A STUDY OF A CLASS OF PERMUTATIONS

BY

KAMAL DANDAN

A STUDY OF A CLASS OF PERMUTATIONS

BY

KAMAL DANDAN

Submitted in Partial Fullfillment for the Requirements
of the Degree Master of Science
in the Mathematics Department of the
American University of Beirut
Beirut, Lebanon,
1965.

Acknowledgements

I wish to thank the professors who helped me during my work on this paper, namely, Prof. Peter Yff (with whom I worked in 1963-64) and Prof. Robert Stoll (with whom I worked in 1964-65).

Table of Contents

Summary

The principal result of this thesis is the derivation of a new set of generators for the symmetric group S_m on m symbols. For each $m > 2$, when $m \equiv 2 \pmod 4$ the permutations $(1, \frac{m-2}{2})_m$, $(1, \frac{m}{2})_m$, and $(1, \frac{m+2}{2})_m$, defined in part 3. of this paper, generate S_m. Then when $m \equiv 3 \pmod 4$ the permutations $(1, \frac{m-1}{2})_m$, $(1, \frac{m+1}{2})_m$, and $(1, \frac{m+3}{2})_m$ generate S_m. Analogous results can be obtained for $m \equiv 0,1 \pmod 4$.

1. A Note on the Genesis of the Permutation Idea

A friend posed the following problem. Given thirteen cards he asked me to arrange the cards in such a way that having finished the arrangement, the following process, say W, applied to the arranged set will yield successively the cards numbered with 1,2,3,...,13 (the cards are numbered from 1 to 13) in that order. The process W is the following: Starting with the set of thirteen cards (face not shown) the topmost card is placed at the bottom then the next card is exposed and put aside. The process is repeated until all the cards are shown, and these must appear in the order 1,2,3,...13.

My ideas on the topic had their start from this simple problem. (The reader should refer to part 3 before reading the next para)

We observe that the permutation $(1,1)_{13}$ can give the solution to the above mentioned problem as shown below. Arranging the permutation rows vertically we have,

1	7
2	1
3	12
4	2
5	8
6	3
7	11
8	4
9	9
10	5
11	13
12	6
13	10

where the left column is transformed into the right column (thus 1 is transformed into 7, 2 into 1 etc.) The right column gives the arrangement of the thirteen cards that one has to start with in order to get the required sequence 1,2,3,...,13, after the process W is appbied to the set of cards.

2. Notes On The Symmetric Group

A permutation of a finite set S of symbols is a one-one mapping of S onto itself. For example, if S = {1,2,3,4,5}, then, the mapping A on S such that A(1) = 3, A(2) = 5, A(3) = 2, A(4) = 1, and A(5) = 4, is a permutation. It is convenient to write $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$ to express the fact that the image of 1 under A is 3, etc.

If L is a permutation of S such that for some subset $\{ s_1, s_2, \ldots, s_k \}$ of S, $L(s_i) = s_{i+1}$, (i = 1,2,...,k-1) and $L(s_k) = s_1$, while the image of each remaining element of S is itself, then L is called a k-cycle, and we write, $L = (s_1, s_2, \ldots, s_k)$.

The product AB of permutations A and B is defined as the permutation obtained by first carrying out A then B. For example, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$

A result of the elementary theory of permutations is that any permutation can be expressed uniquely apart from order as the product of mutually disjoint cycles. For eg. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = (1,3) (2,5,4)$.

The set of all permutations on m symbols form a group under multiplication. This group is called the symmetric group of degree m and is denoted by S_m.

Theorem 1. Any member of S_m can be expressed as a product of cycles from the set { (1,2), (2,3),..., (m-1,m) }.

As every permutation can be expressed as a product of cycles, it suffices to prove that each cycle can be expressed as stated in the theorem. Thus, consider $(p_1, p_2, \ldots, p_r)$, $r \leq m$. We observe that $(p_1, p_2, \ldots, p_r) = (p_1, p_2)(p_1, p_3) \ldots (p_1, p_r)$. The proof is completed by showing that any cycle (h,s), where $h \leq m$ and $s \leq m$ can be expressed as a product of cycles from the set { (1,2), (2,3),..., (m-1,m) }. First we prove that all cycles (1,n) can be expressed in this way. We have,

(1,2)

(1,3) = (1,2) (2,3) (1,2)

(1,4) = (1,3) (3,4) (1,3) , and in general,

(1,n) = (1,n-1) (n-1,n) (1,n-1). Now, having (1,h) and (1,s), we can get (h,s) in the desired form as (h,s) = (1,h) (1,s) (1,h). The above result can be stated thus: The set of permutations { (1,2), (2,3),..., (m-1,m) } generate the symmetric group of order m.

The reader is referred to the book Introduction to the Theory of Finite Groups by Walter Ledermann for a fuller treatment of the ideas presented above.

3. The Permutation $(1,n)_m$

Definition of $(1,n)_m$

Denote by P the set of positive integers and let P_r denote the subset $\{1,2,\ldots,r\}$ of P. For each positive integer n we shall define an operation X on the collection of ordered t-tuples of elements of P_t, for $t = 1,2,\ldots$. The role of this operation is to facilitate the definition of certain permutations.

