

величин, к проверке скорости роста их дисперсий. В ряде случаев это упрощает обоснование их использования в практических задачах (примеры см. в [7]).

Для доказательства теоремы 1 использовался топологический вариант метода моментов, предложенный в [8].

## ЛИТЕРАТУРА

1. *Hoeffding W.* A class of statistics with asymptotically normal distribution // Ann. Math. Statist. 1948. Vol. 19. No. 3. P. 293–325.
2. *Королук В. С., Боровских Ю. В.* Теория  $U$ -статистик. Киев: Наук. думка, 1989.
3. *Михайлов В. Г.* Центральная предельная теорема для числа неполных данных повторений // Теория вероятн. и ее примен. 1975. Т. 20. Вып. 4. С. 880–884.
4. *Шойтов А. М.* Нормальное приближение в задаче об эквивалентных цепочках // Тр. по дискр. матем. 2007. Т. 10. С. 326–349.
5. *Mikhailov V. G. and Mezhenaya N. M.* Normal approximation for  $U$ - and  $V$ -statistics of a stationary absolutely regular sequence // Sib. Elektron. Mat. Izv. 2020. V. 17. P. 672–682.
6. *Doukhan P.* Mixing: Properties and Examples. Lecture Notes in Statistics 85. N.Y.: Springer Verlag, 1994.
7. *Rukhin A., Soto J., Nechvatal J., et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22r1a. Natl. Inst. Stand. Technol. Spec. Publ., 2010.
8. *Janson S.* Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs // Ann. Probab. 1988. V. 16. No. 1. P. 293–325.

УДК 519.1

DOI 10.17223/2226308X/14/3

## О НАИБОЛЬШЕМ ПОРЯДКЕ ПОДСТАНОВОК ЗАДАННОЙ СТЕПЕНИ

В. М. Фомичёв

Необходимым требованием к системе шифрования является достаточно большой порядок группы, которая ассоциируется с шифром (то есть порождается подстановками шифра). В связи с этим представляет интерес величина  $\mu(n)$ , оценивающая порядки циклических групп подстановок степени  $n$ , в том числе циклических групп, порождённых шифрующими подстановками. Известно, что порядок подстановки равен наименьшему общему кратному длин её циклов. Однако мало изучена функция  $\mu(n)$ , принимающая значения, равные наибольшему порядку подстановки степени  $n$ . Показана монотонность функции  $\mu(n)$ , получена двухсторонняя оценка её значений:  $\prod_{\omega(n)} \leq \mu(n) \leq \lceil \sqrt{2(n-1)} \rceil!$ , где  $\prod_{\omega(n)}$  — произведение всех первых (в порядке возрастания) простых чисел, сумма которых не больше  $n$ . Получена асимптотическая оценка нижней границы при больших  $n$ :

$$\mu(n) > 224k!(1,665)^k (\ln k)^{(k-15)/2}$$

при любом  $n \geq 1000$  и  $k = \lfloor \sqrt{2n/\ln n} \rfloor$ .

**Ключевые слова:** порядок подстановки, цикловая структура подстановки, простое число.

Каждая подстановка есть произведение независимых циклов. Если длины циклов подстановки  $g$  равны  $l_1, \dots, l_m$ , то её порядок равен

$$\text{ord } g = \text{НОК}(l_1, \dots, l_m).$$

Если в записи подстановки имеется  $k_i$  циклов длины  $l_i$ ,  $i = 1, \dots, m$ , то это свойство записывается с помощью цикловой структуры  $C(g)$  подстановки  $g$ :

$$C(g) = \{l_1^{[k_1]}, \dots, l_m^{[k_m]}\}; \quad (1)$$

эти числа связаны со степенью  $n$  подстановки равенством

$$k_1 l_1 + \dots + k_m l_m = n.$$

Далее считаем, что длины циклов упорядочены:  $l_1 < \dots < l_m$ .

Обозначим:

- $S_n$  — группа всех подстановок степени  $n$ ;
- $S_n^{(m)}$  — множество всех подстановок степени  $n$ , состоящих из  $m$  циклов,  $1 \leq m \leq n$ ;
- $\text{ORD}_n = \{\text{ord } g : g \in S_n\}$ ;
- $\mu(n) = \max_{g \in S_n} \text{ord } g$ ;
- $g_n^{\max}$  — подстановка  $g \in S_n$ , такая, что  $\text{ord } g = \mu(n)$ .

Необходимым требованием к системе шифрования является достаточно большой порядок группы, которая ассоциируется с шифром (то есть порождается подстановками шифра). В связи с этим представляет интерес величина  $\mu(n)$ , оценивающая порядки циклических групп подстановок степени  $n$ , в том числе циклических групп, порождённых шифрующими подстановками.

