WIKIPEDIA

Random permutation statistics

The **statistics of random permutations**, such as the cycle structure of a random permutation are of fundamental importance in the analysis of algorithms, especially of sorting algorithms, which operate on random permutations. Suppose, for example, that we are using quickselect (a cousin of quicksort) to select a random element of a random permutation. Quickselect will perform a partial sort on the array, as it partitions the array according to the pivot. Hence a permutation will be less disordered after quickselect has been performed. The amount of disorder that remains may be analysed with generating functions. These generating functions depend in a fundamental way on the generating functions of random permutation statistics. Hence it is of vital importance to compute these generating functions.

The article on random permutations contains an introduction to random permutations.

Contents

100 prisoners

The fundamental relation

Permutations are sets of labelled cycles. Using the labelled case of the Flajolet–Sedgewick fundamental theorem and writing $\mathcal{P}$ for the set of permutations and $\mathcal{Z}$ for the singleton set, we have

$$\operatorname{SET}(\operatorname{CYC}(\mathcal{Z})) = \mathcal{P}.$$

Translating into exponential generating functions (EGFs), we have

$$\exp\left(\log \frac{1}{1-z}\right) = \frac{1}{1-z}$$

where we have used the fact that the EGF of the combinatorial species of permutations (there are *n*! permutations of *n* elements) is

$$\sum_{n\geq 0} \frac{n!}{n!} z^n = \frac{1}{1-z}.$$

This one equation allows one to derive a large number of permutation statistics. Firstly, by dropping terms from SET, i.e. exp, we may constrain the *number of cycles* that a permutation contains, e.g. by restricting the EGF to SET_2 we obtain permutations containing two cycles. Secondly, note that the EGF of labelled cycles, i.e. of $\operatorname{CYC}(\mathcal{Z})$, is

$$\sum_{k\geq 1} \frac{(k-1)! z^k}{k!} = \sum_{k\geq 1} \frac{z^k}{k} = \log \frac{1}{1-z}$$

because there are *k*! / *k* labelled cycles. This means that by dropping terms from this generating function, we may constrain the *size of the cycles* that occur in a permutation and obtain an EGF of the permutations containing only cycles of a given size.

Instead of removing and selecting cycles, one can also put different weights on different size cycles. If $b : \mathbb{N} \to \mathbb{R}$ is a weight function that depends only on the size *k* of the cycle and for brevity we write

$$b(\sigma) = \sum_{c\in\sigma} b(c),$$

defining the value of *b* for a permutation σ to be the sum of its values on the cycles, then we may mark cycles of length *k* with $u^{b(k)}$ and obtain a two-variable generating function

$$g(z,u) = 1 + \sum_{n\geq 1} \left(\sum_{\sigma\in S_n} u^{b(\sigma)}\right) \frac{z^n}{n!} = \exp \sum_{k\geq 1} u^{b(k)} \frac{z^k}{k}$$

This is a "mixed" generating function: it is an exponential generating function in *z* and an ordinary generating function in the secondary parameter *u*. Differentiating and evaluating at *u* = 1, we have

$$\left.\frac{\partial}{\partial u} g(z,u)\right|_{u=1} = \frac{1}{1-z} \sum_{k\geq 1} b(k) \frac{z^k}{k} = \sum_{n\geq 1} \left(\sum_{\sigma\in S_n} b(\sigma)\right) \frac{z^n}{n!}$$

This is the probability generating function of the expectation of *b*. In other words, the coefficient of z^n in this power series is the expected value of *b* on permutations in S_n, given that each permutation is chosen with the same probability $1/n!$.

This article uses the coefficient extraction operator $[z^n]$, documented on the page for formal power series.

Number of permutations that are involutions

An involution is a permutation σ so that $\sigma^2 = 1$ under permutation composition. It follows that σ may only contain cycles of length one or two, i.e. the exponential generating function $g(z)$ of these permutations is[1]

$$g(z) = \exp\left(z + \frac{1}{2}z^2\right).$$

This gives the explicit formula for the total number $I(n)$ of involutions among the permutations $\sigma \in S_n$:[1]

$$I(n) = n![z^n]g(z) = n! \sum_{a+2b=n} \frac{1}{a!\, 2^b\, b!} = n! \sum_{b=0}^{\lfloor n/2 \rfloor} \frac{1}{(n-2b)!\, 2^b\, b!}.$$

Dividing by $n!$ yields the probability that a random permutation is an involution. These numbers are known as telephone numbers.

Number of permutations that are *m*th roots of unity

This generalizes the concept of an involution. An *m*th root of unity is a permutation σ so that $\sigma^m = 1$ under permutation composition. Now every time we apply σ we move one step in parallel along all of its cycles. A cycle of length *d* applied *d* times produces the identity permutation on *d* elements (*d* fixed points) and *d* is the smallest value to do so. Hence *m* must be a multiple of all cycle sizes *d*, i.e. the only possible cycles are those whose length *d* is a divisor of *m*. It follows that the EGF $g(x)$ of these permutations is

$$g(z) = \exp\left(\sum_{d|m} \frac{z^d}{d}\right).$$

When $m = p$, where *p* is prime, this simplifies to

$$n![z^n]g(z) = n! \sum_{a+pb=n} \frac{1}{a!\, p^b\, b!} = n! \sum_{b=0}^{\lfloor n/p \rfloor} \frac{1}{(n-pb)!\, p^b\, b!}.$$

Number of permutations of order exactly *k*

This one can be done by Möbius inversion. Working with the same concept as in the previous entry we note that the combinatorial species $\mathcal{Q}$ of permutations whose order divides *k* is given by

$$\mathcal{Q} = \operatorname{SET}\left(\sum_{d|k} \operatorname{CYC}_{=d}(\mathcal{Z})\right).$$

Translation to exponential generating functions we obtain the EGF of permutations whose order divides *k*, which is

$$Q_k(z) = \exp\left(\sum_{d|k} \frac{z^d}{d}\right).$$

Now we can use this generating function to count permutations of order exactly *k*. Let $p_{n,d}$ be the number of permutations on *n* whose order is exactly *d* and $q_{n,k}$ the number of permutations on *n* the permutation count whose order divides *k*. Then we have

$$\sum_{d|k} p_{n,d} = q_{n,k}.$$

It follows by Möbius inversion that

$$\sum_{d|k} q_{n,d} \times \mu(k/d) = p_{n,k}.$$

Therefore, we have the EGF

$$Q(z) = \sum_{d|k} \mu(k/d) \times Q_d(z) = \sum_{d|k} \mu(k/d) \exp\left(\sum_{m|d} \frac{z^m}{m} \right).$$

The desired count is then given by

$$n![z^n]Q(z).$$

This formula produces e.g. for *k* = 6 the EGF

$$Q(z) = \mathrm{e}^z - \mathrm{e}^{z+1/2\,z^2} - \mathrm{e}^{z+1/3\,z^3} + \mathrm{e}^{z+1/2\,z^2+1/3\,z^3+1/6\,z^6}$$

with the sequence of values starting at *n* = 5

$20, 240, 1470, 10640, 83160, 584640, 4496030, 42658440, 371762820, 3594871280, \ldots$ (sequence A061121 in the OEIS)

