The least known length of ordered basis of symmetric group

S. A. Kalinchuk
Yu. L. Sagalovich
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 $X = \{1, \ldots, n\}$.

Let $T_1, T_2, \ldots, T_r$ be an ordered set of transpositions of $S_X$, where $r \leq C^2_{|X|}$. We shall denote such ordered system of transpositions by $\Psi$ and represent as:

$$\Psi = T_1 T_2 \ldots T_r,$$

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

Definition 1. The system $\Psi$ is called ordered basis of symmetric group $S_X$ if any permutation $P_X \in S_X$ can be represented as

$$P_X = T_1^{\gamma_1} \cdot T_2^{\gamma_2} \cdot \ldots \cdot T_r^{\gamma_r},$$

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

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 $\frac{1}{2} C^2_n$. 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

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

The obtained result is based on that the degree $n$ of symmetric group $S_n$ is chosen to be equal to $n = 2^k$, $k \geq 3$. Such choice allows successively partitioning set of permuted 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 $m \geq 2$. Partition the set $X = \{x_1, \ldots, x_{4m}\}$ into two subsets, $O$ and $E$:

$$O \cup E = X, \ O \cap E = \emptyset, \ |O| = |E| = 2m.$$  \hfill (1)

Let $P_X \triangleq P_{O \cup E}$ be any permutation of group $S_X \triangleq S_{O \cup E}$. It is evident that

$$P_{O \cup E} = (O' \ E' \ O'' \ E'') \cdot (\tilde{O}' \ \tilde{E}' \ \tilde{O}'' \ \tilde{E}''),$$

where $O = O' \cup O'' = \tilde{O}' \cup \tilde{O}''$, $E = E' \cup E'' = \tilde{E}' \cup \tilde{E}''$ and notation

$\begin{array}{cccc}
A \triangleq & a_1 & a_2 & \ldots & a_{|A|} \\
B \triangleq & b_1 & b_2 & \ldots & b_{|B|} \\
|A| = |B|.
\end{array}$

Therefore,

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

$$P_{O \cup E} = P_O \cdot P_E \cdot T_{O,E},$$ \hfill (2)

where $P_O$ and $P_E$ are some permutations belonging to symmetric groups $S_O$ and $S_E$ correspondingly, and a permutation $T_{O,E}$ of group $S_{O \cup E}$ has the form as

$$\begin{pmatrix} O^* & E^* \\
E^* & O^* \end{pmatrix} \triangleq (O^*, E^*), \text{ where } O^* \subseteq O, \ E^* \subseteq E.$$  \hfill (3)

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

**Proposition 2.** Let $\Psi_0$ and $\Psi_E$ be ordered bases of groups $S_O$ and $S_E$ correspondingly. Let $\Psi_{O,E}$ be an ordered system of transpositions of group $S_{O \cup E}$, and this system generates permutations of the form $S_O S_E T_{O,E}$. Then the system

$$\Psi_{O \cup E} = \Psi_O \Psi_E \Psi_{O,E}$$  \hfill (4)

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

**Proof** Follows directly from the factorization (2) and that

$$P_O \cdot P_E \cdot T_{O,E} = \frac{P_O S_O^{-1}}{\Psi_O} \cdot \frac{P_E S_E^{-1}}{\Psi_E} \cdot \frac{S_O S_E T_{O,E}}{\Psi_{O,E}}.$$
2.2 Part 2

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

$$\mathcal{O}_1 \cup \mathcal{O}_2 = \mathcal{O}, \quad \mathcal{O}_1 \cap \mathcal{O}_2 = \emptyset, \quad \mathcal{E}_1 \cup \mathcal{E}_2 = \mathcal{E}, \quad \mathcal{E}_1 \cap \mathcal{E}_2 = \emptyset,$$

where $|\mathcal{O}_1| = |\mathcal{O}_2| = |\mathcal{E}_1| = |\mathcal{E}_2| = \frac{1}{2}|X| = m$.

Let $\mathcal{O}_1 = \{o_1, o_2, \ldots, o_m\}, \mathcal{O}_2 = \{o_1', o_2', \ldots, o_m'\}, \mathcal{E}_1 = \{e_1, e_2, \ldots, e_m\}, \mathcal{E}_2 = \{e_1', e_2', \ldots, e_m'\}$.