Тривиальные оценки для порядка подстановок из  $S_n$  имеют вид

$$1 \leq \text{ord } g \leq n!,$$

где нижняя оценка достижима при любом  $n$  для тождественной подстановки и верхняя оценка достижима лишь при  $n \leq 2$ .

Задача нахождения  $\mu(n)$  сводится к определению наибольшего значения  $\text{НОК}(l_1, \dots, l_m)$ , где максимум берётся по всем разбиениям  $n$ -множества на  $m$  непустых блоков порядков  $l_1, \dots, l_m$ .

**Утверждение 1.** Функция  $\mu(n)$  монотонно неубывающая с ростом  $n$ .

**Доказательство.** Пусть  $g = g_n^{\max}$  и цикловая структура подстановки  $g$  определена равенством (1). Возьмём подстановку  $h \in S_{n+1}$  со свойством

$$C(h) = \begin{cases} \{l_1^{[k_1+1]}, \dots, l_m^{[k_m]}\}, & l_1 = 1, \\ \{1^{[1]}, l_1^{[k_1]}, \dots, l_m^{[k_m]}\}, & l_1 > 1. \end{cases}$$

Отсюда  $\mu(n) = \text{ord } g = \text{ord } h \leq \mu(n+1)$ . ■

**Замечание 1.** Функция  $\mu(n)$  не является строго возрастающей. Например,  $\mu(5) = \mu(6)$ , так как

$$\begin{aligned} C(g_5^{\max}) &= \{2^{[1]}, 3^{[1]}\}, \quad \mu(5) = 6, \\ C(g_6^{\max}) &= \{1^{[1]}, 2^{[1]}, 3^{[1]}\} \text{ или } C(g_6^{\max}) = \{6^{[1]}\}, \quad \mu(6) = 6. \end{aligned}$$

**Утверждение 2.** Для любого  $n > 1$

$$\text{ORD}_n \supseteq \{1, \dots, n\}.$$

**Доказательство.** Следует из существования в  $S_n$  подстановки  $g_l$  с цикловой структурой  $C(g_l) = \{1^{[n-l]}, l^{[l]}\}$ ,  $l = 1, \dots, n$ . ■

Множество натуральных чисел  $L = \{l_1, l_2, \dots, l_m\}$ , где  $m > 1$  и  $l_1 < \dots < l_m$ , назовём  $r$ -разреженным,  $r \geq 0$ , если  $l_m - l_1 = m - 1 + r$ ; при  $r = 0$  множество  $L$  назовём сплошным. Множество натуральных чисел  $L' = \{\lambda_1, \lambda_2, \dots, \lambda_m\}$  назовём 2-сжатием множества  $L$ , если положительны обе разности  $\lambda_1 - l_1$  и  $l_m - \lambda_m$ , и 1-сжатием множества  $L$ , если одна из разностей  $\lambda_1 - l_1$  и  $l_m - \lambda_m$  положительна, а другая равна 0.

Обозначим:  $\Sigma(L) = l_1 + l_2 + \dots + l_m$ ;  $Z(L) = l_1 l_2 \dots l_m$ .

**Утверждение 3.** Для любого  $r$ -разреженного множества  $L = \{l_1, l_2, \dots, l_m\}$  имеется сплошное множество  $L'$ , являющееся:

- 1) 2-сжатием множества  $L$  при  $r > 1$ , таким, что  $\Sigma(L) \leq \Sigma(L')$  и  $Z(L) < Z(L')$ ;
- 2) 1-сжатием множества  $L$  при  $r = 1$ , таким, что  $\Sigma(L) \leq \Sigma(L')$  и  $Z(L) < Z(L')$ .

Занумеруем простые числа в порядке возрастания:  $p_1 = 2, p_2 = 3, \dots$

При  $n > 1$  обозначим:  $\Omega(n) = \{(p_{i_1}, \dots, p_{i_r})\}$  — семейство всех множеств простых чисел, для которых  $p_{i_1} + \dots + p_{i_r} \leq n$ ,  $r \leq n/2$ , числа  $i_1, \dots, i_r$  натуральные;  $\Pi(n) = \max_{\Omega(n)} p_{i_1} \dots p_{i_r}$  — наибольшее (по всем наборам из  $\Omega(n)$ ) значение произведения чисел набора.