For *k* = 8 we get the EGF

$$Q(z) = -\mathrm{e}^{z+1/2\,z^2+1/4\,z^4} + \mathrm{e}^{z+1/2\,z^2+1/4\,z^4+1/8\,z^8}$$

with the sequence of values starting at *n* = 8

$5040, 45360, 453600, 3326400, 39916800, 363242880, 3874590720, 34767532800, \ldots$ (sequence A061122 in the OEIS)

Finally for *k* = 12 we get the EGF

$$Q(z) = \mathrm{e}^{z+1/2\,z^2} - \mathrm{e}^{z+1/2\,z^2+1/4\,z^4} - \mathrm{e}^{z+1/2\,z^2+1/3\,z^3+1/6\,z^6} + \mathrm{e}^{z+1/2\,z^2+1/3\,z^3+1/4\,z^4+1/6\,z^6+1/12\,z^{12}}$$

with the sequence of values starting at *n* = 7

$420, 3360, 30240, 403200, 4019400, 80166240, 965284320, 12173441280, 162850287600, \ldots$ (sequence A061125 in the OEIS)

Number of permutations that are derangements

Suppose there are *n* people at a party, each of whom brought an umbrella. At the end of the party everyone picks an umbrella out of the stack of umbrellas and leaves. What is the probability that no one left with his/her own umbrella? This problem is equivalent to counting permutations with no fixed points (called derangements), and hence the EGF, where we subtract out fixed points (cycles of length 1) by removing the term *z* from the fundamental relation is

$$\exp\left(-z + \sum_{k\geq 1} \frac{z^k}{k} \right) = \frac{e^{-z}}{1-z}.$$

Multiplication by $1/(1-z)$ sums the coefficients of e^{-z}, so $D(n)$, the total number of derangements, is given by:

$$D(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \approx \frac{n!}{e}.$$

Hence there are about $n!/e$ derangements and the probability that a random permutation is a derangement is $1/e$.

This result may also be proved by inclusion–exclusion. Using the sets A_p where $1 \leq p \leq n$ to denote the set of permutations that fix *p*, we have

$$\left|\bigcup_p A_p\right| = \sum_p |A_p| \; - \; \sum_{p<q} |A_p \cap A_q| \; + \; \sum_{p<q<r} |A_p \cap A_q \cap A_r| \; - \; \cdots \; \pm \; |A_p \cap \; \cdots \; \cap A_s| \, .$$

This formula counts the number of permutations that have at least one fixed point. The cardinalities are as follows:

$$|A_p| = (n-1)! \; , \;\; |A_p \cap A_q| = (n-2)! \; , \;\; |A_p \cap A_q \cap A_r| = (n-3)! \; , \; \ldots$$

Hence the number of permutations with no fixed point is

$$n! \; - \; \binom{n}{1}(n-1)! \; + \; \binom{n}{2}(n-2)! \; - \; \binom{n}{3}(n-3)! \; + \; \cdots \; \pm \; \binom{n}{n}(n-n)!$$

or

$$n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots \pm \frac{1}{n!}\right) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

and we have the claim.

There is a generalization of these numbers, which is known as rencontres numbers, i.e. the number $D(n,m)$ of permutations of $[n]$ containing *m* fixed points. The corresponding EGF is obtained by marking cycles of size one with the variable *u*, i.e. choosing *b*(*k*) equal to one for $k = 1$ and zero otherwise, which yields the generating function $g(z,u)$ of the set of permutations by the number of fixed points:

$$g(z,u) = \exp\left(-z + uz + \sum_{k\geq 1} \frac{z^k}{k}\right) = \frac{e^{-z}}{1-z} e^{uz}.$$

It follows that

$$[u^m]g(z,u) = \frac{e^{-z}}{1-z} \frac{z^m}{m!}$$

and hence

$$D(n,m) = n![z^n][u^m]g(z,u) = \frac{n!}{m!}[z^{n-m}]\frac{e^{-z}}{1-z} = \frac{n!}{m!} \sum_{k=0}^{n-m} \frac{(-1)^k}{k!}.$$

This immediately implies that

$$D(n,m) = \binom{n}{m} D(n-m, 0) \quad \text{and} \quad \frac{D(n,m)}{n!} \approx \frac{e^{-1}}{m!}$$

for *n* large, *m* fixed.

Order of a random permutation

If *P* is a permutation, the *order* of *P* is the smallest positive integer *n* for which P^n is the identity permutation. This is the least common multiple of the lengths of the cycles of *P*.

A theorem of Goh and Schmutz[2] states that if μ_n is the expected order of a random permutation of size *n*, then

$$\log \mu_n \sim c\sqrt{\frac{n}{\log n}}$$

where the constant c is

$$2\sqrt{2\int_0^\infty \log\log\left(\frac{e}{1-e^{-t}}\right)dt} \approx 1.1178641511899$$

Derangements containing an even and an odd number of cycles

We can use the same construction as in the previous section to compute the number of derangements $D_0(n)$ containing an even number of cycles and the number $D_1(n)$ containing an odd number of cycles. To do this we need to mark all cycles and subtract fixed points, giving

$$g(z,u) = \exp\left(-uz + u\log\frac{1}{1-z}\right) = \exp(-uz)\left(\frac{1}{1-z}\right)^u.$$

Now some very basic reasoning shows that the EGF $q(z)$ of $D_0(n)$ is given by

$$q(z) = \frac{1}{2}\times g(z,-1) + \frac{1}{2}\times g(z,1) = \frac{1}{2}\exp(-z)\frac{1}{1-z} + \frac{1}{2}\exp(z)(1-z).$$

We thus have

$$D_0(n) = n![z^n]q(z) = \frac{1}{2}n!\sum_{k=0}^n \frac{(-1)^k}{k!} + \frac{1}{2}n!\frac{1}{n!} - \frac{1}{2}n!\frac{1}{(n-1)!}$$

which is

$$\frac{1}{2}n!\sum_{k=0}^n \frac{(-1)^k}{k!} + \frac{1}{2}(1-n) \sim \frac{1}{2e}n! + \frac{1}{2}(1-n).$$

Subtracting $D_0(n)$ from $D(n)$, we find

$$D_1(n) = \frac{1}{2}n!\sum_{k=0}^n \frac{(-1)^k}{k!} - \frac{1}{2}(1-n).$$

The difference of these two ($D_0(n)$ and $D_1(n)$) is $n-1$.

