Math 4990: Permutations, Cycles

10/6

Ch. 6

Reminders: • HW#2 is due today

• Midterm 1 is posted, due in a week (11/13)

Today we'll discuss permutations in more detail.

We have so far considered a permutation of $[n]$ to be a word (or list) $p_1 p_2 \cdots p_n$ where $p_i \in [n]$ and each $i \in [n]$ is used once.

e.g. 326541 is a perm. of $[6]$

(one-line notation)

But there's another way to think of permutations: as functions $p: [n] \to [n]$ where $p(i) = p_i$.

---

e.g.

(two-line notation)

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 2 & 6 & 5 & 4 & 1 \end{array}$$

In fact, permutations on $[n]$ = bijections $[n] \to [n]$

Viewing permutations p and q as functions, we can compose them to get another permutation $p \cdot q$: $(p \cdot q)(i) = p(q(i))$.

e.g. $p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $p \cdot q$: $\begin{array}{cccc} & 1 & 2 & 3 \\ q & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 \\ p & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 \end{array} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

In this way, permutations on $[n]$ form what is called a group in algebra. Actually, the name of the group of perm's is the symmetric group, denoted S_n.

Let $p \in S_n$. We can compose p with itself to make $p \cdot p =: p^2$, and similarly

$$\underbrace{p \cdot p \cdot p \cdots p}_{m \text{ terms}} =: p^m \quad \text{for } m \geq 1.$$

What do these iterates p^m look like?

<u>Prop.</u> For any $i \in [n]$, there exists $m \geq 1$ so that $p^m(i) = i$.

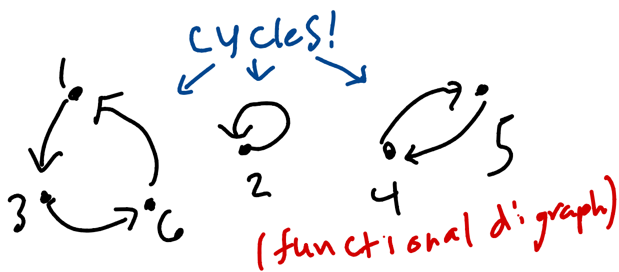
<u>Pf</u>: <u>Pigeon-hole principle!</u> Since $[n]$ is finite, there must be $j > k \geq 1$ so that $p^j(i) = p^k(i)$. Then apply <u>inverse</u> of $p^k = p^{-k}$ to both sides:

$p^{j-k}(i) = i$. ✓ $\square$

So if we keep applying p, from any initial point we'll eventually get back where we started.

Easiest to understand via a picture:

e.g.,
$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix} \iff$$



We see that any permutation decomposes into a union of cycles. This leads to another notation for permutations called cycle notation:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix} \Longleftrightarrow p = (1\,3\,6)(2)(4\,5)$$

think $1 \to 3 \to 6$, $6 \to 1$

Note that there are multiple ways to write a permutation in cycle notation:

$$(1\,3\,6)(2)(4\,5) = (5\,4)(6\,1\,3)(2) = \cdots$$

If we want to fix one particular choice, we can use canonical cycle notation:

- greatest element of every cycle is 1st,
- cycles written in increasing order of their greatest elements L-to-R.

e.g. $p = (\underline{2})(\underline{5}\,4)(\underline{6}\,1\,3)$ ← canonical since $2 < 5 < 6$

<u>Def'n</u> Let $\lambda = (\lambda_1, \dots, \lambda_k)$ be a partition of n. We say that permutation $p \in S_n$ has cycle type (or just type) λ if it has (exactly) k cycles of sizes $\lambda_1, \lambda_2, \dots, \lambda_k$.

<u>e.g.</u> $p = (2)(54)(613)(87)$ has type $(3,2,2,1)$

We can count permutations by type

<u>Thm</u> The number of $p \in S_n$ of type λ

$$= \boxed{\frac{n!}{a_1!\,1^{a_1}\,a_2!\,2^{a_2}\cdots a_n!\,n^{a_n}}},$$ where

$a_i = \#$ of i's in λ for $i = 1, \dots, n$.