**Теорема 1.** Для любого  $n > 3$  верны оценки:

$$\Pi(n) \leq \mu(n) \leq \lceil \sqrt{2(n-1)} \rceil !.$$

**Доказательство.**

Для любого  $n > 3$  и любого набора простых чисел  $(p_{i_1}, \dots, p_{i_r}) \in \Omega_n$  существует подстановка степени  $n$ , содержащая циклы длины  $p_{i_1}, \dots, p_{i_r}$ . Порядок такой подстановки равен  $p_{i_1} \dots p_{i_r}$  в силу попарной взаимной простоты чисел набора. Нижняя оценка доказана.

Пусть подстановка  $g$  степени  $n$  порядка  $\mu(n)$  содержит циклы, множество длин которых есть  $L = \{l_1, \dots, l_m\}$ . Если  $\Sigma(L) = d < n$ , то подстановка  $g$  имеет два или более циклов одинаковой длины  $l_r$ ,  $r \in \{1, \dots, m\}$ , где  $1 \leq l_r \leq n - d$ . Тогда существует подстановка  $h$  степени  $n$  с множеством длин циклов  $L_1 = \{l_1, \dots, l_{m-1}, l_m + l_r\}$ , при этом  $Z(L) < Z(L_1)$ . Отсюда получаем

$$\text{ord } g = \text{НОК}(L) \leq Z(L) < Z(L_1).$$

Рассуждая аналогично, за конечное число шагов перейдём от подстановки  $g$  к подстановке  $g'$  степени  $n$ , у которой длины всех циклов различные и  $\text{ord } g < \Pi(L')$ , где  $L'$  — множество длин всех циклов подстановки  $g'$ . Значит,  $\mu(n)$  не превышает наибольшее значение  $Z(L)$ , где максимум берется по наборам  $L$  для множества всех подстановок степени  $n$  с различными длинами всех циклов.

В соответствии с утверждением 3, верхняя оценка  $Z(L)$  достигается на одной из подстановок степени  $n$ , у которой множество длин циклов  $L$  есть сплошное множество.

Оценим произведение  $\pi(l, m) = (l+1) \dots (l+m)$  при условии, что числа  $l$  и  $m$  таковы, что  $\xi(l, m) = (l+1) + \dots + (l+m)$  есть величина порядка  $n + o(n)$ , что не нарушает справедливость оценки  $\text{ord } g$  с помощью числа  $\pi(l, m)$ .

Суммируя арифметическую прогрессию, получаем

$$\xi(l, m) = (l + (m+1)/2)m = n + o(n). \quad (2)$$

Если при фиксированном  $l > 0$  взять  $m = \left\lceil \sqrt{2(n-l)} \right\rceil$ , то

$$\xi \left( l, \left\lceil \sqrt{2(n-l)} \right\rceil \right) \geq \xi \left( l, \sqrt{2(n-l)} \right) = n + \sqrt{2(n-l)}(l + 1/2) - l.$$

Тогда значение  $\xi \left( l, \left\lceil \sqrt{2(n-l)} \right\rceil \right)$  удовлетворяет (2) при  $l = o(\sqrt{n})$ . Взяв  $l = 1$ ,  $m = \left\lceil \sqrt{2(n-1)} \right\rceil$ , получим

$$\pi \left( 1, \left\lceil \sqrt{2(n-1)} \right\rceil \right) \leq \left\lceil \sqrt{2(n-1)} \right\rceil !.$$

Следовательно,  $\text{ord } g < \left\lceil \sqrt{2(n-1)} \right\rceil !$ . ■

**Следствие 1.** При любом  $n \geq 1000$  и  $k = \left\lfloor \sqrt{2n/\ln n} \right\rfloor$  верна нижняя оценка

$$\mu(n) > 224 k! (1,665)^k (\ln k)^{(k-15)/2}.$$

**Доказательство.** Для получения ограничения снизу для  $\text{ord } g$  оценим произведение первых простых чисел, сумма которых не превышает  $n$ .

В соответствии с верхней оценкой Россера [2]

$$p_k < k \ln k + k \ln \ln k + 8k.$$

Заметим, что  $p_1 + p_2 + p_{15} = 328$ ,  $p_{16} = 53$ . Следовательно, при любом  $n \geq 381$  выполнено условие

$$\Sigma(\{p_1, p_2, \dots, p_k\}) \leq n, \quad (3)$$

если  $k \geq 16$ , и условие

$$\sum_{r=16}^k r \psi(r) \leq n - 328,$$

где  $\psi(r) = \ln r + \ln \ln r + 8$ . Так как при  $r \geq 1$  функция  $\psi(r)$  монотонно возрастает, то

$$\sum_{r=16}^k r \psi(r) < \psi(k) \sum_{r=16}^k r = \psi(k) \frac{(k-15)(k+16)}{2}.$$