For an ordered t-tuple $D_o = (i_1,i_2,\ldots,i_t)$ we define $XD_o = D_1 = (i_{n+2},\ldots,i_t,i_1)$. Thus X shifts the first member of D_o to the last position and then the set $S_1 = (i_2,i_3,\ldots,i_{n+1})$ of n elements is discarded from the new t-tuple formed. Applying X, in turn, to D_1 gives $XD_1 = D_2 = (i_{2n+3},\ldots,i_t,i_1,i_{n+2})$ with $S_2 = (i_{n+3},i_{n+4},\ldots,i_{2n+2})$, another set of n elements discarded as before. This process is continued, thus obtaining successively D_3, $D_4,\ldots$.

Now the following possibilities are considered:

(a) $n|t$. Let $n.d=t$.
We observe that D_o has t elements, D_1 has t-n elements, and in general D_r has t-n.r elements. Then D_d has t-d.n=0 elements.
So $D_d = \emptyset$.

(b) $n\nmid t$. Let $t=n.k+s$, $0<s<m$.
Reasoning as above D_k has s elements. To obtain D_{k+1} we apply X on D_k and then drop a set of s elements S_{k+1} (in this case, as there are less than n elements left all of them are dropped)
So $D_{k+1} = \emptyset$.

Now we define the permutations $(1,n)_m$ of P_m as follows: Starting with $D_o = (1,2,\ldots,m)$, we apply X to D_o etc., obtaining successively D_1, $D_2,\ldots,\emptyset$ with the corresponding sets $S_1,S_2,\ldots,\emptyset$.

We then map the n elements of S_1 on $1,2,\ldots,n$ in the order with which they occur in S_1. Thus the mapped elements of S_1 give $\begin{pmatrix} 2 & 3 & \ldots & n+1 \\ 1 & 2 & \ldots & n \end{pmatrix}$. S_2 is mapped similarly on the next block of n integers in P_m, etc. Now if $n \nmid m$, then some S_i will be reached which has less than n elements (If $m=n.k+s$ then S_i will have s elements as in (b) above). This block of s integers is mapped on the remaining block of s integers in P_m. The above mappings of the S's on segments of P_m define the permutation $(1,n)_m$.

As a numerical example consider $(1,4)_{10}$. Starting with $D_o = (1,2,\ldots,10)$, we apply X to D_o i.e. we shift 1 to a position after 10 and then drop the first 4 integers of the new 10-tuple.

$D_1 = (6,7,8,9,10)$ with $S_1 = (2,3,4,5)$, then
$D_2 = (1,6)$ with $S_2 = (7,8,9,10)$, and
$D_3 = \emptyset$ with $S_3 = (6,1)$.

Mapping S_1, S_2, and S_3 on $P_{10} = (1,2,\ldots,10)$ we obtain

$$\begin{pmatrix} 2 & 3 & 4 & 5 & 7 & 8 & 9 & 10 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix},$$

which is the 10-cycle $(1,10,8,6,9,7,5,4,3,2)$.

In the following discussion the sets $S_1, S_2, \ldots$ will be directly considered and mapped on the proper segments from P_m without further comment.

The Permutation $(1,1)_m$

In this section we will show that $(1,1)_m$ can be expressed in terms of arithmetical functions.

Starting with $D_o = (1,2,\ldots,m)$ we apply X to D_o (we shift 1 to a position after m and then drop the first integer in the new m-tuple) thus obtaining $D_1 = (3,4,\ldots,m,1)$ with 2 mapped on 1, then
$D_2 = (5,6,\ldots,m,1,3)$ with 4 mapped on 2,
etc.

If m is odd then $D_{\frac{m-1}{2}} = (m,1,3,\ldots,m-2)$ is reached, with m-1 mapped on $\frac{m-1}{2}$, and $D_{\frac{m+1}{2}} = (3,\ldots,m-2,m)$ with 1 mapped on $\frac{m+1}{2}$. We observe here that, in general, starting with the integer set $K = (i_1, i_2, \ldots, i_m)$, where m is odd, then i_1 is mapped on $\frac{m+1}{2}$ after applying X successively with $K = D_0$.

Next, if m is even, then $D_{\frac{m}{2}} = (1,3,\ldots,m-1)$, with m mapped on $\frac{m}{2}$. Thus, when m is even, then 1 (i.e. the first element in the integer set that we begin with) assumes, after $\frac{m}{2}$ integers are dropped, the first position in a D-set with $\frac{m}{2}$ elements. Now if $\frac{m}{2}$ is odd then 1 is mapped on $\frac{m}{2} + (\frac{m}{2}+1)/2$; otherwise, 1 becomes the first element in a further D-set with $(\frac{m}{2})/2 = \frac{m}{4}$ elements. The above situation continues as long as the further D-sets that have 1 as first element have an even number of elements. Now, starting with a D-set that has 1 as first element and having h elements, the next D-set which has 1 as first element will have h-h/2 elements. Clearly, a D-set that has 1 as first element and with an odd number of elements will be reached, as the above process can be repeated to obtain further D-sets that have 1 as first element.

