On Permutation Groups

Alan M. Turing[*]

[**Editor's note**]: The beginning of Turing's typescript, including the original title, is missing. The above title was suggested by R. O. Gandy.

... form $U_{n1}U_{n2}\dots U_{nN}$. It is easily seen that the parity of this permutation is that of U^M and therefore that the permutations from the same machine always have the same parity. For the present we shall not however investigate the permutations obtainable with a given machine but those which are obtainable with a given upright and any number of wheels.

Let $H(U)$ or H be the set of permutations obtainable from the upright U. It is easily seen that H is a group, for if P and Q are two permutations obtainable from the upright U, then PQ is obtainable from it by putting the machines giving P and Q in series; (an algebraic argument is almost equally simple). Since H is finite and contained in the symmetric group, this is sufficient to prove it is a group. H may be expressed as the group generated by $U_1, U_2, \dots, U_T$ or again as consisting of all expressions of the form

$$R^{t_0}UR^{t_1}U\dots UR^{t_p},$$

with any p and with the exponents of R totalling zero. It thus differs only slightly from the group $J(U)$ or J generated by U, R, which consists of similar expressions without the restriction on the sum of the exponents. Every member of $J(U)$ is of the form PR^k, where P is in H. H is thus a subgroup of J of index at most T. H is in fact a self-conjugate (or normal) subgroup of J, for it is transformed into itself by the generators U, R of J, i.e. UHU^{-1} is H since U is in H and RU^nU^{-1} is U_{n+1} so RHR^{-1} is H.

We shall say that H or $H(U)$ is *exceptional* if H does not include the whole alternating group A (all even permutations). If H is not exceptional, it will be either A or the symmetric group S (all permutations), according

[*] Typescript from wartime research; title suggested by R.O. Gandy.

as U is even or odd. It is so easy to see in this way whether H is A or S that it is quite adequate in describing it to say that it is unexceptional.

We shall actually investigate J rather than H. J is obviously easier to deal with than H and results for J may be translated into results for H by means of the next theorem.

Theorem I. *The necessary and sufficient condition for H to be unexceptional is that J be unexceptional, provided $U \neq 1$, $T \neq 4$.*

We have shown that H is a self-conjugate subgroup of J. Now if J is unexceptional, it is either A or S and the only self-conjugate subgroups of these if $T + 4 \neq A, S$ and the group consisting of the identity only, and so H must be one of these. The last alternative has been excluded by assuming $U \neq 1$ so that H is A or S, i.e. H is unexceptional. Conversely, if H is unexceptional, so is J since J contains H.

Technique for investigating any particular upright U

In order to prove H is unexceptional, it will suffice to prove J contains all 3-cycles, for if this is so, J will be a self-conjugate subgroup of S and since it is not the identity, it must be either A or S. It would also be sufficient to prove that J contains all 2-cycles. We shall prove the following theorem.

Theorem II. *If J contains a member of the form $(\alpha, R^m\alpha)$ or $(\alpha, R^m\alpha, \beta)$ or $(\alpha, R^m\alpha)(\beta, \gamma)$, where m is prime to T, then it contains all 3-cycles and, in the first of these cases, also all 2-cycles. T must be greater than 4. $(\alpha, R^m\alpha)(\beta, \gamma)$ must not commute with $R^{T/2}$ if T is even.*

Suppose J contains $(\alpha, R^m\alpha)$. We will write α_k for $R^{mk}\alpha$. The symbols $\alpha_0, \alpha_1, \ldots, \alpha_{T-1}$ include all the T symbols. Then J contains $R^{ms}(\alpha_0, \alpha_1)R^{-ms}$, i.e. (α_s, α_{s+1}). It therefore contains (α_0, α_2) since this is $(\alpha_1, \alpha_2)(\alpha_0, \alpha_1)(\alpha_1, \alpha_2)^{-1}$ (if $T > 2$). It contains (α_0, α_3), which is $(\alpha_0, \alpha_2)(\alpha_2, \alpha_3)(\alpha_0, \alpha_2)^{-1}$ if $T > 3$ and repeating this argument it contains (α_0, α_r) for every $0 < r < T$. Finally it contains (α_p, α_q) since this is $R^{mp}(\alpha_0, \alpha_q - p)R^{-mp}$ if $q \neq p \pmod{T}$. Thus J contains every 2-cycle (and every 3-cycle).

Now suppose J contains $(\alpha, R^m\alpha, \beta)$ where m is prime to T. We may express β as $R^{mk}\alpha$. The first step is to prove that J contains an element of the form $(\alpha, R^{m'}\alpha, R^{2m'}\alpha)$, where m' is prime to T. In the case that $2k \equiv 1 \pmod{T}$ we may take $m' = k$ and

$$(\alpha, R^m\alpha, R^{km}\alpha)^{-1} = (\alpha, R^{m'}\alpha, R^{2m'}\alpha).$$

In the case $2k + 1 \equiv 0 \pmod{T}$ we may take $m' = -m$ and so forth. (Here Turing gives a detailed algebraic manipulation showing how to adjust exponents to achieve a triple-cycle whose second exponent is exactly $2m'$.)

Once we have $(\alpha, R^{m'}\alpha, R^{2m'}\alpha)$ with m' prime to T, we can repeat arguments (similar to the 2-cycle case) to show J contains every 3-cycle.

