$$\Psi = \mathcal{T}_1 \ \mathcal{T}_2 \ \dots \ \mathcal{T}_r ,$$

where the transpositions' number r will be denoted by $|\Psi|$.

Definition 1. *The system* Ψ *is called* ordered basis *of symmetric group* S_X *if any permutation* $\mathcal{P}_X \in S_X$ *can be represented as*

$$\mathcal{P}_X = \mathcal{T}_1^{\gamma_1} \cdot \mathcal{T}_2^{\gamma_2} \cdot \ldots \cdot \mathcal{T}_r^{\gamma_r} ,$$

where $\gamma_j \in \{0, 1\}, j = 1, 2, \dots, r$ *. Note that there can exist several vectors* $(\gamma_1, \dots, \gamma_r)$ *representing the same permutation* $\mathcal{P}_X$*.*

In [1], we announced a result that can be easily used to show the existence of algorithms for constructions of ordered bases with the transpositions' number of order $\frac{3}{4} C_n^2$. Also there it was supposed that r should be close to value $n \log_2 n$. This assumption corresponds well to the rough upper bound of factorial

$$n! \leqslant n^n = 2^{n \log_2 n} .$$

The obtained result is based on that the degree n of symmetric group S_n is chosen to be equal to $n = 2^k$, $k \geqslant 3$. Such choice allows successively partitioning set of permutated objects in two equal-sized subsets. At each stage of partition, "mixing" among objects is introduced, for example, by permutation (7). The main results are formed by relations (3) – (6).

2 Main results

2.1 Part 1

Consider a symmetric group S_X at $|X| = 4m$, where $m \geqslant 2$. Partition the set $X = \{x_1, \dots, x_{4m}\}$ into two subsets, $\mathbb{O}$ and $\mathbb{E}$:

$$\mathbb{O} \cup \mathbb{E} = X,\ \mathbb{O} \cap \mathbb{E} = \varnothing,\ |\mathbb{O}| = |\mathbb{E}| = 2m\ . \tag{1}$$

Let $\mathcal{P}_X \triangleq \mathcal{P}_{\mathbb{O}\cup\mathbb{E}}$ be any permutation of group $S_X \triangleq S_{\mathbb{O}\cup\mathbb{E}}$. It is evident that

$$\mathcal{P}_{\mathbb{O}\cup\mathbb{E}} = \left(\begin{array}{cccc} \mathbb{O}' & \mathbb{E}' & \mathbb{O}'' & \mathbb{E}'' \\ \widetilde{\mathbb{O}}' & \widetilde{\mathbb{E}}' & \widetilde{\mathbb{E}}'' & \widetilde{\mathbb{O}}'' \end{array}\right) = \left(\begin{array}{cccc} \mathbb{O}' & \mathbb{O}'' & \mathbb{E}' & \mathbb{E}'' \\ \widetilde{\mathbb{O}}' & \widetilde{\mathbb{O}}'' & \widetilde{\mathbb{E}}' & \widetilde{\mathbb{E}}'' \end{array}\right) \cdot \left(\begin{array}{cc} \widetilde{\mathbb{O}}'' & \widetilde{\mathbb{E}}'' \\ \widetilde{\mathbb{E}}'' & \widetilde{\mathbb{O}}'' \end{array}\right),$$

where $\mathbb{O} = \mathbb{O}' \cup \mathbb{O}'' = \widetilde{\mathbb{O}}' \cup \widetilde{\mathbb{O}}''$, $\mathbb{E} = \mathbb{E}' \cup \mathbb{E}'' = \widetilde{\mathbb{E}}' \cup \widetilde{\mathbb{E}}''$ and notation
$\begin{array}{c} \mathbb{A} \\ \mathbb{B} \end{array} \triangleq \begin{array}{cccc} a_1 & a_2 & \dots & a_{|\mathbb{A}|} \\ b_1 & b_2 & \dots & b_{|\mathbb{B}|} \end{array}$, $\mathbb{A} = \{a_1, a_2, \dots, a_{|\mathbb{A}|}\}$, $\mathbb{B} = \{b_1, b_2, \dots, b_{|\mathbb{B}|}\}$,
$|\mathbb{A}| = |\mathbb{B}|$. Therefore,

