Z. Wahrscheinlichkeitstheorie verw. Geb. 4, 175—186 (1965)

On Some Problems of a Statistical Group-Theory. I

By

P. ERDÖS and P. TURÁN

1. By statistical group-theory we mean the study of those properties of certain complexes of a "large" group which are shared by "most" of these complexes. The group considered in this paper will be S_n, the symmetric group of n letters; its group-elements will be denoted by P. The complexes considered here will be simply the elements P of S_n; the property in question will be the group-order $O(P)$ of P. As to this LANDAU proved (see [4]) for

$$G(n) \overset{\text{def.}}{=} \max_{P \in S_n} O(P)$$

the asymptotical relation

$$\lim_{n \to \infty} \frac{\log G(n)}{\sqrt{n \log n}} = 1 . \tag{1.1}$$

On the other hand P's of order as low as n are "many"; all P's consisting in the canonical cycle-decomposition of a single cycle (of length n) are of order n and their number is

$$(n-1)! = \frac{1}{n} n! , \tag{1.2}$$

which is relatively large. The big contrast between (1.1) and (1.2) would sound a bit discouraging as to a simple law of the distribution. Nevertheless we are going to prove the

Theorem. *For arbitrarily small positive ε, δ and $n > n_0(\varepsilon, \delta)$ the inequality*

$$e^{(1/2-\varepsilon)\log^2 n} \leqq O(P) \leqq e^{(1/2+\varepsilon)\log^2 n}$$

holds, apart from

$$\delta\, n!$$

*exceptional P's at most.**

The value $e^{1/2 \log^2 n}$ falls surprisingly short compared with LANDAU's upper bound in (1.1). We entertain hopes to prove in the next paper of this series that for the number $N(n, t)$ of P's satisfying with an arbitrary fixed real t the inequality

$$\log O(P) \leqq \tfrac{1}{2} \log^2 n + t \log^{3/2} n \tag{1.3}$$

the limes-relation

$$\lim \frac{1}{n!} N(n, t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\lambda^2/2}\, d\lambda \tag{1.4}$$

holds and even with a sharp remainder-term uniformly in n and t. Also the case will be of interest when t varies strongly with n, e.g. $t = n^{1/4}$.

* Actually a bit more; see (7.1) and (14.3); with a little more care our proof had given even the inequality $|\log O(P) - \frac{1}{2}\log^2 n| \leqq \omega(n) \log^{3/2} n$ with $o(n!)$ exceptions at most if only $\omega(n) \to \infty$ with n.

2. Which results were known in this theory? Quite a few only, as far as we know. S. CHOWLA, HERSTEIN and MOORE (see [1]) for $d = 2$, and L. MOSER and WYMAN (see [5]) for $d = p$ (= prime) proved that denoting by $f_d(n)$ the number of P's in S_n with $O(P) = d$, the relation

$$f_p(n) \sim p^{-1/2} \left(\frac{n}{e}\right)^{n(1-1/p)} e^{n^{1/p}} \tag{2.1}$$

holds for fixed p and $n \to \infty$. We were unable to deduce our theorem from (2.1). This is the only one which is *directly* related to our theorem. In our proof of it we needed informations concerning the distribution of the cycle-lengths in the canonical decomposition of the P's; so we found that, denoting the number of cycles by $g(P)$, then — apart from $o(n!)$ P's* — we have

$$g(P) \sim \log n . \tag{2.2}$$

After having a ready manuscript we learned that this theorem was found first by V. L. GONČAROV (see [2]) in 1944 already, even in a sharper form. Actually what we need is not (2.2) but the corresponding theorem for $k(P)$, the number of the *different* cycle-lengths; also here the value $\log n$ is surprisingly low since the *best-possible* limitation, one can give for *all* P's, is the inequality

$$1 \leqq k(P) \leqq \left[\frac{-1 + \sqrt{8n+1}}{2}\right]. \tag{2.3}$$

This sharp preponderance in various problems seems to be characteristical to this theory.**

LANDAU's theorem in (1.1) gives at the same time the asymptotical maximum for the order of cyclic subgroups of S_n. Our theorem does *not* answer to the natural question, what is the „preponderating" order of *non-isomorphic* cyclic subgroups of S_n; perhaps not even the number of non-isomorphic cyclic subgroups of S_n is known. To all these and several other questions of the same sort we hope to return in this series.

We also call the attention to the last sentence of this paper (though we do not formulate it as an independent theorem).

As pointed out by W. H. H. HUDSON (see ROUSE BALL [7]) in devising card tricks by repeating the same shuffling procedure we encounter again problems on the orders of the P's. So using full pack of 52 cards having bad luck in selecting the basic shuffling procedure we can need $G(52) = 180{,}180$ shufflings to come back to the original position of the cards. According to our theorem we need with large probability only

$$e^{1/2 \log^2 52} \sim 2600$$

shufflings.

