SEQUENTIAL GENERATION OF ARRANGEMENTS BY MEANS OF A BASIS OF TRANSPOSITIONS

V. L. Kompel'makher and V. A. Liskovets

UDC 519.1+519.4

It is well known ([1], p. 28) that all n! arrangements of n symbols can be ordered without repetition so that each can be obtained from the previous one by a single transposition. This assertion is used to generate arrangements and in certain theoretical and applied investigations. On the other hand, to generate the symmetric group of permutations of degree n a basis of n − 1 transpositions is sufficient. There naturally arises this question: is it possible to order all arrangements of a given degree so that each can be obtained from the previous one by a single transposition from an arbitrary fixed basis? In this paper we give an affirmative answer to this question. Moreover, for an arbitrary basis of transpositions the arrangements can be ordered so that the first can also be obtained from the last by a single basic transposition. A key role in the proof is played by the star-shaped basis $\{(1, i)\}_{i=2}^{n}$. In this case, which is of practical importance, we describe an effective algorithm for the sequential generation of all arrangements. There is a graphical interpretation of our result. The graph whose vertices are the arrangements of degree n and whose edges correspond to transitions under the transpositions of the given basis is Hamiltonian.

The general question of the possibility of sequentially constructing without repetition all elements of an arbitrary finite group by means of a given system of generators was raised by Rapaport [3] (see also [2]).

Definitions and Lemmas

Let us make a few definitions. We remark that the transposition $t_{i,j}$ = (i, j) interchanges the symbols in the arrangement occupying the i-th and j-th places. A transposition or, in general, a permutation will be written to the left of a symbol or arrangement on which it acts, so that $(t_1 \cdot t_2)(a) = t_1(t_2(a))$.

Let us fix a basis (of transpositions) B in the symmetric group of degree n. A sequence S of d distinct arrangements in which each can be obtained from the previous one by a single transposition of B is called a *regular B-sequence* of length d and degree n (or simply a sentence, since we will consider only regular sequences, if the basis is understood). A regular B-sequence of length n! of arrangements of degree n is called a *complete B-sequence*. By the *carrier* (or *B-carrier*) H = H(S) of a B-sequence S we mean the sequence of d − 1 transpositions indicated in the definition. A sequence of arrangements is uniquely determined by its carrier and its initial arrangement, the choice of which is inessential and which is usually taken to be (1, 2, 3, ..., n). To each carrier H there corresponds a *total permutation* A(H), equal to the product of all transpositions of the carrier in the order indicated, so that the total permutation applied to the first arrangement in the sequence yields the last. A sequence of degree n with carrier H is called *cyclic* if A(H) is a cycle of length n; a sequence is called *closed* if the total permutation of its carrier is a basic transposition. A complete closed B-sequence is called a *Hamiltonian B-sequence.*

The crux of our problem is the question of the existence of Hamiltonian B-sequences of degree n for any n-basis B.

If the total permutation of a carrier is a basic transposition, then we can construct a new carrier as follows. In the first place we put the k-th transposition of the original carrier (k arbitrary), in the second place the next transposition, and so on. After the last transposition of the original carrier we put the total transposition, then the first, the second, and so on up to and including the (k − 2)-nd. We obtain a new carrier with the (k − 1)-st transposition as the total permutation, which is the carrier of the regular B-sequence obtained by the corresponding cyclic shift of the original sequence. Thus, we have proved the following lemma.

LEMMA 1. Given a closed sequence, there exists a sequence of the same arrangements for which the total permutation of the carrier is any transposition occurring in the carrier.

Translated from Kibernetika, No. 3, pp. 17-21, May-June, 1975. Original article submitted March 23, 1973.

LEMMA 2. If there exists a cyclic complete B-sequence of degree n, then there exists a Hamiltonian B_1-sequence of degree n + 1, where B_1 is any basis of degree n + 1 obtained from B by the addition of a single transposition.

Proof. Suppose H is the carrier of a complete B-sequence of degree n to which there corresponds a cyclic total permutation A. If we add to all arrangements a new symbol n + 1 in the (n + 1)-st place, we obtain a regular B_1-sequence of degree n + 1 with the same carrier. The transposition added to B has the form $(a, n + 1)$, $1 \leqslant a \leqslant n$. Consider the following carrier (a carrier will be represented within square brackets):

$$D = [H^{(1)};\ (a, n+1), H^{(2)};\ (a, n+1), \ldots; (a, n+1), H^{(n+1)}],$$

where $H^{(1)} = H^{(2)} = \ldots = H^{(n+1)} = H$.