Proposition 1. *Any permutation $\mathcal{P}_{\mathbb{O}\cup\mathbb{E}}$ of group $S_{\mathbb{O}\cup\mathbb{E}}$ can be factored as*

$$\mathcal{P}_{\mathbb{O}\cup\mathbb{E}} = \mathcal{P}_{\mathbb{O}} \cdot \mathcal{P}_{\mathbb{E}} \cdot \mathcal{T}_{\mathbb{O},\mathbb{E}}\ , \tag{2}$$

where $\mathcal{P}_{\mathbb{O}}$ and $\mathcal{P}_{\mathbb{E}}$ are some permutations belonging to symmetric groups $S_{\mathbb{O}}$ and $S_{\mathbb{E}}$ correspondingly, and a permutation $\mathcal{T}_{\mathbb{O},\mathbb{E}}$ of group $S_{\mathbb{O}\cup\mathbb{E}}$ has the form as

$$\left(\begin{array}{cc} \mathbb{O}^* & \mathbb{E}^* \\ \mathbb{E}^* & \mathbb{O}^* \end{array}\right) \triangleq (\mathbb{O}^*, \mathbb{E}^*),\ \textit{where}\ \mathbb{O}^* \subseteq \mathbb{O},\, \mathbb{E}^* \subseteq \mathbb{E}. \tag{3}$$

Definition 2. *An ordered system of transpositions of group $S_{\mathbb{O}\cup\mathbb{E}}$ is called* system generating permutations of the form $\mathfrak{S}_{\mathbb{O}}\mathfrak{S}_{\mathbb{E}}\mathcal{T}_{\mathbb{O},\mathbb{E}}$, *if $\mathcal{T}_{\mathbb{O},\mathbb{E}}$ can be* any *permutation of the form* (3)*, and $\mathfrak{S}_{\mathbb{O}}$, $\mathfrak{S}_{\mathbb{E}}$ are some permutations of groups $S_{\mathbb{O}}$, $S_{\mathbb{E}}$ correspondingly.*

Proposition 2. *Let $\Psi_{\mathbb{O}}$ and $\Psi_{\mathbb{E}}$ be ordered bases of groups $S_{\mathbb{O}}$ and $S_{\mathbb{E}}$ correspondingly. Let $\Psi_{\mathbb{O},\mathbb{E}}$ be an ordered system of transpositions of group $S_{\mathbb{O}\cup\mathbb{E}}$, and this system generates permutations of the form $\mathfrak{S}_{\mathbb{O}}\mathfrak{S}_{\mathbb{E}}\mathcal{T}_{\mathbb{O},\mathbb{E}}$. Then the system*

$$\Psi_{\mathbb{O}\cup\mathbb{E}} = \Psi_{\mathbb{O}}\, \Psi_{\mathbb{E}}\, \Psi_{\mathbb{O},\mathbb{E}} \tag{4}$$

is the ordered basis of group $S_{\mathbb{O}\cup\mathbb{E}}$.

Proof Follows directly from the factorization (2) and that

$$\mathcal{P}_{\mathbb{O}} \cdot \mathcal{P}_{\mathbb{E}} \cdot \mathcal{T}_{\mathbb{O},\mathbb{E}} = \underbrace{\mathcal{P}_{\mathbb{O}}\mathfrak{S}_{\mathbb{O}}{}^{-1}}_{\Psi_{\mathbb{O}}} \cdot \underbrace{\mathcal{P}_{\mathbb{E}}\mathfrak{S}_{\mathbb{E}}{}^{-1}}_{\Psi_{\mathbb{E}}} \cdot \underbrace{\mathfrak{S}_{\mathbb{O}}\mathfrak{S}_{\mathbb{E}}\mathcal{T}_{\mathbb{O},\mathbb{E}}}_{\Psi_{\mathbb{O},\mathbb{E}}}\ .$$

2.2 Part 2

Partition the set $\mathbb{O}$ into subsets $\mathbb{O}_1$, $\mathbb{O}_2$ and the set $\mathbb{E}$ into subsets $\mathbb{E}_1$, $\mathbb{E}_2$ by the same way as in (1). Thus,

$$\mathbb{O}_1 \cup \mathbb{O}_2 = \mathbb{O},\ \mathbb{O}_1 \cap \mathbb{O}_2 = \varnothing\,, \qquad \mathbb{E}_1 \cup \mathbb{E}_2 = \mathbb{E},\ \mathbb{E}_1 \cap \mathbb{E}_2 = \varnothing\,,$$

where $|\,\mathbb{O}_1| = |\,\mathbb{O}_2| = |\,\mathbb{E}_1| = |\,\mathbb{E}_2| = \frac{1}{4}|\,X| = m$.

Let $\mathbb{O}_1 = \{o_1^1, o_2^1, \ldots, o_m^1\}$, $\mathbb{O}_2 = \{o_1^2, o_2^2, \ldots, o_m^2\}$, $\mathbb{E}_1 = \{e_1^1, e_2^1, \ldots, e_m^1\}$, $\mathbb{E}_2 = \{e_1^2, e_2^2, \ldots, e_m^2\}$.