Thus, in general, letting $m=2^k.q$, where q is odd, 1 is mapped on $2^k.q/2 + 2^k.q/4 + \ldots + 2^k.q/2^k + (q+1)/2 = m - \frac{q-1}{2}$. For $m=2^k.q$, where q is odd the expression $m-(q-1)/2$ will be denoted by $\phi(m)$. Now if e is an integer in P_m then e is mapped on $\frac{e}{2}$ under $(1,1)_m$. Next if e is an odd integer in P_m then e assumes first position in a D-set with $m-\frac{e-1}{2}$ elements (after $\frac{e-1}{2}$ integers, the even integers less than e , are dropped). Then e is mapped on $\frac{e-1}{2} + \phi(m-\frac{e-1}{2})$ under $(1,1)_m$.

$(1,\frac{m-2}{2})_m$, $(1,\frac{m}{2})_m$, $(1,\frac{m+2}{2})_m$

Now we proceed to calculate $(1,n)_m$ for $n=\frac{m-2}{2}$, $\frac{m}{2}$, and $\frac{m+2}{2}$. Let m be even and consider $(1,\frac{m-2}{2})_m$. Operating with X on D_o we obtain D_1, thus $D_o = (1,2,\ldots,m)$ and

$$D_1 = (\tfrac{m+2}{2},\ldots,m,1) \quad \text{with} \begin{pmatrix} 2 & 3 & 4\ldots & m/2 \\ 1 & 2 & 3\ldots & (m-2)/2 \end{pmatrix}$$

where the symbol on the right indicates that the elements of the top row are mapped on the elements of the bottom row, each element mapped on the element directly below it. Next we obtain

$$D_2 = (1,\tfrac{m+2}{2}) \qquad \text{with} \begin{pmatrix} \frac{m+4}{2} & \ldots & m \\ m/2 & \ldots & m-2 \end{pmatrix}$$

$$\text{and } D_3 = \emptyset \qquad \text{with} \begin{pmatrix} \frac{m+2}{2} & 1 \\ m-1 & m \end{pmatrix}$$

Combining the above "segments" we conclude that,

$$(1,\tfrac{m-2}{2})_m = \begin{pmatrix} 2 & 3\ldots\frac{m}{2} & \big\backslash \frac{m+4}{2} & \ldots m & \big\backslash \frac{m+2}{2} & 1 \\ 1 & 2\ldots\frac{m-2}{2} & \big\backslash \frac{m}{2} & \ldots m-2 & \big\backslash m-1 & m \end{pmatrix}$$

, where the slanted lines indicate the different "segments". To obtain the decomposition of this permutation as a product of disjoint cycles we must distinguish between the cases $m \equiv 0 \pmod 4$ and $m \equiv 2 \pmod 4$.

Let $m \equiv 0 \pmod 4$ then $1 \to m \to m-2$ and now $m-2$ goes to (or is mapped into) the next smaller even number, $m-2 \to m-4$ ....

Now $\frac{m}{2}$ is even, so $\frac{m+4}{2}$ is also even and thus we have ,

$m-4 \to \ldots \to \frac{m+4}{2} \to \frac{m}{2} \to \frac{m-2}{2} \to \frac{m-4}{2} \to \ \ldots \to 3 \to 2 \to 1$. Thus a cycle has been isolated, namely, $(1, m, m-2, m-4, \ldots, \frac{m+4}{2}, \frac{m}{2}, \frac{m-2}{2}, \ldots 3, 2)$ with $\frac{3m}{4}$ elements. Next $\frac{m+2}{2} \to m-1$. $m-1$ is odd and is transformed into the next smaller odd number $m-3$. Thus ,

$m-1 \to m-3 \to \ldots \to \frac{m+6}{2} \to \frac{m+2}{2}$. Another cycle is isolated, namely, $(\frac{m+2}{2}, m-1, m-3, \ldots \frac{m+6}{2})$ with $\frac{m}{4}$ elements . Hence $(1, \frac{m-2}{2})_m$ is the product of the above two cycles when $m \equiv 0 \pmod 4$.

Consider now the case $m \equiv 2 \pmod 4$. We have ,

$1 \to m \to m-2 \to \ldots \to \frac{m+6}{2} \to \frac{m+2}{2}$, as now $\frac{m+2}{2}$ is even. Then we have $\frac{m+2}{2} \to m-1 \to \ldots \to \frac{m+4}{2} \to \frac{m}{2} \to \frac{m-2}{2} \to \ldots \to 3 \to 2$, so that $(1, \frac{m-2}{2})_m$ is the m-cycle $(1, m, m-2, \ldots, \frac{m+6}{2}, \frac{m+2}{2}, m-1, \ldots, \frac{m+4}{2}, \frac{m}{2}, \frac{m-2}{2}, \ldots, 3, 2)$ when $m \equiv 2 \pmod 4$.

I proceed now to find the cycles of $(1, \frac{m}{2})_m$ and $(1, \frac{m+2}{2})_m$, when m is even . We consider first $(1, \frac{m}{2})_m$.