One hundred prisoners

A prison warden wants to make room in his prison and is considering liberating one hundred prisoners, thereby freeing one hundred cells. He therefore assembles one hundred prisoners and asks them to play the following game: he lines up one hundred urns in a row, each containing the name of one prisoner, where every prisoner's name occurs exactly once. The game is played as follows: every prisoner is allowed to look inside fifty urns. If he or she does not find his or her name in one of the fifty urns, all prisoners will immediately be executed, otherwise the game continues. The prisoners have a few moments to decide on a strategy, knowing that once the game has begun, they will not be able to communicate with each other, mark the urns in any way or move the urns or the names inside them. Choosing urns at random, their chances of survival are almost zero, but there is a strategy giving them a 30% chance of survival, assuming that the names are assigned to urns randomly – what is it?

First of all, the survival probability using random choices is

$$\left(\frac{\binom{99}{49}}{\binom{100}{50}}\right)^{100} = \frac{1}{2^{100}},$$

so this is definitely not a practical strategy.

The 30% survival strategy is to consider the contents of the urns to be a permutation of the prisoners, and traverse cycles. To keep the notation simple, assign a number to each prisoner, for example by sorting their names alphabetically. The urns may thereafter be considered to contain numbers rather than names. Now clearly the contents of the urns define a permutation. The first prisoner opens the first urn. If he finds his name, he has finished and survives. Otherwise he opens the urn with the number he found in the first urn. The process repeats: the prisoner opens an urn and survives if he finds his name, otherwise he opens the urn with the number just retrieved, up to a limit of fifty urns. The second prisoner starts with urn number two, the third with urn number three, and so on. This strategy is precisely equivalent to a traversal of the cycles of the permutation represented by the urns. Every prisoner starts with the urn bearing his number and keeps on traversing his cycle up to a limit of fifty urns. The number of the urn that contains his number is the pre-image of that number under the permutation. Hence the prisoners survive if all cycles of the permutation contain at most fifty elements. We have to show that this probability is at least 30%.

Note that this assumes that the warden chooses the permutation randomly; if the warden anticipates this strategy, he can simply choose a permutation with a cycle of length 51. To overcome this, the prisoners may agree in advance on a random permutation of their names.

We consider the general case of $2n$ prisoners and n urns being opened. We first calculate the complementary probability, i.e. that there is a cycle of more than n elements. With this in mind, we introduce

$$g(z,u) = \exp\left(z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots + u\frac{z^{n+1}}{n+1} + u\frac{z^{n+2}}{n+2} + \cdots\right)$$

or

$$\frac{1}{1-z}\exp\left((u-1)\left(\frac{z^{n+1}}{n+1} + \frac{z^{n+2}}{n+2} + \cdots\right)\right),$$

so that the desired probability is

$$[z^{2n}][u]g(z,u),$$

because the cycle of more than n elements will necessarily be unique. Using the fact that $2(n+1) > 2n$, we find that

$$[z^{2n}][u]g(z,u) = [z^{2n}][u]\frac{1}{1-z}\left(1 + (u-1)\left(\frac{z^{n+1}}{n+1} + \frac{z^{n+2}}{n+2} + \cdots\right)\right),$$

which yields

$$[z^{2n}][u]g(z,u) = [z^{2n}]\frac{1}{1-z}\left(\frac{z^{n+1}}{n+1} + \frac{z^{n+2}}{n+2} + \cdots\right) = \sum_{k=n+1}^{2n}\frac{1}{k} = H_{2n} - H_n.$$

Finally, using an integral estimate such as Euler–Maclaurin summation, or the asymptotic expansion of the *n*th harmonic number, we obtain

$$H_{2n} - H_n \sim \log 2 - \frac{1}{4n} + \frac{1}{16n^2} - \frac{1}{128n^4} + \frac{1}{256n^6} - \frac{17}{4096n^8} + \cdots,$$

so that

$$[z^{2n}][u]g(z,u) < \log 2 \quad \text{and} \quad 1 - [z^{2n}][u]g(z,u) > 1 - \log 2 = 0.30685281,$$

or at least 30%, as claimed.

A related result is that asymptotically, the expected length of the longest cycle is *λn,* where λ is the Golomb–Dickman constant, approximately 0.62.

This example is due to Anna Gál and Peter Bro Miltersen; consult the paper by Peter Winkler for more information, and see the discussion on *Les-Mathematiques.net.* Consult the references on 100 prisoners for links to these references.

The above computation may be performed in a more simple and direct way, as follows: first note that a permutation of $2n$ elements contains at most one cycle of length strictly greater than n . Thus, if we denote

$$p_k = \Pr[\text{there is a cycle of length } k],$$

then

$$\Pr[\text{there is a cycle of length} > n] = \sum_{k=n+1}^{2n} p_k.$$

For $k > n$, the number of permutations that contain a cycle of length exactly k is

$$\binom{2n}{k} \cdot \frac{k!}{k} \cdot (2n-k)!.$$

Explanation: $\binom{2n}{k}$ is the number of ways of choosing the k elements that comprise the cycle; $\frac{k!}{k}$ is the number of ways of arranging k items in a cycle; and $(2n-k)!$ is the number of ways to permute the remaining elements. There is no double counting here because there is at most one cycle of length k when $k > n$. Thus,

$$p_k = \frac{\binom{2n}{k} \cdot \frac{k!}{k} \cdot (2n-k)!}{(2n)!} = \frac{1}{k}.$$

We conclude that

$$\Pr[\text{there is a cycle of length} > n] = \sum_{k=n+1}^{2n} \frac{1}{k} = H_{2n} - H_n.$$

A variation on the 100 prisoners problem (keys and boxes)

There is a closely related problem that fits the method presented here quite nicely. Say you have *n* ordered boxes. Every box contains a key to some other box or possibly itself giving a permutation of the keys. You are allowed to select *k* of these *n* boxes all at once and break them open simultaneously, gaining access to *k* keys. What is the probability that using these keys you can open all *n* boxes, where you use a found key to open the box it belongs to and repeat.

The mathematical statement of this problem is as follows: pick a random permutation on *n* elements and *k* values from the range *1* to *n*, also at random, call these marks. What is the probability that there is at least one mark on every cycle of the permutation? The claim is this probability is *k/n*.

The species $\mathcal{Q}$ of permutations by cycles with some non-empty subset of every cycle being marked has the specification

$$\mathcal{Q} = \text{SET}\left(\sum_{q\ge 1} \text{CYC}_{=q}(\mathcal{Z}) \times \sum_{p=1}^{q} \binom{q}{p} \mathcal{U}^p\right).$$

The index in the inner sum starts at one because we must have at least one mark on every cycle.