The proof of the theorem will be given in several stages. In Part I. we shall deal with $k(P)$, in Part II. we give the proof of the upper bound, in Part III. that of the lower one in our theorem.

The different cycle-lengths in the canonical cycle-decomposition of P will be denoted throughout by

$$(1 \leqq) n_1 < n_2 < \cdots < n_{k(P)} = n_k \leqq n \tag{2.4}$$

* The o-sign refers throughout this paper to $n \to \infty$.

** Somewhat in the same direction lies the paper of ERDÖS-SZEKERES on the mean-value of $\psi(n)$, the number of non-isomorphic Abelian groups of order n. See ERDÖS-SZEKERES [2].

the number cycles of length n_ν by m_ν so that

$$\sum_{\nu=1}^{k(P)} m_\nu n_\nu = n \tag{2.5}$$

and

$$\sum_{\nu=1}^{k(P)} m_\nu = g(P). \tag{2.6}$$

The dependence of $k(P)$ upon P will not be denoted explicitly later; $c_1, c_2, \ldots$ stand for explicitly calculable positive numerical constants.

Part I

3. We shall state GONČAROV's theorem as

Lemma I. *For any fixed real t for the number $h_n(t)$ of P's satisfying* (see (2.2))

$$g(P) \leqq \log n + t\sqrt{\log n}$$

we have the relation

$$\lim_{n\to\infty} \frac{1}{n!} h_n(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\lambda^2/2}\, d\lambda. \tag{3.1}$$

Applying the wellknown theorem of ESSEEN one could replace the limes-relation in (3.1) by a formula with error-term. We shall use lemma I in the following weaker form.

Corollary I. *If $\omega(n)$ tends to infinity arbitrarily slowly monotonically then for all but $o(n!)$ P's the inequality*

$$|g(P) - \log n| \leqq \omega(n)\sqrt{\log n}$$

holds.

We state the following wellknown result (see e.g. RIORDAN [6]) as

Lemma II. *The number of P's with fixed*

$$k, m_1, \ldots, m_k, n_1, \ldots, n_k$$

(see (2.4), 2.5)) *is*

$$\frac{n!}{m_1!\, m_2! \ldots m_k!\, n_1^{m_1} n_2^{m_2} \ldots n_k^{m_k}}.$$

Let ω_1 and ω_2 be positive integers with

$$20 \leqq \omega_1,\ \omega_2 \leqq n$$

and $\prod_1$ be the set of P's with the following properties. If $n_\nu \leqq \omega_1$ then

$$1 \leqq m_\nu \leqq \omega_2; \tag{3.2}$$

if $n_\nu > \omega_1$ then

$$m_\nu = 1. \tag{3.3}$$

This $\prod_1$ is the set of P's in which only "short" cycles can occur more than once and even these "not too often". Denoting the number of P's of $\prod_1$ by $|\prod_1|$ we assert the

Lemma III. *The inequality*

$$\left|\frac{1}{n!}\left|\prod\nolimits_1\right| - 1\right| < 3\left(\frac{1}{\omega_1} + \frac{1}{\omega_2!}\right)$$

holds.

For the *proof* we remark first that $\frac{1}{n!}\left|\prod_1\right|$ is nothing else than the coefficient of z^n in

$$\prod_{\nu=1}^{\omega_1}\left\{1+\sum_{l=1}^{\omega_2}\frac{1}{l!}\left(\frac{z^\nu}{\nu}\right)^l\right\}\cdot\prod_{\nu=\omega_1+1}^{\infty}\left(1+\frac{z^\nu}{\nu}\right). \tag{3.4}$$

The ν^{th} factor in the first product can be written as

$$e^{z^\nu/\nu}-\sum_{l=\omega_1+1}^{\infty}\frac{1}{l!}\left(\frac{z^\nu}{\nu}\right)^l=e^{z^\nu/\nu}\left\{1-e^{-z^\nu/\nu}\sum_{l=\omega_1+1}^{\infty}\frac{1}{l!}\left(\frac{z^\nu}{\nu}\right)^l\right\}$$

and analogously for the second product. Since for $|z|<1$ we have

$$\prod_{\nu=1}^{\infty}e^{z^\nu/\nu}=\frac{1}{1-z},$$

the product in (3.4) can be written for $|z|<1$ as $\frac{1}{1-z}\,\Omega(z)$, where

$$\Omega(z)=\prod_{\nu=1}^{\omega_1}\left\{1-e^{-z^\nu/\nu}\sum_{l=\omega_2+1}^{\infty}\frac{1}{l!}\left(\frac{z^\nu}{\nu}\right)^l\right\}\cdot\prod_{\nu=\omega_1+1}^{\infty}\left\{1-e^{-z^\nu/\nu}\sum_{l=2}^{\infty}\frac{1}{l!}\left(\frac{z^\nu}{\nu}\right)^l\right\}. \tag{3.5}$$