Starting with $D_0 = (1, 2, \ldots, m)$ we find,

$$D_1 = \left(\frac{m+4}{2}, \frac{m+6}{2}, \ldots, m, 1\right) \quad \text{with} \begin{pmatrix} 2 & 3 & \ldots & \frac{m+2}{2} \\ 1 & 2 & \ldots & \frac{m}{2} \end{pmatrix}$$

$$\text{and } D_2 = \emptyset \qquad \text{with} \begin{pmatrix} \frac{m+6}{2}, \ldots m, 1, \frac{m+4}{2} \\ \frac{m+2}{2} \ldots m-2, m-1, m \end{pmatrix}$$

The commas are inserted in the above symbol for clarity.

Combining the "segments" we get $\begin{pmatrix} 2 & 3\ldots & \frac{m+2}{2} & \frac{m+6}{2} & \ldots m & 1 & \frac{m+4}{2} \\ 1 & 2\ldots & \frac{m}{2} & \frac{m+2}{2} & \ldots m-2 & m-1 & m \end{pmatrix}$

Let $m \equiv 0 \pmod 4$. Proceeding as before to obtain the cycles, we find that $(1,\frac{m}{2})_m$ is the product of the cycles,

$(1,m-1,m-3,\ldots,\frac{m+6}{2},\frac{m+2}{2};\frac{m}{2},\frac{m-2}{2},\ldots,3,2)$ and $(m,m-2,\ldots,\frac{m+4}{2})$.

When $m \equiv 2 \pmod 4$, we get the m-cycle :

$(1,m-1,m-3,\ldots,\frac{m+8}{2},\frac{m+4}{2},m,m-2,m-4,\ldots,\frac{m+6}{2},\frac{m+2}{2},\frac{m}{2},\ldots,3,2)$.

Next, we consider $(1,\frac{m+2}{2})_m$ when m is even.

We start with $D_0 = (1,2,\ldots,m)$

then $D_1 = (\frac{m+6}{2},\frac{m+8}{2},\ldots,m,1)$ with $\begin{pmatrix} 2 & 3 & \ldots & \frac{m+4}{2} \\ 1 & 2 & \ldots & \frac{m+2}{2} \end{pmatrix}$

and $D_2 = \emptyset$ with $\begin{pmatrix} \frac{m+8}{2} & \ldots & m & 1 & \frac{m+6}{2} \\ \frac{m+4}{2} & \ldots & m-2 & m-1 & m \end{pmatrix}$

When $m \equiv 0 \pmod 4$, $(1,\frac{m+2}{2})_m$ is the m-cycle

$(1,m-1\ m-3,\ldots,\frac{m+10}{2},\frac{m+6}{2},m,m-2,\ldots\frac{m+8}{2},\frac{m+4}{2},\frac{m+2}{2},\ldots,3,2)$.

When $m \equiv 2 \pmod 4$, $(1,\frac{m+2}{2})_m$ is the product of the cycle

$(1,m-1,m-3,\ldots,\frac{m+8}{2},\frac{m+4}{2},\frac{m+2}{2},\ldots,3,2)$ and the cycle

$(m,m-2,m-4,\ldots,\frac{m+6}{2})$.

$(1,\frac{m-1}{2})_m$, $(1,\frac{m+1}{2})_m$, and $(1,\frac{m+3}{2})_m$

We next consider the above permutations where m is odd. We start by finding the cycles of the permutation $(1,\frac{m-1}{2})_m$. Let $D_0 = (1,2,\ldots,m)$. Now we apply X to D_0 thus obtaining,

$$D_1 = (\tfrac{m+3}{2},\tfrac{m+5}{2},\ldots,m,1) \quad \text{with} \begin{pmatrix} 2 & 3 & 4 & \ldots & \frac{m+1}{2} \\ 1 & 2 & 3 & \ldots & \frac{m-1}{2} \end{pmatrix}$$

$$\text{Then } D_2 = (\tfrac{m+3}{2}) \quad \text{with} \begin{pmatrix} \frac{m+5}{2} & \ldots & m & 1 \\ \frac{m+1}{2} & \ldots & m-2 & m-1 \end{pmatrix}$$

$$\text{and } D_3 = \emptyset \quad \text{with} \begin{pmatrix} \frac{m+3}{2} \\ m \end{pmatrix}$$

Combining the above segments we obtain,

$$\begin{pmatrix} 2 & 3 & 4 & \ldots & \frac{m+1}{2} & \frac{m+5}{2} & \ldots & m & 1 & \frac{m+3}{2} \\ 1 & 2 & 3 & \ldots & \frac{m-1}{2} & \frac{m+1}{2} & \ldots & m-2 & m-1 & m \end{pmatrix}$$

Now we must distinguish between the cases $m \equiv 1 \pmod 4$ and $m \equiv 3 \pmod 4$. Let $m \equiv 1 \pmod 4$ then $(1,\frac{m-1}{2})_m$ is :

$$(1,m-1,m-3,\ldots,\tfrac{m+7}{2},\tfrac{m+3}{2},m,m-2,\ldots,\tfrac{m+5}{2},\tfrac{m+1}{2},\tfrac{m-1}{2},\ldots,3,2).$$

If $m \equiv 3 \pmod 4$ then $(1,\frac{m-1}{2})$ is the product of the cycles

$(1,m-1,m-3,\ldots,\frac{m+5}{2},\frac{m+1}{2},\frac{m-1}{2},\ldots,3,2)$ and

$(m,m-2,\ldots,\frac{m+7}{2},\frac{m+3}{2})$.