Translating the specification to generating functions we obtain the bivariate generating function

$$G(z,u) = \exp\left(\sum_{q\ge 1} \frac{z^q}{q} \sum_{p=1}^{q} \binom{q}{p} u^p\right).$$

This simplifies to

$$\exp\left(\sum_{q\ge 1} \frac{z^q}{q}(u+1)^q - \sum_{q\ge 1} \frac{z^q}{q}\right)$$

or

$$\exp\left(\log\frac{1}{1-(u+1)z} - \log\frac{1}{1-z}\right) = \frac{1-z}{1-(u+1)z}.$$

In order to extract coefficients from this re-write like so

$$(1-z)\sum_{q\geq 0}(u+1)^q z^q.$$

It now follows that

$$[z^n]G(z,u) = (u+1)^n - (u+1)^{n-1}$$

and hence

$$[u^k][z^n]G(z,u) = \binom{n}{k} - \binom{n-1}{k}.$$

Divide by $\binom{n}{k}$ to obtain

$$1 - \frac{(n-1)!}{k!(n-1-k)!}\frac{k!(n-k)!}{n!} = 1 - \frac{n-k}{n} = \frac{k}{n}.$$

We do not need to divide by *n!* because $G(z,u)$ is exponential in *z*.

Number of permutations containing *m* cycles

Applying the Flajolet–Sedgewick fundamental theorem, i.e. the labelled enumeration theorem with $G = S_m$, to the set

$$\operatorname{SET}_{=m}(\operatorname{CYC}(\mathcal{Z}))$$

we obtain the generating function

$$g_m(z) = \frac{1}{|S_m|}\left(\log\frac{1}{1-z}\right)^m = \frac{1}{m!}\left(\log\frac{1}{1-z}\right)^m.$$

The term

$$(-1)^{n+m} n!\; [z^n] g_m(z) = s(n,m)$$

yields the signed Stirling numbers of the first kind, and $g_m(z)$ is the EGF of the unsigned Stirling numbers of the first kind, i.e.

$$n![z^n]g_m(z) = \left[{n \atop m}\right].$$

We can compute the OGF of the signed Stirling numbers for *n* fixed, i.e.

$$s_n(w) = \sum_{m=0}^{n} s(n,m) w^m.$$

Start with

$$g_m(z) = \sum_{n\geq m}\frac{(-1)^{n+m}}{n!}s(n,m)z^n$$

which yields

$$(-1)^m g_m(z) w^m = \sum_{n\ge m} \frac{(-1)^n}{n!} s(n,m) w^m z^n.$$

Summing this, we obtain

$$\sum_{m\ge 0} (-1)^m g_m(z) w^m = \sum_{m\ge 0} \sum_{n\ge m} \frac{(-1)^n}{n!} s(n,m) w^m z^n = \sum_{n\ge 0} \frac{(-1)^n}{n!} z^n \sum_{m=0}^{n} s(n,m) w^m.$$

Using the formula involving the logarithm for $g_m(z)$ on the left, the definition of $s_n(w)$ on the right, and the binomial theorem, we obtain

$$(1-z)^w = \sum_{n\ge 0} \binom{w}{n} (-1)^n z^n = \sum_{n\ge 0} \frac{(-1)^n}{n!} s_n(w) z^n.$$

Comparing the coefficients of z^n, and using the definition of the binomial coefficient, we finally have

$$s_n(w) = w\,(w-1)\,(w-2)\,\cdots\,(w-(n-1)) = (w)_n,$$

a falling factorial. The computation of the OGF of the unsigned Stirling numbers of the first kind works in a similar way.

Expected number of cycles of a given size *m*

In this problem we use a bivariate generating function *g*(*z*, *u*) as described in the introduction. The value of *b* for a cycle not of size *m* is zero, and one for a cycle of size *m*. We have

$$\left.\frac{\partial}{\partial u} g(z,u)\right|_{u=1} = \frac{1}{1-z} \sum_{k\ge 1} b(k) \frac{z^k}{k} = \frac{1}{1-z} \frac{z^m}{m}$$

or

$$\frac{1}{m} z^m \;+\; \frac{1}{m} z^{m+1} \;+\; \frac{1}{m} z^{m+2} \;+\; \cdots$$

This means that the expected number of cycles of size *m* in a permutation of length *n* less than *m* is zero (obviously). A random permutation of length at least *m* contains on average 1/*m* cycles of length *m*. In particular, a random permutation contains about one fixed point.

The OGF of the expected number of cycles of length less than or equal to *m* is therefore

$$\frac{1}{1-z} \sum_{k=1}^{m} \frac{z^k}{k} \text{ and } [z^n] \frac{1}{1-z} \sum_{k=1}^{m} \frac{z^k}{k} = H_m \text{ for } n \ge m$$

where H_m is the *m*th harmonic number. Hence the expected number of cycles of length at most *m* in a random permutation is about ln *m*.

Moments of fixed points

The mixed GF $g(z,u)$ of the set of permutations by the number of fixed points is

$$g(z,u) = \exp\left(-z + uz + \log \frac{1}{1-z}\right) = \frac{1}{1-z} \exp(-z+uz).$$

Let the random variable *X* be the number of fixed points of a random permutation. Using Stirling numbers of the second kind, we have the following formula for the *m*th moment of *X*:

$$E(X^m) = E\left(\sum_{k=0}^m \left\{ m \atop k \right\} (X)_k\right) = \sum_{k=0}^m \left\{ m \atop k \right\} E((X)_k),$$

where $(X)_k$ is a falling factorial. Using $g(z,u)$, we have

$$E((X)_k) = [z^n]\left(\frac{d}{du}\right)^k g(z,u)\bigg|_{u=1} = [z^n]\frac{z^k}{1-z}\exp(-z+uz)\bigg|_{u=1} = [z^n]\frac{z^k}{1-z},$$

which is zero when $k > n$, and one otherwise. Hence only terms with $k <= n$ contribute to the sum. This yields

$$E(X^m) = \sum_{k=0}^n \left\{ m \atop k \right\}.$$

Expected number of fixed points in random permutation raised to some power k

Suppose you pick a random permutation σ and raise it to some power k, with k a positive integer and ask about the expected number of fixed points in the result. Denote this value by $E[F_k]$.

For every divisor d of k a cycle of length d splits into d fixed points when raised to the power k. Hence we need to mark these cycles with u^d. To illustrate this consider $E[F_6]$.

We get

$$g(z,u) = \exp\left(uz - z + u^2\frac{z^2}{2} - \frac{z^2}{2} + u^3\frac{z^3}{3} - \frac{z^3}{3} + u^6\frac{z^6}{6} - \frac{z^6}{6} + \log\frac{1}{1-z}\right)$$

which is

$$\frac{1}{1-z}\exp\left(uz - z + u^2\frac{z^2}{2} - \frac{z^2}{2} + u^3\frac{z^3}{3} - \frac{z^3}{3} + u^6\frac{z^6}{6} - \frac{z^6}{6}\right).$$

Once more continuing as described in the introduction, we find

$$\frac{\partial}{\partial u}g(z,u)\bigg|_{u=1} = \frac{z+z^2+z^3+z^6}{1-z}\exp\left(uz - z + u^2\frac{z^2}{2} - \frac{z^2}{2} + u^3\frac{z^3}{3} - \frac{z^3}{3} + u^6\frac{z^6}{6} - \frac{z^6}{6}\right)\bigg|_{u=1}$$

which is

$$\frac{z+z^2+z^3+z^6}{1-z}.$$

The conclusion is that $E[F_6] = 4$ for $n \geq 6$ and there are four fixed points on average.