Equating the corresponding coefficients we get

$$\frac{1}{n!}\left|\prod_1\right|-1=\sum_{\mu=1}^{n}\text{coeffs. } z^\mu \text{ in } \Omega(z).$$

Replacing in (3.5) in each factor in curly brackets the term

$$-e^{-z^\nu/\nu} \text{ by } e^{z^\nu/\nu}$$

we obtain instead of $\Omega(z)$ a function $\Omega^*(z)$ whose coefficients (are positive and) majorise the absolute values of the corresponding coefficients of $\Omega(z)$. Hence

$$\begin{aligned}\left|\frac{1}{n!}\left|\prod_1\right|-1\right| &\leqq \sum_{\mu=1}^{n}\text{coeffs. } z^\mu \text{ in } \Omega^*(z)<\Omega^*(1)-\Omega^*(0)\\ &=-1+\prod_{\nu=1}^{\omega_1}\left\{1+e^{1/\nu}\sum_{l=\omega_2+1}^{\infty}\frac{1}{l!}\cdot\frac{1}{\nu^l}\right\}\cdot\prod_{\nu=\omega_1+1}^{\infty}\left\{1+e^{1/\nu}\sum_{l=2}^{\infty}\frac{1}{l!}\cdot\frac{1}{\nu^l}\right\}.\end{aligned} \tag{3.6}$$

Here the first product is

$$\begin{aligned}&<\exp\left\{\sum_{\nu=1}^{\omega_1}e^{1/\nu}\sum_{l=\omega_2+1}^{\infty}\frac{1}{l!}\cdot\frac{1}{\nu^l}\right\}<\\ &<\exp\left\{e\sum_{l=\omega_2+1}^{\infty}\frac{1}{l!}+\frac{e}{(\omega_2+1)!}\sum_{\nu=2}^{\omega_1}\sum_{l=\omega_2+1}^{\infty}\frac{1}{\nu^l}\right\}<\\ &<\exp\left\{\frac{2e}{(\omega_2+1)!}+\frac{2e}{(\omega_2+1)!}\sum_{\nu=2}^{\infty}\frac{1}{\nu^{\omega_2+1}}\right\}<\exp\left\{\frac{15}{(\omega_2+1)!}\right\}\end{aligned}$$

and analogously the second is

$$<\exp\left\{\frac{3}{\omega_1}\right\}.$$

From these and (3.6) we get

$$\left|\frac{1}{n!}\left|\prod_1\right|-1\right)\leqq-1+e^{15/(\omega_2+1)!+3/\omega_1}<3\left(\frac{1}{\omega_1}+\frac{1}{\omega_2!}\right)$$

as stated.

This lemma gives immediately the following three corollaries.

Corollary II. *If* $\omega_1(n)$ and $\omega_2(n)$ *tend arbitrarily slowly monotonically to* ∞, *then the canonical decomposition of all but* $o(n!)$ P's *have the double property that no two cycles of length* $> \omega_1(n)$ *are equally long and at most* $\omega_2(n)$ *cycles can have the same length* $\leqq \omega_1(n)$.

Combining this corollary with Corollary. I. we get the

Corollary III. *Apart from* $o(n!)$ P's *the remaining ones, whose totality we may call* $\prod_2$, *have the properties of Corollary II. and*

$$|k(P) - \log n| < \omega(n)\sqrt{\log n} \tag{3.7}$$

if only $\omega(n)$ *tends to* ∞ *arbitrarily slowly.*

Though we shall not need it here, we formulate the

Corollary IV. *For all fixed real* t's *for the number* $H_n(t)$ *of* P's *satisfying simultaneously* (3.7) *and the two requirements of Corollary II. we have the limit-relation*

$$\lim_{n\to\infty} \frac{1}{n!} H_n(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\lambda^2/2}\, d\lambda .$$

As well-known, the order of P is given by

$$O(P) = [n_1, n_2, \ldots, n_k] \tag{3.8}$$

the bracket stands for the smallest common multiple.

Corollary II. gives for arbitrarily small $\varepsilon > 0$ at once for all but $o(n!)$ P's the inequality

$$O(P) \leqq n_1, n_2 \ldots n_k < n^k < e^{(1+\varepsilon)\log^2 n} . \tag{3.9}$$

But this is much weaker than the upper bound in our theorem.