<u>e.g.</u> $\lambda = (3,2,2,1)$, $a_1 = 1$, $a_2 = 2$, $a_3 = 1$,
$a_m = 0$ $m > 3$

So # perms of type λ $= \dfrac{8!}{1!\,1^1\,2!\,2^2\,1!\,3^1} = \dfrac{8!}{2!\cdot 4\cdot 3!} = 4\cdot 7\cdot 6\cdot 5$
$= 840$

<u>Pf of thm:</u> We'll do a "proof by example". Say $a_1 = 3,\ a_2 = 0,\ a_3 = 2,\ a_4 = 1,\ a_5 = a_6 = \cdots = 0$

To make a perm. of this cycle type, start with any permutation in one-line notation:

$$9\ \ 1\ \ 7\ \ 12\ \ 4\ \ 10\ \ 8\ \ 6\ \ 5\ \ 13\ \ 2\ \ 3\ \ 11$$

Then draw parentheses around a_1 groups of 1 #, a_2 groups of 2, a_3 groups of 3 #'s, etc.:

$$(9)(1)(7)(12\ \ 4\ \ 10)(8\ \ 6\ \ 5)(13\ \ 2\ \ 3\ \ 11)$$

We'll make all perm.'s of type λ this way, but we'll over count:

3 ways to cycle   3 ways to cycle   4 ways to cycle

$$(9)(1)(7)(12\ \ 4\ \ 10)(8\ \ 6\ \ 5)(13\ \ 2\ \ 3\ \ 11)$$

3! ways to permute   2! ways to permute

Dividing $n!$ by $a_1!\,1^{a_1}\,a_2!\,2^{a_2}\,a_3!\,3^{a_3}\cdots$ exactly accounts for the overcounting. $\square$

What if we want to group perm.'s in a coarser way: by **# of cycles**.

Def'n $c(n,k) := \#\, p \in S_n$ w/ k cycles

e.g. $n=3$

$(1)(2)(3)$	$(12)(3)$ $(13)(2)$ $(1)(23)$	(123) (132)
$c(3,3)=1$	$c(3,2)=3$	$c(3,1)=2$

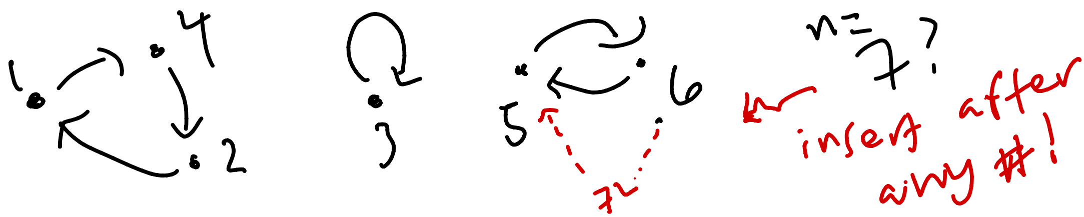
$c(n,k)$ are called **(signless) Stirling #'s of 1st kind.**

They satisfy similar recurrence to $S(n,k)$:

Prop. $c(n,k) = c(n-1,k-1) + (n-1)\cdot c(n-1,k)$

Pf: To make a $p \in S_n$ w/ k cycles from a $p' \in S_{n-1}$, either we add n as a **fixed point** (so p' had $k-1$ cycles), or we stick n **into** a cycle in p' (so p' had k cycles).

There are $(n-1)$ ways to stick n into a cycle:



$\boxtimes$

+ Similar algebraic formula for $c(n,k)$:

<u>Thm</u> $$\sum_{k=1}^{n} c(n,k)\, x^k = x(x+1)\cdots(x+(n-1))$$

<u>Pf</u>: We'll prove by induction, using recurrence.

Let $f_n(x) := x(x+1)\cdots(x+(n-1)) = \sum_{k=1}^{n} a_{n,k}\, x^k$.