The number of arrangements in the sequence corresponding to the carrier D is (n + 1)!; we wll show that they are distinct. Indeed, the transpositions of the carrier H do not affect the symbol occupying the (n + 1)-st place. Thus, it suffices to show that on applying $H^{(i)}$ and $H^{(j)}$, $i \neq j$, different symbols occupy the (n + 1)-st place. But this follows from the cyclicity of the permutation $(a, n + 1)A$, which is the total permutation of the carrier $[(a, n + 1), H]$. Thus, we have constructed a carrier which produces a complete regular B_1-sequence. To the carrier corresponds the permutation $A((a, n + 1)A)^n = (a, n + 1)$, i.e., this sequence is Hamiltonian. The lemma is proved.

In the proof of Lemma 2 we constructed a new sequence of degree n + 1 by repeatedly using carriers of a sequence of degree n. The carrier of a complete sequence of degree n + 1 of the form

$$[H_1; (a, n+1), H_2; (a, n+1), \ldots; (a, n+1), H_{n+1}],$$

where H_i is the carrier of a complete sequence of degree n, is called a *block carrier.* The corresponding sequence is called a *block sequence.* A part of such a sequence of length n! with the same symbol in the (n + 1)-st place is called an *n-block*, and the corresponding carrier H_i is called a *block* of the carrier.

Main Theorem

Let us now state the main result of this paper.

THEOREM. Given any basis of transpositions, there exists a Hamiltonian sequence of arrangements.

Proof. As is well known, any basis Q_n of the symmetric group of degree n can be represented as a tree with n labeled vertices (see [2], p. 28). Therefore, by a suitable relabeling it can be represented in the following form: Q_n, $n \geqslant 3$, is the union of the star-shaped basis

$$Z = Z_{k+1} = \{(1, 2), (1, 3), \ldots, (1, k+1)\},$$
$$2 \leqslant k \leqslant n-1,$$

and a set $G = G(Q_n)$ of $d(Q_n) = n - k - 1$ transpositions which do not move the elements in the first and second places such that any symbol m, $k + 1 < m \leqslant n$, occurs in exactly one transposition $(l, m) \in G$ with $2 < l < m$. In particular, the symbol n (and also the symbol 2) occurs in a unique transposition of Q_n.

1. First consider the case where G is empty, i.e., $Q_n = Z_n = Z$. We will prove the theorem by induction. For n = 2 and n = 3 the theorem is obvious. Suppose the assertion is true for some odd $n = m \geqslant 3$. Then, by Lemma 1, there exists a carrier H_k of a complete sequence of arrangements of degree m with total transposition (1, k), $2 \leqslant k \leqslant m$.

Consider the following block carrier:

$$F = F_{m+1} = [H_m; (1, m+1), H_{m-1};\ (1, m+1), H_{m-2}; \ldots; H_2; (1, m+1), H_m;\ (1, m+1), H_m].$$

This carrier produces (m + 1)! arrangements of degree m + 1; we will show that these are distinct. Indeed, let the initial arrangement be (1 2 ... m m + 1). then for $1 < k \leqslant m$ the total permutation (1, m)(1, m + 1) (1, m − 1)(1, m + 1) ... (1, m − k + 2)(1, m + 1) of the first k − 1 blocks of the carrier puts in the (m + 1)-st place the symbol m − k + 2. This is also easily verified for k = m + 1 and is obvious for the (m + 1)-st element of the first block. Thus, the arrangements of different blocks are distinct. Therefore, the carrier F produces a complete Z-sequence of degree m + 1. Its total permutation is A(F) = (1, m)(1, m + 1) (1, m − 1)(1, m + 1)(1, m − 2) ... (1, 2)(1, m + 1) × (1, m) (1, m + 1) (1, m) = $\begin{pmatrix} 123 \ldots m-1 & m & m+1 \\ 345 \ldots m+1 & 2 & 1 \end{pmatrix}$.

Since m + 1 is even, A(F) is a cyclic permutation. By Lemma 2, there exists a Hamiltonian Z-sequence of degree m + 2. Thus, we have proved that for any odd degree there exists a Hamiltonian Z-sequence.