Finally, if J contains $(\alpha, R^m\alpha)(\beta, \gamma)$ with m prime to T and $(\alpha, R^m\alpha)(\beta, \gamma)$ does not commute with $R^{T/2}$ (if T is even), then by further algebraic transformations one obtains a 3-cycle (and in some cases 2-cycles) in J. The conditions m prime to T and non-commutation with $R^{T/2}$ prevent certain intransitive or commutative sub-cases that give rise to *exceptional* subgroups.

Thus Theorem II tells us that finding any permutation in J of one of those forms (and satisfying the prime-to-T or non-commutativity condition) forces J to contain all 2-cycles or all 3-cycles, hence J is A or S. In the few remaining cases, special "exceptional" groups arise.

It is very easy to apply Theorem II. We may first express $U, UR, UR^2, \ldots$ in cycles; this may be done for instance by writing the alphabets out double and also writing out the sequence $UA, UB, \ldots, UZ$. By putting the former above the latter in various positions we get the permutations UR^s. Among these we may look for the permutations which have a 3-cycle and all other cycles of length prime to 3. By raising this to an appropriate power we obtain a 3-cycle which may or may not satisfy the conditions in Theorem II. If we are not successful we may use other permutations in J. We may also be able in a similar way to generate a permutation which is a pair of 2-cycles.

Example. The following upright was chosen at random:

$$A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z$$

$$M\ N\ Y\ T\ F\ B\ G\ R\ S\ L\ A\ X\ O\ E\ W\ K\ P\ C\ J\ Q\ Z\ D\ H\ V\ U\ I$$

In cycles it is

$$(AMOWHRCYUZISJLXVDTQPK)(BNEF)(G) = U.$$

Then

$$U^{22} = (BE)(NF).$$

The distance BE is 3, which is prime to 26. The distance NF is 8. Hence Theorem II applies and J includes the whole of A, and therefore H includes A.

Systematic search for exceptional groups. Theory

In examining all possible uprights for a given T the main difficulty lies in the large number of uprights involved. Once it has been proved that a particular upright is unexceptional, the same will follow for a great number of others. More generally given any upright we can find a great number of others which generate either the same group H or an isomorphic group. If we can classify these uprights together in some way we shall enormously reduce the labour, since we shall only need to investigate one member of each class. The chief principles which enable us to find equivalent uprights are:

(i) If $U' = R^{m'}UR^{n}$, then $H(U') = H(U)$;

(ii) If V commutes with (R), then $H(VUV^{-1}) \cong H(U)$;

(iii) If $U' = U^{m}$ and $U = U^{m'}$, then $H(U) = H(U')$.

(N.B. If V commutes with (R), then $VRV^{-1} = R^{k}$, some k.)

The principle (i) is the one of which we make the most systematic use. Our method depends on the fact that there are very few U for which none of the permutations $R^{m}UR^{n}$ leave two letters invariant (in other words there are very few U without a beetle) and none if T is even. We therefore investigate separately the U with no beetles and the U with beetles.

U with no beetle

We can find an expression which determines the classes of permutations obtainable from one another by multiplication right or left by powers of R as follows. Let

$$UR^{n+1}Z = R^{(n)}UR^{n'}Z;$$

(here Z represents the last letter of the alphabet however many characters there may be in it). Then we take the numbers $f(1)f(2)\ldots f(T)$ as describing the classes containing U. It may be verified that from these numbers and UZ it is possible to recover U; in fact they describe what is in common between $U, RU, R^{2}U, \ldots$. However if we move some of the numbers from the end of the sequence to the beginning, we shall be describing $UR^{m}, RUR^{m}, \ldots$.

An example may help. Consider the permutation $U = (ABCDG)$ of seven letters. Write it as

$$A\ B\ C\ D\ E\ F\ G$$

$$B\ C\ D\ G\ E\ F\ A.$$

The numbers are the differences of consecutive letters in $B\,C\,D\,G\,E\,F\,A$, i.e. $1, 1, 3, 5, 1, 2, 1$. The permutation R^2UR is

$$A\ B\ C\ D\ E\ F\ G$$

$$E\ F\ B\ G\ A\ C\ D$$

and the numbers $1, 3, 5, 1, 2, 1, 1$ are obtainable by shifting the first figure to the end.

If then we take the various forms $f(1)f(2)\dots f(T)$, $f(T)f(1)f(2)\dots f(T-1)$, etc., and select that which, regarded as an arabic numeral, would be the smallest, we shall have a way of describing all the permutations R^mUR^n. We may call the resulting figure the *invariant* of U.

When we are investigating the cases where U has no beetle, the invariant is very restricted. It cannot contain Fig. 1. More generally the numbers

$$0,\ f(1)-1,\ f(1)+f(2)-2,\ f(1)+f(2)+f(3)-3,\ \dots$$

(essentially one of the "rods") must be all different. These restrictions are so powerful that we normally find very few cases other than where U is a power of R. When T is even there are no such cases (as is well known): if there were the numbers $0, 1, \dots, T-1$ in some order and would total $\frac{1}{2}T(T-1)$ modulo T. But $0, f(1), f(1)+f(2), \dots$ are also all different and must total $\frac{1}{2}T(T-1)$ modulo T, and likewise $0, 1, \dots, T-1$ total the same so that $0, f(1)-1, f(1)+f(2)-2, \dots$ total 0 mod T, i.e. $\frac{1}{2}T(T-1)$ is 0 mod T, which is not so if T is even.

