

Cycle structure of compositions of random involutions

Michael Lugo

University of Pennsylvania, Graduate Student Combinatorics Seminar

October 28, 2009

Question

The number of involutions in the symmetric group S_n is asymptotically

$$\sqrt{n!}e^{\sqrt{n}}(8\pi en)^{-1/4}.$$

WHY?

- 1 Pattern avoidance
 - What is pattern avoidance?
 - Pattern-avoiding involutions
- 2 Permutations with all cycle lengths in a finite set
 - Hayman's method
 - Counting by cycle type
- 3 The graph theoretic decomposition
 - Trivariate generating function for partial matchings
- 4 Asymptotics
 - The “exponential of a pole” schema
 - Cycle structure
- 5 Factorization into involutions
 - The simple cases
 - Building up general factorizations
 - An Erdős-Turán-type theorem

What is pattern avoidance?

Definition

We say a permutation $\sigma \in S_n$ *contains* a pattern $\pi \in S_k$ (which is another permutation) if σ contains a subsequence of length k with the same order relations as π . If σ does not contain π , then σ *avoids* π or is π -*avoiding*.

Examples:

- Inversions are 21-patterns. $n(n-1)\cdots 1$ is the only 21-avoiding permutation of $[n]$.
- **1524376** is 231-avoiding, but not 213-avoiding

The Catalan numbers

Theorem (Knuth, 1973)

All patterns of length 3 satisfy $S_n(\pi) = C_n$.

Proof.

For 132 there's a bijection with binary trees. 213, 312, 231 by symmetry. For 123, consider a 132-avoiding permutation such as **67341258**. Leave the left-to-right minima fixed and put the others in decreasing order: **68371542**. 321 by symmetry. □

We say all the patterns of length 3 are *Wilf-equivalent*. In general, π and ρ are Wilf-equivalent if $S_n(\pi) = S_n(\rho)$ for all n .

Note $C_n \sim 4^n / \sqrt{\pi n^3}$.

The Stanley-Wilf conjecture

Theorem (Stanley-Wilf conjecture; Marcus-Tardos 2004)

For any pattern π , $S_n(\pi)$ is bounded above by $L(\pi)^n$ for some constant $L(\pi)$ depending on π .

- Arratia (1999) showed that the S-W conjecture is equivalent to the existence of $\lim_{n \rightarrow \infty} |S_n(\pi)|^{1/n}$ for each π ; this limit is $L(\pi)$.
- Marcus and Tardos proof uses pattern avoidance in 0 – 1 matrices. Gives $L(\pi) \leq 2k^4 \binom{k^2}{k}$ where $k = |\pi|$. So $|S_n(123)| \leq 13608^n$; hardly a surprise! “Typical” constants more like k^2 .

Pattern-avoiding involutions

Let $I_n(\pi)$ be the number of π -avoiding involutions of $[n]$. Then:

- In all cases where an asymptotic formula for $I_n(\pi)$ is known, $L_i(\pi) := \lim_{n \rightarrow \infty} |I_n(\pi)|^{1/n}$ exists.
- If $L(\pi)$ is also known, then $L_i(\pi)^2 = L(\pi)$.
- Length 3 (Simion-Schmidt 1985): $I_n(\pi) = \binom{n}{\lfloor n/2 \rfloor} \sim 2^n / \sqrt{\pi n}$ if $\pi \in \{123, 132, 213, 321\}$. $I_n(\pi) = 2^{n-1}$ if $\pi = 231$ or 312 .
- “Involutory Wilf-equivalence” is stronger than Wilf-equivalence!

Surprise: The number of π -avoiding involutions is roughly the *square root* of the number of π -avoiding permutations.

Why square roots?

In certain senses an involution is “half of a permutation”.

- The RSK correspondence associates permutations with pairs of standard Young tableaux (P, Q) of the same shape. For an involution $P = Q$.
- The *graph* of a permutation $\sigma \in \mathcal{S}_n$ is $\{(i, \sigma(i)) : i \in [n]\}$. Involutions are symmetric across the diagonal.
- Most permutations can be *factored* into involutions in a small number of ways (more on this later!)

The events “the top half of σ avoids π ” and “the bottom half of σ avoids π ” don’t depend very strongly on each other, and σ avoids π is almost their conjunction. (But not exactly! This is off by a polynomial factor!)