Значит, условие (3) удовлетворено, если

$$\psi(k) \frac{(k-15)(k+16)}{2} \leq n - 328. \quad (4)$$

В частности, при  $n \geq 1000$  и  $16 \leq k \leq \left\lfloor \sqrt{2n/\ln n} \right\rfloor$  имеем

$$\begin{aligned} \frac{(k-15)(k+16)}{2} &\leq \frac{n}{\ln n} + \sqrt{\frac{n}{2 \ln n}} - 120, \\ \psi(k) &= \frac{1}{2} \ln 2n - \frac{1}{2} \ln \ln n + \ln \left( \frac{1}{2} \ln 2n - \frac{1}{2} \ln \ln n \right) + 8. \end{aligned} \quad (5)$$

Заметим, что при  $n \geq 1000$

$$\ln \left( \frac{1}{2} \ln 2n - \frac{1}{2} \ln \ln n \right) + 8 < 6,145 \cdot \ln \ln n,$$

тогда

$$\psi(k) < \frac{1}{2} \ln 2n + 5,645 \cdot \ln \ln n. \quad (6)$$

Следовательно, при  $n \geq 1000$  и  $16 \leq k \leq \left\lfloor \sqrt{2n/\ln n} \right\rfloor$  из (4)–(6) получаем

$$\frac{n \ln 2n}{2 \ln n} + \ln 2n \sqrt{\frac{n}{8 \ln n}} - 60 \ln 2n + 5,645 \cdot \ln \ln n \left( \frac{n}{\ln n} + \sqrt{\frac{n}{2 \ln n}} - 120 \right) \leq n - 328.$$

Так как при  $n \geq 1000$  это неравенство выполнено, то условие (3) удовлетворено при  $16 \leq k \leq \left\lfloor \sqrt{2n/\ln n} \right\rfloor$ . Отсюда  $\omega(n) \geq \left\lfloor \sqrt{2n/\ln n} \right\rfloor$  при  $n \geq 1000$  и по теореме 1

$$\mu(n) \geq p_1 p_2 \dots p_k$$

при указанных  $k$ . Оценим произведение простых чисел.

Обозначим константу  $c_{15} = p_1 p_2 \dots p_{15} = 614889782588491410$ .

В соответствии с оценкой Россера  $p_r > r \ln r$ , где  $r > 1$  [2], по теореме 1 при  $n \geq 1000$  и  $k = \left\lfloor \sqrt{2n/\ln n} \right\rfloor$  получаем

$$\mu(n) > c_{15} \prod_{r=16}^k r \ln r = c_{15} \frac{k!}{15!} \prod_{r=16}^k \ln r > 4,7 \cdot 10^5 k! \prod_{r=16}^k \ln r. \quad (7)$$

Функция  $\ln r$  выпуклая вверх, тогда

$$(\ln r)^2 > \ln(r-h) \ln(r+h)$$

при любых  $r > 1$  и  $h < r$ . Следовательно, при  $k \geq 16$

$$\prod_{r=16}^k \ln r > (\ln 16)^{(k-15)/2} (\ln k)^{(k-15)/2}.$$

Заметим, что  $\sqrt{\ln 16} > 1,665$  и  $4,7 \cdot 10^5 (\ln 16)^{-15/2} > 224$ . Отсюда и из (7) следует нужная оценка для  $\mu(n)$ . ■

В таблице приведены оценки и точные значения функции  $\mu(n)$  для  $n \leq 12$ .

| $n$                                        | 4         | 5           | 6           | 7            | 8            | 9            | 10             | 11             | 12             |
|--------------------------------------------|-----------|-------------|-------------|--------------|--------------|--------------|----------------|----------------|----------------|
| Верхняя оценка                             | 6         | 6           | 24          | 24           | 24           | 24           | 120            | 120            | 120            |
| Точное значение, длины циклов $g_n^{\max}$ | 4,<br>4   | 6,<br>2+3   | 6,<br>6     | 12,<br>3+4   | 15,<br>3+5   | 15,<br>1+3+5 | 30,<br>2+3+5   | 30,<br>1+2+3+5 | 60,<br>3+4+5   |
| Нижняя оценка по наборам простых чисел     | 3,<br>{3} | 6,<br>{2,3} | 6,<br>{2,3} | 10,<br>{2,5} | 15,<br>{3,5} | 15,<br>{3,5} | 30,<br>{2,3,5} | 30,<br>{2,3,5} | 42,<br>{2,3,7} |

## ЛИТЕРАТУРА

1. Rosser B. The  $n$ -th prime is greater than  $n \log n$  // Proc. London Math. Soc. 1939. V. 45. P. 21–44.