

# On permutations missing short cycles

Eugenijus MANSTAVIČIUS\* (VU)

*e-mail: eugenijus.manstavicius@maf.vu.lt*

Let  $\mathbb{S}_n$  denote the symmetric group of permutations  $\sigma$  acting on  $n \geq 1$  letters. Each  $\sigma \in \mathbb{S}_n$  has a unique representation (up to the order) by the product of independent cycles  $\kappa$

$$\sigma = \kappa_1 \cdots \kappa_w, \tag{1}$$

where  $w = w(\sigma)$  denotes the number of cycles. Let  $\nu_n$  be the uniform probability measure on  $\mathbb{S}_n$  (Haar measure). Set  $L_m(\bar{k}) = 1k_1 + \cdots + mk_m$  for arbitrary  $0 \leq m \leq n$  and a vector  $\bar{k} = (k_1, \dots, k_n) \in \mathbb{Z}^+$ . If  $k_j(\sigma)$  denotes the number of cycles of length  $j$  in (1), then the vector  $\bar{k}(\sigma) := (k_1(\sigma), \dots, k_n(\sigma))$ , called *structure vector* of the random permutation  $\sigma$ , satisfies the relation  $L_n(\bar{k}(\sigma)) = n$ . It is well known that the distribution of  $\bar{k}(\sigma)$  is

$$\nu_n(\bar{k}(\sigma) = \bar{k}) = \mathbf{1}_{\{L_n(\bar{k}) = n\}} \prod_{j=1}^n \frac{1}{j^{k_j} k_j!} =: \mathbf{1}_{\{L_n(\bar{k}) = n\}} P_n(\bar{k}), \quad \bar{k} \in \mathbb{Z}^+.$$

To avoid a possible misunderstanding, we stress that here and in the sequel  $\bar{k}$  and  $k_j$  denote deterministic quantities while  $\bar{k}(\sigma)$  and  $k_j(\sigma)$  are random.

Dealing with the value distribution problems with respect to  $\nu_n$  of mappings defined on  $\mathbb{S}_n$  via  $\bar{k}(\sigma)$ , we need asymptotic formulas for the probability of permutations without cycles which lengths belong to a given set. For  $J \subset [n] := \{1, \dots, n\}$ , we denote

$$\nu(n, J) = \nu_n(k_j(\sigma) = 0 \forall j \in J) = \sum_{\substack{L_n(\bar{k}) = n \\ k_j = 0, j \in J}} P_n(\bar{k}).$$

So, the problem is to investigate  $\nu(n, J)$ .

We start with two inequalities. Set  $K = \sum_{j \in J} 1/j$ .

**Theorem 1.** *We have*

$$\exp\{-e^{7K}\} \ll \nu(n, J) \ll e^{-K}.$$

with absolute constants in the symbol  $\ll$ , an analog of  $O(\cdot)$ .

---

\*Supported by a Lithuanian State Stipend of the Highest Rank.

The lower bound of  $\nu(n, J)$  has been established in author's paper [5]. With more effort the exponent 7 in the left-hand side can be substituted by 6 but this lower bound cannot be beyond  $\exp\{-(1 + o(1))Ke^K\}$  as  $K \rightarrow \infty$ .

The upper inequality follows from the following mean-value estimate for a completely multiplicative function

$$f(\sigma) = \prod_{j=1}^n f_j^{k_j(\sigma)}, \quad 0^0 := 1,$$

where  $f_j \in \mathbb{R}$  for  $1 \leq j \leq n$ . Set

$$M_n(f) = \frac{1}{n!} \sum_{\sigma \in \mathcal{S}_n} f(\sigma) = \sum_{\substack{L_n(k)=n \\ k_j \geq 1, j \in [n]}} \prod_{j=1}^n \left(\frac{f_j}{j}\right)^{k_j} \frac{1}{k_j!}.$$

**Lemma.** *If  $f_j \in [0, 1]$ , then*

$$M_n(f) \ll \exp \left\{ \sum_{j=1}^n \frac{f_j - 1}{j} \right\} \tag{2}$$

with an absolute constant in the symbol  $\ll$ .