Consider an ordered system of transpositions $\Psi^{\pi_1;\,\pi_2}_{\mathbb{O}_1,\mathbb{E}_2;\,\mathbb{O}_2,\mathbb{E}_1}$ consisting of m transpositions of the form $(o_i^1, e^2_{\pi_1(i)})$ and m transpositions of the form $(o_j^2, e^1_{\pi_2(j)})$, where $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant m$, and π_1, π_2 are some permutations defined on the set $\{1, 2, \ldots, m\}$. In expanded form such system is represented as:

$$\Psi^{\pi_1;\,\pi_2}_{\mathbb{O}_1,\mathbb{E}_2;\,\mathbb{O}_2,\mathbb{E}_1} = \Big(o_1^1, e^2_{\pi_1(1)}\Big)\cdots\Big(o_m^1, e^2_{\pi_1(m)}\Big)\ \Big(o_1^2, e^1_{\pi_2(1)}\Big)\cdots\Big(o_m^2, e^1_{\pi_2(m)}\Big)$$

Definition 3. *Consider* $\widetilde{\mathbb{O}} \subseteq \mathbb{O}$, $\widetilde{\mathbb{E}} \subseteq \mathbb{E}$.

Let $\widetilde{\mathbb{O}} \overset{\pi_1;\,\pi_2}{\succ\circ\prec} \widetilde{\mathbb{E}}$ *denote that at any* $\tilde{o} \in \widetilde{\mathbb{O}}$ *and* $\tilde{e} \in \widetilde{\mathbb{E}}$ *transposition* $(\tilde{o}, \tilde{e})$ *does not belong to the system* $\Psi^{\pi_1;\,\pi_2}_{\mathbb{O}_1,\mathbb{E}_2;\,\mathbb{O}_2,\mathbb{E}_1}$.

If $\widetilde{\mathbb{O}} = \{\tilde{o}_1, \tilde{o}_2, \ldots, \tilde{o}_v\}$, $\widetilde{\mathbb{E}} = \{\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_v\}$, $|\widetilde{\mathbb{O}}| = |\widetilde{\mathbb{E}}| = v$ *then let* $\widetilde{\mathbb{O}} \overset{\pi_1;\,\pi_2}{\succ\bullet\prec} \widetilde{\mathbb{E}}$ *denote that all transpositions* $(\tilde{o}_i, \tilde{e}_i)$, $1 \leqslant i \leqslant v$, *belong to the system* $\Psi^{\pi_1;\,\pi_2}_{\mathbb{O}_1,\mathbb{E}_2;\,\mathbb{O}_2,\mathbb{E}_1}$.

Proposition 3. *Let* $\Psi_{\mathbb{O}_1,\mathbb{E}_1}$ *and* $\Psi_{\mathbb{O}_2,\mathbb{E}_2}$ *be some ordered systems of transpositions generating permutations of the forms* $\mathfrak{S}_{\mathbb{O}_1}\mathfrak{S}_{\mathbb{E}_1}\mathcal{T}_{\mathbb{O}_1,\,\mathbb{E}_1}$ *and* $\mathfrak{S}_{\mathbb{O}_2}\mathfrak{S}_{\mathbb{E}_2}\mathcal{T}_{\mathbb{O}_2,\,\mathbb{E}_2}$ *correspondingly. Then the system*

$$\Psi_{\mathbb{O},\mathbb{E}} = \Psi_{\mathbb{O}_1,\mathbb{E}_1}\Psi_{\mathbb{O}_2,\mathbb{E}_2}\,\Psi^{\pi_1;\,\pi_2}_{\mathbb{O}_1,\mathbb{E}_2;\,\mathbb{O}_2,\mathbb{E}_1} \tag{5}$$

generates permutations of the form $\mathfrak{S}_{\mathbb{O}}\mathfrak{S}_{\mathbb{E}}\mathcal{T}_{\mathbb{O},\,\mathbb{E}}$ *at any* π_1 *and* π_2.

Proof. Consider any permutation $\mathcal{T}_{\mathbb{O},\,\mathbb{E}} = (\mathbb{O}^*, \mathbb{E}^*)$, where $\mathbb{O}^* \subseteq \mathbb{O}$, $\mathbb{E}^* \subseteq \mathbb{E}$. Suppose $\mathbb{O}^* = \mathbb{O}_1^* \cup \mathbb{O}_2^*$ and $\mathbb{E}^* = \mathbb{E}_1^* \cup \mathbb{E}_2^*$, where $\mathbb{O}_1^* \subseteq \mathbb{O}_1$, $\mathbb{O}_2^* \subseteq \mathbb{O}_2$, $\mathbb{E}_1^* \subseteq \mathbb{E}_1$, $\mathbb{E}_2^* \subseteq \mathbb{E}_2$.