U with a beetle

We select a permutation R^mUR^n which leaves two letters invariant to represent U. One of these may be taken to be A, if necessary by transforming with a further power of R. By means of principle (ii) we can also reduce the possibilities for a second letter. If the letters which were originally fixed were A and R^sA, we can transform them to A and R^sA provided that the highest common factor of T and t is the same as the highest common factor of T and s, since there is a V satisfying $VA = A$ and $VR^tV^{-1} = R^s, V(R)V^{-1} = (R)$. We therefore have to consider various pairs of letters left invariant such as A, R^tA; the various t to be considered should run through the numbers which divide T, omitting T itself but including 1. For each such t we then write down the permutations leaving A, R^tA invariant. We arrange them by classes of conjugates in S, and reduce them by means of principle (iii) as we write them down. Further reduction may afterwards be done by principle (ii) in a very special way: if V interchanges A and R^tA we can apply it. It is best probably to number the permutations and with each to give also the number t of that with which it is paired. Very many will be found self-paired.

The detailed search

$T = 1, 2, 3, 4.$ It is not difficult to prove that there are no exceptional groups when $T = 1, 2$ or 3. The case $T = 4$ needs special investigation as it has been expressly excluded from Theorem I. The exceptional uprights in this case are

$$(1), \quad (13)(24), \quad (13)(24) \quad (12)(34) \quad (32)(14) \quad (1234) \quad (4321).$$

The exceptional groups H are the identity, the cyclic groups ((1234)) and ((13)(24)), the 4-group, consisting of the identity and all permutations of the form $(\alpha\beta)(\gamma\delta)$, and a group isomorphic with the 4-group and generated by (13) and (24).

$T = 5.$ With the theory we have developed, this case is also very trivial. There are no U without beetles except those with invariant

$$22222, \quad 33333, \quad 44444.$$

These together prove the numatizer of (R). And this leaves only the permutations leaving two letters invariant, and these are all covered by Theorem II, since 5 is prime. Thus the only exceptional U are the members of the numatizer of (R), 20 in number.

$T = 6.$ Since 6 is even we do not need to consider U without beetles. Our representative U will then always leave two letters invariant, and again will come under Theorem II immediately. U can only be exceptional by being intransitive or commuting with R^3. The total number which commute with R^3 is 48 and the number which have the intransitivity sets $(ACE)(BDF)$ is 36. These include 6 which commute with R^3. Those with intransitivity set

(AD, BE, CF) all commute with R^3. Thus the total number of exceptional U is $48 + 36 - 6 = 78$ out of a possible 720.

$T = 7$. The uprights without beetles are the members of the numatizer of (R) and those with the invariant 2335564 and its reversal. The latter however are unexceptional. A representative U is $(BCGEDF)$ and U^2R is $(AG)(BEC)(DF)$ which is evidently unexceptional (square it). For the uprights with beetles we may take $t = 1$ only, i.e. we can always suppose A and B both invariant. Simple application of Theorem I shows that we need only consider cases of 5-cycles and principle (iii) shows that we can take it that $UC = G$, i.e. we have reduced the representative permutations U to the form $(A)(B)(G\alpha\beta\gamma C)$. The permutation V which interchanges A and B is $(AB)(CG)(DF)(E)$. Thus we need in the end only consider

$$(GDFEC) \quad \text{self paired}$$

$$(GFDEC) \quad \text{paired} \quad (\ldots)\ldots$$

(and so on; Turing lists each 5-cycle in detail)

By multiplying these with powers of R they may all be shown unexceptional.

We have also the case of the group generated by $(AE)(BC)$ specifically mentioned in Theorem II. This gives the group of symmetry of the 7-point geometry [see Fig. 2]. There are actually only two isomorphic groups of this kind, generated by $(BC)(AE)$ and by $(BE)(FD)$.

Invariants involved

$(BC)(AE)$ group: 1556245, 1323354, 4444444, 1264663, 1111111, 2222222

$(BE)(FD)$ group reverses: 1542655, 1453323, 4444444, 1366462, 1111111, 2222222

Invariants of numatizer of (R): 3333333, 5555555, 6666666, 4444444, 1111111, 2222222.

$$6 \times 49 + 6 \times 7 = 6 \times 7 \times 8 = 336$$

i.e. 336 exceptional uprights.

$T = 8$. This needs rather more investigation than the previous cases partly because it is the largest number yet considered and partly because it has more factors. Obviously the permutations which commute with (R) or with a power of R or generate an intransitive group will be exceptional. We will consider that we are looking for other forms of exceptional upright.

We have various means for dealing with permutations:

(a) We may show that the group is the same as that generated by an upright to be considered later. A special case of this occurs when $t = 1$. One of the forms R^sU may be of a type to be considered under $t = 2$ or $t = 4$. This may be detected by writing down the figures $m_1, m_2, \dots$ where $R^{m_i} + r + H = UR^jH$. (Turing's notation for slides and conjugation classes follows here.)