*Proof.* We can use the generating function

$$1 + \sum_{n=1}^{\infty} M_n(f)x^n = \exp \left\{ \sum_{j=1}^{\infty} \frac{f_j x^j}{j} \right\}.$$

Differentiating it and comparing the coefficients, we obtain

$$M_n(f) = \frac{1}{n} \sum_{j=0}^{n-1} f_j M_{n-j}(f), \quad M_0(f) := 1.$$

This recurrence falls within the scope of those investigated by A. Hildebrand and G. Tenenbaum [2]. Theorem 2 of their paper implies (2). The lemma is proved.

General mean-value theorems for multiplicative functions on combinatorial structures have been established in [6]. They yield asymptotic formulae for  $\nu(n, J)$  under certain regularity conditions for  $J$ . If  $J \subset [\varepsilon_n n, n]$  for some  $\varepsilon_n > 0, \varepsilon_n \rightarrow 0$  such that  $\varepsilon_n n \rightarrow \infty$  at a certain speed, instead of the estimates in Theorem 1, using the saddle point method, we can obtain a more exact asymptotic expression. As it has been observed in author's paper [3], such formulas can also be derived from the relevant results on polynomials over a finite field  $\mathbb{F}_q$  missing irreducible factors of large degree. Actually, that is possible if these results hold uniformly in the number  $q$  of elements of the field. The next theorem

has been proved going along this path. Note, that papers [1], [3], [4], and [8] contain a rather comprehensive historical survey on the problem for polynomials over a finite field.

Let  $\rho(x)$  be the Dickman function defined as the continuous solution to the equation  $x\rho'(x) + \rho(x-1) = 0$  for  $x > 1$  and  $\rho(x) = 1$  for  $0 \leq x \leq 1$ .

**Theorem 2.** *Let  $2 \leq m \leq n$ . For arbitrary constant  $C > 0$ , uniformly in  $y := n/m \leq Cm/\log m$ , we have*

$$\nu(n, (m, n]) = \sum_{L_n(\bar{k})=n} \prod_{j=1}^m \frac{1}{j^{k_j} k_j!} = \rho(y) \left( 1 + O\left(\frac{1+y \log y}{m}\right) \right).$$

*Proof.* See Corollaries 1 and 2 in [4].

Investigating  $\nu(n, [m])$ , where  $[m] = \{1, \dots, m\}$ , as in [1], [3], and [4], we could exploit analytic methods. Nevertheless, one of the purposes of this remark is to demonstrate sieve ideas proposed by R. Warlimont [10]. We will establish a result already announced in [7].

The Buchstab's function  $\omega(x)$  is defined as the continuous solution to the equation  $(x\omega(x))' = \omega(x-1)$  if  $x \geq 2$  satisfying  $\omega(x) = 1/x$  for  $1 \leq x \leq 2$ . Let  $\gamma$  be the Euler constant.

**Theorem 3.** *For  $n, m \geq 1$  and  $y = n/m \geq 1$ , we have*

$$\begin{aligned} \nu(n, [m]) &= \sum_{\substack{L_n(\bar{k})=n \\ k_j=0, j \leq m}} P_n(\bar{k}) = \exp \left\{ - \sum_{j \leq m} 1/j \right\} \left( e^\gamma \omega(y) + O\left(\frac{1}{m}\right) \right) \\ &= \frac{e^{-\gamma}}{m} \left( 1 + O(y^{-y/2}) + O\left(\frac{1}{m}\right) \right). \end{aligned}$$

*Proof.* The last equality in the theorem follows from the asymptotic expression for the Buchstab's function (see [9], p. 401).

