

Counting permutations

Lecture 11

Matt Olechnowicz & Shuyang Shen

Department of Mathematics
University of Toronto

Jun 9, 2020 13–14 EDT

Whereas enumerating the elements of cyclic groups and dihedral groups isn't too difficult, enumerating the elements of symmetric groups is a lot more involved.

For example, the elements of D_n are all either r^k or fr^k for $0 \leq k < n$, so it's easy to count elements with a certain property, like a given order.

Indeed, we were able to compute φ_G for G cyclic or dihedral, finding that

$$\varphi_{C_n}(d) = \begin{cases} \varphi(d) & \text{if } d \mid n \\ 0 & \text{otherwise} \end{cases}$$

and

$$\varphi_{D_n}(2) = \begin{cases} n & \text{if } n \text{ is odd} \\ n+1 & \text{if } n \text{ is even} \end{cases}$$

while $\varphi_{D_n}(d) = \varphi_{C_n}(d)$ for $d \neq 2$.

Because the elements of S_n have much clunkier descriptions—two-line notation, disjoint cycle decomposition—they aren't so easy to enumerate. For example, there doesn't exist a simple formula for φ_{S_n} .

But hey—we *do* know that k -cycles have order k , so let's start by counting those, and see where to go from there.

Counting cycles

How would you write down a 4-cycle in S_5 ? It needs to be something of the form

$$(a \ b \ c \ d)$$

with $a, b, c, d \in \{1, 2, 3, 4, 5\}$ all distinct; and these 4 letters admit $4!$ orderings, but of course the cycles

$$(a \ b \ c \ d), \quad (b \ c \ d \ a), \quad (c \ d \ a \ b), \quad \text{and} \quad (d \ a \ b \ c)$$

are all the same function.

So it seems that we have $\binom{5}{4} = 5$ choices for the subset, and $4!$ ways to order it, but we get a new cycle only a quarter of the time.

These ideas are what's behind the next Proposition.

Proposition

The number of k -cycles in S_n is $\binom{n}{k} \frac{k!}{k}$.

Proof.

There are $\binom{n}{k}$ ways to pick the k elements to be cyclically permuted.

Since a cycle can be written in multiple ways by “rotating”, there is always a representation in which the first element is smallest.

Once that's fixed, there are $(k - 1)!$ ways to order the remaining elements. ■

Example

The number of 4-cycles in S_5 is

$$\binom{5}{4} \cdot \frac{4!}{4} = 5 \cdot 6 = 30.$$

Here they are:

subset	cycles
$\{1, 2, 3, 4\}$	$(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$
$\{1, 2, 3, 5\}$	$(1\ 2\ 3\ 5), (1\ 2\ 5\ 3), (1\ 3\ 2\ 5), (1\ 3\ 5\ 2), (1\ 5\ 2\ 3), (1\ 5\ 3\ 2)$
$\{1, 2, 4, 5\}$	$(1\ 2\ 4\ 5), (1\ 2\ 5\ 4), (1\ 4\ 2\ 5), (1\ 4\ 5\ 2), (1\ 5\ 2\ 4), (1\ 5\ 4\ 2)$
$\{1, 3, 4, 5\}$	$(1\ 3\ 4\ 5), (1\ 3\ 5\ 4), (1\ 4\ 3\ 5), (1\ 4\ 5\ 3), (1\ 5\ 3\ 4), (1\ 5\ 4\ 3)$
$\{2, 3, 4, 5\}$	$(2\ 3\ 4\ 5), (2\ 3\ 5\ 4), (2\ 4\ 3\ 5), (2\ 4\ 5\ 3), (2\ 5\ 3\ 4), (2\ 5\ 4\ 3)$

Counting permutations of a given cycle type

As we've seen, not every permutation is a cycle. Yet to go from counting cycles to counting everything is too big of a leap, so let's start small.

Exercise

Write down all the non-cyclic permutations of S_4 (other than the identity).

You should have found just three of them:

$$(1\ 2)(3\ 4), \quad (1\ 3)(2\ 4), \quad \text{and} \quad (1\ 4)(2\ 3).$$

Note they all have the form $(a\ b)(c\ d)$.

