BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 15, Number 2, October 1986

# THE ASYMPTOTICS OF $e^{P(z)}$ AND THE NUMBER OF ELEMENTS OF EACH ORDER IN $S_n$

HERBERT S. WILF

ABSTRACT. We answer a question that was raised in 1952 by Chowla, Herstein and Scott, concerning the asymptotic behavior of the number of elements of order $m$ in the symmetric group $S_n$, for fixed $m$, as $n \to \infty$. The methods used include Hayman's method for asymptotics of coefficients of analytic functions, and the Lagrange inversion formula. The question had previously been answered only for prime $m$.

**1. Introduction.** In 1952 Chowla, Herstein and Scott [**2**] asked for the asymptotic behavior, for large $n$, of the number $f(m,n)$ of solutions of the equation $x^m = 1$ in the symmetric group $S_n$. They found the generating function and some recurrence relations for the $f(m,n)$.

In 1955 Moser and Wyman [**4**] found the answer when $m = 2$, i.e., they counted the involutions in $S_n$, for large $n$. Then they developed a method [**5**] that permitted them to solve the problem when $m = p$, a prime number.

The problem is discussed further in Bender [**10**], §8.1.

In this paper we will give an explicit answer that is valid for every $m$.

The ingredients of the solution are the following.

1° *Hayman's method.* In 1956 W. K. Hayman developed a general method for finding the asymptotic behavior of the coefficients of analytic functions (some later developments of the theory are in [**11**, **12**]). This method has already had a number of applications to combinatorial problems. Hayman's machinery allows us to take the first step in the solution of the present problem.

The unfinished business that it leaves is that the answer is expressed in terms of a root of a certain equation, and that root must be determined with considerable accuracy in order to get an explicit asymptotic result.

2° *Lagrange's inversion formula.* We will use the famous inversion formula of Lagrange to find the solution of the polynomial equation referred to above. Remarkably, what it gives is the root expressed as an infinite series that is at once convergent and asymptotic.

The unfinished business that it leaves is that the coefficients of the series in question are given implicitly, but we want an explicit solution.

3° *Special properties.* Until this point the analysis will have been quite general, and applicable to any problem of the type considered. To get explicit

Received by the editors January 8, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 05A05, 05A15, 05A20, 10A50, 30D15, 41A60.
*Key words and phrases.* Symmetric group, Hayman's method, Lagrange inversion, involutions, order, asymptotic..
Supported in part by the U.S. Office of Naval Research.


0273-0979/86 $1.00 + $.25 per page

values for the coefficients mentioned above, however, one has to use specific properties of the problem of the orders of elements of $S_n$. The most useful special property turns out to be this: if the order of an element divides $m$ and is $< m$ then it is $\leq m/2$. (!)

**2. Statement of results.** Let

$$f(m,n) = |\{x \in S_n \mid x^m = 1\}|.$$

It was found in [**2**], and can also be obtained quickly from the exponential formula, that

$$\sum_{n\geq 0} \frac{f(m,n)}{n!} x^n = \exp\left\{\sum_{d|m} \frac{x^d}{d}\right\} \qquad (m = 1,2,\ldots). \tag{2.1}$$

When $m = 2$, Moser and Wyman found that the number $f(2,n)$ of involutions of $n$ letters satisfies

$$f(2,n) \sim \frac{1}{\sqrt{2}} n^{n/2} \exp(-n/2 - 1/4 + \sqrt{n}). \tag{2.2}$$

If $m$ is an odd prime $p$, they showed that

$$f(p,n) \sim \frac{1}{\sqrt{p}} n^{n(1-1/p)} \exp(-n(1-1/p) + n^{1/p}). \tag{2.3}$$

The main result of the present paper is the following. Define

$$\varepsilon_{m,n} = \begin{cases} 1/(2m^2 n) & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd,} \end{cases} \tag{2.4}$$

and

$$\tau = \tau(m,n) = n^{-1/m}\left\{1 + \frac{1}{mn} \sum_{\substack{d|m \\ d<m}} n^{d/m} + \varepsilon_{m,n}\right\}. \tag{2.5}$$

Then for fixed $m$, as $n \to \infty$ we have

$$f(m,n)/n! \sim \frac{\tau^n}{\sqrt{2\pi mn}} \exp\left\{\sum_{d|m} \frac{1}{d\tau^d}\right\}. \tag{2.6}$$

It is easy to check that (2.6) reduces to (2.2), (2.3) in those special cases. If $g(m,n)$ is the number of elements of $S_n$ of order $m$ then evidently

$$g(m,n) = \sum_{d|m} \mu(m/d) f(d,n) \qquad (m = 1,2,\ldots),$$

hence the result (2.6) applies without change to $g(m,n)$ also.