The general procedure is

$$g(z,u) = \exp\left(\sum_{d|k}\left(u^d\frac{z^d}{d} - \frac{z^d}{d}\right) + \log\frac{1}{1-z}\right) = \frac{1}{1-z}\exp\left(\sum_{d|k}\left(u^d\frac{z^d}{d} - \frac{z^d}{d}\right)\right).$$

Once more continuing as before, we find

$$\frac{\partial}{\partial u}g(z,u)\bigg|_{u=1} = \frac{\sum_{d|k} z^d}{1-z}\exp\left(\sum_{d|k}\left(u^d\frac{z^d}{d} - \frac{z^d}{d}\right)\right)\bigg|_{u=1} = \frac{\sum_{d|k} z^d}{1-z}.$$

We have shown that the value of $E[F_k]$ is equal to $\tau(k)$ (the number of divisors of k) as soon as $n \geq k$. It starts out at 1 for $n = 1$ and increases by one every time n hits a divisor of k up to and including k itself.

Expected number of cycles of any length of a random permutation

We construct the bivariate generating function $g(z, u)$ using $b(k)$, where $b(k)$ is one for all cycles (every cycle contributes one to the total number of cycles).

Note that $g(z, u)$ has the closed form

$$g(z,u) = \left(\frac{1}{1-z}\right)^u$$

and generates the unsigned Stirling numbers of the first kind.

We have

$$\left.\frac{\partial}{\partial u} g(z,u)\right|_{u=1} = \frac{1}{1-z}\sum_{k\geq 1} b(k)\frac{z^k}{k} = \frac{1}{1-z}\sum_{k\geq 1}\frac{z^k}{k} = \frac{1}{1-z}\log\frac{1}{1-z}.$$

Hence the expected number of cycles is the harmonic number H_n, or about $\log n$.

Number of permutations with a cycle of length larger than $n/2$

(Note that Section One hundred prisoners contains exactly the same problem with a very similar calculation, plus also a simpler elementary proof.)

Once more, start with the exponential generating function $g(z, u)$, this time of the class $\mathcal{P}$ of permutations according to size where cycles of length more than $n/2$ are marked with the variable u:

$$g(z,u) = \exp\left(u\sum_{k>\lfloor\frac{n}{2}\rfloor}^{\infty}\frac{z^k}{k} + \sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\frac{z^k}{k}\right).$$

There can only be one cycle of length more than $\frac{n}{2}$, hence the answer to the question is given by

$$n![uz^n]g(z,u) = n![z^n]\exp\left(\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\frac{z^k}{k}\right)\sum_{k>\lfloor\frac{n}{2}\rfloor}^{\infty}\frac{z^k}{k}$$

or

$$n![z^n]\exp\left(\log\frac{1}{1-z} - \sum_{k>\lfloor\frac{n}{2}\rfloor}^{\infty}\frac{z^k}{k}\right)\sum_{k>\lfloor\frac{n}{2}\rfloor}^{\infty}\frac{z^k}{k}$$

which is

$$n![z^n]\frac{1}{1-z}\exp\left(-\sum_{k>\lfloor\frac{n}{2}\rfloor}^{\infty}\frac{z^k}{k}\right)\sum_{k>\lfloor\frac{n}{2}\rfloor}^{\infty}\frac{z^k}{k} = n![z^n]\frac{1}{1-z}\sum_{m=0}^{\infty}\frac{(-1)^m}{m!}\left(\sum_{k>\lfloor\frac{n}{2}\rfloor}^{\infty}\frac{z^k}{k}\right)^{m+1}$$

The exponent of z in the term being raised to the power $m + 1$ is larger than $\lfloor\frac{n}{2}\rfloor$ and hence no value for $m > 0$ can possibly contribute to $[z^n]$.

It follows that the answer is

$$n![z^n]\frac{1}{1-z}\sum_{k>\lfloor\frac{n}{2}\rfloor}^{\infty}\frac{z^k}{k} = n!\sum_{k=\lfloor\frac{n}{2}\rfloor+1}^{n}\frac{1}{k}.$$

The sum has an alternate representation that one encounters e.g. in the OEIS OEIS: A024167.

$$\sum_{k=1}^{n}\frac{1}{k} - \sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\frac{1}{k} = \sum_{k=1}^{n}\frac{1}{k} - 2\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\frac{1}{2k} = \sum_{\substack{k=1\\k\text{ even}}}^{n}(1-2)\frac{1}{k} + \sum_{\substack{k=1\\k\text{ odd}}}^{n}\frac{1}{k}$$

finally giving

$$n!\sum_{k=1}^{n}\frac{(-1)^{k+1}}{k} \sim n!\log 2.$$

Expected number of transpositions of a random permutation

We can use the disjoint cycle decomposition of a permutation to factorize it as a product of transpositions by replacing a cycle of length *k* by *k* − 1 transpositions. E.g. the cycle $(1\ 2\ 34)$ factors as $(1\ 2)\ (2\ 3)\ (3\ 4)$. The function $b(k)$ for cycles is equal to $k-1$ and we obtain

$$g(z,u) = \left(\frac{1}{1-uz}\right)^{1/u}$$

and

$$\left.\frac{\partial}{\partial u}g(z,u)\right|_{u=1} = \frac{1}{1-z}\sum_{k\geq 1}(k-1)\frac{z^k}{k} = \frac{z}{(1-z)^2} - \frac{1}{1-z}\log\frac{1}{1-z}.$$

Hence the expected number of transpositions $T(n)$ is

$$T(n) = n - H_n$$

where H_n is the n^{th} Harmonic number. We could also have obtained this formula by noting that the number of transpositions is obtained by adding the lengths of all cycles (which gives *n*) and subtracting one for every cycle (which gives $\log n$ by the previous section).

Note that $g(z,u)$ again generates the unsigned Stirling numbers of the first kind, but in reverse order. More precisely, we have

$$(-1)^m n!\ [z^n][u^m]g(z,u) = \left[{n \atop n-m}\right]$$

To see this, note that the above is equivalent to

$$(-1)^{n+m}n!\ [z^n][u^m]g(z,u)|_{u=1/u}|_{z=uz} = \left[{n \atop m}\right]$$

and that

$$[u^m]g(z,u)|_{u=1/u}|_{z=uz} = [u^m]\left(\frac{1}{1-z}\right)^u = \frac{1}{m!}\left(\log\frac{1}{1-z}\right)^m,$$

which we saw to be the EGF of the unsigned Stirling numbers of the first kind in the section on permutations consisting of precisely *m* cycles.

