Aula 20: Aspectos enumerativos do grupo simétrico: Permutações, ciclos e números de Stirling de primeira espécie

oazenhas

Abril 21, 2015

Permutações

Definição *Seja X um conjunto finito. Uma permutação de X é uma ordenação qualquer dos elementos de X, isto é, uma palavra no alfabeto X usando toda as letras uma única vez. Equivalentemente, é uma bijecção $X \to X$.*

Usualmente consideramos $X = \{1, \ldots, n\}$. As permutações podem ser entendidas como ordenações lineares de objectos distintos, usualmente elementos de $\{1, \ldots, n\}$, ou como bijecções de $\{1, \ldots, n\}$ para $\{1, \ldots, n\}$.
A permutação $a_1 a_2 \cdots a_n$, escrita na forma de uma palavra, dos elementos do conjunto $\{1, \ldots, n\}$, pode ser vista como sendo a única função (bijectiva) $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ tal que $\sigma(i) = a_i$, $i = 1, \ldots, n$,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

Por outro lado, toda a permutação σ, entendida como função bijectiva $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, pode ser representada pela palavra $\sigma = \sigma(1)\sigma(2)\cdots\sigma(n)$
Exemplo $n = 6$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix} = 234165$$

Permutações

- O produto de permutações, entendido como composição de funções, é novamente uma permutação

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 5 & 2 & 6 \end{pmatrix}$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 6 & 2 \end{pmatrix}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 6 & 3 & 5 \end{pmatrix}$$

$$\sigma\tau(i) := \sigma(\tau(i))$$

- *O produto de permutações não é uma operação comutativa.* Em geral, $\tau\sigma \neq \sigma\tau$.

  (Recorde a definição de matriz de permutação e note que o produto de permutações corresponde ao produto das respectivas matrizes de permutação. Como sabe o produto de matrizes não é uma operação comutativa.)

Grupo simétrico de ordem n

- A permutação identidade $id = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.
- Toda a permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$ tem uma inversa (única) σ^{-1}, com respeito à operação composição, isto é, $\sigma\sigma^{-1} = \sigma^{-1}\sigma = id$,
$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$
$$\sigma^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 & 6 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}$$
$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = id = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$
- A composição é uma operação asociativa $(\sigma\tau)\xi = \sigma(\tau\xi)$.
- O conjunto de todas as permutações de $\{1, 2, \ldots, n\}$ com a composição de funções tem estrutura de grupo e é chamado o *grupo simétrico de ordem n*, denotado usualmente por $\mathfrak{S}_n$. $\mathfrak{S}_n$ é um grupo não comutativo par $n \geq 3$. O número de elementos deste grupo é $n!$.

Ciclos e permutações

Definição Uma permutação cíclica, ou simplesmente ciclo, de comprimento k, é uma permutação da forma

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ a_2 & a_3 & \cdots & a_k & a_1 \end{pmatrix}$$

que denotaremos por $(a_1\, a_2\, \cdots\, a_k)$. Um ciclo de comprimento 1, (a_1), é dito um ponto fixo. Um ciclo de comprimento dois é chamado uma transposição $\begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$.

O ciclo acima $\pi = (a_1\, a_2\, \cdots\, a_k)$ pode ser visualizado por

$$- - - - - - - - - - -$$

$$\downarrow \qquad\qquad\qquad\qquad\qquad\qquad |$$

$$a_1 \to a_2 \to \cdots \to a_{k-1} \to a_k$$

$$\pi(a_1) = a_2 \quad \pi(a_2) = a_3 \quad \ldots \quad \pi(a_k) = a_1$$

Note que, $\pi^k(a_i) = a_i$, $i = 1, \ldots, k$, e se $k|m$ então $\pi^m(a_i) = a_i$, $i = 1, \ldots, k$.

Ciclos e permutações

Exemplo

- Ciclo de comprimento 4

$$\pi = \begin{pmatrix} 2 & 4 & 7 & 8 \\ 4 & 7 & 8 & 2 \end{pmatrix} = (2\,4\,7\,8)$$

  Note que $\pi(2) = 4$, $\pi^2(2) = 7$, $\pi^3(2) = 8$, $\pi^4(2) = 2$, quatro é o menor inteiro positivo m tal que $\pi^m(2) = 2$. Qual é o menor inteiro positivo m tal que $\pi^m(4) = 4$?