**3. The first step: Hayman's method.** In his 1956 paper Hayman considered, among other problems, the question of the asymptotic behavior of $\{a_n\}$ defined by

$$\sum_{n\geq 0} a_n z^n = e^{P(z)} \tag{3.1}$$

where

$$P(z) = \sum_{l=1}^{m} c_l z^l \tag{3.2}$$

is a polynomial of degree exactly $m$. The conditions on $P(z)$ are that $\exists n_0 \ni \forall n > n_0 \colon a_n > 0$. He then showed that

$$a_n \sim \frac{e^{P(r_n)}}{\sqrt{2\pi m n}\, r_n^n} \qquad (n \to \infty) \tag{3.3}$$

where $r_n$ is the positive real root of the equation

$$rP'(r) = n. \tag{3.4}$$

The usefulness of this answer depends on our being able to estimate the root of (3.4) with sufficient precision to allow $r_n^n$ and $e^{P(r_n)}$ to be estimated asymptotically also. In some applications of this method, such as to the growth of Bell numbers, this estimation has posed questions of extreme difficulty. In others it may be trivial. In this application it is do-able, as we will see. It is clear that for the root of (3.4) we have

$$r_n \sim (n/mc_m)^{1/m}$$

and therefore in order to estimate $r_n^n$ we will need $r_n$ itself with an error of $o(n^{-1+1/m})$ or better. This precision would also suffice for estimating $e^{P(r_n)}$ in (3.3).

Hence our next task will be to estimate the root of (3.4) with the required precision.

**4. The second step: Lagrange inversion.** The form of the Lagrange inversion formula that we will use [**9**, p. 132] is this. If $u = u(t)$ is the solution of the equation $u = t\phi(u)$, where $\phi$ is analytic in some disc centered at the origin, then

$$u(t) = \sum_{l \geq 1} \beta_l t^l / l, \tag{4.1}$$

where each $\beta_l$ is the coefficient of $u^{l-1}$ in the expansion of $\phi(u)^l$, and the expansion (4.1) converges in a suitable disc about the origin.

To bring the equation (3.4) that we wish to solve into this form we put $u = r_n^{-1}$, $t = n^{-1/m}$ and

$$\phi(u) = \left\{ \sum_{l=1}^{m} l c_l u^{m-l} \right\}^{1/m} = \{u^{m-1} P'(1/u)\}^{1/m}. \tag{4.2}$$

It now follows from the Lagrange inversion formula that the solution $r = r_n$ of (3.4) is of the form

$$\frac{1}{r_n} = \sum_{l=1}^{\infty} \frac{\beta_l}{l n^{l/m}} \tag{4.3}$$

where

$$\beta_l = \text{Coeff}_{u^{l-1}} \{[u^{m-1} P'(1/u)]^{l/m}\} \qquad (l = 1, 2, \ldots). \tag{4.4}$$

The series (4.3) is convergent, by Lagrange's theorem, for all sufficiently large $n$, and it is obviously asymptotic as well.

For our present purposes there is more precision in (4.3) than we need. In order to estimate $r_n^n$ we will need only the terms $l \leq m+1$ in (4.3). We can summarize these observations in the following

PROPOSITION. *The coefficients* $\{a_n\}$ *of* (3.1) *satisfy*

$$a_n \sim \frac{e^{P(\rho_n)}}{\sqrt{2\pi m n}\,\rho_n^n}$$

*where*

$$\frac{1}{\rho_n} = \sum_{l=1}^{m+1} \frac{\beta_l}{l n^{l/m}}$$

*and the* $\beta$*'s are given by* (4.4).

It remains to deal with the numbers $\beta_l$ of (4.4), which are presented there in a somewhat opaque fashion, as the $(l-1)$st coefficient of a function which itself depends on $l$.

