Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in
DISCRETE
MATHEMATICS

www.elsevier.com/locate/endm

Permutations without long or short cycles

Eugenijus Manstavičius [1]

Faculty of Mathematics and Informatics
Vilnius University
Vilnius, Lithuania

Robertas Petuchovas [2]

Faculty of Mathematics and Informatics
Vilnius University
Vilnius, Lithuania

Abstract

We explore probabilities that a permutation sampled from a finite symmetric group uniformly at random has only short or long cycles. Asymptotic formulas, as the order of the group increases, valid in specified regions are obtained using the saddle point method. As an application, we establish a formula with remainder term estimate for the total variation distance between the count process of the multiplicities of cycle lengths in the random permutation and a relevant process defined via independent Poisson random variables.

Keywords: symmetric group, random permutation, local probabilities, cyclic structure, total variation distance

[1] Email: eugenijus.manstavicius@mif.vu.lt

[2] Email: robertas.petuchovas@mif.vu.lt

Introduction

We explore the probabilities $\nu(n,r)$ and $\nu(n,[r])$ that a permutation sampled from the symmetric group $\mathbf{S}_n$ uniformly at random has cycles of lengths, respectively, not exceeding r and greater than r, where $1 \leq r \leq n$ and $n \to \infty$. Asymptotic formulas valid in specified regions for the ratio n/r are obtained using the saddle point method. Demonstrating possible applications we establish an asymptotic formula with the remainder term estimate of the total variation distance between the count process of the multiplicities of cycle lengths in the random permutation and a relevant process defined via independent Poisson random variables.

Our leading idea is to adopt the methodology elaborated in numerous number theoretical papers dealing with integer numbers missing small or large prime factors. This theory is well exposed in the book by G. Tenenbaum [18] and in more recent works. By analogy, a similar theory was carried out for polynomials over a finite field (see, for example, [15], [5]) and generalized to the so-called additive arithmetical semigroups (see [21], [13], [12]). The survey [9] discusses the parallelism between the theories. One should also mention attempts to examine the same problem for general decomposable structures (see [7], [4] to list but a few). So far, the obtained results do not overtake the level of research achieved for natural numbers.

Let us focus on permutations $\sigma \in \mathbf{S}_n$. There exists a vast literature dealing with the case when n/r is small. If $L_n(\sigma)$ denotes the longest cycle length, then the result by V.L. Goncharov [6] from 1944 shows that

$$\nu(n, n/u) = \frac{1}{n!}|\{\sigma \in \mathcal{S}_n : \; L_n(\sigma) \leq n/u\}| = \rho(u) + o(1)$$

uniformly in $u \geq 1$. Here $\rho(u)$ is the Dickman function defined as the continuous solution to the difference-differential equation

$$u\rho'(u) + \rho(u-1) = 0$$

with the initial condition $\rho(u) = 1$ for $0 \leq u \leq 1$. Theorem 4.13 in [2], confined to permutations, yields

$$\nu(n,r) = \rho(u)(1 + o(1))$$

if $n/r \to u \in (0, \infty)$. As a byproduct of enumeration of elements in an additive arithmetical semigroup missing large factors, the last relation (extended to a larger region for n/r) appeared earlier in the first author's paper [12]. The result is also contained in our first theorem.

In what follows, we write $f(x) = Bg(x)$ if $|f(x)| \leq C|g(x)|$ in an indicated region for $x \in \mathbf{R}$ with an absolute constant $C > 0$.

Theorem 0.1 *If* $\sqrt{n\log n}\le r\le n$ *and* $n\ge 2$, *then*

$$\nu(n,r)=\rho\Big(\frac{n}{r}\Big)\Big(1+\frac{Bn\log(n/r+1)}{r^2}\Big).$$

The saddle point approximation was usually applied in the case of small r. In particular, we have from B. Harris and L. Schoenfeld [10] that

$$\nu(n,r)=\frac{q(x)}{\sqrt{2\pi\lambda(x)}}\left(1+O_r\Big(\frac{1}{n}\Big)\right) \tag{1}$$

for an arbitrary fixed r. Here

$$q(x):=\frac{1}{x^n}\exp\left\{\sum_{j=1}^{r}\frac{x^j}{j}\right\},\qquad \lambda(x):=\sum_{j=1}^{r}jx^j,$$

and $x:=x(n,r)$ is unique positive solution to the saddle point equation

$$\sum_{j=1}^{r}x^j=n.$$

Theorem 1 is indispensable seeking extensions of (1).