(b) One of the slides R^sU may be one to be considered later under the same value of t.

(c) The square or some other power may be proved unexceptional. (We thus reduce the 6-cycles whose squares and cubes are unexceptional.)

(d) One of the slides R^sU may be unexceptional (indicated by "slide, O.K.").

(e) One of the commutators UR^sUR^{-s} may be unexceptional (indicated by "the value of the commutator and O.K.").

When all these fail, a query will be shown and the upright investigated further later.

$t = 1$.

We may first go over the main plan, considering separately what is to be done with the various classes of conjugates in the symmetric group.

- *6-cycles.* These are left aside till the double threes have been considered.
- *Double threes.* These are arranged in pairs (as transformed by $(CH)(EF)(DG) = V$ which leaves A, B fixed and satisfies $VRV^{-1} = R^{-1}$) and dealt with in detail.
- *Triple twos.* Very few of these need to be considered in detail. (Various pair arguments as Turing enumerates them.)

- *Four-and-twos.* They need only be considered when their squares are intransitive or commute with R^4 by Theorem II.
- *Other cases.* They consist of ones where 3 or more letters are invariant and are immediately reducible to $t = 2$ or $t = 4$.

Double threes.

$$\text{(CDE)(FGH)} \quad (sp.) \quad \text{(CDE)(FHG)} \quad (sp.)$$

. . . (Turing shows algebraic products like (CDE)(FGH)(DEF)(GHA) = (DC)(EGF)(HA) . . . are all O.K. or reduce to 2-cycles or 3-cycles.)

(And so forth; Turing enumerates systematically all cycle structures for $T = 8$, analyzing commutators, slides, or squares and cubes, to show they are "O.K." or lead to a known exceptional group.)

Hence by these methods, each possible structure is either shown unexceptional (i.e. H is A or S) or else shown to be one of the special intransitive/commuting forms giving an exceptional subgroup.

[End of typescript as preserved]

[Page 135]

. . . We have avoided using (a) and (b) owing to the inapplicability for the 6-cycles.

The upright $(CDF)(EGH)$ is *exceptional* and the corresponding group consists of the elements with the invariants

11111111	8 elements	11111111
12214554	64 elements	25527667
13272315	64 elements	13245423
16573756	64 elements	34657564
24636425	64 elements	14737415
33476674	64 elements	12216336
77777777	8 elements	77777777

(total of 336 elements)

Transformation of the group with $(AG)(CH)(EC)$, which commutes with R, gives another group which contains $(CFG)(DEH)$.

The invariants of this latter group are given in the last column. These invariants are useful for verifying that other exceptional uprights belong to these groups.

We have to investigate the 6-cycles whose squares are exceptional. They are shown below.

$(CEDGFH)$	X
$(CGDHFE)$	invariant 15132723 (above)
$(CHDEFG)$	X
$(CDFEGH)$	invariant 12216336 (above)
$(CEFHGD)$	X
$(CHFDGE)$	X
$(CDEFGH)$	X
$(CFEHGD)$	X
$(CHEDGF)$	X
$(CDEHGF)$	slide $(ABDH)(CE)$ O.K.
$(CHEFGD)$	X
$(CFEDGH)$	X

It is not easy to prove directly that the elements with the above invariants form a group. However in this case we can manage by guessing what the group is. The order of the group being 336 it is natural to suppose that it is connected with the group of symmetry of the 7-point geometry, which is a well-known simple group of order 168. The even permutations in our group will form a group of order 168, which might with luck be isomorphic with the group of the 7-point geometry. This in fact turns out to be so.

In order not to confuse the notation we will denote the points of the 7-point geometry by a, b, c, d, e, f, g [see Fig. 3*]. We naturally try to express the group of symmetry as a group of permutations of some eight objects, in order to tie it up with the groups found above. These groups may perhaps be called K and K'. The standard technique for representing a group as a group of permutations of m objects is to find a subgroup of index m, and to consider the cosets of the subgroup as forming the m objects. In this case we want a subgroup of order 21, and such a subgroup is the normalizer of

$((abcegfd))$. The cosets of this group are enumerated below in shortened form. Each line represents seven permutations, obtainable from one another by moving letters from one end to the other. Each coset has been given a name which is a capital letter.

A	$abcegfd$	
B	$abgdcfe$	
C	$acdgfeb$	
D	$aefbged$	
		... (similar 7-permutation lines)
		...
a	$acgdbef$	
a	$agcebdf$	
a	$adfbcge$	
a	$afgdebc$	

[Turing's text continues listing cosets E, F, G, H likewise, each line containing 7 permutations with letters shifted.]

Now the symmetry group contains the permutation $(abgc)(fe)$ which induces the permutation $(ACEG)(BDFH)$ of the cosets. It also contains $(abc)(def)$ which induces $(ADH)(BCG)$. Now if we identify the cosets with the eight symbols permuted in the group J (as the notation is intended to suggest), we see that $(ACEG)(BDFH)$ is R^2 and that $(ADH)(BCG)$ has the invariant 14737415, one of those of the group K'. It can then be easily verified that the symmetry group also induces in the cosets permutations with all the other invariants of K', and also that $(ACEG)(BDFH)$ and $(ADH)(BCG)$ generate the whole symmetry group. Since this is of order 168 and since it contains the even permutations in K', numbering 168, it must coincide with the intersection of K' and A.