- $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$$

$$\begin{array}{lll} \sigma(1) = 3, & \sigma^2(1) = 1 & \sigma(2) = 2 \\ \sigma(4) = 5, & \sigma^2(4) = 6, & \sigma^3(4) = 4 \end{array}$$

  σ permuta os elementos $1, 3$ entre eles, fixa 2, e permuta os elementos $4, 5, 6$ entre eles.

$$\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} = (1\ 3) = (1\ \sigma(1))$$

$$(2)$$

$$\begin{pmatrix} 4 & 5 & 6 \\ 5 & 6 & 4 \end{pmatrix} = (4\ \ \sigma(4)\ \ \sigma^2(4)) = (4\ 5\ 6)$$

Ciclos e permutações

Lema *Se* $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ *é uma permutação e* $x \in \{1, 2, \ldots, n\}$, *então existe um inteiro positivo* $1 \leq i \leq n$ *tal que* $\sigma^i(x) = x$.

Prova Consideremos $x, \sigma(x), \sigma^2(x), \ldots, \sigma^n(x)$. Pelo princípio do pombal, se temos $n + 1$ bolas e n caixas, então, ou $\sigma^i(x) = x$, para algum $1 \leq i \leq n$, ou $\sigma^j(x) = \sigma^k(x)$, com $1 \leq j < k \leq n$.
No último caso, aplicando σ^{-1} a ambos lados desta igualdade, j vezes, temos

$$x = (\sigma^{-1})^j \sigma^j(x) = (\sigma^{-1})^j \sigma^j \sigma^{k-j}(x) = \sigma^{k-j}(x).$$

Ou seja, $\sigma^{k-j}(x) = x$, com $1 \leq k - j < n$. $\square$

Seja $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ uma permutação e $x \in \{1, 2, \ldots, n\}$. Seja i o menor inteiro positivo tal que $\sigma^i(x) = x$ e consideremos o conjunto $S = \{x, \sigma(x), \ldots, \sigma^{i-1}(x)\}$. Note que $\sigma^r(x) \neq \sigma^s(x)$, $1 \leq r < s \leq i - 1$. Caso contrário, $\sigma^{s-r}(x) = x$ com $1 \leq s - r < i$. Então

$$(x\, \sigma(x)\, \sigma^2(x)\ \ldots\ \sigma^{i-1}(x))$$

é uma permutação cíclica do conjunto S.

Vamos provar que este ciclo é o único ciclo de σ que contém x.

Exemplo $\begin{pmatrix} 4 & 5 & 6 \\ 5 & 6 & 4 \end{pmatrix} = (4\ \ \sigma(4)\ \ \sigma^2(4)) = (4\ 5\ 6)$ é o único ciclo de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$$

que contém 4.

Lema. Dado $\sigma \in \mathfrak{S}_n$, todo o elemento de $\{1, 2, \ldots, n\}$ é membro de um único ciclo de σ.

Prova. Seja $x \in \{1, 2, \ldots, n\}$ e i o menor inteiro positivo tal que $\sigma^i(x) = x$. Então

$$(x,\, \sigma(x)\, \sigma^2(x)\; \ldots\; \sigma^{i-1}(x))$$

é um ciclo de σ, com comprmento i, contendo x.
Da definição de ciclo concluímos que σ permuta os elementos de $S = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{i-1}(x)\}$ entre si.
Se $y = \sigma(x)$, então i é o menor inteiro positivo tal que $\sigma^i(y) = y$, e $(y\, \sigma(y)\; \ldots\; \sigma^{i-1}(y))$ é um ciclo de comprimento i,

$$\begin{aligned}(y\, \sigma(y)\; \ldots\; \sigma^{i-1}(y)) &= (\sigma(x)\, \sigma^2(x) \ldots \sigma^{i-1}(x)\, \sigma^i(x) = x) \\ &= (x\, \sigma(x)\; \ldots \sigma^{i-1}(x))\end{aligned}$$

que é precisamente o ciclo de comprimento i acima.
Em geral, se $y = \sigma^j(x)$, $1 \leq j \leq i-1$, i é o menor inteiro positivo tal que $\sigma^i(y) = y$,

$$\begin{gathered}(y\, \sigma(y)\; \ldots\; \sigma^{i-1}(y)) = \\ = (\sigma^j(x)\, \sigma^{j+1}(x)\; \ldots\; \sigma^{j+i-j}(x) = x\; \sigma(x)\; \ldots\; \sigma^{j+i-1}(x) = \sigma^{j-1}(x)) \\ = (x\, \sigma(x)\, \sigma^2(x)\; \ldots\; \sigma^{i-1}(x))\end{gathered}$$

é o ciclo de comprimento i acima. Portanto, cada elemento da permutação σ pertence a um e um só ciclo de σ. $\square$

Se σ_1 e σ_2 são ciclos distintos de σ então são permutações cíclicas de subconjuntos disjuntos de $\{1, \ldots, n\}$ e dizemos que σ_1 e σ_2 são ciclos disjuntos. Os ciclos de σ definem então uma partição de $\{1, \ldots, n\}$.