Next we consider $(1,\frac{m+1}{2})_m$.

Let $D_0 = (1,2,\ldots,m)$. We apply X to D_0 thus obtaining,

$$D_1 = \left(\frac{m+5}{2}, \frac{m+7}{2}, \ldots, m, 1\right) \qquad \text{with} \quad \begin{pmatrix} 2 & 3 & 4 & \ldots & \frac{m+3}{2} \\ 1 & 2 & 3 & \ldots & \frac{m+1}{2} \end{pmatrix}$$

$$\text{Then} \quad D_2 = \emptyset \qquad \text{with} \quad \begin{pmatrix} \frac{m+7}{2} & \ldots & m & 1 & \frac{m+5}{2} \\ \frac{m+3}{2} & \ldots & m-2 & m-1 & m \end{pmatrix}.$$

Combining the "segments" we obtain

$$\begin{pmatrix} 2 & 3 & 4 & \ldots & \frac{m+3}{2} & \frac{m+7}{2} & \ldots m & 1 & \frac{m+5}{2} \\ 1 & 2 & 3 & \ldots & \frac{m+1}{2} & \frac{m+3}{2} & \ldots m-2 & m-1 & m \end{pmatrix}$$

When $m \equiv 1 \pmod 4$ then $(1,\frac{m+1}{2})_m$ is the product of the cycles $(1,m-1,m-3,\ldots,\frac{m+7}{2},\frac{m+3}{2},\frac{m+1}{2},\ldots,3,2)$ and $(m,m-2,\ldots,\frac{m+9}{2},\frac{m+5}{2})$. Next when $m \equiv 3 \pmod 4$ then $(1,\frac{m+1}{2})_m$ is the m-cycle $(1,m-1,m-3,\ldots,\frac{m+9}{2},\frac{m+5}{2},m,m-2,\ldots,\frac{m+7}{2},\frac{m+3}{2},\frac{m+1}{2},\ldots,3,2)$

Finally we consider $(1,\frac{m+3}{2})_m$. When $m \equiv 1 \pmod 4$ then $(1,\frac{m+3}{2})_m$ is the m-cycle

$$(1,m-1,m-3,\ldots,\frac{m+11}{2},\frac{m+7}{2},m,m-2,\ldots,\frac{m+9}{2},\frac{m+5}{2},\frac{m+3}{2},\ldots,3,2)$$

When $m \equiv 3 \pmod 4$ then $(1,\frac{m+3}{2})_m$ is the product of the cycles $(1,m-1,\ldots,\frac{m+9}{2},\frac{m+5}{2},\frac{m+3}{2},\ldots,3,2)$ and $(m,m-2,\ldots,\frac{m+11}{2},\frac{m+7}{2})$. The details are left for the reader to supply.

4. Relations Between $(1,n)_m$ and S_m

The Case $m \equiv 2 \pmod 4$

We have shown in part 3. of this paper that when $m \equiv 2 \pmod 4$

then: $\quad (1,\frac{m-2}{2})_m = (1,m,m-2,\ldots,\frac{m+6}{2},\frac{m+2}{2},m-1,m-3,\ldots,\frac{m+4}{2},\frac{m}{2},\frac{m-2}{2},\ldots,2)$

and $(1,\frac{m}{2})_m = (1,m-1,m-3,\ldots,\frac{m+4}{2},m,m-2,\ldots,\frac{m+6}{2},\frac{m+2}{2},\frac{m}{2},\frac{m-2}{2},\ldots,3,2)$

and $(1,\frac{m+2}{2})_m$ is the product of $(m,m-2,m-4,\ldots,\frac{m+6}{2})$ and

$(1,m-1,m-3,m-5,\ldots,\frac{m+4}{2},\frac{m+2}{2},\frac{m}{2},\frac{m-2}{2},\ldots,2)$. That is,

$(1,\frac{m+2}{2})_m = (m,m-2,m-4,\ldots,\frac{m+6}{2})\,(1,m-1,m-3,\ldots,\frac{m+4}{2},\frac{m+2}{2},\frac{m}{2},\frac{m-2}{2},\ldots,2)$.

The last line is included to make it easier for the reader to follow the computations that will follow.

Lemma Let A be a cycle that maps s on t. If A maps c on d then the cycle (c,d) can be expressed in terms of A and the cycle (s,t).

Let A = (a,b,...,s,t,u,...,y). Consider now $A\,(s,t)\,A^{-1} = (t,u)$. Now clearly any cycle (c,d) where A maps c on d can be obtained in terms of A and (s,t). Note that this lemma is applicable when A is a cycle of a permutation that has other cycles that are disjoint with A.

Theorem When $m \equiv 2 \pmod 4$ then the permutations $(1,\frac{m-2}{2})_m$, $(1,\frac{m}{2})_m$ and $(1,\frac{m+2}{2})_m$ generate S_m.