Expected cycle size of a random element

We select a random element *q* of a random permutation σ and ask about the expected size of the cycle that contains *q*. Here the function $b(k)$ is equal to k^2, because a cycle of length *k* contributes *k* elements that are on cycles of length *k*. Note that unlike the previous computations, we need to average out this parameter after we extract it from the generating function (divide by *n*). We have

$$\frac{\partial}{\partial u} g(z,u)\bigg|_{u=1} = \frac{1}{1-z} \sum_{k\ge 1} k^2 \frac{z^k}{k} = \frac{1}{1-z} \frac{z}{(1-z)^2} = \frac{z}{(1-z)^3}.$$

Hence the expected length of the cycle that contains *q* is

$$\frac{1}{n}[z^n]\frac{z}{(1-z)^3} = \frac{1}{n}\frac{1}{2}n(n+1) = \frac{1}{2}(n+1).$$

Probability that a random element lies on a cycle of size *m*

This average parameter represents the probability that if we again select a random element of $[n]$ of a random permutation, the element lies on a cycle of size *m*. The function $b(k)$ is equal to m for $m = k$ and zero otherwise, because only cycles of length *m* contribute, namely *m* elements that lie on a cycle of length *m*. We have

$$\frac{\partial}{\partial u} g(z,u)\bigg|_{u=1} = \frac{1}{1-z} \sum_{k\ge 1} b(k) \frac{z^k}{k} = \frac{1}{1-z}\, m\, \frac{z^m}{m} = \frac{z^m}{1-z}.$$

It follows that the probability that a random element lies on a cycle of length *m* is

$$\frac{1}{n}[z^n]\frac{z^m}{1-z} = \begin{cases} \frac{1}{n}, & \text{if } n \ge m \\ 0, & \text{otherwise.} \end{cases}$$

Probability that a random subset of [*n*] lies on the same cycle

Select a random subset *Q* of [*n*] containing *m* elements and a random permutation, and ask about the probability that all elements of *Q* lie on the same cycle. This is another average parameter. The function *b*(*k*) is equal to $\binom{k}{m}$, because a cycle of length *k* contributes $\binom{k}{m}$ subsets of size *m*, where $\binom{k}{m} = 0$ for *k* < *m*. This yields

$$\frac{\partial}{\partial u} g(z,u)\bigg|_{u=1} = \frac{1}{1-z} \sum_{k\ge m} \binom{k}{m} \frac{z^k}{k} = \frac{1}{1-z}\frac{1}{m}\frac{z^m}{(1-z)^m} = \frac{1}{m}\frac{z^m}{(1-z)^{m+1}}.$$

Averaging out we obtain that the probability of the elements of *Q* being on the same cycle is

$$\binom{n}{m}^{-1}[z^n]\frac{1}{m}\frac{z^m}{(1-z)^{m+1}} = \binom{n}{m}^{-1}\frac{1}{m}[z^{n-m}]\frac{1}{(1-z)^{m+1}}$$

or

$$\frac{1}{m}\binom{n}{m}^{-1}\binom{(n-m)\ +\ m}{m} = \frac{1}{m}.$$

In particular, the probability that two elements $p < q$ are on the same cycle is 1/2.

Number of permutations containing an even number of even cycles

We may use the Flajolet–Sedgewick fundamental theorem directly and compute more advanced permutation statistics. (Check that page for an explanation of how the operators we will use are computed.) For example, the set of permutations containing an even number of even cycles is given by

$$\operatorname{SET}(\operatorname{CYC}_{\operatorname{odd}}(\mathcal{Z}))\operatorname{SET}_{\operatorname{even}}(\operatorname{CYC}_{\operatorname{even}}(\mathcal{Z})).$$

Translating to exponential generating functions (EGFs), we obtain

$$\exp\left(\frac{1}{2}\log\frac{1+z}{1-z}\right)\cosh\left(\frac{1}{2}\log\frac{1}{1-z^2}\right)$$

or

$$\frac{1}{2}\exp\left(\frac{1}{2}\left(\log\frac{1+z}{1-z}+\log\frac{1}{1-z^2}\right)\right)+\frac{1}{2}\exp\left(\frac{1}{2}\left(\log\frac{1+z}{1-z}-\log\frac{1}{1-z^2}\right)\right).$$

This simplifies to

$$\frac{1}{2}\exp\left(\frac{1}{2}\log\frac{1}{(1-z)^2}\right)+\frac{1}{2}\exp\left(\frac{1}{2}\log(1+z)^2\right)$$

or

$$\frac{1}{2}\frac{1}{1-z}+\frac{1}{2}(1+z)=1+z+\frac{1}{2}\frac{z^2}{1-z}.$$

This says that there is one permutation of size zero containing an even number of even cycles (the empty permutation, which contains zero cycles of even length), one such permutation of size one (the fixed point, which also contains zero cycles of even length), and that for $n \geq 2$, there are $n!/2$ such permutations.

Permutations that are squares

Consider what happens when we square a permutation. Fixed points are mapped to fixed points. Odd cycles are mapped to odd cycles in a one-to-one correspondence, e.g. $(1\ 8\ 9\ 11\ 13)$ turns into $(1\ 9\ 13\ 8\ 11)$. Even cycles split in two and produce a pair of cycles of half the size of the original cycle, e.g. $(5\ 13\ 6\ 9)$ turns into $(5\ 6)\ (9\ 13)$. Hence permutations that are squares may contain any number of odd cycles, and an even number of cycles of size two, an even number of cycles of size four etc., and are given by

$$\operatorname{SET}(\operatorname{CYC}_{\operatorname{odd}}(\mathcal{Z}))\operatorname{SET}_{\operatorname{even}}(\operatorname{CYC}_{=2}(\mathcal{Z}))\operatorname{SET}_{\operatorname{even}}(\operatorname{CYC}_{=4}(\mathcal{Z}))\operatorname{SET}_{\operatorname{even}}(\operatorname{CYC}_{=6}(\mathcal{Z}))\cdots$$

which yields the EGF

$$\exp\left(\frac{1}{2}\log\frac{1+z}{1-z}\right)\prod_{m\geq 1}\cosh\frac{z^{2m}}{2m}=\sqrt{\frac{1+z}{1-z}}\prod_{m\geq 1}\cosh\frac{z^{2m}}{2m}.$$

Odd cycle invariants

The types of permutations presented in the preceding two sections, i.e. permutations containing an even number of even cycles and permutations that are squares, are examples of so-called **odd cycle invariants**, studied by Sung and Zhang (see external links). The term odd cycle invariant simply means that membership in the respective combinatorial class is independent of the size and number of odd cycles occurring in the permutation. In fact we can prove that all odd cycle invariants obey a simple recurrence, which we will derive. First, here are some more examples of odd cycle invariants.