Exemplo Os ciclos de 321564 são $(3\,1)$, (2) e $(5\,6\,4)$. Ou seja $\{1, 3\}$, $\{2\}$, e $\{4, 5, 6\}$ definem uma partição de $\{1, 2, 3, 4, 5, 6\}$.

Ciclos distintos σ_1 e σ_2 de σ são permutações cíclicas de subconjuntos disjuntos S_1 e S_2 de $\{1, \ldots, n\}$. Então, pondo $\sigma_1(x) = x$ para $x \in \{1, \ldots, n\} \setminus S_1$, e $\sigma_2(x) = x$ para $x \in \{1, \ldots, n\} \setminus S_2$, concluímos que σ_1 e σ_2 comutam,

$$\sigma_1 \sigma_2 = \sigma_2 \sigma_1.$$

Podemos então escrever

Corolário. *Dado $n \geq 1$, toda a permutação $\sigma \in \mathfrak{S}_n$ pode ser decomposta de modo único, a menos da ordem, em ciclos dois a dois disjuntos, $\sigma_1, \sigma_2, \ldots, \sigma_k$, isto é,*
- cada ciclo σ_i tem comprimento ≥ 1,
- quaisquer dois ciclos σ_i, σ_j não têm elementos em comum,
- $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$.

Decomposição cíclica de $321564 = (31)(2)(564)$.

Forma canónica da decomposição cíclica

- Um ciclo pode ser escrito de várias maneiras:
  $(31) = (13)$, $\sigma(3) = 1$, $\sigma(1) = 3$,
  $(564) = (645) = (456)$ $\sigma(5) = 6$ $\sigma(6) = 4$ $\sigma(4) = 5$;
  e o produto de dois ciclos disjuntos comuta. $(564)(31) = (31)(564)$
- O ciclo $(a_1\, a_2, \ldots, a_k)$ pode ser escrito de k maneiras distintas.

Forma canónica da decomposição cíclica

- *Forma canónica da decomposição cíclica*: cada ciclo é escrito com o seu maior elemento em primeiro lugar e os ciclos são escritos por ordem crescente dos seus primeiros elementos.

$$2135647 = (21)(3)(645)(7)$$

$$2451376 = (412)(53)(76)$$

Tipo de uma permutação

- Uma permutação σ de $\mathfrak{S}_n$ diz-se do tipo $(a_1, a_2, \ldots, a_n)$, onde $1.a_1 + 2.a_2 + 3.a_3 + \cdots + n.a_n = n$, se tem a_i ciclos de comprimento i, para $i = 1, \ldots, n$.
- $n = 9$

  $\sigma = (35146)(879)(2)$ é do tipo $(1, 0, 1, 0, 1, 0, 0, 0, 0)$,

  $\sigma = (351468)(7)(9)(2)$ é do tipo $(3, 0, 0, 0, 0, 1, 0, 0, 0)$,

  $\sigma = (351468792)$ é do tipo $(0, 0, 0, 0, 0, 0, 0, 0, 1)$,

  $id = (3)(5)(1)(4)(6)(8)(7)(9)(2)$ é do tipo $(9, 0, 0, 0, 0, 0, 0, 0, 0)$.
- Quando a permutação de $\mathfrak{S}_n$ só é constuituída apenas por ciclos de comprimento 1 é do tipo $(n, 0, \ldots, 0)$ e temos a permutação identidade.
- Uma permutação de $\mathfrak{S}_n$ é do tipo $(0, \ldots, 0, 1)$ se e só se é um ciclo de comprimento n.

- Quantos ciclos distintos de comprimento 4 podemos formar em $\{1, 2, 3, 4\}$? E quantos ciclos distintos de comprimento n podemos formar em $\{1, 2, \ldots, n\}$?