Hayman's method

Theorem (Hayman, 1956)

Consider a polynomial $\sum c_n z^n$, and $f(z) = \sum a_n z^n$ its exponential. Then

$$a_n \sim \frac{f(r_n)}{r_n^n \sqrt{2\pi b(r_n)}}$$

where $a(z) = \sum n c_n z^n$, r_n is the positive real root of $a(z) = n$, and $b(z) = \sum n^2 c_n z^n$.

(More generally, $f(z)$ can be an “admissible function”.)

If we start with the polynomial z we recover Stirling's formula; Hayman's paper is “A generalization of Stirling's formula”.

Counting S -permutations

I use this to prove:

Theorem (L., 2009)

Let S be a finite set of positive integers, with $m = \max S$. Let $n!p_n$ be the number of S -permutations of n . Then

$$p_n \cdot n^{1/m} \sim \exp(f_S(n^{1/m})) n^{-1/2+1/2m} C_S$$

for a polynomial f_S of degree $m - 1$ and constant C_S which can be explicitly computed. In particular $\lim_{n \rightarrow \infty} \frac{\log p_n}{\log n!} = -1/m$

That is, the probability that a permutation of $[n]$ is an S -permutation is $n!^{-1/m}$ times a subexponential factor.

An example computation (I)

Consider $S = \{1, 2, 3\}$. Then r_n is the root of $z + z^2 + z^3 = n$;

$$r_n = n^{-1/3} - \frac{1}{3} - \frac{2}{9}n^{-1/3} + \frac{7}{81}n^{-2/3} + O(1/n)$$

Then write r_n^n as a series in n :

$$r_n^n = n^{n/3} \exp \left(n \log \left(1 - \frac{1}{3}n^{-1/3} - \frac{2}{9}n^{-2/3} + \frac{7}{81}n^{-1} + O(n^{-4/3}) \right) \right)$$

Recall $\log(1+x) = x - x^2/2 + \dots$:

$$r_n^n \sim n^{n/3} \exp \left(-\frac{1}{3}n^{2/3} - \frac{5}{18}n^{1/3} \right)$$

An example computation (II)

Also, $b(r_n) = r_n + 2r_n^2 + 3r_n^3 \sim 3r_n^3 \sim 3n$. And

$$f(r_n) = \exp\left(r_n + \frac{1}{2}r_n^2 + \frac{1}{3}r_n^3\right) \sim \exp\left(\frac{n}{3} + \frac{1}{6}n^{2/3} + \frac{5}{9}n^{1/3} - \frac{5}{18}\right)$$

So derive leading-term asymptotics for p_n :

$$p_n \sim \frac{\exp\left(\frac{n}{3} + \frac{1}{6}n^{2/3} + \frac{5}{9}n^{1/3} - \frac{5}{18}\right)}{n^{n/3} \exp\left(-\frac{1}{3}n^{2/3} - \frac{5}{18}n^{1/3}\right) \sqrt{6\pi n}}$$

and by Stirling's approximation,

$$p_n \cdot n!^{1/3} \sim \exp\left(\frac{1}{2}n^{2/3} + \frac{5}{6}n^{1/3}\right) n^{-1/3} \cdot \left(\frac{e^5}{2^6 3^9 \pi^6}\right)^{1/18}$$

Cycle structure of S -permutations: theorem

Theorem

The expected number of cycles of length k in an S -permutation chosen uniformly at random, where $k \in S$ and $m = \max S$, is asymptotic to $n^{k/m}/k$ as $n \rightarrow \infty$.

For example: a typical involution on $[n]$ has \sqrt{n} fixed points. This fact was known, but surprised me when I rediscovered it. I would have expected either a constant or a constant multiple of n , but the truth lies in between.

Cycle structure of S -permutations: proof

- Let $a_n = n!p_n$ be the number of S -permutations of $[n]$.
- GF counting by size and number of k -cycles:

$$G(z, u) = \exp \left(\left(\sum_{s \in S} z^s / s \right) + (u - 1)z^k / k \right)$$

- Mean number of k -cycles in S -permutations:

$$\frac{[z^n] G_u(z, 1)}{[z^n] G(z, 1)} = \frac{[z^n] \frac{1}{k} z^k G(z, 1)}{[z^n] G(z, 1)} = \frac{1}{k} \frac{p_{n-k}}{p_n}$$