Example

Let's count permutations of the form $(a\ b)(c\ d)$ in S_5 .

There are $5!$ ways to list the 5 numbers in some order

$$a\ b\ c\ d\ e$$

However, the 2-cycles $(a\ b)$ and $(c\ d)$ commute (because they are disjoint), so

$$(a\ b)(c\ d) = (c\ d)(a\ b),$$

giving 2 ways of writing one permutation.

Another redundancy is that there are 2 ways to write each constituent cycle, namely

$$(a\ b) = (b\ a) \quad \text{and} \quad (c\ d) = (d\ c).$$

Example (continued...)

This gives 4 more ways to write one permutation:

$$(a\ b)(c\ d) = (b\ a)(c\ d) = (a\ b)(d\ c) = (b\ a)(d\ c).$$

These two redundancies don't interact, because the first one commutes the cycles around each other while the second one rotates the cycles in place.

Overall, therefore, each individual permutation is counted $2 \cdot 4 = 8$ times, so we have $\frac{5!}{8} = 15$ distinct permutations of the form $(a\ b)(c\ d)$ in S_5 .

Exercise

What are they?

The ideas from this example can be generalized to give a proof of the next Proposition.

Proposition

The number of permutations in S_n with cycle type $(c_1, c_2, \dots, c_n)$ is

$$\frac{n!}{\prod_l l^{c_l} c_l!}$$

where the product ranges over $l = 1, \dots, n$.

Remark

Note that if $c_l = 0$ then $l^{c_l} c_l! = l^0 0! = 1$, so we can ignore such terms.

Example

4-cycles in S_5 have cycle type $(1, 0, 0, 1, 0)$. By the formula, the number of 4-cycles in S_5 is

$$\frac{5!}{1^1 1! \cdot 4^1 1!} = \frac{5!}{4} = 30,$$

as we saw before.

Example

Permutations of the form $(a\ b)(c\ d)$ in S_5 have cycle type $(1, 2, 0, 0, 0)$. By the formula, their number is

$$\frac{5!}{2^2 2!} = \frac{120}{8} = 15$$

as we saw before.

Exercise

How many permutations of the form $(a\ b)(c\ d\ e)$ are there in S_5 ?
Can you list them?

Counting cycle types

Now that we can count the number of permutations of a given cycle type, a natural question presents itself:

What are all the possible cycle types of permutations on n letters?

Exercise

Answer the question for $n = 4$.

The key to enumerating the possible cycle types in S_n lies in the counting formula

$$\sum_{l \geq 1} l c_l = n.$$

Written in full, the counting formula says

$$\underbrace{1 + \cdots + 1}_{c_1} + \underbrace{2 + \cdots + 2}_{c_2} + \underbrace{3 + \cdots + 3}_{c_3} + \cdots = n.$$

Thus, each cycle type gives rise to a *partition* of n —a way to write n as a sum of positive integers (order not mattering).

Example

n	partitions	n	partitions
1	1	4	1 + 1 + 1 + 1
2	1 + 1		1 + 1 + 2
	2		2 + 2
3	1 + 1 + 1		1 + 3
	1 + 2		4
	3		

Conversely, each partition

$$n = a_1 + \cdots + a_k$$

gives rise to a cycle type by letting c_l be the number of a 's that equal l . Thus, we have proved:

Proposition

The number of cycle types in S_n equals the number of partitions of n .

Example

The partitions of 5 and the corresponding cycle types are

$5 = 1 + 1 + 1 + 1 + 1$	$(5, 0, 0, 0, 0)$
$= 1 + 1 + 1 + 2$	$(3, 1, 0, 0, 0)$
$= 1 + 1 + 3$	$(2, 0, 1, 0, 0)$
$= 1 + 2 + 2$	$(1, 2, 0, 0, 0)$
$= 2 + 3$	$(0, 1, 1, 0, 0)$
$= 1 + 4$	$(1, 0, 0, 1, 0)$
$= 5$	$(0, 0, 0, 0, 1)$

Exercise

To which partition of 4 does the cycle type $(1, 0, 1, 0)$ correspond?