  Todo o ciclo, na notação ciclíca, pode ser escrito com o seu maior elemento em primeiro lugar. Basta escrever todos os ciclos de comprimento 4, no conjunto $\{1, 2, 3, 4\}$, pondo o 4 em primeiro lugar: $(4\,a\,b\,c)$ onde abc percorre todas as permutações de $\{1, 2, 3\}$. No total temos 3! ciclos de comprimento 4 no conjunto $\{1, 2, 3, 4\}$.,

  $$(4\,1\,2\,3) \quad (4\,2\,1\,3) \quad (4\,1\,3\,2) \quad (4\,2\,3\,1) \quad (4\,3\,2\,1) \quad (4\,3\,1\,2).$$

  Esta pergunta é o mesmo que perguntar de quantas maneiras podemos sentar n pessoas à volta de uma mesa circular, assumindo que as cadeiras estão igualmente espaçadas à volta desta e que não distiguimos uma mesa que se obtenha desta por uma rotação qualquer das pessoas à volta da mesma.

  Senta-se em primeiro lugar a pessoa designada por n, e as restantes $n - 1$ pessoas podem ser sentadas de $(n - 1)!$ maneiras nos restantes $n - 1$ lugares.

  Os ciclos distintos são $(n\,a_1 \cdots a_{n-1})$ onde $a_1 \cdots a_{n-1}$ é uma permutação qualquer de $\{1, \ldots, n - 1\}$.

Fórmula para o número de permutações de um dado tipo

Quantas permutações de n elementos do tipo $(0, 0, \ldots, 0, 1)$, isto é, que constituem um ciclo de comprimento n, existem?

$$(n-1)!$$

Proposição O número de permutações de n elementos do tipo $(a_1, a_2, \ldots, a_n)$, isto é, com a_1 ciclos de comprimento 1, a_2 ciclos de comprimento 2, $\ldots$, a_n ciclos de comprimento n, é

$$\frac{n!}{a_1! 1^{a_1} a_2! 2^{a_2} \ldots a_n! n^{a_n}}.$$

Contar permutações de um tipo dado

- Escrevamos os números de 1 até n numa linha por uma odem qualquer, em seguida, indo da esquerda para a direita inserimos pares de parenteses de acordo com o tamanho requerido dos ciclos: primeiro a_1 pares de parenteses para criar a_1 ciclos de comprimento 1; depois a_2 pares de parenteses para criar a_2 ciclos de comprimento 2, etc. Deste modo obtemos uma permutação do tipo requerido em que os comprimentos dos ciclos são crescentes da esquerda para a direita.

  Existem $n!$ maneiras de fazer isto – o número de maneiras de escrever os números de 1 até n numa linha, e existe uma só maneira de inserir os parenteses de modo a obter a sucessão de comprimentos descrita.

  Contudo existem diversas maneiras de escrever os n inteiros que conduzem à mesma permutação depois de inseridos os partenteses.

  Quantas?

Contar permutações de um tipo dado

- Contudo existem diversas maneiras de escrever os n inteiros que conduzem a mesma permutação depois de inseridos os parenteses.

  Quantas?

  Os elementos de um mesmo ciclo de comprimento i podem ser ordenados de i diferentes maneiras e ainda conduzem ao mesmo ciclo. Portanto, toda a permutação pode ser obtida de pelo menos

$$\prod_{i=1}^{n} i^{a_i}$$

  maneiras (existem a_i ciclos de comprimento i).

Contar permutações de um tipo dado

- Além disso, se existem duas maneiras de escrever os n inteiros que resultam em permutações que têm exactamente os mesmos ciclos de comprimento i, apenas por ordem diferente, então novamente elas conduzem à mesma permutação. Os a_i ciclos podem ser permutados de $a_i!$ diferentes maneiras, e a permutação dos ciclos pode ser feita independentemente da ordem dos elementos dentro de cada ciclo.

  Acabámos de mostrar que cada permutação pode ser obtida de

$$\prod_{i=1}^{n} i^{a_i} a_i! = a_1! 1^{a_1} a_2! 2^{a_2} \dots a_n! n^{a_n}.$$

  maneiras.

  O número de permutações do tipo $(a_1, a_2, \dots, a_n)$ é então

$$\frac{n!}{a_1! 1^{a_1} a_2! 2^{a_2} \dots a_n! n^{a_n}}.$$

Definição. *$c_{n,k}$ denota o número de permutações de n elementos com precisamente k ciclos na sua decomposição cíclica.*

Alguns valores: $c_{n,k} = 0$, $k > n$, $c(n,0) = 0$, $c(n,n) = 1$, $c(n,1) = (n-1)!$, $c_{n,n-1} = \binom{n}{2}$.