Consider an ordered system of transpositions $\Psi_{\alpha_1, \beta_1; \alpha_2, \beta_2}^{\pi_1, \pi_2}$ consisting of $m$ transpositions of the form $(o_i, e_{\pi_1(i)})$ and $\beta$ transpositions of the form $(o_i', e_{\pi_2(i)})$, where $1 \leq i \leq m$, $1 \leq \beta \leq m$, and $\pi_1, \pi_2$ are some permutations defined on the set $\{1, 2, \ldots, m\}$. In expanded form such system is represented as:

$$\Psi_{\alpha_1, \beta_1; \alpha_2, \beta_2}^{\pi_1, \pi_2} = \left(o_1, e_{\pi_1(1)}^{\pi_1}ight) \cdots \left(o_m, e_{\pi_1(m)}^{\pi_1}\right) \left(o_1', e_{\pi_2(1)}^{\pi_2}\right) \cdots \left(o_m', e_{\pi_2(m)}^{\pi_2}\right).$$

**Definition 3.** Consider $\tilde{\mathcal{O}} \subseteq \mathcal{O}, \tilde{\mathcal{E}} \subseteq \mathcal{E}$.

Let $\tilde{\mathcal{O}} \not\sim_{\pi_1, \pi_2} \tilde{\mathcal{E}}$ denote that at any $\tilde{o} \in \tilde{\mathcal{O}}$ and $\tilde{e} \in \tilde{\mathcal{E}}$ transposition $(\tilde{o}, \tilde{e})$ does not belong to the system $\Psi_{\alpha_1, \beta_1; \alpha_2, \beta_2}^{\pi_1, \pi_2}$.

If $\tilde{\mathcal{O}} = \{\tilde{o}_1, \tilde{o}_2, \ldots, \tilde{o}_v\}, \tilde{\mathcal{E}} = \{\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_v\}, |\tilde{\mathcal{O}}| = |\tilde{\mathcal{E}}| = v$ then let $\tilde{\mathcal{O}} \not\sim_{\pi_1, \pi_2} \tilde{\mathcal{E}}$ denote that all transpositions $(\tilde{o}_i, \tilde{e}_i), 1 \leq i \leq v$, belong to the system $\Psi_{\alpha_1, \beta_1; \alpha_2, \beta_2}^{\pi_1, \pi_2}$.

**Proposition 3.** Let $\Psi_{\alpha_1, \beta_1}$ and $\Psi_{\alpha_2, \beta_2}$ be some ordered systems of transpositions generating permutations of the forms $\mathcal{G}_{\alpha_1, \beta_1} \mathcal{T}_{\alpha_1, \beta_1}$ and $\mathcal{G}_{\alpha_2, \beta_2} \mathcal{T}_{\alpha_2, \beta_2}$ correspondingly. Then the system

$$\Psi_{\alpha, \beta} = \Psi_{\alpha_1, \beta_1} \Psi_{\alpha_2, \beta_2} \Psi_{\alpha_1, \beta_1}^{\pi_1, \pi_2} \Psi_{\alpha_2, \beta_2}^{\pi_1, \pi_2}$$

generates permutations of the form $\mathcal{G}_{\alpha, \beta} \mathcal{T}_{\alpha, \beta}$ at any $\pi_1$ and $\pi_2$.

**Proof.** Consider any permutation $\mathcal{T}_{\alpha, \beta} = (\mathcal{O}^*, \mathcal{E}^*)$, where $\mathcal{O}^* \subseteq \mathcal{O}, \mathcal{E}^* \subseteq \mathcal{E}$.

Suppose $\mathcal{O}^* = \mathcal{O}_1^* \cup \mathcal{O}_2^* \subseteq \mathcal{E}^* = \mathcal{E}_1^* \cup \mathcal{E}_2^*$, where $\mathcal{O}_1^* \subseteq \mathcal{O}_1, \mathcal{O}_2^* \subseteq \mathcal{O}_2, \mathcal{E}_1^* \subseteq \mathcal{E}_1, \mathcal{E}_2^* \subseteq \mathcal{E}_2$.