It now only remains to prove that the expressions of form S and SR, where S is in $K' \cap A$, form a group. This will follow if we can prove that R^2 belongs to $K' \cap A$ and that RSR^{-1} belongs to $K' \cap A$ whenever S belongs to it. We know the former already and the latter follows at once from our invariant system; K' consists of complete sets of permutations having certain invariants.

Triple twos. As explained above we do not need to consider any except the ones without the pairs (CH), (DH) or (GC). This leaves:

$$(CD)(EF)(GH), \quad (CD)(EF)(GH) \cdot (EF)(GH)(AB), \quad \ldots$$

[Turing enumerates each product, checking if it is O.K. or reduces to a known case.]

Fours-and-twos. Omitting those whose squares are unexceptional and those with $UH = C$ and their pairs, we have only:

$(CDEF)(HG)$	X
$(CDGF)(HE)$	X
$(CGHD)(FC)$	X
$(DEHG)(FC)$	pair
$(FEHG)(CD)$	pair

$t = 2$.

We find it worthwhile to apply the principle (ii) on a rather large scale. There are four permutations V which leave A and C fixed; they are

$$\begin{array}{cccccccc} A & B & C & D & E & F & G & H \\ C & B & A & H & G & F & E & D \\ C & F & A & D & G & B & E & H \\ A & F & C & H & E & B & G & D \end{array}$$

From a single permutation we thus obtain as many as four generating isomorphic groups J, e.g. from $(BDEFHG)$ we get:

$$(BDEFHG), \quad (BHGFDE), \quad (FDBGHE), \quad (FHEBDG).$$

These may be transformed into equivalent forms and the alphabetically earliest chosen. We permit taking the reciprocal as a form of transformation. Thus we get $(BDEFHG)$, $(BEDFGH)$?, $(BGDFEH)$?, $(BDCFHE)$. By these means we reduce the 6-cycles that need be considered down to 18. As before we actually consider first their squares (double threes) in the hope that they will be unexceptional and the 6-cycle need not be specially investigated.

6-cycles and double threes

$(BDEFGH)$ slide $(ACF)(BFDHE)$ O.K. indirect

$(BDEFHG)$ slide $(AB)(CEFHD)$ O.K.

$(BDEGFH)$ $(BEF)(DGH) \cdot (CFG)(EHA) = (AFH)(CBEDG)$ O.K.

$(BDEGHF)$ slide $(AD)(FCB)$ O.K.

$(BDEHFG)$ slide $(BAG)(DCEH)$ O.K.

$(BDEHGF)$ invariant 34657564, giving group K'

$(BDFEHG)$ slide $(BA)(DCFGH)$ O.K.

$(BDFGHE)$ slide $(BA)(CFD)(HEG)$ O.K.

$(BDFHGE)$ slide $(BAEH)(DCF)$ O.K.

$(BDGFEH)$ invariant 34657564, giving group K'

$(BDGHEF)$ slide $(CAE)(FHDGB)$ O.K. indirect

$(BDGHFE)$ $(BGF)(DHE) \cdot (CHG)(EAF) = (ABGCE)(DHF)$ O.K. indirect

$(BDHEFG)$ slide $(BAFG)(DCH)$ O.K.

$(BDHEGF)$ slide $(AH)(BCEDF)$ O.K.

$(BDHFEG)$ slide $(DAEH)(FCG)$ O.K.

$(BDHGEF)$ slide $(AD)(HBFCE)$ O.K.

$(BDHGFE)$ slide $(CAE)(DHBFG)$ O.K. indirect

$(BEDHGF)$ slide $(AED)(CF)$ O.K.

Above analyses are done on the squares of the 6-cycles, i.e. on the double threes. We must now investigate the cases of 6-cycles where the double threes were exceptional.

$(BDEHGF)$	slide $(BAG)(FH)(CD)$ O.K.
$(BDGHEF)$	slide $(BAEGH)(CD)$ O.K.
$(BF)(DG)(EH)$	X
$(BF)(DH)(EG)$	intransitive
$(BG)(DF)(EH)$	slide $(AGEDH)(BCF)$
$(BG)(DH)(EF)$	X
$(BH)(DF)(EG)$	intransitive
$(BH)(DG)(EF)$	$(AH)(BCG)(DF)$ slide O.K.
$(BE)(DH)(FG)$	X
$(BG)(DH)(FE)$	X
$(BH)(DG)(FE)$	slide $(AH)(BCG)(DF)$
$(BF)(DE)(GH)$	X
$(BH)(DE)(GF)$	slide $(AH)(BCEG)$
$(BH)(DF)(GE)$	intransitive
$(BE)(DF)(HG)$	slide $(ACBFG)(EH)$
$(BE)(DG)(HF)$	slide $(AEH)(BCGFD)$
$(BF)(DG)(HE)$	X
$(BG)(DE)(HF)$	slide $(ACDHG)(BE)$
$(BG)(DF)(HE)$	$(AGEDH)(BCF)$ slide O.K.
$(BH)(EG)(DF)$	intransitive

Fours and twos and fours. We only need consider those whose squares are intransitive or commute with R^4.