Let $\mathbb{O}^* = \{o_1, o_2, \ldots, o_t\}$, $\mathbb{E}^* = \{e_1, e_2, \ldots, e_t\}$, and let $\mathbb{O}^*_\alpha = \{o_1^\alpha, o_2^\alpha, \ldots, o_t^\alpha\}$, $\mathbb{E}^*_\beta = \{e_1^\beta, e_2^\beta, \ldots, e_t^\beta\}$ be the sets obtained by renumbering elements of the corresponding sets $\mathbb{O}^*$, $\mathbb{E}^*$ by means of permutations α, β defined on the set $\{1, 2, \ldots, t\}$: $o_i^\alpha = o_{\alpha(i)}$, $e_i^\beta = e_{\beta(i)}$, $1 \leqslant i \leqslant t$. It is obvious that at any α, β there exist such permutations $\widetilde{\mathfrak{S}}_{\mathbb{O}}$, $\widetilde{\mathfrak{S}}_{\mathbb{E}}$ of groups $S_{\mathbb{O}}$, $S_{\mathbb{E}}$ correspondingly that $(\mathbb{O}^*, \mathbb{E}^*) = \widetilde{\mathfrak{S}}_{\mathbb{O}}\widetilde{\mathfrak{S}}_{\mathbb{E}} \cdot (\mathbb{O}^*_\alpha, \mathbb{E}^*_\beta)$.

The sets $\mathbb{O}_1^*$, $\mathbb{O}_2^*$, $\mathbb{E}_1^*$, $\mathbb{E}_2^*$ can be partitioned into the following subsets:

$O_1' \overset{\pi_1;\pi_2}{\succ\circ\prec} E_2'$; $\quad O_1'' \overset{\pi_1;\pi_2}{\succ\bullet\prec} E_2''$; $\quad O_1' \cup O_1'' = \mathbb{O}_1^*$, $E_2' \cup E_2'' = \mathbb{E}_2^*$, $O_1' \cap O_1'' = \varnothing$, $E_2' \cap E_2'' = \varnothing$;
$O_2' \overset{\pi_1;\pi_2}{\succ\circ\prec} E_1'$; $\quad O_2'' \overset{\pi_1;\pi_2}{\succ\bullet\prec} E_1''$; $\quad O_2' \cup O_2'' = \mathbb{O}_2^*$, $E_1' \cup E_1'' = \mathbb{E}_1^*$, $O_2' \cap O_2'' = \varnothing$, $E_1' \cap E_1'' = \varnothing$;
$O' = O_1' \cup O_2'$; $\quad E' = E_1' \cup E_2'$; $\quad O' \overset{\pi_1;\pi_2}{\succ\circ\prec} E'$, $|O'| = |E'|$.

There exists such renumbering of elements for each of the sets $\mathbb{O}^*$, $\mathbb{E}^*$ that

$$\mathcal{T}_{\mathbb{O},\mathbb{E}} = (\mathbb{O}^*, \mathbb{E}^*) = \widetilde{\mathfrak{S}}_{\mathbb{O}}' \widetilde{\mathfrak{S}}_{\mathbb{E}}' \cdot (O', E')(O_1'', E_2'')(O_2'', E_1'') \,.$$

Whereas $|O'| = |O_1'| + |O_2'| = |E_1'| + |E_2'| = |E'|$, three cases are possible: 1) $|O_1'| = |E_1'|$, $|O_2'| = |E_2'|$; 2) $|O_1'| > |E_1'|$, $|O_2'| < |E_2'|$; 3) $|O_1'| < |E_1'|$, $|O_2'| > |E_2'|$.

Without loss of generality consider only case 2) : $|O_1'| > |E_1'|$, $|O_2'| < |E_2'|$.

Let $\mathcal{O}_1 \cup \widehat{\mathcal{O}}_1 = O_1'$, $\mathcal{O}_1 \cap \widehat{\mathcal{O}}_1 = \varnothing$, $\mathcal{E}_2 \cup \widehat{\mathcal{E}}_2 = E_2'$, $\mathcal{E}_2 \cap \widehat{\mathcal{E}}_2 = \varnothing$, $\widehat{\mathcal{E}}_1 = E_1'$, $\widehat{\mathcal{O}}_2 = O_2'$, where $|\mathcal{O}_1| = |\mathcal{E}_1|$, $|\mathcal{O}_2| = |\mathcal{E}_2|$, $|\widehat{\mathcal{O}}_1| = |\widehat{\mathcal{E}}_2|$. Also $\widehat{\mathcal{O}}_1 \overset{\pi_1;\pi_2}{\succ\circ\prec} \widehat{\mathcal{E}}_2$, since $O' \overset{\pi_1;\pi_2}{\succ\circ\prec} E'$.