Let $\mathcal{O}_*= \{o_1, o_2, \ldots, o_t\}, \mathcal{E}_* = \{e_1, e_2, \ldots, e_t\}$, and let $\mathcal{O}_*^\alpha = \{o_{\alpha(i)}^\alpha, o_{\beta(i)}^\beta\}, \mathcal{E}_*^\beta = \{e_{\beta(i)}^\beta, e_{\alpha(i)}^\alpha\}$ be the sets obtained by renumbering elements of the corresponding sets $\mathcal{O}^*, \mathcal{E}^*$ by means of permutations $\alpha, \beta$ defined on the set $\{1, 2, \ldots, t\}$: $o_{\alpha(i)}^\alpha = o_{\alpha(i)}^\alpha, e_{\beta(i)}^\beta = e_{\beta(i)}^\beta, 1 \leq i \leq \beta$. It is obvious that at any $\alpha, \beta$ there exist such permutations $\mathcal{G}_{\alpha, \beta}$ of groups $\mathcal{G}_\alpha, \mathcal{G}_\beta$ correspondingly that $(\mathcal{O}^*, \mathcal{E}^*) = \mathcal{G}_{\alpha, \beta} \mathcal{G}_\alpha \mathcal{G}_\beta$.
The sets $O_1^*, O_2^*, E_1^*, E_2^*$ can be partitioned into the following subsets:

- $O_1' \supset O_1^* \subset E_2'$;
- $O_2' \supset O_2^* \subset E_2'$; 
- $O_1' \cap O_1^* = \emptyset, E_2' \cap E_2^* = \emptyset$;
- $O_2' \cap O_2^* = \emptyset, E_2' \cap E_2^* = \emptyset$;
- $O_1' \cup O_2' = E \cup E_2'$;
- $O_1'' \supset O_1^* \subset E'$; 
- $O_2'' \supset O_2^* \subset E'$;
- $O_1'' \cap O_1^* = \emptyset, E_1'' \cap E_1^* = \emptyset$;
- $O_2'' \cap O_2^* = \emptyset, E_2'' \cap E_2^* = \emptyset$.

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

$$T_{O^*, E^*} = (O^*, E^*) = \tilde{E} \tilde{E} \tilde{E} \cdot (O', E')(O_1', E_1') \cdot (O_2', E_2').$$

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 $O_1 \cup \tilde{O}_1 = O_1$, $O_1 \cap \tilde{O}_1 = \emptyset$, $E_2 \cup \tilde{E}_2 = E'_2$, $E_2 \cap \tilde{E}_2 = \emptyset$, $\tilde{O}_1 = E_1'$, $\tilde{O}_2 = O_2'$, where $|O_1'| = |E_1'|$, $|O_2'| = |E_2'|$, $|\tilde{O}_1| = |\tilde{E}_2|$. Also $\tilde{O}_1 \supset \tilde{O}_1 \supset \tilde{E}_2$, since $O' > E'$.

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

$$(O', E') = \tilde{E} \tilde{E} \tilde{E} \cdot (O_1, E_1)(O_2, E_2)(\tilde{O}_1, \tilde{E}_2).$$

It is clear, there exist such sets $\tilde{O}_2 \subset O_2$, $\tilde{E}_1 \subset E_1$ that

$$\tilde{O}_2 \supset \tilde{O}_1 \subset \tilde{E}_2, |\tilde{O}_2| = |\tilde{E}_2|; \tilde{O}_2 \cap \tilde{E}_2 = \emptyset, E_1 \cap \tilde{E}_1 = \emptyset.$$

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

This implies that

$$(O', E') = \tilde{E} \tilde{E} \tilde{E} \cdot (O_1, E_1)(O_2, E_2) \cdot (\tilde{O}_1, \tilde{E}_2)(\tilde{O}_2, \tilde{E}_2) \cdot (\tilde{O}_1, \tilde{E}_1)(\tilde{O}_2, \tilde{E}_2) \cdot (\tilde{O}_2, \tilde{E}_1).$$

Since $O_1 \cap \tilde{O}_1 = \emptyset, O_2 \cap \tilde{O}_2 = \emptyset, E_1 \cap \tilde{E}_1 = \emptyset, E_2 \cap \tilde{E}_2 = \emptyset$, it follows that

$$T_{O^*, E^*} = \tilde{E} \tilde{E} \tilde{E} \cdot (O_1, E_1)(O_2, E_2) \cdot (\tilde{O}_1, \tilde{E}_2)(\tilde{O}_2, \tilde{E}_2) \cdot (\tilde{O}_1, \tilde{E}_1)(\tilde{O}_2, \tilde{E}_2) \cdot (\tilde{O}_2, \tilde{E}_1).$$