**5. The third step: a bit of luck.** In order to proceed we must confront the specific polynomial

$$P(z) = \sum_{d|m} z^d/d$$

that we are interested in. First recall that the precision with which we need to know $r_n$ is

$$r_n = n^{1/m} + \cdots + o(n^{-1+1/m}). \tag{5.1}$$

Next, the $\beta$'s are the coefficients of

$$\begin{aligned} \{u^{m-1}P'(1/u)\}^{l/m} &= \left\{\sum_{d|m} u^{m-d}\right\}^{l/m} \\ &= \{1 + u^{m-d_2} + \cdots + u^{m-d_k}\}^{l/m} \\ &= 1 + \frac{l}{m}(u^{m-d_2} + \cdots + u^{m-d_k}) \\ &\quad + \frac{1}{2}\frac{l}{m}\left(\frac{l}{m} - 1\right)(u^{m-d_2} + \cdots + u^{m-d_k})^2 + \cdots \end{aligned} \tag{5.2}$$

Consider the powers of $u$ that appear in the first parenthesis. Since $d_2 \leq m/2$, $m - d_2 \geq m/2$, and those exponents of $u$ must lie in $[m/2, m-1]$. In the square of that first parenthesis there appear exponents in the range $[m, 2m-2]$, and so forth. It follows that if all we need are $\beta_1, \beta_2, \ldots, \beta_{m+1}$ then we will correctly find all of them by retaining only the terms shown in the last member of (5.2) above.

More precisely, we have

$$\beta_l = \begin{cases} 1, & \text{if } l = 1, \\ l/m, & \text{if } l = m - d + 1, d|m, d < m, \\ (1 + 1/m)/2m, & \text{if } l = m+1 \text{ and } m \text{ is even.} \\ 0, & \text{for all other } l \leq m+1. \end{cases} \tag{5.3}$$

Now from the expansion (4.3) we have

$$\frac{1}{r_n} = \frac{1}{n^{1/m}} + \frac{1}{m} \sum_{\substack{d|m \\ d<m}} \frac{1}{n^{1-d/m+1/m}} + \frac{\varepsilon_{m,n}}{n^{1/m}} + o(n^{-1-1/m}), \tag{5.4}$$

where $\varepsilon_{m,n}$ is given by (2.4).

The estimate (5.4) has the required accuracy, and so we obtain

$$\frac{1}{r_n^n} \sim \frac{\{1 + \frac{1}{mn} \sum' n^{d/m} + \varepsilon_{m,n}\}^n}{n^{n/m}}, \tag{5.5}$$

where the '$\sum'$' is a sum over the proper divisors $d$ of $m$, and the result (2.6) is proved.

## REFERENCES

1. S. Chowla, I. N. Herstein and K. Moore, *On recursions connected with symmetric groups*. I, Canad. J. Math. **3** (1951), 328–334.

2. S. Chowla, I. N. Herstein and W. R. Scott, *The solutions of $x^d = 1$ in symmetric groups*, Norske Vid. Selsk. **25** (1952), 29–31.

3. E. Jacobsthal, *Sur le nombre d'éléments du group symmetrique $S_n$ dont l'ordre est un nombre premier*, Norske Vid. Selsk. **21** (1949), 49–51.

4. L. Moser and M. Wyman, *On solutions of $x^d = 1$ in symmetric groups*, Canad. J. Math. **7** (1955), 159–168.

5. ——, *Asymptotic expansions*, Canad. J. Math. **8** (1956), 225–233.

6. W. K. Hayman, *A generalisation of Stirling's formula*, J. Reine Angew. Math. **196** (1956), 67–95.

7. L. Moser and M. Wyman, *Asymptotic expansions*. II, Canad. J. Math. **9** (1957), 194–209.

8. Max Wyman, *Asymptotic behavior of Laurent coefficients*, Canad. J. Math. **11** (1959), 534–555.

9. E. T. Whittaker and G. N. Watson, *A course of modern analysis*, 4th ed., Cambridge, 1958.

10. Edward A. Bender, *Asymptotic methods in enumeration*, SIAM Rev. **16** (1974), 485–515.

11. B. Harris and L. Schoenfeld, *Asymptotic expansions for the coefficients of analytic functions*, Illinois J. Math. **12** (1968), 264–277.

12. A. M. Odlyzko and L. B. Richmond, *Asymptotic expansions for the coefficients of analytic generating functions*. Aeq. Math. **28** (1985), 50–63.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PENNSYLVANIA 19104