- $p_{n-k}/p_n \sim (n-k)!^{-1/m}/n!^{-1/m} = \binom{n}{k}^{1/m} \sim n^{k/m}$

Counting by cycle type

If $S = \{k\}$, then the number of S -permutations is

$$\frac{n!}{(n/k)!k^{(n/k)}} = \frac{1 \cdot 2 \cdot \dots \cdot n}{k \cdot 2k \cdot \dots \cdot n} \sim \frac{n! \frac{(k-1)}{k}}{(2\pi n)^{1/2-1/2k} k^{-1/2}}$$

If S is not a singleton, the number of S -permutations is:

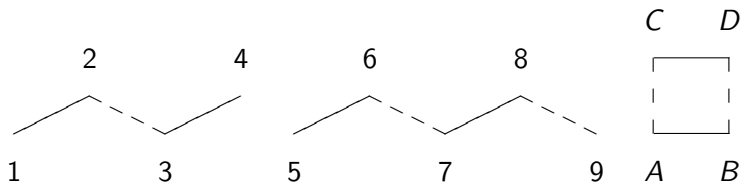
$$\sum_{c_1 s_1 + \dots + c_j s_j = n} \frac{n!}{c_1! \cdots c_j! s_1^{c_1} \cdots s_j^{c_j}}$$

The summand is maximized when $c_r \approx \alpha^{s_r} / s_r$, where α is the root of $z^{s_1} + \dots + z^{s_j} = n$.

This gives the location of the most common cycle type. Falloff is Gaussian.

Involutions as partial matchings

- We can identify an involution of $[n]$ with a partial matching on $[n]$.
- Cycles correspond to edges.
- A composition of involutions corresponds to a partial matching with 2-colored edges



$$(1342)(57986)(AD)(BC) = (1)(23)(4)(5)(67)(89)(AC)(BD) \\ \circ (12)(34)(56)(78)(9)(AB)(CD)$$

Comparison to 2-regular graphs

- 2-regular graphs have the egf

$$\exp\left(\frac{z^3}{6} + \frac{z^4}{8} + \frac{z^5}{10} + \dots\right) = \frac{e^{-z/2 - z^2/4}}{\sqrt{1 - z^2}}$$

- This is similar to the Ewens sampling formula with weight $1/2$; a typical 2-regular graph has $(\log n)/2$ cycles
- We have “almost 2-regular graphs” here – components are paths or cycles
- Paths predominate! Involutions have \sqrt{n} fixed points; all those fixed points are ends of paths.

The possible components: cycles

- Connected components of $\sigma \cup \tau$ are either cycles of even length, or paths
- Number of labelled cycles of length n is $n!/(2n)$
- Two ways to color a cycle of even length, no ways to color one of odd length
- $(n - 1)!$ possible even cycles, no odd cycles
- egf for cycles (compare 2-regular graphs):

$$1! \frac{z^2}{2!} + 3! \frac{z^4}{4!} + 5! \frac{z^6}{6!} + \dots = \frac{1}{2} \log \frac{1}{1 - z^2}$$

The possible components: paths

- $n!/2$ labelled paths of length $n \geq 2$ (1 for $n = 1$)
- Two colorings for each path of length $n \geq 2$ (pick an edge, the rest is forced)
- egf for paths is $z + z^2 + z^3 + \dots = z/(1 - z)$
- Compare “fragmented permutations” or “sets of lists”

Putting it together

Theorem

The trivariate generating function for pairs of partial matchings, counted by size (z , exponential) and number of paths and cycles (u and v , ordinary) is

$$Q(z, u, v) = \exp\left(\frac{uz}{1-z} - \frac{v}{2} \log(1-z^2)\right)$$

Corollary

The egf for pairs of involutions is

$$P(z) := Q(z, 1, 1) = \frac{e^{z/(1-z)}}{\sqrt{1-z^2}} = 1 + z + 2^2 \frac{z^2}{2!} + 4^2 \frac{z^3}{3!} + 10^2 \frac{z^4}{4!} + \dots$$

The generating function for pairs of involutions

Theorem

The generating function of pairs of involutions (σ, τ) , counted by size and number of cycles in $\tau \circ \sigma$, is

$$R(z, u) = Q(z, u, u^2) \cdot \frac{\exp\left(\frac{uz}{1-z}\right)}{(1-z^2)^{u^2/2}}$$

Each path in $\sigma \cup \tau$ corresponds to one cycle in $\tau \circ \sigma$.