The permutations having all cycles longer than  $m$  for  $n/2 \leq m < n$  are only the cycles of length  $n$ . Hence  $\nu(n, [m]) = (n-1)!/n! = 1/n$ . Thus, since  $\omega(n/m) = m/n$ , in this case, we obtain the assertion.

Now let  $m < n/2$  and let  $n$  be sufficiently large. We start with the identity

$$\begin{aligned} n\nu(n, [m]) &= \sum_{\substack{L_n(\bar{k})=n \\ k_j=0, j \leq m}} P_n(\bar{k}) \sum_{j=m+1}^n j k_j = \sum_{\substack{jk \leq n \\ j > m}} j k \sum_{\substack{L_n(\bar{k})=n, k_j=k \\ k_i=0, i \leq m}} P_n(\bar{k}) \\ &= \sum_{\substack{jk \leq n \\ j > m}} \frac{jk}{j^k k!} \sum_{\substack{L_n(\bar{k})=n-jk, k_j=0 \\ k_i=0, i \leq m}} P_n(\bar{k}) = \sum_{\substack{jk \leq n \\ j > m}} \frac{j^{1-k}}{(k-1)!} \nu(n-jk, [m] \cup \{j\}). \quad (3) \end{aligned}$$

Here and in the sequel, we suppose that  $\nu(0, A) = 1$  for any set  $A$ . To derive a formula for  $\nu(n, [m])$  from (3), we do some “bootstrapping”. Observe that the summands corresponding to  $k \geq 3$  can be neglected. Indeed, using Theorem 1, we obtain

$$\begin{aligned} \sum_{\substack{jk \leq n \\ j > m, k \geq 3}} \frac{j^{1-k}}{(k-1)!} \nu(n-jk, [m] \cup \{j\}) &\ll \sum_{\substack{j^{(k+1)} \leq n/2 \\ j > m, k \geq 2}} \frac{1}{j^k k!} \exp \left\{ - \sum_{j \leq m} \frac{1}{j} \right\} \\ &+ \sum_{\substack{j^{(k+1)} > n/2 \\ k \geq 2}} \frac{1}{j^k k!} \ll \frac{1}{m} \sum_{j > m} \left( e^{1/j} - 1 - \frac{1}{j} \right) + \frac{1}{n} \ll \frac{1}{m^2} + \frac{1}{n}. \end{aligned}$$

Similarly, for  $m < j \leq n/2$ , we have

$$\begin{aligned} \nu(n-j, [m] \cup \{j\}) &= \nu(n-j, [m]) - \sum_{1 \leq k \leq (n-j)/j} \frac{1}{j^k k!} \nu(n-j(k+1), [m] \cup \{j\}) \\ &= \nu(n-j, [m]) - \frac{1}{j} \nu(n-2j, [m] \cup \{j\}) + O \left( \frac{1}{mj^2} + \frac{1}{n^2} \right). \end{aligned}$$

Inserting the last two estimates into (3), we obtain

$$\begin{aligned} n\nu(n, [m]) &= \sum_{m < j \leq n/2} \nu(n-j, [m] \cup \{j\}) + \sum_{n/2 < j \leq n} \nu(n-j, [m]) \\ &+ \sum_{m < j \leq n/2} \frac{1}{j} \nu(n-2j, [m] \cup \{j\}) + O \left( \frac{1}{m^2} + \frac{1}{n} \right) \\ &= \sum_{m < j \leq n} \nu(n-j, [m]) + O \left( \frac{1}{m^2} + \frac{1}{n} \right) \\ &= 1 + \sum_{m < j < n-m} \nu(n-j, [m]) + O \left( \frac{1}{m^2} + \frac{1}{n} \right). \end{aligned} \tag{4}$$

A similar approximate recurrence equation has been solved by R. Warlimont [10]. For completeness, we just repeat his argument. If  $W(k, m) := m\nu(k, [m]) - \omega(k/m)$ , then (4) becomes

$$W(n, m) = \frac{1}{n} \sum_{m < k < n-m} W(k, m) + \frac{m}{n} - \omega \left( \frac{n}{m} \right) + \frac{1}{n} \sum_{m < k < n-m} \omega \left( \frac{k}{m} \right) + O \left( \frac{1}{n} \right). \tag{5}$$