Let us now consider even degrees. It is easy to construct a Hamiltonian Z-sequence for n = 4.* Suppose there exists a Hamiltonian Z-sequence for an even $m \geqslant 4$; we will show that such a sequence exists for n = m + 2. Again by Lemma 1, there exists a Hamiltonian Z-sequence of degree m with carrier H_k having total transposition (1, k), k = 2, ..., m. Let $b = (r_2 r_3 \dots r_m)$ be some arrangement of the symbols 2, 3, ..., m. Consider the following block carrier:

$$C(b) = [H_{r_2}; (1, m+1), H_{r_m}; (1, m+1), H_{r_2};$$
$$(1, m+1), H_{r_3}; \dots; H_{r_{m-1}}; (1, m+1), H_{r_m}].$$

As above, it is easy to show that this carrier produces a regular Z-sequence of degree m + 1. The total permutation corresponding to this carrier has the form

$$A(b) = \begin{pmatrix} 1 & m+1 & r_{m-1} & r_{m-3} \dots r_7 & r_5 & r_3 & r_m & r_{m-2} \dots r_6 & r_4 & r_2 \\ m+1 & r_{m-1} & r_{m-3} & r_{m-5} \dots r_5 & r_3 & r_m & r_{m-2} & r_{m-4} \dots r_4 & 1 & r_2 \end{pmatrix}.$$

(note, by the way, that it must be odd).

By Lemma 1 and the assertion of the theorem proved above, there exists for $Z = Z_{m+1}$ with even m a carrier N_k of a Hamiltonian Z-sequence of degree m + 1 corresponding to any basic transposition of Z_{m+1}. To construct a Hamiltonian Z_{m+2}-sequence we consider the following block carrier:

$$K = [N_{m+1}; (1, m+2), N_m; (1, m+2), N_{m-1}; \dots; N_2; (1, m+2), C(b); (1, m+2), C(b')],$$

where $b' = (r'_2 r'_3 \dots r'_m)$ is some arrangement of the symbols 2, 3, ..., m. There corresponds to this carrier the total permutation

$$T = \begin{pmatrix} 1 & 2 & 3 & 4 \dots & m & m+1 & m+2 \\ 3 & 4 & 5 & 6 \dots & m+2 & 1 & 2 \end{pmatrix} A(b) \cdot (1, m+2) \cdot A(b').$$

(compare with K and F_{m+2}). Choose b and b' so that

$$T = (1, m + 2).$$

This equality represents an equation in the unknowns $r_2, r_3, \dots, r_m, r'_2, r'_3, \dots, r'_m$. Put $r_i = r'_i$ for i = 3, $i \geqslant 5$ and $r_2 = r'_4$, $r_4 = r'_2$. Then $T(r_2) = 2$, which implies that $r_2 = 2$. Analogously, we determine in succession the following values of the unknowns: $r_4 = 3$, $r_6 = 4$, $r_8 = 5, \dots, r_m = \frac{m}{2} + 1$, $r_3 = \frac{m}{2} + 2, \dots, r_{m-1} = m$. Consequently, we can take $b = \left(2 \left(\frac{m}{2} + 2\right) 3 \left(\frac{m}{2} + 3\right) 4 \dots (m-1) \frac{m}{2}\, m \left(\frac{m}{2} + 1\right)\right)$, $b' = \left(3 \left(\frac{m}{2} + 2\right) 2 \left(\frac{m}{2} + 3\right) 4 \dots m \left(\frac{m}{2} + 1\right)\right)$.

Thus, we have found the explicit form of the permutations A(b) and A(b'), hence also of the desired carrier K whose total permutation is a transposition of Z_{m+2}. Exactly as for the carrier F it can be proved that the carrier K produces a regular Z-sequence of degree m + 2. Thus, the assertion of the theorem is proved for the basis Z.

2. Let us say that a Q_n-carrier H possesses property II if in the corresponding regular sequence of arrangements beginning with $(\alpha_1 \alpha_2 \dots \alpha_m)$, $m \geqslant n$, there exists for any j, $3 \leqslant j \leqslant n$, and any i, $i \leqslant n$, an arrangement with the symbol α_i in the j-th place which can be obtained from the previous arrangement by the transposition (1, 2) or is the initial arrangement. We denote by Π' the analogous property satisfied for all k, $3 \leqslant j \leqslant n - 1$, and all i, $1 \leqslant n - 1$. Clearly, these properties do not depend on the choice of initial arrangement. Moreover, if H possesses property Π (or Π') and is the carrier of a closed sequence, then it is obvious that any carrier obtained from H by a cyclic shift possesses the same property.