Part II

4. In order to prove the upper bound in our theorem we shall show that if $\omega_1(n)$ tends to ∞ monotonically arbitrarily slowly, then for all but $o(n!)$ P's the n_ν-numbers (in (2.4)) are in a certain sense equi-distributed in the interval $1 \leqq x \leqq n$. More exactly we mean the following. We define N by

$$N = [k^{1/3}] . \tag{4.1}$$

For each $P \in \prod_2$ we can determine uniquely the nonnegative integers

$$S_1, S_2, \ldots, S_N \tag{4.2}$$

so that

$$\begin{aligned} 1 \leqq n_1 < n_2 < \cdots < n_{S_1} \leqq n^{1/N} < n_{S_1+1} < \cdots < n_{S_1+S_2} \leqq n^{2/N} < \\ < n_{S_1+S_2+1} < \cdots < n_{S_1+S_2+\cdots+S_N} = n_k \leqq n ; \end{aligned} \tag{4.3}$$

if there is no n_j e.g. in $n^{1/N} < x \leqq n^{2/N}$ we have $S_2 = 0$ etc.

Of course $S_\nu = S_\nu(P)$ and

$$S_1 + S_2 + \cdots + S_N = k . \tag{4.4}$$

Let $\prod_3$ mean the subset of $\prod_2$ whose P's satisfy the inequality

$$\max_{\mu=1,\dots,N}\left|S_\mu-\frac{k}{N}\right|\leqq\left(\frac{k}{N}\right)^{4/5} \tag{4.5}$$

and let $|\prod_3|$ be the number of its P's. Then we assert the

Lemma IV.
$$\lim_{n\to\infty}\frac{1}{n!}|\prod_3|=1\,.$$

5. For the proof of this lemma it will be sufficient to show that if E_1 stands for the subset of $\prod_2$ for which (4.5) is false, i.e. the inequality

$$\max_{\mu=1,2,\dots,N}\left|S_\mu-\frac{k}{N}\right|>\left(\frac{k}{N}\right)^{4/5} \tag{5.1}$$

holds, and $|E_1|$ for the number of its P's, then the estimation

$$\frac{1}{n!}|E_1|<4^{\omega_1(n)}e^{-1/5\log^{2/5}n} \tag{5.2}$$

holds for $n>c_1$ (of course $\omega_1(n)$ must be $<1/10\log^{2/5}n$ say).

In order to prove (5.2) we write, using lemma II.

$$\frac{1}{n!}|E_1|=\sum_k\sum_{j=1}^{\omega_1}\sum_{\substack{m_\nu,\,n_\nu\\ P\in E_1}}\frac{1}{m_1!\dots m_j!\,n_1^{m_1}\dots n_j^{m_j}n_{j+1}\dots n_k} \tag{5.3}$$

where $j=j(P)$ denotes the number of different cycle-lengths not exceeding $\omega_1(n)$. We can perform easily the summation with respect to

$$m_1,m_2,\dots,m_j\,;$$

this cannot exceed the quantity

$$\sum_{m_1=1}^{\infty}\dots\sum_{m_j=1}^{\infty}\frac{1}{m_1!\,m_2!\dots m_j!}\cdot\frac{1}{n_1^{m_1}n_2^{m_2}\dots n_j^{m_j}}=\prod_{\nu=1}^{j}(e^{1/n_\nu}-1)<\frac{2^{\omega_1}}{n_1n_2\dots n_j}$$

and hence

$$\frac{1}{n!}|E_1|\leqq\omega_1\,2^{\omega_1}\sum_k{\sum}'\frac{1}{n_1n_2\dots n_k}<4^{\omega_1}\sum_k{\sum}'\frac{1}{n_1n_2\dots n_k}, \tag{5.4}$$

where the prime indicates that the summation is extended to all n_ν-systems with properties (2.4) and (4.3)—(5.1). Since for $n>c_2$ we have

$$2\log n>\log n+\omega(n)\sqrt{\log n}\geqq k$$

and from (2.4)

$$2n_k\log n\geqq k\,n_k\geqq\sum_{\nu=1}^{k}n_\nu=n-\sum_{\nu=1}^{j}(m_\nu-1)\,n_\nu\geqq n-\omega_1^2\,\omega_2>\frac{n}{2}$$

we get

$$\frac{1}{n_k}<\frac{4\log n}{n} \tag{5.5}$$

and hence

$$\frac{1}{n!}|E_1|<4^{\omega_1(n)+2}\frac{\log n}{n}\sum_k{\sum}''\frac{1}{n_1n_2\dots n_{k-1}}\underline{\underline{\text{def.}}}\,4^{\omega_1(n)+2}\frac{\log n}{n}\sum_k S_k \tag{5.6}$$

where $\sum''$ refers to the systems

$$1 \leqq n_1 < n_2 < \cdots < n_{k-1} < n \tag{5.7}$$

restricted by (4.3)—(5.1).