Each cycle in $\sigma \cup \tau$ corresponds to two cycles in $\tau \circ \sigma$.

Wright's expansions

Theorem (Wright, 1932)

Let

$$c_n = [z^n](1 - z)^\beta \Phi(z) \exp(1/(1 - z))$$

, with $\beta \in \mathbb{C}$, Φ regular in the unit disc. Then

$$c_n = \frac{1}{n^{\beta/2+3/4}} \left[\exp(2\sqrt{n}) \frac{1}{2\sqrt{\pi}} \Phi(1) e^{1/2} \right] (1 + O(n^{-1/2}))$$

Wright also gives further terms of the asymptotic series, replaces $\exp(1/(1 - z))$ with $\exp(\sigma/(1 - z))$, and shows how to handle an extra factor of $(\log 1/(1 - z))^k$.

Exponentials of a pole lead to square roots

- With $\Phi(z) = e^{-z}/\sqrt{1+z}$, $\beta = -1/2$ we get $[z^n]P(z) = \frac{1}{\sqrt{8\pi en}} \exp(2\sqrt{en})$.
- This is the square of our previous subexponential factor, as expected.
- “Sets of lists” counted by $\exp(z/(1-z))$ also have about \sqrt{n} components.
- Partitions: recall $p(n) \sim \exp(\pi\sqrt{2n/3})/4n\sqrt{3}$ (Hardy, Ramanujan, Rademacher). The partition generating function is an “exponential of a pole”. This foreshadows results like: the mean number of parts of a partition of n is near $\pi^{-1}\sqrt{3n/2} \log n$; for partitions into distinct parts, $\frac{2\sqrt{3} \log 2}{\pi} \sqrt{n}$; limiting shapes of Young diagrams upon scaling by \sqrt{n} (conjugation!).

Partitions and square roots

The generating function for integer partitions is

$$P(z) = \prod_{k \geq 1} \frac{1}{1 - z^k} = \exp \sum_{k \geq 1} -\log(1 - z^k) = \exp \sum_{k \geq 1} \sum_{j \geq 1} \frac{z^{jk}}{j}.$$

Group together terms with the same exponent:

$$\sum_{n \geq 1} \left(\sum_{d|n} \frac{1}{d} \right) z^n = \sum_{n \geq 1} \frac{\sigma(n)}{n} z^n$$

and “everybody knows” $\sigma(n)/n$ has average value 2, so

$P(z)$ “ \approx ” $\exp(2/(1 - z))$. (I put this in quotes because it’s not true! In reality replace 2 with $\pi^2/6 = \zeta(2)$.)

Distribution of number of k -cycles

Theorem (L., 2009)

The distribution of the number of k -cycles of the composition of a pair of random involutions of $[n]$ converges in distribution to $\mathcal{P}(1) + 2 \cdot \mathcal{P}(1/k)$. (\mathcal{P} is Poisson, the two are independent.)

Idea of proof: write the generating function for compositions by pairs and number of k -cycles,

$$P(z, u) = \frac{\exp(z/(1-z))}{\sqrt{1-z^2}} \exp\left((u-1)z^k + (u^2-1)\frac{z^{2k}}{2k}\right).$$

The second factor is the factorial moment generating function of $\mathcal{P}(1) + 2\mathcal{P}(1/k)$. Then prove a lemma showing that distributions arising from $P(z, u) = Q(z)e^{R(z, u)}$ converge to the distribution with factorial mgf $e^{R(1, u)}$, if that distribution is determined by its moments.

Distribution of total number of cycles (I)

Theorem (L., 2009)

The mean number of cycles in a composition of two involutions of $[n]$ chosen uniformly at random is $\sqrt{n} + \frac{1}{2} \log n + O(1)$.

Proof: the bivariate generating function counting superpositions of partial matchings by size and number of paths is

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

and so the mean number of paths is

$$\frac{[z^n] \partial_u Q(z, 1, 1)}{[z^n] Q(z, 1, 1)} = \frac{[z^n] \frac{z}{1-z} \frac{\exp(z/(1-z))}{\sqrt{1-z^2}}}{[z^n] \frac{\exp(z/(1-z))}{\sqrt{1-z^2}}}.$$

Distribution of total number of cycles (II)

We can use Wright's theorem to extract coefficients:

$$\frac{(e^{2\sqrt{n}}/\sqrt{8\pi e})(1 + O(n^{-1/2}))}{(e^{2\sqrt{n}}/\sqrt{8\pi en})(1 + O(n^{-1/2}))} = \sqrt{n} + O(1)$$

We get \sqrt{n} since numerator has $\beta = 3/2$, denominator has $\beta = 1/2$; basically the extra factor of $1 - z$.