We remark that in our block construction the carrier of a Hamiltonian Z-sequence of degree n possesses property Π. Let us prove this assertion by induction on n. For n = 3 it can be verified directly. Suppose it is true for some n = m $\geqslant$ 3; let us prove it for n = m + 1. Since the constructed carriers have a block structure and all blocks are obtained by a cyclic shift from a carrier of smaller degree, it suffices for the proof to show that by means of the transposition (1. 2) we can obtain an arrangement with the symbol m + 1 in an arbitrary place different from the first and the second, and with an arbitrary element in the (m + 1)-st place. The first part of the statement follows immediately from the fact that the carrier of any m-block possesses

*This can be done, for example, by means of the carrier $K = [N_3; (1, 4), N_2; (1, 4), N_3; (1, 4), N_2]$, where $N_2 = [(1, 3), (1, 2), (1, 3), (1, 2), (1, 3)]$, $N_3 = [(1, 2), (1, 3), (1, 2), (1, 3), (1, 2)]$.

property Π and that there are blocks for which one of the moved symbols (i.e., a symbol in one of the first m places) is m + 1. The second follows from the fact that distinct m-blocks contain distinct symbols in the (m + 1)-st place and their carriers contain the transposition (1, 2).

3. Suppose now that $G(Q_n)$ is nonempty, i.e., $d(Q_n) > 0$.

We will prove an assertion stronger than that of the theorem, namely, for any basis Q_n there exists a Hamiltonian sequence with total permutation (1, 2) whose carrier $E(Q_n)$ possesses property Π. The proof is by induction on the size of $G(Q_n)$ and uses the fact that the assertion was proved (in Sec. 2) when G is empty. Suppose the assertion is true for bases Q with d(Q) = d, d ⩾ 0; let us prove it for Q_n with $d(Q_n) = d + 1$. There exists in Q_n a unique transposition of the form (*a*, n), where $a \geqslant 3$. Therefore, $Q_n = Q_{n-1} \cup \{(a, n)\}$, where $d(Q_{n-1}) = d$. The carrier $E = E(Q_{n-1})$ satisfies our assumption. Put $E'_1 = E$ and consider the carrier $E_2 = [E'_1; (a, n), E]$. It corresponds to a regular closed Q_n-sequence S_2 of length 2(n − 1)!, has total permutation (1, 2)(*a*, n)(1, 2) = (*a*, n), and possesses property Π'. We pass by a cyclic shift from E_2 to a carrier E'_2 with total transposition (1, 2), which occurs in E_2 in a place such that in the *a*-th place of the arrangement of S_2 obtained by its application there occurs a symbol not found in the n-th place of the arrangements of S_2. This is possible by property Π' and the fact that not all symbols occur in the n-th place (only two do). Then $E_3 = [E'_2; (a, n), E]$ corresponds to a regular closed sequence of length 3(n − 1)! and possesses property Π'. This allows us to pass in a similar way to E'_3, and so on. At the (n − 1)-st step we obtain the carrier $E_n = E'_{n-1}$; (*a*, n), E] of a Hamiltonian Q_n-sequence. According to the construction and in view of property Π for E, the sequence corresponding to E_i and beginning with $(\alpha_1 \alpha_2 ... \alpha_n)$, contains arrangements obtained from the previous ones by the transposition (1, 2) with the symbol α_n in any place other than the first, second, and n-th, and with certain i − 1 symbols different from α_n in the n-th place. When i = n, this together with property Π' means that E_n possesses property Π. To complete the proof we need only obtain from E_n by a cyclic shift a carrier E'_n with total transposition (1, 2) and put $E(Q_n) = E'_n$. The theorem is completely proved.

Remark 1. As Rapaport showed in [3], it is easy to construct a Hamiltonain sequence of arrangements with carrier of the form D with respect to the basis of degree n consisting of the permutations (1, 2), (1, 2)(3, 4), (1, 2)(3, 4)(5, 6), ..., (2, 3), (2, 3)(4, 5), and (2, 3)(4, 5)(6, 7), ... Moreover, she established the existence of a Hamiltonian sequence with respect to the basis consisting of the three permutations (1, 2), (1, 2)(3, 4)(5, 6) ..., and (2, 3)(4, 5)(6, 7) ... .

Remark 2. For the chain-basis of transpositions {(i, i + 1)} there exists the following simple algorithm for constructing a Hamiltonian sequence, which was given in [4], a carrier of degree n(n ⩾ 3) is obtained from a carrier of degree n − 1 by inserting before each transposition and at the end a chain of transpositions which successively move the symbol n from one end to the other. More precisely, we insert in turn the chains (n, n − 1), (n − 1, n − 2), ..., (2, 1) and (1, 2), (2, 3), ..., (n − 1, n), beginning with the first, and at each insertion the symbols of the following transposition are increased by 1, since all symbols of the previous arrangement of degree n − 1 are shifted one place to the right.

An Algorithm for Generating Arrangements

The simplest way to generate arrangements with respect to the basis Z is by successively constructing carriers of the form D and F (when n is even the resulting sequence of arrangements is not Hamiltonian). It is evident from the construction of D and F that the resulting sequence possesses the following important property.