There exists such renumbering of elements for each of the sets O', E' that

$$(O', E') = \widetilde{\mathfrak{S}}_{\mathbb{O}}'' \widetilde{\mathfrak{S}}_{\mathbb{E}}'' \cdot (\mathcal{O}_1, \mathcal{E}_1)(\mathcal{O}_2, \mathcal{E}_2)(\widehat{\mathcal{O}}_1, \widehat{\mathcal{E}}_2) \,.$$

It is clear, there exist such sets $\widehat{\mathcal{O}}_2 \in \mathbb{O}_2$, $\widehat{\mathcal{E}}_1 \in \mathbb{E}_1$ that

$$\widehat{\mathcal{O}}_2 \overset{\pi_1;\pi_2}{\succ\bullet\prec} \widehat{\mathcal{E}}_1,\ |\widehat{\mathcal{O}}_2| = |\widehat{\mathcal{E}}_1| = |\widehat{\mathcal{O}}_1| = |\widehat{\mathcal{E}}_2|;\ \mathcal{O}_2 \cap \widehat{\mathcal{O}}_2 = \varnothing,\ \mathcal{E}_1 \cap \widehat{\mathcal{E}}_1 = \varnothing \,.$$

It is also evident that $(\widehat{\mathcal{O}}_1, \widehat{\mathcal{E}}_2) = (\widehat{\mathcal{O}}_1, \widehat{\mathcal{O}}_2)(\widehat{\mathcal{E}}_1, \widehat{\mathcal{E}}_2) \cdot (\widehat{\mathcal{O}}_1, \widehat{\mathcal{E}}_1)(\widehat{\mathcal{O}}_2, \widehat{\mathcal{E}}_2) \cdot (\widehat{\mathcal{O}}_2, \widehat{\mathcal{E}}_1)$.

This implies that

$$(O', E') = \widetilde{\mathfrak{S}}_{\mathbb{O}}'' \widetilde{\mathfrak{S}}_{\mathbb{E}}'' \cdot (\mathcal{O}_1, \mathcal{E}_1)(\mathcal{O}_2, \mathcal{E}_2) \cdot (\widehat{\mathcal{O}}_1, \widehat{\mathcal{O}}_2)(\widehat{\mathcal{E}}_1, \widehat{\mathcal{E}}_2) \cdot (\widehat{\mathcal{O}}_1, \widehat{\mathcal{E}}_1)(\widehat{\mathcal{O}}_2, \widehat{\mathcal{E}}_2) \cdot (\widehat{\mathcal{O}}_2, \widehat{\mathcal{E}}_1) \,.$$

Since $\mathcal{O}_1 \cap \widehat{\mathcal{O}}_1 = \varnothing$, $\mathcal{O}_2 \cap \widehat{\mathcal{O}}_2 = \varnothing$, $\mathcal{E}_1 \cap \widehat{\mathcal{E}}_1 = \varnothing$, $\mathcal{E}_2 \cap \widehat{\mathcal{E}}_2 = \varnothing$, it follows that

$$\mathcal{T}_{\mathbb{O},\mathbb{E}} = \widetilde{\mathfrak{S}}_{\mathbb{O}}' \widetilde{\mathfrak{S}}_{\mathbb{O}}'' (\widehat{\mathcal{O}}_1, \widehat{\mathcal{O}}_2) \cdot \widetilde{\mathfrak{S}}_{\mathbb{E}}' \widetilde{\mathfrak{S}}_{\mathbb{E}}'' (\widehat{\mathcal{E}}_1, \widehat{\mathcal{E}}_2) \cdot (\mathcal{O}_1, \mathcal{E}_1)(\widehat{\mathcal{O}}_1, \widehat{\mathcal{E}}_1) \cdot (\mathcal{O}_2, \mathcal{E}_2)(\widehat{\mathcal{O}}_2, \widehat{\mathcal{E}}_2) \cdot (O_1'', E_2'')(\widehat{\mathcal{O}}_2, \widehat{\mathcal{E}}_1)(O_2'', E_1'') \,.$$