Let us consider now for a fixed k the quantity S_k. We have

$$S_k \leqq \sum_{S_1,\ldots,S_N}{}' \left(\sum_{\substack{1 \leqq n_1 < \\ < \cdots < n_{S_1} \leqq n^{1/N}}} \frac{1}{n_1 n_2 \ldots n_{S_1}} \right) \left(\sum_{\substack{n^{1/N} < n_{S_1+1} < \\ < \cdots < n_{S_1+S_2} \leqq n^{2/N}}} \frac{1}{n_{S_1+1} \cdots n_{S_1+S_2}} \right) \cdot$$
$$\cdot \cdots \left(\sum_{\substack{n^{N-1/N} < n_{S_1+\cdots+S_{N-1}+1} < \\ < \cdots < n_{k-1} \leqq n}} \frac{1}{n_{S_1+S_2+\cdots+S_{N-1}+1} \cdots n_{k-1}} \right),$$

where the prime indicates that (5.1) must be satisfied. Hence

$$S_k \leqq \sum_{S_1,\ldots,S_N}{}' \frac{1}{S_1!\,S_2! \ldots S_N!} \left(\sum_{1 \leqq l \leqq n^{1/N}} \frac{1}{l} \right)^{S_1} \left(\sum_{n^{1/N} < l \leqq n^{2/N}} \frac{1}{l} \right)^{S_2} \left(\sum_{n^{N-1/N} < l \leqq n} \frac{1}{l} \right)^{S_N}. \tag{5.8}$$

Since for $n > c_3$

$$\sum_{n^{\nu-1/N} < l \leqq n^{\nu/N}} \frac{1}{l} < \frac{1}{N} \log n + 1,$$

(4.4), (5.8) and (5.6) give, changing also the order of summations, the inequality

$$\frac{1}{n!} |E_1| < \frac{4^{\omega_1+2} \log n}{n} \cdot \sum_k \frac{\left(\frac{1}{N} \log n + 1\right)^k}{k!} \sum_{S_1,\ldots,S_N}{}' \frac{k!}{S_1!\,S_2! \ldots S_N!}. \tag{5.9}$$

6. Now we estimate the inner sum in (5.9) using (5.1). If e.g. $\mu = 1$ this can be written as

$$\sum_{|S_1 - k/N| > (k/N)^{4/5}} \binom{k}{S_1} \sum_{S_2+\cdots+S_N = k-S_1} \frac{(k-S_1)!}{S_2!\,S_3! \ldots S_N!} = \sum_{|S_1 - k/N| > (k/N)^{4/5}} \binom{k}{S_1} (N-1)^{k-S_1}$$
$$= N^k \sum_{|S_1 - k/N| > (k/N)^{4/5}} \binom{k}{S_1} \left(1 - \frac{1}{N}\right)^{k-S_1} \left(\frac{1}{N}\right)^{S_1}.$$

But for $n > c_4$ the last sum, owing to the law of large numbers cannot exceed the quantity

$$\frac{2}{\sqrt{2\pi}} \int_{-\infty}^{-(k/N)^{3/10}} e^{-1/2\,\tau^2} d\tau < e^{-1/3\,k^{2/5}}.$$

The same holds for $\mu = 2, 3, \ldots, N$ too; hence (5.9) gives the estimation

$$\frac{1}{n!} |E_1| < \frac{4^{\omega_1+3} \log^2 n}{n} \sum_{|k - \log n| \leqq \omega(n)\sqrt{\log n}} e^{-1/3\,k^{2/5}} \frac{(\log n + N)^k}{k!} < \frac{4^{\omega_1+3} \cdot e^{-1/4 \log^{2/5} n}}{n} \cdot$$
$$\cdot \sum_k \frac{(\log n + (2 \log n)^{1/3})^k}{k!} = \frac{4^{\omega_1+3}\, e^{-1/4 \log^{2/5} n}}{n} \cdot n\, e^{(2 \log n)^{1/3}} < 4^{\omega_1} \cdot e^{-1/5 \log^{2/5} n}$$

for $n > c_5$, which proves lemma IV.

7. Lemma IV. gives the possibility to improve (3.9). We get this time

$$O(P) \leqq n_1 n_2 \ldots n_k \leqq (n^{1/N})^{S_1} (n^{2/N})^{S_2} \ldots (n^{N/N})^{S_N} \leqq n^{(N+1)/2 \max_\mu S_\mu}$$

and owing to lemma IV.

$$O(P) \leqq n^{(N+1)/2\,(k/N + (k/N)^{4/5})} < n^{k/2 + k^{4/5} N^{1/5}}$$

for $n > c_6$ which is only another form of the assertion, (even with

$$O(P) \leqq e^{1/2\log^2 n + 2(\log n)^{28/15}} \tag{7.1}$$

for all but $o(n!)$ P's).