COROLLARY. A complete Z-sequence of degree n constructed by means of carriers of the form D or F (depending on the parity of n) is a natural extension of the analogous sequence of degree n − 1.

This property allows us to consider the corresponding carrier as an infinitely extended sequence of transpositions. We now give an algorithm for finding the transposition occurring in the (N − 1)-st place of this carrier. We will assume that in the construction of F_{m+1} the block H_k is obtained from $H = H_m$ by a shift to the first occurrence of the transposition (1, k).* Obviously, it first occurs in the (k − 1)!-st place.

We expand the number N(N > 1) in terms of the factorials of the natural numbers:

$$N = a_1 1! + a_2 2! + \dots + a_l l!,$$

*Another convenient method would be to switch in H the names of the symbols m and k.

where $0 \leqslant a_i \leqslant i$, $a_l > 0$. Obviously, this expansion is uniquely determined. Let $\varphi_k(i, j)$ denote the transposition occurring in the (i − 1)-st place in the j-th block of the carrier of degree k + 1 (each block has its own numbering), where $2 \leqslant i \leqslant k!$, $1 \leqslant j \leqslant k+1$. By construction, the first arrangement of a k-block is obtained by the transposition (1, k + 1), so that we put

$$\varphi_k(1, j) = (1, k+1) \qquad (*)$$

for all j, $1 < j \leqslant k + 1$.

We are interested in the value $\varphi_{l+1}(N, 1)$. It is easy to see that $\varphi_{l+1}(N, 1) = \varphi_l(M, j)$, where

$$(M, j) = \begin{cases} (l!, a_l), & \text{if } N = a_l l!; \\ (N - a_l l!, a_l + 1) & \text{otherwise.} \end{cases}$$

Also, when j > 1

$$\varphi_l(M, j) = \begin{cases} \varphi_l(M, 1), & \text{if } l \text{ is even or } j = l,\ l+1; \\ \varphi_l(K, 1) & \text{otherwise.} \end{cases}$$

The value K is determined as follows. In the present case we are dealing with the j-th block of the carrier F_{l+1} with total permutation $(1, l - j + 1)$. Thus, this block is obtained from $H = H_l$ by a shift by $(l - j)!$. Thus, $K = M + (l - j)!$ if $M + (l - j)! \leqslant l!$, and $K = M + (l - j)! - l!$ otherwise.

It remains to consider j = 1, $N = l!$. The last block of a carrier of degree $l + 1$ is a carrier of degree l. Therefore, $\varphi_l(l!, 1) = \varphi_{l-1}((l-1)!, 1) = \ldots = \varphi_2(2, 1) = (1, 2)$, i.e.,

$$\varphi_l(l!, 1) = (1, 2), \qquad l \geqslant 1. \qquad (**)$$

In at most l steps involving the above reduction of N to M and K we arrive at the possibility of using (*) or (**), which yields the desired transposition.

Here are the first 24 transpositions of the carrier under consideration [where, for brevity, we simply write k instead of (1, k)]: [2,3,2,3,2,4,3,2,3,2,3,4, 2,3,2,3,2,4,2,3,2,3,2,5].

Note that in this carrier of degree n the transposition (1, 2) occurs $\left(1 - \frac{1}{2!} - \frac{1}{4!} - \frac{1}{6!} - \ldots - \frac{1}{\left(2\left[\frac{n}{2}\right]\right)!}\right)$ times.

Using the block nature of the construction, the N-th arrangement of the sequence can be found without finding all previous arrangements. Namely, let $\omega_k(j)$ denote the total permutation of the j-th k-block of the carrier. Its form is evident from the construction of F and D. Let

$$\Delta_{k,j}^{(N)} = \begin{cases} 0, & \text{if } a_1 = a_2 = \ldots = a_{k-1} = 0,\ a_k = j,\ k \geqslant 1; \\ 1 & \text{otherwise.} \end{cases}$$

Then it is easy to show that the N-th arrangement of the sequence is obtained from the initial one by applying the permutation

$$g_N = \prod_{k=l}^{1} \prod_{j=1}^{a_k} \omega_k(j)\,(1, k+1)^{\Delta_{k,j}^{(N)}},$$

where the inner product is taken to be the identity permutation if $a_k = 0$.

LITERATURE CITED

1. A. G. Kurosh, A Course in Higher Algebra [in Russian], Nauka, Moscow (1971).
2. O. Ore, Theory of Graphs, American Mathematical Society (1967).
3. E. S. Rapaport, "Cayley color groups and Hamilton lines," Scripta Math., 24, No. 1 (1959).
4. S. M. Johnson, "Generation of permutations by adjacent transpositions," Math. Comput., 17, No. 83 (1963).