$(EBGD)([FH])$	$(FBGD)([CE])$ O.K.
$(EBGF)([DH])$	$(EBFC)$ O.K. $(ABFC)(DG)$ O.K.
$(EBGH)([FD])$	$(EBGA)$ O.K. $(GBAE)(CD)$ O.K.
$(EDGB)([FH])$	$(HDGB)$ O.K. $(HDAB)(EC)$ O.K.
$(EDGH)([BF])$	$(HDGA)$ O.K. $(HDCA)(BE)$ O.K.
$(EFGH)([DB])$	$(EGHA)$ O.K. $(CGHA)(DB)$ O.K.

There are none which leave A, C fixed and commute with R^4 except $(BDFH), (BHFD)$ which is intransitive anyway.

5-cycles. These 5-cycles are given in pairs which are equivalent by principle (ii).

$(DEFGH)$ s.p. $(DEFGH)(EFGHA)^{-1} = (DEA)$ O.K.
$(DEFHG)$ slide $(BAGDC)(FH)$ O.K. indirect
$(DEHGF)$
$(DEGFH)$ slide $(BADC)(FGH)$ O.K.
$(DEHFG)$
$(DEGHF)$ s.p. slide $(EAGCH)(DFB)$ O.K. indirect
$(BEFGH)$ slide $(BA)(CED)$ O.K.
$(BEHFG)$ slide $(BAGH)(CDE)$ O.K.
$(BEGHF)$ s.p. slide $(BA)(CED)(FGH)$ O.K.
$(BEGFH)$ s.p. slide $(BAG)(DCE)$ O.K.
$(BEFGH)$ slide $(AF)(BE)(CGDH)$ O.K.
$(BDHGF)$ slide $(BACH)(DC)(EF)$ O.K.
$(BDFHG)$ slide $(BAGH)(DC)(EF)$ O.K.
$(BDGFH)$ s.p. slide $(BAFEG)(CD)$ O.K.
$(BDHFG)$ s.p. slide $(BAFEH)(CD)$ O.K.

$t = 4$.

The permutations V which commute with (R) and leave A, E invariant or interchange them are:

$$\begin{array}{cccccccc}
A & B & C & D & E & F & G & H \\
A & D & G & B & E & H & C & F \\
E & H & C & F & A & D & G & B \\
A & H & G & F & E & D & C & B \\
E & D & C & B & A & H & G & F \\
A & F & C & H & E & B & G & D \\
E & B & G & D & A & F & C & H \\
E & F & G & H & A & B & C & D
\end{array}$$

6-cycles and double threes. As usual we actually examine the double threes although we test the 6-cycles.

$(BCDFGH)$ commutes with R^4 (both $(BCDFGH)$ and
$(BDG)(CFH)$ and $(EF)(CG)(DH)$)

$(BCDFHG)$ slide $(BA)(EHCDF)$ O.K.

$(BCDGHF)$ slide $(AB)(CDG)(HFE)$ O.K.

$(BCDGHF)$ invariant 33476674 group K
6-cycle invariant 12214554 group K
triple two invariant 77777777 part of numatizer of (R)

$(BCFDGH)$ slide $(CAB)(EDFHG)$ O.K.

$(BCFDHG)$ slide $(BA)(CFEGH)$ O.K.

$(BCFHGD)$ slide $(BADH)(FEC)$ O.K.

$(BCGDFH)$ slide $(BACG)(EHF)$ O.K.

$(BCGDHF)$ invariant 27652765 commutes with R^4
6-cycle slide $(CAD)(FHB)$ reducing to a $t = 2$ case already considered
triple two slide $(AHDG)(CEF)$ O.K.

$(BCGFDH)$ invariant 33476674 group K
6-cycle slide $(BA)(DG)(FEH)$ O.K.
triple two $(BF)(CD)(GH)$ commutes with R^4
slide $(BA)(DFECG)$ O.K.

$(BCGHDF)$ commutes with R^4
6-cycle slide $(AE)(HFC)$ O.K.
triple two $(AH)(CD)(GF)$ slide $(ABCDH)(EGF)$ O.K.

$(BCGHFD)$ slide $(CAF)(EHBDG)$ O.K.

Triple twos (remaining).

$(BF)(CH)(DG)$	commutes with R^4
$(BG)(CH)(DF)$	slide $(AHG)(BFCE)$ O.K.
$(BD)(CG)(FH)$	commutes with R^4
$(BD)(CH)(FG)$	slide $(AHDG)(CEF)$ O.K.
$(BH)(CG)(DF)$	intransitive
$(BD)(CF)(GH)$	$(BD)(CF)(GH) \cdot (CE)(DG)(HA) = (AGBDH)(CEF)$ O.K.
$(BF)(CH)(GD)$	commutes with R^4
$(BH)(CF)(GD)$	$(BH)(CF)(GD) \cdot (DB)(EH)(AF) = (DHEBG)(FBC)$ O.K.

Fives.

$(CDFGH)$	slide $(BAC)(EF)$ O.K.
$(CDHFG)$	
$(CDFHG)$	slide $(BAGHC)(FE)$ O.K.
$(CDHGF)$	
$(CDGFH)$	slide $(BAC)(EGDF)$ O.K.
$(CDGHF)$	

The 5-cycles where two fixed letters were at distance 2 were considered under $t = 2$.