Each of the systems $\Psi_{O_1, E_1}, \Psi_{O_2, E_2}$ generates permutations of the forms $G_{O_1} G_{E_1} T_{O_1, E_1}, G_{O_2} G_{E_2} T_{O_2, E_2}$ correspondingly. Suppose

$$T_{O_1, E_1} = (O_1, E_1)(\tilde{O}_1, \tilde{E}_1), T_{O_2, E_2} = (O_2, E_2)(\tilde{O}_2, \tilde{E}_2).$$

Then

$$G_{O} G_{E} T_{O, E} = G_{O_1} G_{E_1} T_{O_1, E_1} \cdot G_{O_2} G_{E_2} T_{O_2, E_2} \cdot (O_1'', E_2')(\tilde{O}_2, \tilde{E}_2) \cdot (O_1', E_1')(\tilde{O}_1, \tilde{E}_1),$$

where $G_{O}^{-1} = \tilde{E} \tilde{E} \tilde{E} \cdot (O_1, E_1)(O_2, E_2) \cdot (\tilde{O}_1, \tilde{E}_2)(\tilde{O}_2, \tilde{E}_2)$.

Each of three permutations marked out in previous expression is generated by corresponding ordered system of transpositions.

Based on the fact that the permutation $T_{O, E}$ is any, it follows that the system $\Psi_{O, E}$ generates permutations of the form $G_{O} G_{E} T_{O, E}$ at any $\pi_1$ and $\pi_2$ as they have been chosen 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 \( n = 2^k, k \geq 3 \).

At each step some sets are partitioned into two equal-sized subsets, that is, if \( |A| = 2t \) then \( |A_1| = |A_2| = t \). 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 \( \mathcal{A} = \{a_1, a_2, a_3, a_4\} \) then

\[
\Psi_{\mathcal{A}} = (a_1, a_3)(a_1, a_4)(a_2, a_3)(a_1, a_2)(a_3, a_4)
\]

is the ordered basis of group \( S_\mathcal{A} \).

Suppose that in relation (5) for all subsets

\[
\pi_1 = \pi_2 = \begin{pmatrix} 1 & 2 & \ldots & m-1 & m \\ m & m-1 & \ldots & 2 & 1 \end{pmatrix}, \ 1 \leq m \leq 2^{k-2}.
\]

(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

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

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

\[
\Psi_{X^{00}, X^{01}} = \Psi_{X^{00}, X^{01}} \Psi_{X^{00}, X^{01}} \Psi_{X^{00}, X^{01}} \Psi_{X^{10}, X^{11}} \Psi_{X^{10}, X^{11}} \Psi_{X^{00}, X^{01}} \Psi_{X^{10}, X^{11}} \Psi_{X^{10}, X^{11}}.
\]

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

\[
\Psi_{X^0, X^1} = \Psi_{X^0, X^1} \Psi_{X^0, X^1} \Psi_{X^0, X^1} \Psi_{X^0, X^1} \Psi_{X^0, X^1} \Psi_{X^0, X^1} \Psi_{X^0, X^1} \Psi_{X^0, X^1}.
\]

Whereas \( |X^{00}| = |X^{01}| = |X^{10}| = |X^{11}| = 4 \), then applying (6), we obtain
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 $|\Psi_{O,2}| = r(n)$, $|\Psi_{O_1,E_1}| = |\Psi_{O_2,E_2}| = r\left(\frac{n}{2}\right)$. Since $|\Psi_{O_1,E_2;O_2,E_1}| = \frac{n}{2}$ then $r(n) = 2 \cdot r\left(\frac{n}{2}\right) + \frac{n}{2}$, and $r(2) = 1$. Therefore,

$$|\Psi_{O_2}| = r(n) = \frac{n}{2} \log_2 n.$$ 

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

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

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

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

This implies that at $n = 2^k$ the ordered basis constructed by such recurrent way consists of $O(n \log_2^n)$ 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