The number of partitions of n is known as the *partition function* $p(n)$. There is no simple formula for $p(n)$, but here is a list of values for small n :

n	1	2	3	4	5	6	7	8	9	10
$p(n)$	1	2	3	5	7	11	15	22	30	42

The symmetric totient function

Unfortunately, there is no nice formula for $\varphi_{S_n}(d)$, the number of elements of order d in S_n . [See [here](#).]

But for any given n and d , we *can*, in theory, compute $\varphi_{S_n}(d)$ using everything we've learned so far.

Here's the procedure. For each partition of n ,

- (i) obtain the corresponding cycle type $(c_1, \dots, c_n)$
- (ii) compute the order of any permutation of that type using the $\text{lcm}\{l : c_l > 0\}$ formula
- (iii) count the number of permutations of that type using the $n! / \prod_l l^{c_l} c_l!$ formula

Example

S_2 has $p(2) = 2$ distinct cycle types:

partition	cycle type	order	number
1 + 1			
2			

Therefore $\varphi_{S_2}(1) = 1$ and $\varphi_{S_2}(2) = 1$.

Example

S_3 has $p(3) = 3$ distinct cycle types:

partition	cycle type	order	number
$1 + 1 + 1$			
$1 + 2$			
3			

Therefore

d	1	2	3
$\varphi_{S_3}(d)$	1		

Example

S_4 has $p(4) = 5$ distinct cycle types:

partition	cycle type	order	number
$1 + 1 + 1 + 1$			
$1 + 1 + 2$			
$1 + 3$			
$2 + 2$			
4			

Therefore

d	1	2	3	4
$\varphi_{S_4}(d)$	1			

Example

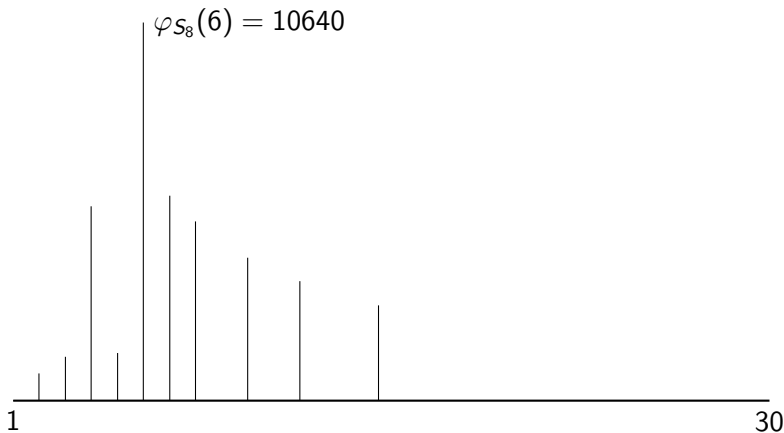
partition	cycle type	order	number
$1 + 1 + 1 + 1 + 1$			
$1 + 1 + 1 + 2$			
$1 + 1 + 3$			
$1 + 2 + 2$			
$2 + 3$			
$1 + 4$			
5			

Therefore

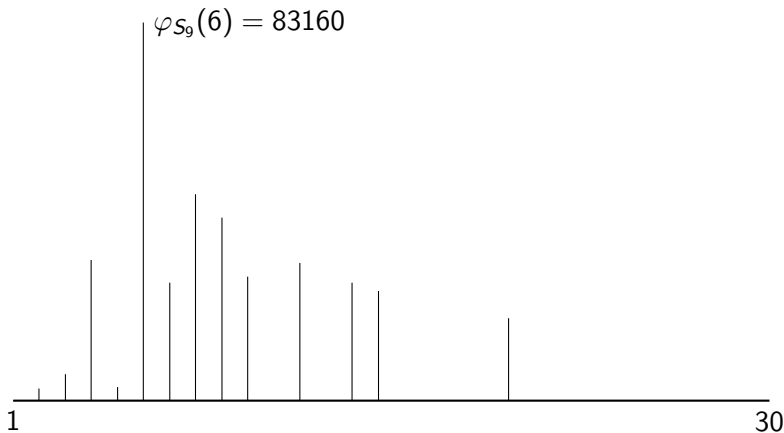
d	1	2	3	4	5	6
$\varphi_{S_5}(d)$	1					

On Homework 3 you will do the above for S_6 .