Part III

8. Before turning to the proof of the lower bound we need some further lemmata. Let $U(m)$ stand for the number of different prime-factors of m, further $Q(m)$ resp. $q(m)$ for the maximal resp. minimal prime-factors of m. Then each integer $m \leqq n$ can obviously uniquely be decomposed in the form

$$m = a(m)\,b(m) \tag{8.1}$$

where

$$Q(a(m)) \leqq \log^6 n \tag{8.2}$$

$$q(b(m)) > \log^6 n\,. \tag{8.3}$$

Let further be R the set of integers defined by

$$m \leqq n\,, \quad a(m) \geqq e^{(\log\log n)^4}\,. \tag{8.4}$$

Then we assert the

Lemma V. *For $n > c_7$ the inequality*

$$\sum_{m \in R} \frac{1}{a(m)} < \frac{1}{\log^{10} n}$$

holds (the summation being extended only to different $a(m)$-values!).

9. For the proof of this lemma we split our sum in the form

$$\sum_{\substack{m \in R \\ U(m) \leqq \log\log n}} \frac{1}{a(m)} + \sum_{l > \log\log n} \sum_{\substack{m \in R \\ U(m) = l}} \frac{1}{a(m)} \underline{\underline{\text{def.}}}\, K_1 + K_2\,. \tag{9.1}$$

The inner sum in K_2 is evidently for $n > c_8$

$$\leqq \frac{1}{l!}\left(\sum_{\substack{p,\,\alpha \\ p \leqq \log^6 n}} \frac{1}{p^\alpha}\right)^l < \frac{1}{l!}\,(2\log\log\log n)^l$$

and thus

$$K_2 < \sum_{l > \log\log n} \frac{1}{l!}\,(2\log\log\log n)^l < e^{-1/2\log\log n \log\log\log n} < \frac{1}{2\log^{10} n}\,. \tag{9.2}$$

As to K_1 let us observe that each term of it contains, as factor, a "large" prime-power. Namely if t is the maximal exponent in $a(m)$, then owing to (8.1) and (8.4) and $U(m) \leqq \log\log n$ we have

$$(\log^6 n)^{t \log\log n} \geqq e^{(\log\log n)^4}$$

i.e.

$$t \geqq \frac{1}{6}\,(\log\log n)^2\,.$$

Thus all m-values of K_1 are divisible by a prime-power p^t satisfying the inequalities

$$2^{1/6(\log\log n)^6} \leqq p^t \leqq n\,, \quad p \leqq \log^6 n\,. \tag{9.3}$$

Fixing this p^t the contribution of the terms divisible by this p^t is (roughly)

$$\leqq p^{-t} \sum_{m \leqq n} \frac{1}{m} < 2 \log n \cdot p^{-t}$$

i.e.

$$K_1 < 2 \log n \sum p^{-t}$$

where the summation is restricted by (9.3). Since the number of terms is

$$< \frac{\log n}{\log 2} \cdot \log^6 n < 2 \log^7 n$$

(9.3) gives for $n > c_9$

$$K_1 < 2 \log n \cdot 2 \log^7 n \cdot 2^{-1/6 (\log \log n)^2} < \frac{1}{2 \log^{10} n} .$$

This, (9.2) and (9.1) prove lemma V.

10. Next let $\prod\prod_4$ be the subset of $\prod\prod_3$ (defined before lemma IV.) with the additional property

$$Q((n_\mu, n_\nu)) \leqq \log^6 n \tag{10.1}$$

for each $1 \leqq \mu < \nu \leqq k-1$ pairs and $|\prod\prod_4|$ be the number of its P's. Then we assert the

Lemma VI. *The relation*

$$\lim_{n \to \infty} \frac{1}{n!} |\prod\prod_4| = 1$$

holds.

In other words for almost all P's, in addition to what was previously said, no pair n_μ, n_ν $(1 \leqq \mu < \nu \leqq k-1)$ have "large" common prime-factors.

11. The lemma will obviously be proved if we can show that, denoting by E_2 the subset of $\prod\prod_3$ whose elements have the property

$$\max_{1 \leqq \mu < \nu \leqq k-1} Q((n_\mu, n_\nu)) > \log^6 n \tag{11.1}$$

and denoting by $|E_2|$ the number of its P's, the inequality

$$\frac{1}{n!} |E_2| < \frac{4^{\omega_1(n)+6}}{\log n} \tag{11.2}$$

holds. For the proof of this assertion we can start from (5.6) in the form

$$\frac{1}{n!} |E_2| < 4^{\omega_1(n)+2} \frac{\log n}{n} \sum_{|k - \log n| \leqq \log^{3/4} n} {\sum}''' \frac{1}{n_1 n_2 \dots n_{k-1}} \tag{11.3}$$

where $\sum'''$ refers beside (5.7) also to the restriction (11.1). Fixing the μ, ν pair in (11.1) as