We consider the following computations:

$$(1,\tfrac{m-2}{2})_m^{-1}(1,\tfrac{m+2}{2})_m = (\tfrac{m}{2},\tfrac{m+2}{2},m,m-1)$$

$$(1,\tfrac{m}{2})_m^{-1}(1,\tfrac{m-2}{2})_m = (m-1,m,\tfrac{m}{2})$$

$(\frac{m}{2},\frac{m+2}{2},m,m-1)(m-1,m,\frac{m}{2}) = (\frac{m}{2},\frac{m+2}{2})$. Now applying the lemma with $A = (1,\frac{m}{2})_m$ and using the cycle $(\frac{m}{2},\frac{m+2}{2})$ we conclude that the cycles $(\frac{m}{2},\frac{m-2}{2})$, ...,(3,2), (2,1) can be expressed in terms of $(1,\frac{m}{2})_m$ and $(\frac{m}{2},\frac{m+2}{2})$. Next consider the following:

$$(1,\tfrac{m}{2})_m(1,\tfrac{m+2}{2})_m^{-1} = (\tfrac{m+4}{2},\tfrac{m+6}{2})$$

$$(1,\tfrac{m+2}{2})_m(\tfrac{m}{2},\tfrac{m+2}{2})(1,\tfrac{m-2}{2})_m^{-1} = (\tfrac{m+2}{2},\tfrac{m+6}{2},1)$$

Now (1,2) (2,3) (1,2) = (1,3)

(1,3) (3,4) (1,3) = (1,4) ,

etc. Thus from (1,2), (2,3),..., and $(\frac{m}{2},\frac{m+2}{2})$, $(1,\frac{m+2}{2})$ can be obtained. Then

$$(1,\tfrac{m+2}{2})(\tfrac{m+2}{2},\tfrac{m+6}{2},1)^{-1} = (\tfrac{m+2}{2},\tfrac{m+6}{2})$$

$$(\tfrac{m+2}{2},\tfrac{m+6}{2})(\tfrac{m+4}{2},\tfrac{m+6}{2})(\tfrac{m+2}{2},\tfrac{m+6}{2}) = (\tfrac{m+2}{2},\tfrac{m+4}{2})$$

$$(1,\tfrac{m}{2})_m^{-1}(1,\tfrac{m+2}{2})_m = (\tfrac{m+2}{2},m)$$

Now from $(\frac{m}{2},\frac{m+2}{2})$ and $(\frac{m+2}{2},m)$, $(m/2,m)$ can be obtained.

$(\frac{m}{2}, m)\ (m-1, m, \frac{m}{2}) = (m-1, m)$

$(1, \frac{m-2}{2})_m\ (\frac{m+2}{2}, \frac{m+6}{2})\ (1, \frac{m-2}{2})_m^{-1} = (\frac{m+6}{2}, \frac{m+10}{2})$.

In a similar way $(\frac{m+10}{2}, \frac{m+14}{2}), \ldots, (m-2, m), (m, 1)$ can be obtained.

Now $(m, m-1)$ and $(m-2, m)$ give $(m-1, m-2)$, then

$(m-1, m-3)$ and $(m-1, m-2)$ give $(m-2, m-3)$

$(m-2, m-4)$ and $(m-2, m-3)$ give $(m-3, m-4)$

$\vdots$

$(\frac{m+6}{2}, \frac{m+2}{2})$ and $(\frac{m+6}{2}, \frac{m+4}{2})$ give $(\frac{m+4}{2}, \frac{m+2}{2})$. Thus the cycles $(1,2), (2,3), \ldots, (m-1, m)$ can be obtained in terms of the three permutations $(1, \frac{m-2}{2})_m$, $(1, \frac{m}{2})_m$, and $(1, \frac{m+2}{2})_m$, and it follows that S_m is generated by the latter as it is generated by the former. Analogous results can be obtained for the case $m \equiv 0 \pmod 4$

<u>The Case $m \equiv 3 \pmod 4$</u>

Let $m \equiv 3 \pmod 4$ then

$(1, \frac{m-1}{2})_m = (1, m-1, m-3, \ldots, \frac{m+5}{2}, \frac{m+1}{2}, \frac{m-1}{2}, \frac{m-3}{2}, \ldots, 2)\ (m, m-2, \ldots, \frac{m+7}{2}, \frac{m+3}{2})$

$(1, \frac{m+1}{2})_m = (1, m-1, m-3, \ldots, \frac{m+5}{2}, m, m-2, m-4, \ldots, \frac{m+7}{2}, \frac{m+3}{2}, \frac{m+1}{2}, \ldots, 2)$

$(1, \frac{m+3}{2})_m = (1, m-1, \ldots, \frac{m+5}{2}, \frac{m+3}{2}, \frac{m+1}{2}, \frac{m-1}{2}, \ldots, 2)\ (m, m-2, \ldots, \frac{m+7}{2})$.

<u>Theorem</u> When $m \equiv 3 \pmod 4$ then the permutations $(1, \frac{m-1}{2})_m$, $(1, \frac{m+1}{2})_m$, and $(1, \frac{m+3}{2})_m$ generate S_m. The proof is on the next page.