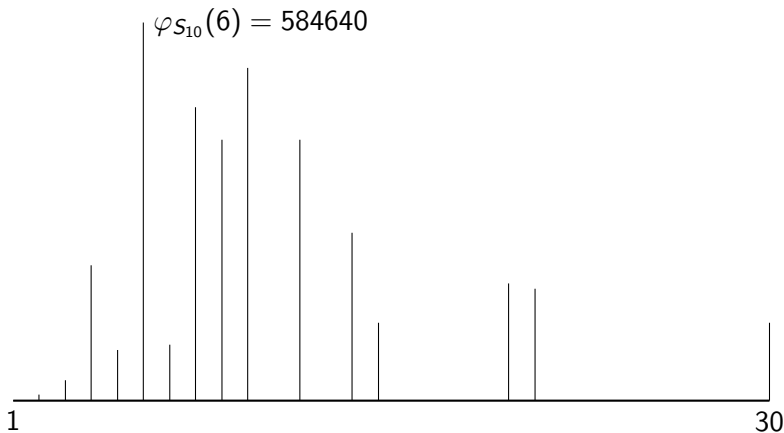
The symmetric totient function is highly unpredictable. Here are some plots of φ_{S_n} for various n , along with their maximum values.



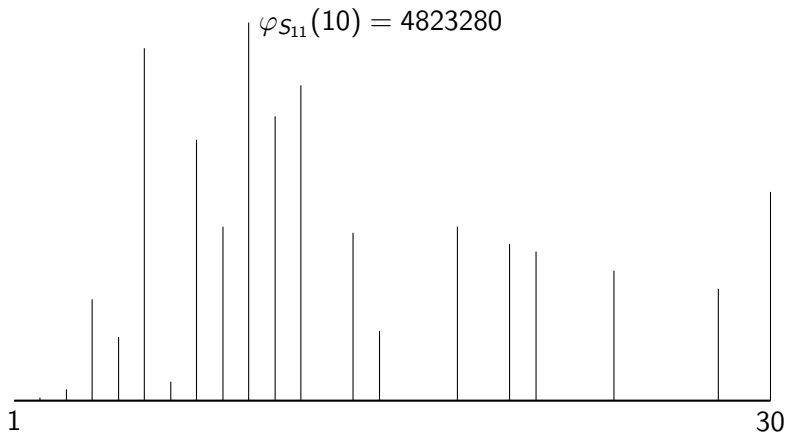
The symmetric totient function is highly unpredictable. Here are some plots of φ_{S_n} for various n , along with their maximum values.



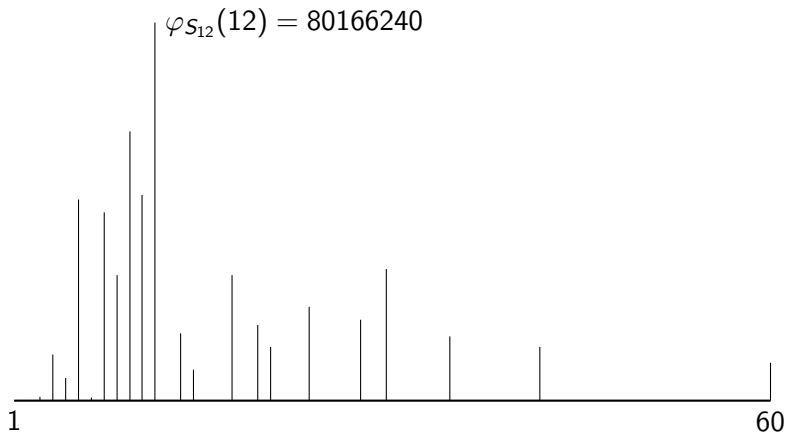
The symmetric totient function is highly unpredictable. Here are some plots of φ_{S_n} for various n , along with their maximum values.