The mean number of *graph-cycles* comes from $Q(z, 1, \nu)$; it involves a log so I won't do the details, but it's $\frac{1}{4} \log n + O(n^{-1/2} \log n)$. Each gives rise to two permutation cycles.

A perplexing fact: the probability that a superposition of two random partial matchings of $[n]$ has no cyclic components is $\sim \sqrt{2}n^{-1/4}$.

Factoring an n -cycle

There are n ways to factor an n -cycle into two involutions.
 For example, the cycle (1234) is

$$\begin{array}{cc}
 (1)(24)(3) \circ (14)(23) & \begin{array}{c} 4 \quad 3 \\ \diagdown \quad \diagup \\ 1 \quad 2 \\ \diagup \quad \diagdown \\ 4 \quad 3 \end{array} & (2)(13)(4) \circ (12)(34) & \begin{array}{c} 1 \quad 4 \\ \diagdown \quad \diagup \\ 2 \quad 3 \\ \diagup \quad \diagdown \\ 4 \quad 3 \end{array} \\
 (41)(32) \circ (4)(13)(2) & \begin{array}{c} 1 \quad 2 \\ \diagdown \quad \diagup \\ 4 \quad 3 \\ \diagup \quad \diagdown \\ 4 \quad 3 \end{array} & (12)(43) \circ (24)(1)(3) & \begin{array}{c} 1 \quad 2 \\ \diagdown \quad \diagup \\ 4 \quad 3 \\ \diagup \quad \diagdown \\ 4 \quad 3 \end{array}
 \end{array}$$

A lone n -cycle comes from an n -path in the graph. Draw an n -path with edges in alternating colors. Place 1. The rest is forced.
 Also a special case of Goupil and Schaeffer 1998, on factoring an n -cycle into permutations of types λ and μ .

Factoring a permutation with two disjoint n -cycles

Lemma

Let π be a permutation of $[2n]$ consisting of two n -cycles. The number of solutions to $\pi = \tau \circ \sigma$ where the graph $\sigma \cup \tau$ is a $2n$ -cycle is n .

Proof: WLOG let $\pi = (1, 2, \dots, n)(n+1, n+2, \dots, 2n)$. Draw a $2n$ -cycle with alternately colored edges.

- There are $2n$ ways to place 1 (any vertex). 2 through n are forced.
- There are n ways to place $n+1$ (any remaining vertex). $n+2$ through $2n$ are forced.
- The unlabeled cycle has $2n$ symmetries (the symmetries of the n -gon), so each cycle is generated $2n$ times.
- There are $(2n^2)/(2n)$ distinct labelings/factorizations.

The number of factorizations: theorem

Theorem (L., 2009)

Let $f(r, k) = \sum_{j=0}^{\lfloor r/2 \rfloor} \frac{r!}{(r-2j)!j!2^j} k^{r-j}$. Let π be a permutation of $[n]$ with c_k cycles of length k , for each k . Then

$$F(\pi) = \prod_{k=1}^n f(c_k, k)$$

is the number of factorizations of π into involutions.

$f(r, k)$ is the number of partial matchings of $[r]$ with k -colored components.

The number of factorizations: examples

If π has all cycle lengths distinct, then the number of factorizations $\pi = \tau \circ \sigma$ is the product of its cycle lengths

Example:

$$\begin{aligned} (123) &= (23)(1) \circ (13)(2) = (31)(2) \circ (21)(3) = (12)(3) \circ (32)(1) \\ (4567) &= (4)(75)(6) \circ (47)(56) = (5)(46)(7) \circ (54)(67) \\ &= (6)(57)(4) \circ (65)(74) = (7)(64)(5) \circ (76)(45) \end{aligned}$$

So there are $3 \times 4 = 12$ factorizations of $(123)(4567)$.

But $(123)(456)$ has 12 factorizations as well: $9 = 3 \times 3$ which handle each cycle separately, and the three “mixing” factorizations:

$(42)(53)(61) \circ (14)(25)(36)$ is an example.