Applying

$$x\omega(x) - 1 = \int_1^{x-1} \omega(t) dt$$

for  $x \geq 2$ , we first obtain

$$\begin{aligned} \frac{1}{n} \sum_{m < k < n-m} \omega\left(\frac{k}{m}\right) &= \frac{1}{n} \int_m^{n-m} \omega\left(\frac{t}{m}\right) dt + O\left(\frac{1}{n}\right) \\ &= \frac{m}{n} \int_1^{n/m-1} \omega(t) dt + O\left(\frac{1}{n}\right) = \omega\left(\frac{n}{m}\right) - \frac{m}{n} + O\left(\frac{1}{n}\right). \end{aligned}$$

Further, inserting this into (5), we have

$$|W(n, m)| \leq \frac{1}{n} \sum_{m < k < n-m} |W(k, m)| + \frac{C}{n} \quad (6)$$

with some  $C > 0$ . Our purpose now is to show that  $|W(n, m)| \leq C/m$ . For that, we apply induction with respect to  $r \geq 1$  taking  $n/r \leq m < n$ . The case  $1 \leq r < 2$  has been considered at the very beginning of the proof. Assume the induction assertion for  $r \geq 2$  and take  $n/(r+1) \leq m < n$ . Now  $m < k < n-m$  implies  $k/r \leq m < k$ , thus from (5) and (6), it follows that

$$|W(n, m)| \leq \frac{1}{n} \left( (n-2m) \frac{C}{m} + C \right) = \frac{1}{n} \left( \frac{Cn}{m} - C \right) \leq \frac{C}{m}.$$

This is the desired inequality. The theorem is proved.

## References

- [1] T. Garefalakis, D. Panario, *Polynomials over finite fields free from large and small degree irreducible factors*, Manuscript, 25 p. (2002).
- [2] A. Hildebrand, G. Tenenbaum, On some Tauberian theorems related to the prime number theorem, *Compositio Math.*, **90**(3), 315–349 (1994).
- [3] E. Manstavičius, Semigroup elements free of large prime factors, in: *New Trends in Probab. and Statist.*, F. Schweiger and E. Manstavičius (Eds.), VSP/TEV, Utrecht/Vilnius (1992), pp. 135–153.
- [4] E. Manstavičius, Remarks on the semigroup elements free of large prime factors, *Lith. Math. J.*, **32**(4), 400–409 (1992).
- [5] E. Manstavičius, On random permutations without cycles of some lengths, *Period. Math. Hungar.*, **42**(1-2), 37–44 (2001).
- [6] E. Manstavičius, Mappings on decomposable combinatorial structures: analytic approach, *Combinatorics, Probab., Computing*, **11**, 61–78 (2002).
- [7] E. Manstavičius, Value distribution of additive functions on the symmetric group, in: *Abstracts of the 8th Vilnius Conference on Probab. Theory and Math. Statistics*, TEV, Vilnius (2002), pp. 194–195.
- [8] K. Soundararajan, *Smooth polynomials: analogies and asymptotics*, Manuscript, 16 p. (1995).
- [9] G. Tenenbaum, Introduction to analytic and probabilistic number theory, *Cambridge Tracts in Math.*, **46**, Cambridge University Press (1995).
- [10] R. Warlimont, Arithmetical semigroups II: sieving by large and small prime elements. Sets of multiples, *Manuscripta Math.*, **71**, 197–221 (1991).

## Kėliniai be trumpų ciklu

E. Manstavičius

Išvesta simetrinės grupės keitinių be trumpų ciklu skaičiaus asimptotinė formulė. Pagrindinis narys išreikštas per tam tikros diferencialinės lygties su vėluojančiu argumentu sprendinį.