The outcome for $T = 8$ is then that the *exceptional* uprights are all either

(a) intransitive, or product of an intransitive upright with R,

(b) commuting with R^4,

(c) members of the groups K, K'.

Let us now calculate the number of exceptional uprights. The number in K and K' omitting those with invariants 11111111 and 77777777 is $2 \times 336 - 32 = 640$. Those with invariants 11111111 and 77777777 are also intransitive, the condition for intransitivity being that all figures are even or all odd. The condition for commuting with R^4 is that the invariant is of the form *abcdabcd*. Thus these 16 elements are also of this kind, but no other members of K, K' are. There are $2 \times (4!)^2 = 1152$ intransitive uprights or 1152 and there are $2^4 \times (4!) = 384$ that commute with R^4. The intransitive ones that commute with R^4 are determined on giving the values of UA, UB (which must be of opposite parity). They number $8 \times 4 = 32$.

Final account

K and K'	640
intransitive	1152
commute with R^4 (with omissions)	352
	2144

Total of all uprights = 40320.

We now turn to a rather different topic in connection with the use of identical drums. Even if we know that all permutations are possible, will they be equally frequent? Fortunately, we can answer this in the affirmative. The problem will be examined under slightly more general conditions. No assumptions will be made about the relationship between the generators $U_1, \ldots, U_k$ and we will not assume that the basic group is the symmetric group but some other finite group G.

Let us suppose that we feed a certain frequency distribution of group elements into a wheel; how can we calculate the frequency distribution of the group elements at the output of the wheel? Let $g(a)$ be the proportion of the input elements which are a, and let $f(a)$ be the proportion of group elements effected by the wheel which are a, i.e., denoting the order of the group by h,

$$f(a) = h^{-1} \sum_{r=1}^{k} 1, \quad U_r = a.$$

Then we get output a if the input is b and the wheel effects the group element ab^{-1}, for any b. The proportion of such cases is $f(ab^{-1})\, g(b)$, or allowing for the different values of b, a total proportion of

$$\sum_b f(ab^{-1})\, g(b).$$

If then we define the operator R_f by the equation

$$(R_f g)(a) \ = \ \sum_b f(ab^{-1})\, g(b),$$

we can say that the frequency distribution for n wheels is given by $R_f^{n-1} f$. We wish to determine how this function behaves with increasing n.

We consider the real-valued functions on the group as forming an Euclidean space of h dimensions, where h is the order of the group H. We may put (g, k) for the scalar product $h^{-1} \sum_a g(a)\, k(a)$ and $\|g\|$ for the distance $(g, g)^{1/2}$ from the origin. We may also put $\overline{g}$ for the mean value $h^{-1} \sum_a g(a)$. Schwarz's inequality gives at once $\|g\| \geq \overline{g}$, and if we suppose $g(a) \geq 0$ for all a, $g(a) > 0$ for some a, we shall have $\overline{g} > 0$. We will also suppose $f(a) \geq 0$ for all a, $f(a) > 0$ for some a, $\overline{f} = 1$. Then we have the next lemma.

Lemma (a). *If $\overline{f} = 1$, then $\|R_f g\| \leq \|g\|$ and equality holds only if $g(ab^{-1}x)/g(x)$ is independent of x for any a, b for which $f(a) \neq 0$ and $f(b) \neq 0$.*

First note that

$$\Big(h^{-1} \sum_x g(x)\, g(cx)\Big)^2 \;\leq\; h^{-2} \sum_x (g(x))^2 \,\sum_x (g(cx))^2 \;=\; (h^{-1} \sum_x (g(x))^2)^2 \;=\; \|g\|^4,$$

equality holding if $g(cx)/g(x)$ is independent of x. Then

$$\|R_f g\|^2 = h^{-1} \sum_{a,b,x} f(ab^{-1})\, g(b)\, f(ax^{-1})\, g(x) = h^{-1} \sum_{c,u,x} f(c)\, f(cu)\, g(ux)\, g(x) \;\leq\; \sum_{c,u} f(c)\, f(cu)\, \|g$$

equality holding in the case mentioned.

Let us define the *limiting distribution* for f as the condensation points of the sequence $g,\ R_f g,\ R_f^2 g, \ldots$. Then Lemma (a) will enable us to prove the following theorem.

Theorem III. *The limiting distributions for f are constant throughout the cosets of a certain self-conjugate subgroup H_1 of H. H_1 consists of all expressions of the form $U_{r_1}^{m_1} U_{r_2}^{m_2} \ldots U_{r_p}^{m_p}$, where the sum $\sum m_q$ of exponents is zero. The factor group H/H_1 is cyclic. In the case that g is f, the limiting distributions each have the value zero except in one coset of H_1.*

Let k be a limiting distribution. Let it be the limit of the sequence $R_f^{n_r} g,\ R_f^{n_r+1} g, \ldots$ Then

$$\|R_f^{n_r} g\| \;\geq\; \|R_f^{n_r+1} g\| \;\geq\; \|R_f^{n'_r+1} g\| \;\geq\; \|k\|.$$