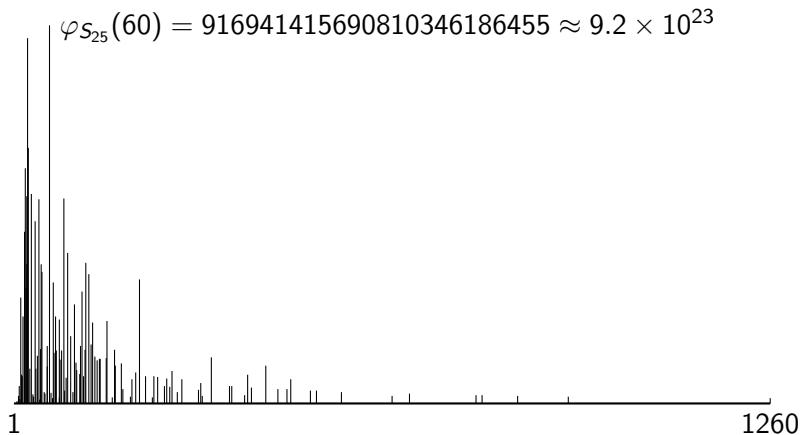
The symmetric totient function is highly unpredictable. Here are some plots of φ_{S_n} for various n , along with their maximum values.



The symmetric totient function is highly unpredictable. Here are some plots of φ_{S_n} for various n , along with their maximum values.



The symmetric totient function is highly unpredictable. Here are some plots of φ_{S_n} for various n , along with their maximum values.



Landau's function

What's the largest possible order of a permutation on n letters? In other words, what is

$$g(n) = \max\{o(\sigma) : \sigma \in S_n\}?$$

Based on our examples above, we know

n	1	2	3	4	5
$g(n)$	1	2	3	4	6

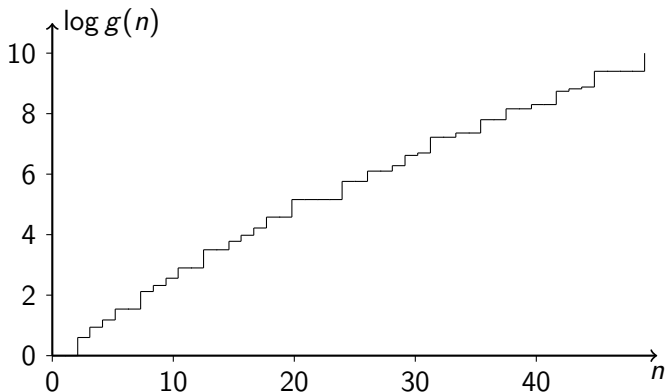
but these initial data are a misleading indicator of the growth of g ; it's not hard to show that $g(7) = 12$, $g(15) = 105$, and $g(36) = 13860$.

g is known as *Landau's function*, after the German number theorist Edmund Landau who, in 1902, proved that

$$\log g(n) \sim \sqrt{n \log n} \quad (n \rightarrow \infty)$$

so that $g(n) \approx e^{\sqrt{n \log n}}$ for large n .

Landau's function is very strange—although it never decreases, there are arbitrarily long stretches where it doesn't increase, either. It's just flat. Here is a plot of the growth of $\log g(n)$ for $n < 48$.



Even more intriguing is its unexpected connection to the [Riemann hypothesis](#). While the Prime Number Theorem says that the number of primes up to x is asymptotic to

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \quad (x \rightarrow \infty)$$

the Riemann hypothesis is equivalent to the inequality

$$g(n) < \sqrt{\text{Li}^{-1}(n)}$$

for all large n .

The exponent of the symmetric group

We can also compute the exponent of the first five symmetric groups. By the formula you proved in Homework 2,

$$\exp(G) = \text{lcm}\{o(g) : g \in G\},$$

we have

n	1	2	3	4	5
$\exp(S_n)$	1	2	6	12	60

Exercise

Show that $\exp(S_n) = \text{lcm}\{1, 2, \dots, n\}$ for all $n \geq 1$.

[You may not appeal to this Exercise on Homework 3.]