Permutations where the sum of the lengths of the even cycles is six

This class has the specification

$$\mathrm{SET}(\mathrm{CYC}_{\mathrm{odd}}(\mathcal{Z}))\,(\mathrm{SET}_{=3}(\mathrm{CYC}_{=2}(\mathcal{Z})) + \mathrm{CYC}_{=2}(\mathcal{Z})\,\mathrm{CYC}_{=4}(\mathcal{Z}) + \mathrm{CYC}_{=6}(\mathcal{Z}))$$

and the generating function

$$\sqrt{\frac{1+z}{1-z}}\left(\frac{1}{6}\left(\frac{z^2}{2}\right)^3 + \frac{z^2}{2}\frac{z^4}{4} + \frac{z^6}{6}\right) = \frac{5}{16}z^6\sqrt{\frac{1+z}{1-z}}.$$

The first few values are

$$0, 0, 0, 0, 0, 225, 1575, 6300, 56700, 425250, 4677750, 46777500, 608107500, \ldots$$

Permutations where all even cycles have the same length

This class has the specification

$$\mathrm{SET}(\mathrm{CYC}_{\mathrm{odd}}(\mathcal{Z}))\,(\mathrm{SET}_{\geq 1}(\mathrm{CYC}_{=2}(\mathcal{Z})) + \mathrm{SET}_{\geq 1}(\mathrm{CYC}_{=4}(\mathcal{Z})) + \mathrm{SET}_{\geq 1}(\mathrm{CYC}_{=6}(\mathcal{Z})) + \cdots)$$

and the generating function

$$\sqrt{\frac{1+z}{1-z}}\left(\exp\left(\frac{z^2}{2}\right) - 1 + \exp\left(\frac{z^4}{4}\right) - 1 + \exp\left(\frac{z^6}{6}\right) - 1 + \cdots\right).$$

There is a semantic nuance here. We could consider permutations containing no even cycles as belonging to this class, since zero is even. The first few values are

$$0, 1, 3, 15, 75, 405, 2835, 22155, 199395, 1828575, \ldots$$

Permutations where the maximum length of an even cycle is four

This class has the specification

$$\mathrm{SET}(\mathrm{CYC}_{\mathrm{odd}}(\mathcal{Z}))\,\mathrm{SET}(\mathrm{CYC}_{=2}(\mathcal{Z}) + \mathrm{CYC}_{=4}(\mathcal{Z}))$$

and the generating function

$$\sqrt{\frac{1+z}{1-z}}\exp\left(\frac{z^2}{2} + \frac{z^4}{4}\right).$$

The first few values are

$$1, 2, 6, 24, 120, 600, 4200, 28560, 257040, 2207520, 24282720, 258128640, \ldots$$

The recurrence

Observe carefully how the specifications of the even cycle component are constructed. It is best to think of them in terms of parse trees. These trees have three levels. The nodes at the lowest level represent sums of products of even-length cycles of the singleton $\mathcal{Z}$. The nodes at the middle level represent restrictions of the set operator. Finally the node at the top level sums products of contributions from the middle level. Note that restrictions of the set operator, when applied to a generating function that is even, will preserve this feature, i.e. produce another even generating function. But all the inputs to the set operators are even since they arise from even-length cycles. The result is that all generating functions involved have the form

$$g(z) = h(z)\sqrt{\frac{1+z}{1-z}},$$

where $h(z)$ is an even function. This means that

$$\frac{1}{1+z}\; g(z) = h(z)\; \frac{1}{\sqrt{1-z^2}}$$

is even, too, and hence

$$\frac{1}{1+z}\; g(z) = \frac{1}{1-z}\; g(-z) \quad \text{or} \quad (1-z)\; g(z) = (1+z)\; g(-z).$$

Letting $g_n = [z^n]g(z)$ and extracting coefficients, we find that

$$\frac{g_{2m+1}}{(2m+1)!} - \frac{g_{2m}}{(2m)!} = -\frac{g_{2m+1}}{(2m+1)!} + \frac{g_{2m}}{(2m)!} \quad \text{or} \quad 2\frac{g_{2m+1}}{(2m+1)!} = 2\frac{g_{2m}}{(2m)!}$$

which yields the recurrence

$$g_{2m+1} = (2m+1)g_{2m}\,.$$

A problem from the 2005 Putnam competition

A link to the Putnam competition website appears in the section External links. The problem asks for a proof that

$$\sum_{\pi\in S_n} \frac{\sigma(\pi)}{\nu(\pi)+1} = (-1)^{n+1}\,\frac{n}{n+1},$$

where the sum is over all $n!$ permutations of $[n]$, $\sigma(\pi)$ is the sign of π, i.e. $\sigma(\pi) = 1$ if π is even and $\sigma(\pi) = -1$ if π is odd, and $\nu(\pi)$ is the number of fixed points of π.

Now the sign of π is given by

$$\sigma(\pi) = \prod_{c\in\pi} (-1)^{|c|-1},$$

where the product is over all cycles *c* of π, as explained e.g. on the page on even and odd permutations.

Hence we consider the combinatorial class

$$\textrm{SET}(-\mathcal{Z} + \mathcal{V}\mathcal{Z} + \textrm{CYC}_{=1}(\mathcal{Z}) + \mathcal{U}\,\textrm{CYC}_{=2}(\mathcal{Z}) + \mathcal{U}^2\,\textrm{CYC}_{=3}(\mathcal{Z}) + \mathcal{U}^3\,\textrm{CYC}_{=4}(\mathcal{Z}) + \cdots)$$

where $\mathcal{U}$ marks one minus the length of a contributing cycle, and $\mathcal{V}$ marks fixed points. Translating to generating functions, we obtain

$$g(z,u,v) = \exp\left(-z + vz + \sum_{k\ge 1} u^{k-1}\,\frac{z^k}{k}\right)$$

or

$$\exp\left(-z + vz + \frac{1}{u}\log\frac{1}{1-uz}\right) = \exp(-z+vz)\left(\frac{1}{1-uz}\right)^{1/u}.$$

Now we have

$$n![z^n]g(z,-1,v) = n![z^n]\exp(-z+vz)(1+z) = \sum_{\pi\in S_n} \sigma(\pi)v^{\nu(\pi)}$$

and hence the desired quantity is given by

$$n![z^n]\int_0^1 g(z,-1,v)dv = \sum_{\pi\in S_n} \frac{\sigma(\pi)}{\nu(\pi)+1}.$$

Doing the computation, we obtain

$$\int_0^1 g(z,-1,v)dv = \exp(-z)(1+z)\left(\frac{1}{z}\exp(z) - \frac{1}{z}\right)$$

or

$$\left(\frac{1}{z}+1\right)(1-\exp(-z)) = \frac{1}{z} + 1 - \exp(-z) - \frac{1}{z}\exp(-z).$$

Extracting coefficients, we find that the coefficient of $1/z$ is zero. The constant is one, which does not agree with the formula (should be zero). For n positive, however, we obtain

$$n![z^n]\left(-\exp(-z) - \frac{1}{z}\exp(-z)\right) = n!\left(-(-1)^n\frac{1}{n!} - (-1)^{n+1}\frac{1}{(n+1)!}\right)$$

or

$$(-1)^{n+1}\left(1 - \frac{1}{n+1}\right) = (-1)^{n+1}\frac{n}{n+1},$$

which is the desired result.