Then $f_n(x) = f_{n-1}(x)\cdot(x+(n-1))$

$$\Rightarrow \sum a_{n,k}\, x^k = \left(\sum a_{n-1,k}\, x^k\right)\cdot(x+(n-1))$$

$$= \sum a_{n-1,k}\, x^{k+1} + (n-1)\cdot\sum a_{n-1,k}\, x^k$$

$$= \sum a_{n-1,k-1}\, x^k + \sum (n-1)\cdot a_{n-1,k}\, x^k$$

$$= \sum \left(a_{n-1,k-1} + (n-1)\, a_{n-1,k}\right) x^k$$

Extract coefficient of x^k in this equality:

$$a_{n,k} = a_{n-1,k-1} + (n-1)\, a_{n-1,k}$$

$\Rightarrow$ $a_{n,k}$ satisfy the same recurrence as $c(n,k)$.

Easy to check base cases agree too. ✓ $\boxtimes$

On worksheet you'll give a combinatorial pf of thm.

Recall (*) $\displaystyle\sum_{k=1}^{n} S(n,k)\,(x)_k = x^n$, where

$$(x)_k := x(x-1)(x-2)\cdots(x-(k-1)) \quad \text{"falling factorial"}$$

In $\displaystyle\sum_{k=1}^{n} c(n,k)\, x^k = x(x+1)\cdots(x+(n-1))$

if we substitute $x := -x$ then we get

(**) $\displaystyle\sum_{k=1}^{n} s(n,k)\, x^k = (x)_n$, where $s(n,k) := (-1)^{n-k} c(n,k)$

are the signed Stirling #'s of 1st kind.

Eqn's (*) and (**) say $S(n,k)$ and $s(n,k)$ are inverse "change of basis" coefficients. (between x^n and $(x)_n$)

Another very powerful tool for understanding the cycle structure of permutations is the so-called "fundamental bijection" (Foata). It's a bijection $S_n \to S_n$ that goes as follows:
$p \mapsto \hat{p}$

- write $p \in S_n$ in canonical cycle notation
- erase the parentheses + interpet in 1-line notation.

Eg: $p = (\underline{2})(\underline{5}\,4)(\underline{6}\,1\,3) \to \hat{p} = 254613$

canonical!

$(= (1\,2\,5)(3\,4\,6))$

Why is $p \to \hat{p}$ a bijection?

Given $\hat{p}$ look for left-to-right maxima: #'s > all #'s to their left.

e.g. $\hat{p} = \underline{2}\,\underline{5}\,4\,\underline{6}\,1\,3$ ← LR maxima underlined

These tell you where to place ('s.

$p = (\underline{2})(\underline{5}\,4)(\underline{6}\,1\,3)$

//

$p \to \hat{p}$ lets us understand typical cycle structure.

<u>Prop</u>. For any $i \in [n]$, Prob. that i is in a k-cycle ($1 \le k \le n$) in a random $p \in S_n$ is $\frac{1}{n}$.

<u>Pf</u>. Since all $i \in [n]$ 'look the same' up to relabeling, can prove this for $i = n$. Then n is in a k-cycle in p iff n is the k^{th} to last letter in $\hat{p}$:

e.g. $p = (2)(541)(613) \to \hat{p} = 254613$ 3rd to last letter!

6 is in 3-cycle

But clearly n is k^{th} to last letter $\frac{1}{n}$ of the time! $\boxtimes$

<u>Cor</u> Avg. # of k-cycles in random $p \in S_n = \frac{1}{k}$

<u>Pf</u>. # of k-cycles in $p \in S_n = \frac{1}{k} \cdot \#\, i \in [n]$ in a k-cycle in p

by prev. prop.

So avg # of k cycles $= \frac{1}{k} \cdot n \cdot \frac{1}{n} = \frac{1}{k}$. ✓ $\boxtimes$

<u>Cor</u>. Avg. # of cycles in a random $p \in S_n$

$= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \sim \log(n)$. //

Now let's take a break...

And when we come back, let's work in breakout groups on the worksheet, where you'll use the fund. bij. $p \to \hat{p}$ to give a combinatorial proof of

$$\sum_{k=1}^{n} C(n,k)\, x^{k} = x(x+1)\cdots(x+(n-1))$$