The number of factorizations: proof

- Consider each cycle length separately. Enough to show $f(r, k)$ is the number of factorizations of a permutation of type k^r into involutions.
- Pair up cycles which come from the same cycle in the graph $\sigma \cup \tau$
- Unpaired cycles come from paths in $\sigma \cup \tau$
- Each pair of cycles has k^2 factorizations; each lone cycle has k factorizations
- If there are k pairs of cycles, there are $r - j$ components to factor, thus k^{r-j} factorizations
- There are $r!/((r - 2j)!j!2^j)$ ways to pick the k disjoint pairs.
- Sum over k to get $f(r, k)$; take product over cycle lengths

The lognormal distribution

Theorem (L., 2009)

Let π be a random permutation in the sharp-cutoff model with parameter n . Then as $n \rightarrow \infty$,

$$\lim_{n \rightarrow \infty} \mathbb{P}_n^* \left(\frac{\log(F(\pi)) - \frac{1}{2}(\log n)^2}{\frac{1}{3}(\log n)^3} \leq x \right) \rightarrow \Phi(x).$$

I call this “Erdős-Turán-type” because the distribution of the order of a random permutation is the same; this result is due to Erdős and Turán. The order of a permutation is the least common multiple of its cycle lengths, so this may be a coincidence.

Sketch of the proof

- Let $\mu_k = \mathbb{E}(\log f(X_k, k))$. Then

$$\mu_k = e^{-1/k} \sum_{r \geq 1} \frac{1}{r!} \log f(r, k).$$

- From the Taylor series for $\log(1+x)$ get an asymptotic series for $\log f(r, k)$, and add, to get

$$\mu_k = \frac{\log k}{k} + \frac{1}{2k^3} - \frac{1}{4k^4} - \frac{1}{3k^5} + O(k^{-6}).$$

- Similarly derive an asymptotic series for $\mathbb{E}(\log^2 f(X_k, k))$ and $\mathbb{V}(\log f(X_k, k))$; $\mathbb{V}(\log f(X_k, k)) := \sigma_k^2 \sim (\log k)^2/k$

Sketch of the proof, continued

- $\mathbb{E}(\log F(\pi)) = \sum_{k=1}^n \mu_k \sim \sum_{k=1}^n (\log k)/k \sim \frac{1}{2}(\log n)^2$
- $\mathbb{V}(\log F(\pi)) = \sum_{k=1}^n \sigma_k^2 \sim \sum_{k=1}^n (\log^2 k)/k \sim \frac{1}{3}(\log n)^3$
- = holds since

$$\mathbb{E}(\log F(\pi)) = \mathbb{E}(\log \prod_{k=1}^n f(X_k, k)) = \mathbb{E} \sum_{k=1}^n \log f(X_k, k)$$
- The second \sim holds since

$$\int_{k=1}^n \frac{\log k}{k} dk = \frac{1}{2}(\log^2 n), \quad \int_{k=1}^n \frac{\log^2 k}{k} dk = \frac{1}{3}(\log^3 n)$$

(then Euler-Maclaurin summation)

- No individual term in the sum is too large, so we get normality (Lyapunov's theorem)

Why the sharp-cutoff model?

- Computationally simple. Finite sums, no weights to fight with. (In this respect it beats the Boltzmann model.)
- The X_k (number of cycles of each length) are independent.
- From numerical work: for random permutations of a fixed size

$$\lim_{n \rightarrow \infty} \mathbb{P}_n^* \left(\frac{\log(F(\pi)) - \frac{1}{2}(\log n)^2}{c(\log n)^3} \leq x \right) \rightarrow \Phi(x)$$

for some $c \approx 0.16$. (I don't think it's $1/6$.)

Some observations on the distribution

- The median of $F(\pi)$ is near $\exp(\frac{1}{2}(\log n)^2) = n^{(\log n)/2}$.
- But the mean is $e^{2\sqrt{n}}(8\pi en)^{-1/2}$ – much larger
- This indicates the distribution is very skewed!
- Permutations with many factorizations have lots of short cycles.
- A permutation of $n = k(k+1)/2$ with one cycle of each length $1, 2, \dots, k$ has $k! \approx (\sqrt{2n})^{\sqrt{2n}} \approx n^{\sqrt{n/2}} \approx \exp(\sqrt{n/2} \log n)$ factorizations.
- The identity permutation has $\approx \sqrt{n}!$ factorizations; one for each involution!
- Maybe typical compositions of involutions “look like” typical permutations with \sqrt{n} cycles?