We consider the following computations:

$(1,\frac{m-1}{2})_m^{-1}(1,\frac{m+3}{2})_m = (\frac{m+1}{2},\frac{m+3}{2},m)$

$(1,\frac{m+1}{2})_m^{-1}(1,\frac{m-1}{2})_m = (\frac{m+1}{2}, m)$

Now form the product,

$(\frac{m+1}{2},\frac{m+3}{2},m)(\frac{m+1}{2},m) = (\frac{m+1}{2},\frac{m+3}{2})$.

Using $(1,\frac{m+1}{2})_m$ and $(\frac{m+1}{2}, \frac{m+3}{2})$ we can obtain

$(\frac{m+1}{2},\frac{m-1}{2}),\ldots,(3,2),(2,1)$, by the lemma.

$(1,\frac{m+3}{2})_m(\frac{m+1}{2}, \frac{m-1}{2})(1,\frac{m+3}{2})_m^{-1} = (\frac{m+1}{2},\frac{m+3}{2})$

From $(1,\frac{m+1}{2})_m$ and $(\frac{m+1}{2},\frac{m+3}{2})$: $(\frac{m+3}{2},\frac{m+7}{2}),\ldots,(m-4,m-2),(m-2,m)$

can be obtained, and from $(1,\frac{m-1}{2})_m$ and $(\frac{m-1}{2}, \frac{m+1}{2})$,

$(\frac{m+1}{2}, \frac{m+5}{2}),\ldots,(m-3,m-1)$ can be obtained.

Now $(\frac{m+1}{2},\frac{m+3}{2})$ and $(\frac{m+1}{2}, \frac{m+5}{2})$ give $(\frac{m+3}{2},\frac{m+5}{2})$

$(\frac{m+3}{2}, \frac{m+5}{2})$ and $(\frac{m+3}{2}, \frac{m+7}{2})$ give $(\frac{m+5}{2}, \frac{m+7}{2})$

$\vdots$

$(m-3,m-2)$ and $(m-3,m-1)$ give $(m-2,m-1)$

$(m-2,m-1)$ and $(m-2,m)$ give $(m-1,m)$.

Thus all the cycles $(1,2), (2,3),\ldots,(m-1,m)$ can be obtained in terms of the permutations $(1,\frac{m-1}{2})_m$, $(1,\frac{m+1}{2})_m$ and $(1,\frac{m+3}{2})_m$.

It follows that these three permutations generate S_m.

Analogous results can be obtained for the case $m \equiv 1 \pmod 4$.

5. A Note on the General Permutation $(k,n)_m$

The idea of the permutation $(1,n)_m$ discussed in part 3 can be generalized. A permutation $(k,n)_m$, $k \leq m-1$, is defined in a similar way to $(1,n)_m$ except that now k elements (not one element) are shifted by the operation X(the shifted elements change their position as a block i.e. they keep their original order). $(k,n)_m$ can be characterized as follows:

Consider a set of m empty pigeon-holes numbered with 1,2,...,m. The following process is carried out: A set of m fill-in blocks numbered 1,2,...,m is given. Now we count k empty pigeon-holes starting from 1 and proceeding from one hole to the next in succession. We then fill in with the blocks numbered from 1 to n the n successive pigeon-holes starting with the hole numbered k+1 . Next we count another set of k empty pigeon-holes proceeding from one empty hole to the next empty hole (after the last hole,numbered m, is reached we start counting from hole number 1). Now we fill in the next n empty pigeon-holes with the blocks numbered n+1,...,2n, again going from one empty hole to the next empty hole. The process is continued until the fill-in set is exhausted. Note that the final set of fill-in blocks may consist of less than n blocks (when n does not divide m).

In the double array let the top row consist of the numbers of the fill-in blocks and let the lower row consist of the original numbers of the pigeon holes:

$$\begin{matrix} h_1 & h_2 & \dots & h_m \\ 1 & 2 & \dots & m \end{matrix}$$

The double array, considered as a permutation, is the permutation $(k,n)_m$. The proof is left as an exercise. An example of the above process is given, with $m = 9$, $k = 2$, $n = 3$. Note: Dots are used in the squares to signify that they are empty.

Step no.									
1	.	.	.	.	.	.	.	.	.
2	.	.	1	2	3	.	.	.	.
3	6	.	1	2	3	.	.	4	5
4	6	8	1	2	3	9	7	4	5

thus giving the permutation $(2,3)_9 \quad \begin{pmatrix} 6 & 8 & 1 & 2 & 3 & 9 & 7 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$.

6 Some Results and Exercises

Denote the permutation $(1,1)_m$ defined in part 5 of this paper by E_m. If E_m maps an integer s on the integer f then denote f by $E_m(s)$. The characterization of E_m, as shown in part 3 can be written as follows:

when s is even then $E_m(s) = \frac{s}{2}$;

when s is odd then $E_m(s) = (s-1)/2 + \phi(m - \frac{s-1}{2})$.

Next we define E'_m as follows:

when s is even then $E'_m(s) = \frac{s}{2} + \phi(m - s/2)$

when s is odd then $E'_m(s) = (s+1)/2$.