Each of the systems $\Psi_{\mathbb{O}_1,\mathbb{E}_1}$, $\Psi_{\mathbb{O}_2,\mathbb{E}_2}$ generates permutations of the forms $\mathfrak{S}_{\mathbb{O}_1} \mathfrak{S}_{\mathbb{E}_1} \mathcal{T}_{\mathbb{O}_1,\mathbb{E}_1}$, $\mathfrak{S}_{\mathbb{O}_2} \mathfrak{S}_{\mathbb{E}_2} \mathcal{T}_{\mathbb{O}_2,\mathbb{E}_2}$ correspondingly. Suppose $\mathcal{T}_{\mathbb{O}_1,\mathbb{E}_1} = (\mathcal{O}_1, \mathcal{E}_1)(\widehat{\mathcal{O}}_1, \widehat{\mathcal{E}}_1)$, $\mathcal{T}_{\mathbb{O}_2,\mathbb{E}_2} = (\mathcal{O}_2, \mathcal{E}_2)(\widehat{\mathcal{O}}_2, \widehat{\mathcal{E}}_2)$. Then

$$\mathfrak{S}_{\mathbb{O}} \mathfrak{S}_{\mathbb{E}} \mathcal{T}_{\mathbb{O},\mathbb{E}} = \underbrace{\mathfrak{S}_{\mathbb{O}_1} \mathfrak{S}_{\mathbb{E}_1} \mathcal{T}_{\mathbb{O}_1,\mathbb{E}_1}}_{\Psi_{\mathbb{O}_1,\mathbb{E}_1}} \cdot \underbrace{\mathfrak{S}_{\mathbb{O}_2} \mathfrak{S}_{\mathbb{E}_2} \mathcal{T}_{\mathbb{O}_2,\mathbb{E}_2}}_{\Psi_{\mathbb{O}_2,\mathbb{E}_2}} \cdot \underbrace{(O_1'', E_2'')(\widehat{\mathcal{O}}_2, \widehat{\mathcal{E}}_1)(O_2'', E_1'')}_{\Psi^{\pi_1;\pi_2}_{\mathbb{O}_1,\mathbb{E}_2;\mathbb{O}_2,\mathbb{E}_1}} \,,$$

where $\mathfrak{S}_{\mathbb{O}}^{-1} = \widetilde{\mathfrak{S}}_{\mathbb{O}}' \widetilde{\mathfrak{S}}_{\mathbb{O}}'' (\widehat{\mathcal{O}}_1, \widehat{\mathcal{O}}_2) \cdot \mathfrak{S}_{\mathbb{O}_1}^{-1} \mathfrak{S}_{\mathbb{O}_2}^{-1}$, $\mathfrak{S}_{\mathbb{E}}^{-1} = \widetilde{\mathfrak{S}}_{\mathbb{E}}' \widetilde{\mathfrak{S}}_{\mathbb{E}}'' (\widehat{\mathcal{E}}_1, \widehat{\mathcal{E}}_2) \cdot \mathfrak{S}_{\mathbb{E}_1}^{-1} \mathfrak{S}_{\mathbb{E}_2}^{-1}$. Each of three permutations marked out in previous expression is generated by corresponding ordered system of transpositions.

Based on that the permutation $\mathcal{T}_{\mathbb{O},\mathbb{E}}$ is any, it follows that the system $\Psi_{\mathbb{O},\mathbb{E}}$ generates permutations of the form $\mathfrak{S}_{\mathbb{O}} \mathfrak{S}_{\mathbb{E}} \mathcal{T}_{\mathbb{O},\mathbb{E}}$ at any π_1 and π_2 as they have been choosing at random. Proposition is proved.

2.3 Part 3

Using relations (4) and (5), we recurrently construct an ordered basis of symmetric group S_n at $n = 2^k$, $k \geqslant 3$.

At each step some sets are partitioned into two equal-sized subsets, that is, if $|\mathbb{A}| = 2t$ then $|\mathbb{A}_1| = |\mathbb{A}_2| = t$. By analogy we shall partition the original set $X = \{1, 2, 3, \ldots, 2^k\}$ and apply (4) to being divided subsets till their minimal size is equal to 4. Let us use that if $\mathbb{A} = \{a_1, a_2, a_3, a_4\}$ then

$$\Psi_{\mathbb{A}} = (a_1, a_3)(a_1, a_4)(a_2, a_3)(a_1, a_2)(a_3, a_4) \tag{6}$$

is the ordered basis of group $S_{\mathbb{A}}$.

Suppose that in relation (5) for all subsets

$$\pi_1 = \pi_2 = \begin{pmatrix} 1 & 2 & \ldots & m-1 & m \\ m & m-1 & \ldots & 2 & 1 \end{pmatrix}, \ 1 \leqslant m \leqslant 2^{k-2}\,. \tag{7}$$

We shall apply (5) until the minimal size of subsets is equal to 2.