$$k-2, \quad k-1 \quad \text{say}$$

the corresponding part of the double-sum as (11.3) is

$$< \sum_{p > \log^6 n} \frac{1}{p^2} {\sum}''' \frac{1}{n_1 n_2 \dots n_{k-3} n'_{k-2} n'_{k-1}} <$$

$$< \sum_{p > \log^6 n} \frac{\left(\log \frac{n}{p} + 1\right)^2}{p^2} \sum_{1 \leqq n_1 < \dots < n_{k-3} \leqq n} \frac{1}{n_1 n_2 \dots n_{k-3}} <$$

$$< \log^2 n \left(\sum_{p > \log^6 n} \frac{1}{p^2} \right) \frac{(1 + \log n)^{k-3}}{(k-3)!} .$$

Summing for all μ, ν-pairs we get for $\sum'''$ the upper bound

$$\binom{[2\log n]}{2}\log^2 n\cdot\frac{1}{\log^6 n}\frac{(1+\log n)^{k-3}}{(k-3)!}<\frac{4}{\log^2 n}\cdot\frac{(1+\log n)^{k-3}}{(k-3)!}.$$

Summation with respect to k gives from (11.3)

$$\frac{1}{n!}|E_2|<\frac{4^{\omega_1+2}\log n}{n}\cdot\frac{4}{\log^2 n}\cdot en<\frac{4^{\omega_1+6}}{\log n}$$

as stated.

12. *We* have to make a final selection from $\prod\prod_4$. For all of its P's we form their canonical decomposition and for all n_ν cycle-lengths the decomposition (8.1)

$$n_\nu=a(n_\nu)\,b(n_\nu)\qquad(a(n_\nu),\ b(n_\nu)\text{ functions of }P)\tag{12.1}$$

shortly. Let $\prod\prod_5$ be the subset of $\prod\prod_4$, for whose P's the inequality

$$\max_{\nu=1,\dots,k-1}a(n_\nu)\leqq e^{(\log\log n)^4}$$

holds. Denoting by $|\prod\prod_5|$ the number of these P's we assert the

Lemma VII. *The relation*

$$\lim_{n\to\infty}\frac{1}{n!}|\prod\prod_5|=1$$

holds.

By other words for almost all P's, in addition to what was previously said, the contribution of the "not too large" prime-factors of the P's is "not too large".

13. Again the lemma will be proved if we can show that, denoting by E_3 the subset of $\prod\prod_4$ whose elements have the property

$$\max_{\nu=1,\dots,k-1}a(n_\nu)>e^{(\log\log n)^4}\tag{13.1}$$

and denoting by $|E_3|$ the number of its P's, the inequality

$$\frac{1}{n!}|E_3|<\frac{4^{\omega_1+5}}{\log^7 n}\tag{13.2}$$

holds.

For the proof of this assertion we can start again from (5.6) in the form

$$\frac{1}{n!}|E_3|<4^{\omega_1+2}\frac{\log n}{n}\sum_k{\sum}^*\frac{1}{n_1n_2\dots n_{k-1}}\tag{13.3}$$

where $\sum^*$ means that in addition to the properties of $\prod\prod_4$ also (13.1) is fulfilled. We split the inner sum (13.3) into k partial-sums, the μ^{th} of which replaces (13.1) by

$$a(n_\mu)>e^{(\log\log n)^4}.\tag{13.4}$$

First we perform the summation with respect to the n_j's with $j\neq\mu$; this gives at most

$$\frac{(1+\log n)^{k-2}}{(k-2)!}.$$

Next we perform the summation with respect to n_μ but taking in account (13.4). Fixing a value for $a(n_\mu)$ the corresponding n_μ's contribute to our sum by

$$\frac{1}{a(n_\mu)}(1+\log n)$$

at most; thus

$$\sum{}^{*}\frac{1}{n_1 n_2 \dots n_{k-1}} < \sum_{\mu}\frac{(1+\log n)^{k-2}}{(k-2)!}\cdot 2\log n \sum_{R}\frac{1}{a(n_\mu)}.$$

Using lemma V. this is

$$< \sum_{\mu}\frac{(1+\log n)^{k-2}}{(k-2)!}\cdot\frac{2}{\log^9 n}.$$

Summing with respect to μ gives

$$\sum{}^{*} < \frac{2}{\log^8 n}\cdot\frac{(1+\log n)^{k-2}}{(k-2)!}.$$

Putting this in (13.3) we get

$$\frac{1}{n!}|E_3| < \frac{4^{\omega+3}}{n\log^7 n}\sum_{k}\frac{(1+\log n)^{k-2}}{(k-2)!} < \frac{4^{\omega+5}}{\log^7 n}$$

which proves lemma VII.

