The number of cycles in a random permutation

23 November, 2011 in expository, math.CO, math.PR | Tags: bijective proof, cycles, permutations, Stirling numbers of the first kind

Let n be a natural number, and let $\sigma : \{1,\dots,n\} \to \{1,\dots,n\}$ be a permutation of $\{1,\dots,n\}$, drawn uniformly at random. Using the cycle decomposition, one can view σ as the disjoint union of cycles of varying lengths (from 1 to n). For each $1 \leq k \leq n$, let C_k denote the number of cycles of σ of length k; thus the C_k are natural number-valued random variables with the constraint

$$\sum_{k=1}^n kC_k = n. \qquad (1)$$

We let $C := \sum_{k=1}^n C_k$ be the number of cycles (of arbitrary length); this is another natural number-valued random variable, of size at most n.

I recently had need to understand the distribution of the random variables C_k and C. As it turns out this is an extremely classical subject, but as an exercise I worked out what I needed using a quite tedious computation involving generating functions that I will not reproduce here. But the resulting identities I got were so nice, that they strongly suggested the existence of elementary bijective (or "double counting") proofs, in which the identities are proven with a minimum of computation, by interpreting each side of the identity as the cardinality (or probability) of the same quantity (or event), viewed in two different ways. I then found these bijective proofs, which I found to be rather cute; again, these are all extremely classical (closely related, for instance, to Stirling numbers of the first kind), but I thought some readers might be interested in trying to find these proofs themselves as an exercise (and I also wanted a place to write the identities down so I could retrieve them later), so I have listed the identities I found below.

1. For any $1 \leq k \leq n$, one has $\mathbf{E} C_k = \frac{1}{k}$. In particular, $\mathbf{E} C = 1 + \frac{1}{2} + \ldots + \frac{1}{n} = \log n + O(1)$.
2. More generally, for any $1 \leq k \leq n$ and $j \geq 1$ with $jk \leq n$, one has $\mathbf{E}\binom{C_k}{j} = \frac{1}{k^j j!}$.
3. More generally still, for any $1 \leq k_1 < \ldots < k_r \leq n$ and $j_1,\dots,j_r \geq 1$ with $\sum_{i=1}^r j_i k_i \leq n$, one has
$$\mathbf{E} \prod_{i=1}^r \binom{C_{k_i}}{j_i} = \prod_{i=1}^r \frac{1}{k_i^{j_i} j_i!}.$$
4. In particular, we have *Cauchy's formula*: if $\sum_{k=1}^n j_k k = n$, then the probability that $C_k = j_k$ for all $k = 1,\dots,n$ is precisely $\prod_{k=1}^n \frac{1}{k^{j_k} j_k!}$. (This in particular leads to a reasonably tractable formula for the joint generating function of the C_k, which is what I initially used to compute everything that I needed, before finding the slicker bijective proofs.)
5. For fixed k, C_k converges in distribution as $n \to \infty$ to the Poisson distribution of intensity $\frac{1}{k}$.
6. More generally, for fixed $1 \leq k_1 < \ldots < k_r$, $C_{k_1},\dots,C_{k_r}$ converge in joint distribution to r independent Poisson distributions of intensity $\frac{1}{k_1},\dots,\frac{1}{k_r}$ respectively. (A more precise version of this claim can be found in this paper of Arratia and Tavaré.)
7. One has $\mathbf{E} 2^C = n+1$.
8. More generally, one has $\mathbf{E} m^C = \binom{n+m-1}{n}$ for all natural numbers m.

20 comments

Comments feed for this article

23 November, 2011 at 9:02 am
Greg Martin

Terry – are the distributions of the lengths of the longest cycle and shortest cycle also known?

2 0 Rate This
Reply

23 November, 2011 at 9:24 am
Terence Tao

This paper of Lloyd and Shepp seems to answer such questions fairly definitively, though the answers are somewhat messy.

3 0 Rate This
Reply

23 November, 2011 at 9:15 am
Qiaochu Yuan

For what it's worth, the joint generating function of the C_k can be computed using Polya's enumeration theorem, and it also has an elegant explanation in terms of combinatorial species (see my blog posts here and here for details).

5 0 Rate This
Reply

23 November, 2011 at 9:39 am
Anonymous

Typo in the first paragraph. 'brandom' should be 'random'. *[Corrected, thanks – T.]*

0 0 Rate This
Reply

24 November, 2011 at 5:24 am
Ben Green

There is a play (!) on this kind of thing by our friend Andrew Granville and his sister.

http://www.maa.org/mathtourist/mathtourist_01_06_10.html

I recall the accompanying music, which was in 29 time, making me feel rather queasy.