Example. Consider $n = 2^3 = 8$, $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Let $X^0 = \{1, 3, 5, 7, 9, 11, 13, 15\}$, $X^1 = \{2, 4, 6, 8, 10, 12, 14, 16\}$, $X^{00} = \{1, 5, 9, 13\}$, $X^{01} = \{3, 7, 11, 15\}$, $X^{10} = \{2, 6, 10, 14\}$, $X^{11} = \{4, 8, 12, 16\}$. Then

$$\Psi_X = \Psi_{X^0}\Psi_{X^1}\ \Psi_{X^0,X^1} = \Psi_{X^{00}}\Psi_{X^{01}}\ \Psi_{X^{00},X^{01}}\ \ \Psi_{X^{10}}\Psi_{X^{11}}\ \Psi_{X^{10},X^{11}}\ \ \Psi_{X^0,X^1}\,.$$

Let ${X^{00}}_0 = \{1, 5\}$, ${X^{00}}_1 = \{9, 13\}$, ${X^{01}}_0 = \{3, 7\}$, ${X^{01}}_1 = \{11, 15\}$, ${X^{10}}_0 = \{2, 6\}$, ${X^{10}}_1 = \{10, 14\}$, ${X^{11}}_0 = \{4, 8\}$, ${X^{11}}_1 = \{12, 16\}$. Then

$$\begin{aligned} \Psi_{X^{00},X^{01}} &= \Psi_{{X^{00}}_0,{X^{01}}_0}\Psi_{{X^{00}}_1,{X^{01}}_1}\Psi^{\pi_1;\,\pi_2}_{{X^{00}}_0,{X^{01}}_1;\,{X^{00}}_1,{X^{01}}_0} \\ \Psi_{X^{10},X^{11}} &= \Psi_{{X^{10}}_0,{X^{11}}_0}\Psi_{{X^{10}}_1,{X^{11}}_1}\Psi^{\pi_1;\,\pi_2}_{{X^{10}}_0,{X^{11}}_1;\,{X^{10}}_1,{X^{11}}_0} \end{aligned}$$

Let ${X^0}_0 = \{1, 3, 5, 7\}$, ${X^0}_1 = \{9, 11, 13, 15\}$, ${X^1}_0 = \{2, 4, 6, 8\}$, ${X^1}_1 = \{10, 12, 14, 16\}$, ${X^0}_{00} = \{1, 3\}$, ${X^0}_{01} = \{5, 7\}$, ${X^0}_{10} = \{9, 11\}$, ${X^0}_{11} = \{13, 15\}$, ${X^1}_{00} = \{2, 4\}$, ${X^1}_{01} = \{6, 8\}$, ${X^1}_{10} = \{10, 12\}$, ${X^1}_{11} = \{14, 16\}$. Then

$$\begin{aligned} \Psi_{X^0,X^1} &= \Psi_{{X^0}_0,{X^1}_0}\Psi_{{X^0}_1,{X^1}_1}\Psi^{\pi_1;\,\pi_2}_{{X^0}_0,{X^1}_1;\,{X^0}_1,{X^1}_0}\,, \\ \Psi_{{X^0}_0,{X^1}_0} &= \Psi_{{X^0}_{00},{X^1}_{00}}\Psi_{{X^0}_{01},{X^1}_{01}}\Psi^{\pi_1;\,\pi_2}_{{X^0}_{00},{X^1}_{01};\,{X^0}_{01},{X^1}_{00}}\,, \\ \Psi_{{X^0}_1,{X^1}_1} &= \Psi_{{X^0}_{10},{X^1}_{10}}\Psi_{{X^0}_{11},{X^1}_{11}}\Psi^{\pi_1;\,\pi_2}_{{X^0}_{10},{X^1}_{11};\,{X^0}_{11},{X^1}_{10}} \end{aligned}$$