<u>Lemma</u> $\phi(2a) = \phi(a) + a$.

Let $a = 2^k.q$ where q is odd and k>1.

$$\phi(2a) = \phi(2^{k+1}.q)$$
$$= 2^{k+1}.q - \frac{q-1}{2}$$

$$\phi(a)+a= 2^k.q + \frac{q-1}{2} + 2^k.q$$
$$= 2^{k+1}.q - \frac{q-1}{2}$$

Hence $\phi(2a) = \phi(a) + a$. Now let k = 1, then

$$\phi(2a) = 2a - \frac{a-1}{2} = (3a+1)/2$$

$$\phi(a) + a = a + \frac{a+1}{2} = (3a+1)/2$$

Hence $\phi(2a) = \phi(a) + a$.

<u>Theorem</u> Let $m = 2v + 1$, for $v = 0,1,2,\ldots$, then

$$E_m(2u - 1) = \frac{m-1}{2} + E_{\frac{m+1}{2}}(u).$$

(i) Let u be odd, then

$$E_m(2u-1) = \frac{2u-2}{2} + \phi(2v+1 - \frac{2u-2}{2})$$
$$= u-1 + \frac{2v+2-u+1}{2}$$

$E_m(2u-1) = \frac{u+1}{2} + v$.

Now $\frac{m-1}{2} + E'_{\frac{m+1}{2}}(u) = v + \frac{u+1}{2}$

Thus $E_m(2u-1) = \frac{m-1}{2} + E'_{\frac{m+1}{2}}(u)$.

(ii) Let u be even, then

$$E_m(2u-1) = \frac{2u-2}{2} + \phi(2v+1 - \frac{2u-2}{2})$$

$$= u-1 + \phi(2v + 2 - u)$$

$$= u-1 + v+1-\frac{u}{2} + \phi(v+1-\frac{u}{2}) \quad \text{by the lemma.}$$

But $\frac{m-1}{2} + E'_{\frac{m+1}{2}}(u) = v + \frac{u}{2} + \phi(v + 1 - \frac{u}{2})$

Hence $E_m(2u-1) = \frac{m-1}{2} + E'_{\frac{m+1}{2}}(u)$.

<u>Exercises</u>

(a) Prove that when $m = 2v$, $v=1,2,\ldots$ then

$E_m(2u-1) = \frac{m}{2} + E_{\frac{m}{2}}(u)$.

(b) When $2v > 4$,

$(1,1)_{2v}$ and $(1,1)_{2v-1}$ have no cycle in common.

(c) $(1,1)_{12v+7}$ $v=0,1,2,\ldots$ leaves at least one integer fixed.

7. Program for $(1,1)_m$

I used the following program to obtain the cycles of the permutation $(1,1)_m$ for $m = 26,\ldots,100$. The first part of the program(1-34) is a translation into FORTRAN of the mechanical process presented in part   of this paper. The second part of the program(35-62) is used to obtain the cycles of $(1,1)_m$, printed in order. The program steps are printed according to the requirements of FORTRAN.

The Program

```
SEQ   STMNT   FORTRAN STATEMENT
1             DIMENSION ITAB(100)
2             DO 100 M=26,100
3             DO 11 K=1,M
4     11      ITAB(K)=0
5             K=1
6             J=1
7     10      L=J+1
8     13      IF(M-L)21,12,12
9     21      L=1
10    12      IF(ITAB(J)+ITAB(L))1,2,3
11     1      PRINT 7
12     7      FORMAT(14H PROGRAM ERROR)
13     2      ITAB(L)=K
14            K=K+1
15            IF(M-L)1,70,71
16    70      L=0
17    71      J=L+1
18            IF(M-K)16,17,17
19    17      IF(ITAB(J))1,20,25
20    25      IF(M-J)80,75,80
21    75      J=0
22    80      J=J+1
23            GOTO17
24    20      CONTINUE
25            IF(M-K)16,10,70
26            L=L+1
27            GO TO 13
28    16      CONTINUE
29            PRINT 15,M
30    15      FORMAT(I5//)
31            PRINT 59
```

```
STMNT   FORTRAN STATEMENT
  59    FORMAT(//27H TRANSFORMS OF ODD INTEGERS)
        PRINT69,(J,ITAB(J),J=1,M,2)
  69    FORMAT(I5,I5//)
        DIMENSION MC(100)
        IK=0
        J=1
  29    N=J
        K=1
  49    MC(K)=ITAB(J)
        ITAB(J)=0
        IF(MC(K)-N)1,55,53
  53    J=MC(K)
        K=K+1
        GO TO 49
  55    IK=K+IK
        PRINT303,K,(MC(N),N=1,K)
 303    FORMAT(I3,20(I3,1X,))
        PRINT 78
  78    FORMAT(//)
        IF(M-IK)1,301,91
  91    J=MC(K)
  56    IF(ITAB(J+1))1,58,59
  58    J=J+1
        GO TO 56
  59    J=J+1
        GO TO 29
 301    CONTINUE
        PRINT 47
  47    FORMAT(//21H CYCLES PRINTED ABOVE///)
 100    CONTINUE
        END
```