Now $\|R_f^{n_r} g\|/\|k\| \to 1$ as r tends to infinity and therefore $\|R_f^{n_r+1} g\|/\|R_f^{n_r} g\| \to 1$. But $\|R_f u\|/\|u\|$ is a continuous function of u and therefore taking the limit of the sequence $\|R_f^{n_r} k\|/\|k\| = 1$. Applying Lemma (a) to this we see that there is a function $\varphi_1(y)$ defined for all expressions of the form ab^{-1} where $f(a) \neq 0,\ f(b) \neq 0$ such that

$$k(jx) \ = \ \varphi_1(y)\, k(x) \quad \text{if } jx = ab^{-1}x,$$

for all x. By applying the same argument with $R_f^n - f$ in place of f we find that there is a function $\varphi_u(y)$ defined for all expressions of the form $a_1\, a_2^{-1} \ldots a_n\, b_n^{-1}$ where $f(a_1), f(a_2), \ldots, f(b_1)$ are all different from 0 such that

$$k(yx) \ = \ \varphi_u(y)\, k(x), \quad \text{all } x,$$

whenever $\varphi_u(y)$ is defined. The various functions $\varphi_u(y)$ must agree whenever their domains of definition overlap, and they may therefore be all represented by one symbol φ. In fact we may say $\varphi(y)$ is defined and has value α whenever $k(jx) = \alpha\, k(x)$ for all x. It now appears that the domain of definition of $\varphi(y)$ is a group, for if $k(y_1 x) = \alpha_1 k(x)$ for all x and $k(y_2 x) = \alpha_2 k(x)$ for all x, then

$$k(y_1 y_2 x) = \varphi(y_1)\, \varphi(y_2)\, k(x).$$

If y_1, y_2 belong to the domain of definition of φ, so does $y_1 y_2$ and $\varphi(y_1 y_2) = \varphi(y_1)\, \varphi(y_2)$.

It is now immediately seen that the domain of definition is H_1. The function φ is a one-dimensional representation of H_1 but it is real and positive and therefore has the value 1 throughout H_1. This last argument may also be expressed without the use of representation theory thus. Since H_1 is finite, any element y of it satisfies an equation $y^m = 1$ and therefore

$$(\varphi(y))^m \ = \ \varphi(y^m) \ = \ \varphi(y^m) \ = \ 1.$$

But since $g(x)$ is always nonnegative, $\varphi(y) \geq 0$ and so $\varphi(y) = 1$. This implies that $g(x)$ is constant throughout each coset of H_1.

It now only remains to investigate the character of the group H_1. It is easily seen to be self-conjugate, since if aba^{-1} belongs to H_1 and b to H, the total of exponents of group generators U_r in aba^{-1} must be 0, those in a^{-1} cancelling with those in a; hence aba^{-1} belongs to H_1 if b does; H_1 is self-conjugate.

Now let us take a particular generator U_1, say. Then the cosets $H_1U_1^m$ exhaust the group H. For if p is an element of H, it will be a product of generators; let the total of exponents be m. Then pU_1^{-m} has total exponents 0 and so belongs to H_1, i.e. p belongs to $H_1U_1^m$, i.e. these cosets exhaust H. If U_1^s is the lowest power of U_1 which belongs to H_1, then H/H_1 is evidently isomorphic with the cyclic group of order s.

In the case that g is f, all the group elements for which $R_f^{n-1}f$ is not zero are products of n generators and therefore belong to $H_1U_1^m$.

Example. As an example let us consider the quaternion group consisting of

$$1,\ i,\ j,\ k,\ i',\ j',\ k'$$

with the table

	1	i	j	k	i'	j'	k'
1	1	i	j	k	i'	j'	k'
i	i'	k	j'	i'	1	k'	j
j	k'	i'	j'	j'	k	1	i'
k	j	i'	k'	j'	i	j'	i
i'	i	j'	i'	k'	1	i'	k
j'	k	i	i'	j'	k'	i'	i
k'	j'	i'	i	k	j	i	i'

...

[Page 144 ends; Turing's manuscript continues with further tables and group-theoretic arguments.]

[Page 145]

... and let U_1 be i and U_2 be j. The various functions $R_f^{n-1}f$ are given in the table

n	1	i	j	k	i'	j'	k'
1	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0
2	0	0	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{4}$
3	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0
4	$\frac{1}{4}$	0	0	$\frac{1}{4}$	0	0	$\frac{1}{4}$
5	0	$\frac{1}{4}$	0	0	$\frac{1}{4}$	$\frac{1}{4}$	0
6	$\frac{1}{4}$	0	0	$\frac{1}{4}$	0	0	$\frac{1}{4}$

It is seen that the group H_1 is the group generated by k; it has a factor group which is cyclic of order 2.

Case of symmetric and alternating groups

In the case under consideration at the beginning of our analysis, H was either the symmetric or the alternating group unless the upright U was exceptional. In this case H_1 is also either the symmetric or the alternating group, for it is self-conjugate in H. It will be the alternating group if the generators are all of the same parity and the symmetric group otherwise. We therefore conclude that

> *when the upright is not exceptional the distributions with large numbers of wheels are uniform throughout the alternating group (even permutations). If odd permutations are possible with the given upright and number of wheels, the distribution is uniform throughout the symmetric group (all permutations).*