Theorem 0.2 *If* $1\le r\le n$, *then*

$$\nu(n,r)=\frac{q(x)}{\sqrt{2\pi\lambda(x)}}\left(1+\frac{Br}{n}\right).$$

We infer from the latter a relation which is circulating in an erroneous form (see [1], [16], [20]).

Theorem 0.3 *If* $2\le r\le\log n$, *then*

$$n!\nu(n,r)=\frac{1}{\sqrt{r}}n^{n(1-1/r)}\exp\Big\{\sum_{N=0}^{r}d_{rN}n^{(r-N)/r}\Big\}(1+Bn^{-1/r}).$$

Here $d_{r0}=-1+1/r$,

$$d_{r,r}=-\frac{1}{r}\sum_{j=2}^{r}\frac{1}{j}$$

and

$$d_{rN}=\frac{\Gamma(N+N/r)}{(r-N)\Gamma(N+1)\Gamma(1+N/r)}$$

if $1\le N\le r-1$. *Here* $\Gamma(z)$ *denotes the Euler gamma-function.*

The detailed proofs of Theorems 1, 2 and 3 are exposed in our preprint [14]. Similar results have been obtained on the dual problem, i.e. on the probability

$\nu(n,[r])$. Below, we present one of them. Let $\omega(u)$ denote Buchstab's function [18] defined as a solution to difference-differential equation

$$(v\omega(v))' = w(u-1)$$

for $v > 2$ with the initial condition $\omega(v) = 1/v$ if $1 \leq v \leq 2$. For convenience, we extend the definition by $\omega(v) = 0$ for $v < 1$.

Theorem 0.4 *Let $u := n/r$. There exists an absolute constant $a > 0$ such that*

$$\nu(n,[r]) = \mathrm{e}^{-\sum_{j=1}^{r}\frac{1}{j}}\left(\mathrm{e}^{\gamma}\omega(u) + B\frac{\mathrm{e}^{-au/\log^2(1+u)}}{r}\right). \tag{2}$$

for $\sqrt{n\log n} \leq r < n$.

Estimate (2) sharpens the first result of this type obtained in [11] and that in subsequent papers [4] and [8].

The next result concerns the total variation distance $d_n(r)$ between the distribution of a random vector (r.v.) $\bar{k}_r(\sigma) := (k_1(\sigma),\dots,k_r(\sigma))$ under the uniform measure in $\mathbf{S}_n$, where $k_j(\sigma)$ counts the number of cycles in σ of length j, and the distribution of a r.v. $\bar{Z}_r = (Z_1,\dots,Z_r)$, where $Z_1,\dots,Z_r$ are independent Poisson r. variables defined on some probability space and such that $\mathbf{E}Z_j = 1/j$. Upper estimates of $d_r(n)$, often called Fundamental Lemmas, play an essential role dealing with value distribution of statistics defined on $\bar{k}_r(\sigma)$. We refer to the concise book [2] for more information.

Basing upon some heuristics given in [3], D. Stark [17] established an approximation of $d_n(r)$ involving a function

$$H(u) := \frac{1}{2}\int\limits_0^\infty |\omega(u-v) - \mathrm{e}^{-\gamma}|\rho(v)dv + \frac{\rho(u)}{2}.$$

It was proved in [17] that $d_n(r) \to H(\beta)$ if $n/r \to \beta \in [1,\infty)$ as $n \to \infty$. The well known relation $d_n(r) = o(1)$ if $r = o(n)$ could be also recalled. We extended Stark's result and obtained a remainder term estimate.

Theorem 0.5 *If $\sqrt{n\log n} \leq r \leq n$ and $u = n/r$, then*

$$d_n(r) = H(u)\Big(1 + B\frac{u^{3/2}\log^2(u+1)}{r}\Big). \tag{3}$$

Tenenbaum's argument given in paper [19] was very helpful in proving the last theorem.