- Classificando as permutações de acordo com seu número de ciclos, como o número de ciclos de uma permutação de n elementos varia entre 1 e n, obtemos

$$\sum_{k=0}^{n} c_{n,k} = n!$$

- *Relação de recorrência*

$$c_{n,k} = c_{n-1,k-1} + (n-1)c_{n-1,k}, \quad n > 1.$$

- *Relação de recorrência*

$$c_{n,k} = c_{n-1,k-1} + (n-1)c_{n-1,k}, \quad n > 1.$$

O lado esquerdo desta igualdade conta o número de permutações de n elementos com k ciclos. Vamos ver que o lado esquerdo também. Consideremos uma dessas permutações com k ciclos. Então nessa permutação ou n forma um ciclo por si próprio ou não.

No primeiro caso, os restantes $n-1$ elementos formam $k-1$ ciclos e $c_{n-1,k-1}$ conta precisamente essas permutações.

No segundo caso, n pertence a um ciclo de comprimento pelo menos dois e, portanto, os restantes $n-1$ elementos formam k ciclos onde se acrescenta n de alguma maneira. Esses k ciclos podem ser formados de $c_{n-1,k}$ maneiras. Em cada um dessas maneiras, o elemento n pode ser acrescentado à frente de cada um dos $n-1$ elementos que constituem esses k ciclos. Isto multiplica o número de possibilidades por $n-1$ o que explica a segunda parcela do lado direito da igualdade.

Proposição Seja $n \geq 1$,

$$x(x+1)(x+2)\cdots(x+n-1) = \sum_{k=0}^{n} c_{n,k} x^k.$$

Prova Por indução sobre n.
Para $n = 1$, $x = c_{1,0} + c_{1,1}x^1$, $c_{1,1} = 1$, $c_{1,0} = 0$.
Seja $n \geq 2$,

$$x(x+1)(x+2)\cdots(x+n-2)(x+n-1) = \left(\sum_{k=0}^{n-1} c_{n-1,k} x^k\right)(x+n-1)$$

$$= \sum_{k=0}^{n-1} c_{n-1,k} x^{k+1} + \sum_{k=0}^{n-1}(n-1)c_{n-1,k} x^k$$

$$= \sum_{k=1}^{n} c_{n-1,k-1} x^k + \sum_{k=0}^{n}(n-1)c_{n-1,k} x^k, \quad c_{n-1,n} = 0$$

$$= \sum_{k=1}^{n} \left[c_{n-1,k-1} + (n-1)c_{n-1,k}\right] x^k + (n-1)c_{n-1,0}x^0, \quad c_{n-1,0} = c_{n,0} = 0$$

$$= \sum_{k=0}^{n} c_{n,k} x^k.$$

Considere

$$x(x+1)(x+2)\cdots(x+n-1) = \sum_{k=0}^{n} c_{n,k} x^k.$$

Substitua x por $-x$ na igualdade acima e multiplique ambos os membros por $(-1)^n$, obtém-se

$$\sum_{k=0}^{n} (-1)^{n-k} c_{n,k} x^k = x(x-1)(x-2)\cdots(x-n+1).$$

Note que $(-1)^n = (-1)^{n-k}(-1)^{2k} = (-1)^{n-k}$.

Definição Seja $s_{n,k} := (-1)^{n-k} c_{n,k}$. Este número é chamado Stirling de primeira espécie. A $c_{n,k}$ também se chama o número de Stirling de primeira espécie sem sinal.

Bibliografia

- Martin Aigner, A course in Enumeration, Springer, 2010.
- Keneth Bogart, Combinatorics Through Guided Discovery.
- Miklós Bóna, A Walk through Combinatorics, World Scientific, 2002.
- Richard Brualdi, Introductory Combinatorics, Pearson/Prentice Hall, 2010.
- Domingos M. Cardoso, Jerzy Szymanski, Mohammad Rostami, Matemática Discreta, Combinatória, Teoria dos grafos, Algoritmos, Escolar Editora, 2009.
- George E. Martin, Counting: The Art of Enumerative Combinatorics, Springer, 2001.
- J. M. Simões Pereira, Matemática Discreta: Tópicos de Combinatória. Editora Luz da Vida. 2006.