1 0 Rate This
Reply

25 November, 2011 at 2:27 pm
Greg Martin

29 time?

0 0 Rate This
Reply

26 November, 2011 at 10:04 am
Emmanuel Kowalski

The play was supposed to come out as a comics, but I don't know what happened to that project…

More mathematically, the book of Arratia, Barbour and Tavaré, "Logarithmic combinatorial structures" (see http://www.ems-ph.org/books/book.php?proj_nr=15) contains many generalizations, treated in a uniform manner.

0 0 Rate This

Reply

---

28 November, 2011 at 4:19 am
Lam. S.

Flajolet and Knuth studied a similar problem in the graph theory context:

http://hal.inria.fr/docs/00/07/56/66/PDF/RR-0888.pdf

1 0 Rate This
Reply

---

28 November, 2011 at 9:00 pm
A central limit theorem for the determinant of a Wigner matrix « What's new

[…] complicated (and uses facts about the distribution of cycles in random permutations, mentioned in this previous post), but one can compute that is comparable to for GUE and for GOE. (The discrepancy here comes […]

0 0 Rate This
Reply

---

30 November, 2011 at 3:50 am
kate

Love your blog. Hardcore math I see.

0 0 Rate This
Reply

---

3 December, 2011 at 11:03 am
Slipper.Mystery

One word puzzle that employs a property of random permutations, specifically the (relatively low) probability of large cycles, is the 100 prisoners. This wikipedia entry (not among those you've linked) contains other useful identities.

See also
condemned prisoners from someone who liked your reprise of the blue-eyed islanders.

The problem also shows up in this
tribute to Martin Gardner.

1 0 Rate This
Reply

---

6 December, 2011 at 8:15 am
john mangual

I wonder what application you have in mind. There are lots of permutation group actions whose orbit structure we might be interested in.

0 0 Rate This
Reply

---

7 January, 2012 at 11:51 pm
Manjunath Krishnapur

The chinese restaurant construction of a uniform random permutation probably yields all these in the cleanest way – for example, the number of cycles has the same distribution as a sum of independent Bernoullis with parameters 1, 1/2, 1/ 3, …,1/n.

1 0 Rate This
Reply

---

26 December, 2012 at 7:28 am
Vineet George

I have done extensive research on combination and permutation and found consistent and uniform result. This result which I have found is written on a book known as Junction (an art of counting combination and permutation). To view one of the result of my research work then log on to the site https://sites.google.com/site/junctionslpresentation/home

also see: https://sites.google.com/site/junctionslpresentation/proof-for-advance-permutation

0 2 Rate This
Reply

21 September, 2013 at 5:07 pm
The Poisson-Dirichlet process, and large prime factors of a random number | What's new

[…] Again, we prove this proposition below the fold. Now we turn to the second way (a topic, incidentally, that was briefly touched upon in this previous blog post): […]

0 0 Rate This

Reply

9 August, 2014 at 10:59 pm
Sungjin Kim

While I prepare for TA session for probability class, I found that the first one $\mathbf{E}C_k = 1/k$ has a probabilistic proof:
Let A_i be the event that i is contained in a k-cycle. $1 \leq i \leq n$.
Then $kC_k = \sum 1_{A_i}$ where 1_A is the indicator function.
$\mathbf{E}kC_k = k\mathbf{E}C_k = \sum P(A_i) = \sum 1/n = 1$ follows from combinatorial counting argument.

2 3 Rate This

Reply

15 July, 2015 at 2:44 pm
Cycles of a random permutation, and irreducible factors of a random polynomial | What's new

[…] (Prime number theorem for permutations) A randomly selected permutation of will be a cycle with probability exactly . (This was noted in this previous blog post.) […]

0 0 Rate This

Reply

28 June, 2016 at 7:01 pm
Sungjin Kim

I think #8 holds in general for complex z as an application of Stirling number of first kind.

0 0 Rate This

Reply

13 April, 2017 at 5:36 pm
Counting objects up to isomorphism: groupoid cardinality | What's new

[…] a cardinality that converges in distribution to the Poisson distribution of rate (as discussed in this previous post), thus we see that the fixed points of a large random permutation asymptotically are distributed […]

0 0 Rate This

Reply