Intertwining of number-theoretical and combinatorial ideas in the field and details of proofs will be discussed during the talk.

References

[1] T. Amdeberhan and V.H. Moll, "Involutions and their progenies", http://arxiv.org/abs/1406.2356v1, 2014.

[2] R. Arratia, A.D. Barbour, and S. Tavaré, "Logarithmic Combinatorial Structures: A Probabilistic Approach", EMS Publishing House, Zürich, 2003.

[3] R. Arratia and S. Tavaré, *The cycle structure of random permutations*, Ann. Probab., **20** (1992), 3, 1567-1591.

[4] E.A. Bender, A. Mashatan, D. Panario, and L.B. Richmond, *Asymptotics of combinatorial structures with large smallest component*, J. Comb. Th., Ser. A, **107** (2004), 117–125.

[5] T. Garefalakis and D. Panario, *Polynomials over finite fields free from large and small degree irreducible factors. Analysis of algorithms*, J. Algorithms , **44** (2002), 1, 98–120.

[6] V.L. Goncharov, *On the field of combinatorial analysis*, Izv. Akad. Nauk SSSR, Ser. Mat., **8** (1944), 3–48 (Russian). Translation in Transl. AMS, Ser. 2, **19** (1962), 1–46.

[7] X. Gourdon, *Largest component in random combinatorial structures*, Discrete Math., **180** (1998), 185–209.

[8] A. Granville, *Cycle lengths in a permutation are typically Poisson*, Electronic J. Comb., **13** (2006), #R107.

[9] A. Granville, *Smooth numbers: computational number theory and beyond.* In: Algorithmic Number Theory, MSRI Publications, **44** (2008), p. 267–323.

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

[11] E. Manstavičius, *On permutations missing short cycles*, Lietuvos matem. rink., spec. issue, **42** (2002), 1–6.

[12] E. Manstavičius, *Remarks on the semigroup elements free of large prime factors*, Lith. Math. J., **32** (1992), 4, 400–410.

[13] E. Manstavičius, *Semigroup elements free of large prime factors.* In: *Analytic and Probabilistic Methods in Number Theory*, New Trends in Probability and Statistics, vol. 2, F. Schweiger and E. Manstavičius (Eds), TEV/Vilnius and VSP/Utrecht, 1992, p. 135–153.

[14] E. Manstavičius and R. Petuchovas, “Local probabilities for random permutations without long cycles”, http://arxiv.org/abs/1501.00136v1, 2014.

[15] A.M. Odlyzko, *Discrete logarithms and smooth polynomials.* In: Finite Fields: Theory, Applications and Algorithms, Contemporary Math., **168** (1993), p. 269–278.

[16] V.N. Sachkov, *Asymptotic formulas and limit distributions for combinatorial configurations generated by polynomials*, Discrete Math., **19** (2007), 3, 3–14 (Russian). Translation in Discrete Math. Appl., **17** (2007), 4, 319–330.

[17] D. Stark, *Explicit limits of total variation distance in approximations of random logarithmic assemblies by related Poisson processes*, Combinatorics, Probab. Comput., **6** (1997), 87–105.

[18] G. Tenenbaum, “Introduction to Analytic and Probabilistic Number Theory”, Cambridge Univ. Press, 1995.

[19] G. Tenenbaum, *Crible d’Ératosthène et modèle de Kubilius.* In: Number Theory in Progress, Proc. Conf. in Honor of Andrzej Schinzel, Zakopane, Poland, 1997. K. Gyory, H. Iwaniec, J. Urbanowicz (Eds.), Walter de Gruyter, Berlin, New York, 1999, p. 1099–1129.

[20] A.N. Timashov, *Random permutations with cycle lengths in a given finite set*, Discrete Math., **20** (2008), 1, 25–37 (Russian). Translation in Discrete Math. Appl., **18** (2008), 1, 25–39.

[21] R. Warlimont, *Arithmetical semigroups, II: sieving by large and small prime elements, sets of multiples*, Manuscripta Math., **71** (1991), 197–221.