Whereas $|X^{00}| = |X^{01}| = |X^{10}| = |X^{11}| = 4$, then applying (6), we obtain

$$
\begin{aligned}
\Psi_X = \; & \underbrace{(1,9)(1,13)(5,9)(1,5)(9,13)}_{\Psi_{X^{00}}} \; \underbrace{(3,11)(3,15)(7,11)(3,7)(11,15)}_{\Psi_{X^{01}}} \\
& \underbrace{(1,3)(5,7)\;(1,7)(5,3)}_{\Psi_{{X^{00}}_0,{X^{01}}_0}} \; \underbrace{(9,11)(13,15)\;(9,15)(13,11)}_{\Psi_{{X^{00}}_1,{X^{01}}_1}} \; \underbrace{(1,15)(5,11)\;(9,7)(13,3)}_{\Psi^{\pi_1;\,\pi_2}_{{X^{00}}_0,{X^{01}}_1;\,{X^{00}}_1,{X^{01}}_0}} \\
& \underbrace{(2,10)(2,14)(6,10)(2,6)(10,14)}_{\Psi_{X^{10}}} \; \underbrace{(4,12)(4,16)(8,12)(4,8)(12,16)}_{\Psi_{X^{11}}} \\
& \underbrace{(2,4)(6,8)\;(2,8)(6,4)}_{\Psi_{{X^{10}}_0,{X^{11}}_0}} \; \underbrace{(10,12)(14,16)\;(10,16)(14,12)}_{\Psi_{{X^{10}}_1,{X^{11}}_1}} \; \underbrace{(2,16)(6,12)\;(10,8)(14,4)}_{\Psi^{\pi_1;\,\pi_2}_{{X^{10}}_0,{X^{11}}_1;\,{X^{10}}_1,{X^{11}}_0}} \\
& \underbrace{(1,2)(3,4)\;(1,4)(3,2)}_{\Psi_{{X^0}_{00},{X^1}_{00}}} \; \underbrace{(5,6)(7,8)\;(5,8)(7,6)}_{\Psi_{{X^0}_{01},{X^1}_{01}}} \; \underbrace{(1,8)(3,6)\;(5,4)(7,2)}_{\Psi^{\pi_1;\,\pi_2}_{{X^0}_{00},{X^1}_{01};\,{X^0}_{01},{X^1}_{00}}} \\
& \underbrace{(9,10)(11,12)\;(9,12)(11,10)}_{\Psi_{{X^0}_{10},{X^1}_{10}}} \; \underbrace{(13,14)(15,16)\;(13,16)(15,14)}_{\Psi_{{X^0}_{11},{X^1}_{11}}} \; \underbrace{(9,16)(11,14)\;(13,12)(15,10)}_{\Psi^{\pi_1;\,\pi_2}_{{X^0}_{10},{X^1}_{11};\,{X^0}_{11},{X^1}_{10}}} \\
& \underbrace{(1,16)(3,14)(5,12)(7,10)\;(9,8)(11,6)(13,4)(15,2)}_{\Psi^{\pi_1;\,\pi_2}_{{X^0}_0,{X^1}_1;\,{X^0}_1,{X^1}_0}}
\end{aligned}
$$

It is easy to see that such construction of ordered basis results in the following recurrent relations for the number of transpositions in ordered systems involved in construction.

Consider relation (5). Let $|\Psi_{\mathbb{O},\mathbb{E}}| = r(n)$, $|\Psi_{\mathbb{O}_1,\mathbb{E}_1}| = |\Psi_{\mathbb{O}_2,\mathbb{E}_2}| = r\left(\frac{n}{2}\right)$.

Since $|\Psi^{\pi_1;\,\pi_2}_{\mathbb{O}_1,\mathbb{E}_2;\,\mathbb{O}_2,\mathbb{E}_1}| = \frac{n}{2}$ then $r(n) = 2 \cdot r\left(\frac{n}{2}\right) + \frac{n}{2}$, and $r(2) = 1$. Therefore,

$$|\Psi_{\mathbb{O},\mathbb{E}}| = r(n) = \frac{n}{2} \log_2 n \; .$$

Consider relation (4). Let $|\Psi_{\mathbb{O}\cup\mathbb{E}}| = l(n)$, $|\Psi_{\mathbb{O}}| = |\Psi_{\mathbb{E}}| = l\left(\frac{n}{2}\right)$. Then

$$l(n) = 2 \cdot l\left(\frac{n}{2}\right) + r(n) \; .$$

Since also $l(4) = 5$ (it follows from (6)) then

$$|\Psi_n| = l(n) = \frac{n}{4} \cdot (\log_2^2 n + \log_2 n - 1) = O(n \log_2^2 n) \; .$$

This implies that at $n = 2^k$ the ordered basis constructed by such recurrent way consists of $O(n \log_2^2 n)$ transpositions. Note that this number differs from the lower bound estimation for the number of transpositions in ordered bases, namely, differs from $\log_2 n!$ only in factor $O(\log_2 n)$.

References

[1] S. A. Kalinchuk, Yu. L. Sagalovich, The problem of minimal ordered basis of symmetric group, *Proc. Tenth Intern. Workshop ACCT*, Zvenigorod, Russia, Sept. 2006, 139-142.