14. Now we are in the position to establish the lower bound in our theorem. According to lemma VII. apart from $o(n!)$ P's the remaining ones have the following properties ($\omega_1(n)$, $\omega_2(n)$ and $\omega(n)$ equals $\sqrt{\log\log n}$ e.g.)

a) $|k(P)-\log n| \leqq \omega(n)\sqrt{\log n}$

b) no two n_ν-cycles of length $\geqq \omega_1(n)$ in P have the same length

c) at most $\omega_2(n)$-cycles in P can have the same length $\leqq \omega_1(n)$,

d) the different cycle-lengths in P are "equidistributed" in the sense (4.3)—(4.5)

e) no n_μ, n_ν pairs ($1 \leqq \mu < \nu \leqq k-1$) have a common prime-factor $> \log^6 n$.

f) for all n_ν cycle-lengths the contribution of the prime-factors not exceeding $\log^6 n$ cannot exceed $\exp.((\log\log n)^4)$.

For these P's we have with the notation (8.1)—(8.3) the inequality

$$O(P) = [n_1, \dots, n_k] \geqq [b(n_1), b(n_2), \dots, b(n_{k-1})] \tag{14.1}$$

and *since owing to the definition of* $b(n_\nu)$ *and property e., we have*

$$(b(n_\mu), b(n_\nu)) = 1$$

also

$$[b(n_1), b(n_2), \dots, b(n_{k-1})] = b(n_1)b(n_2)\dots b(n_{k-1}) = \frac{n_1 n_2 \dots n_{k-1}}{a(n_1)a(n_2)\dots a(n_{k-1})}$$

and thus from (14.1)

$$O(P) \geqq \frac{n_1 n_2 \dots n_k}{a(n_1)a(n_2)\dots a(n_{k-1})}\frac{1}{n}. \tag{14.2}$$

But owing to properties f) and a)

$$a(n_1)a(n_2)\dots a(n_{k-1}) \leqq e^{(\log\log n)^4 2\log n}$$

we get for the remaining P's, i.e. for all but $o(n!)$ P's

$$O(P) \geqq n_1 n_2 \dots n_k \cdot e^{-3\log n(\log\log n)^4}. \tag{14.2}$$

The lower bound will be established at once using property d). This gives namely

$$n_1 n_2 \dots n_k \geqq (n^{1/N})^{S_2} (n^{2/N})^{S_3} \dots (n^{(N-1)/N})^{S_N} \geqq n^{(N-1)/2 \min_\mu S_\mu}.$$

But from (4.5)

$$\min_\mu S_\mu \geqq \frac{k}{N} - \left(\frac{k}{N}\right)^{4/5}$$

i.e.

$$n_1 n_2 \dots n_k > n^{k/2 - 2k^{4/5} N^{1/5}} > e^{1/2 \log^2 n - 3 \log^{28/15} n}$$

which establishes the upper bound for $n > c_{10}$ (even with

$$O(P) > e^{1/2 \log^2 n - 4 \log^{28/15} n} \tag{14.3}$$

for all but $o(n!)$ P's).

Finally we remark that what we actually proved (see (14.2) and (3.9)) is that apart from $o(n!)$ P's the inequality

$$e^{-3 \log n (\log\log n)^4} \leqq \frac{O(P)}{n_1 n_2 \dots n_k} \leqq 1 \tag{14.4}$$

holds i.e. $O(P)$ is "essentially" $n_1 n_2 \dots n_k$, for "almost all" P's.

References

[1] CHOWLA, S., I. N. HERSTEIN, and K. MOORE: On recursions connected with symmetric groups I. Canadian J. Math. **3**, 328—334 (1951).

[2] ERDÖS, P., and G. SZEKERES: Über die Anzahl der Abelschen Gruppen gegebener Ordnung. Acta Litt. Sci. Szeged **7**, 95—102 (1934).

[3] GONČAROV, V. L.: On the field of combinatory analysis. Izvestija Akad. Nauk SSSR Ser. mat. **8**, 3—48 (1944); (see also Translations of the Amer. Math. Soc. Ser. **2**. **19**, 1—46 (1962).

[4] LANDAU, E.: Handbuch der Lehre von der Verteilung der Primzahlen. Bd. **I**. p. 222 (1909).

[5] MOSER, L., and M. WYMAN: On the solutions of $x^d = 1$ in symmetric groups. Canadian J. Math. **7**, 159—188 (1955).

[6] RIORDAN, I.: An introduction to combinatorial analysis. New York: 1958. in particular p. 67.

[7] ROUSE BALL, W. W.: Mathematical Recreations and Essays. Revised by H. S. M. COXETER, Eleventh edition 1939. See in part. p. 310—312.

Magyar Tudományos Akadémia,
Matematikai Kutató Intézete,
Reáltanoda u. 13—15
Budapest V., Ungarn

(Received May 5, 1965)