As an interesting aside, we observe that $g(z,u,v)$ may be used to evaluate the following determinant of an $n \times n$ matrix:

$$d(n) = \det(A_n) = \begin{vmatrix} a & b & b & \cdots & b \\ b & a & b & \cdots & b \\ b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & a \end{vmatrix}.$$

where $a, b \neq 0$. Recall the formula for the determinant:

$$\det(A) = \sum_{\pi\in S_n} \sigma(\pi)\prod_{i=1}^n A_{i,\pi(i)}.$$

Now the value of the product on the right for a permutation π is $a^f b^{n-f}$, where f is the number of fixed points of π. Hence

$$d(n) = b^n n![z^n]g\left(z,-1,\frac{a}{b}\right) = b^n n![z^n]\exp\left(\frac{a-b}{b}z\right)(1+z)$$

which yields

$$b^n\left(\frac{a-b}{b}\right)^n + b^n n\left(\frac{a-b}{b}\right)^{n-1} = (a-b)^n + nb(a-b)^{n-1}$$

and finally

$$d(n) = (a+(n-1)b)(a-b)^{n-1}\,.$$

The difference between the number of cycles in even and odd permutations

Here we seek to show that this difference is given by

$$(-1)^n(n-2)!$$

Recall that the sign $\sigma(\pi)$ of a permutation π is given by

$$\sigma(\pi) = \prod_{c\in\pi}(-1)^{|c|-1}$$

where the product ranges over the cycles c from the disjoint cycle composition of π.

It follows that the combinatorial species $\mathcal{Q}$ that reflects the signs and the cycle count of the set of permutations is given by

$$\mathcal{Q} = \textsc{SET}(\mathcal{V}\,\textsc{CYC}_1(\mathcal{Z}) + \mathcal{U}\mathcal{V}\,\textsc{CYC}_{=2}(\mathcal{Z})) + \mathcal{U}^2\mathcal{V}\,\textsc{CYC}_{=3}(\mathcal{Z}) + \mathcal{U}^3\mathcal{V}\,\textsc{CYC}_{=4}(\mathcal{Z}) + \mathcal{U}^4\mathcal{V}\,\textsc{CYC}_{=5}(\mathcal{Z}) + \cdots)$$

where we have used $\mathcal{U}$ to mark signs and $\mathcal{V}$ for the cycle count.

Translating to generating functions we have

$$Q(z,u,v) = \exp\left(v\frac{z}{1} + vu\frac{z^2}{2} + vu^2\frac{z^3}{3} + vu^3\frac{z^4}{4} + vu^4\frac{z^5}{5} + \cdots\right).$$

This simplifies to

$$Q(z,u,v) = \exp\left(\frac{v}{u}\left(\frac{zu}{1} + \frac{z^2u^2}{2} + \frac{z^3u^3}{3} + \frac{z^4u^4}{4} + \frac{z^5u^5}{5} + \cdots\right)\right)$$

which is

$$\exp\left(\frac{v}{u}\log\frac{1}{1-uz}\right) = \left(\frac{1}{1-uz}\right)^{\frac{v}{u}}.$$

Now the two generating functions $Q_1(z,v)$ and $Q_2(z,v)$ of even and odd permutations by cycle count are given by

$$Q_1(z,v) = \frac{1}{2}Q(z,+1,v) + \frac{1}{2}Q(z,-1,v) = \frac{1}{2}\left(\frac{1}{1-z}\right)^v + \frac{1}{2}\left(\frac{1}{1+z}\right)^{-v}$$

and

$$Q_2(z,v) = \frac{1}{2}Q(z,+1,v) - \frac{1}{2}Q(z,-1,v) = \frac{1}{2}\left(\frac{1}{1-z}\right)^v - \frac{1}{2}\left(\frac{1}{1+z}\right)^{-v}.$$

We require the quantity

$$G(z,v) = \frac{d}{dv}(Q_1(z,v) - Q_2(z,v))\Bigg|_{v=1}$$

which is

$$\frac{d}{dv}\left(\frac{1}{1+z}\right)^{-v}\Bigg|_{v=1} = -\log\frac{1}{1+z}\left(\frac{1}{1+z}\right)^{-v}\Bigg|_{v=1} = -(1+z)\log\frac{1}{1+z}.$$

Finally, extracting coefficients from this generating function, we obtain

$$-n![z^n](1+z)\log\frac{1}{1+z} = -n!\left(\frac{(-1)^n}{n} + \frac{(-1)^{n-1}}{n-1}\right)$$

which is

$$-n!(-1)^{n-1}\left(-\frac{1}{n} + \frac{1}{n-1}\right) = n!(-1)^n \frac{n-(n-1)}{n(n-1)}$$

which is in turn

$$n!(-1)^n \frac{1}{n(n-1)} = (-1)^n (n-2)!$$

This concludes the proof.

See also

- Golomb–Dickman constant

References

1. Chowla, S.; Herstein, I. N.; Moore, W. K. (1951), "On recursions connected with symmetric groups. I", *Canadian Journal of Mathematics*, **3**: 328–334, doi:10.4153/CJM-1951-038-3 (https://doi.org/10.4153%2FCJM-1951-038-3), MR 0041849 (https://mathscinet.ams.org/mathscinet-getitem?mr=0041849), S2CID 123802787 (https://api.semanticscholar.org/CorpusID:123802787)
2. Goh, William M.Y.; Schmutz, Eric (1991). "The Expected order of a Random Permutation" (https://web.archive.org/web/20200225162216/https://academic.oup.com/blms/article/23/1/34/288444). *Bulletin of the London Mathematical Society*. **23** (1): 34–42. doi:10.1112/blms/23.1.34 (https://doi.org/10.1112%2Fblms%2F23.1.34). Archived from the original (https://academic.oup.com/blms/article-abstract/23/1/34/288444) on February 25, 2020. Alt URL (http://www.pages.drexel.edu/~schmutze/PAPERS/musn.pdf)

External links

- Sung, Philip; Zhang, Yan (2003). "Recurring Recurrences in Counting Permutations". CiteSeerX 10.1.1.91.1088 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.91.1088).
- Marko Riedel et al., *The difference of number of cycles of even and odd permutations (https://math.stackexchange.com/q/495487)*
- Marko Riedel et al., *Keys inside closed boxes, a question on probability (https://math.stackexchange.com/q/73896)*

100 prisoners

- Various authors, *Permutations with a cycle > n/2 (https://math.stackexchange.com/q/259351)*
- Various authors, *A property of derangements (https://math.stackexchange.com/q/347260)*
- Various authors, *Expected number of fixed points (https://math.stackexchange.com/q/349118)*
- Peter Winkler, *Seven puzzles you think you must not have heard correctly (http://www.math.dartmouth.edu/~pw/solutions.pdf)*
- Various authors, *Les-Mathematiques.net (http://les-mathematiques.net)*. *Cent prisonniers (http://les-mathematiques.u-strasbg.fr/phorum5/read.php?12,341672)* (in French)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Random_permutation_statistics&oldid=1118739971"

organization.