Complemento para a disciplina de Matemática Discreta

versão 16

Jerônimo C. Pellegrini

2 de abril de 2017

Sumário

Nomenclatura

$!n$ quantidade de permutações caóticas de n elementos, página 40

2^X conjunto das partes de X, página 3

$[x^n]$ coeficiente de x^n em função geradora ordinária, página 48

$\aleph_0$ cardinalidade de $\mathbb{N}$, página 14

$\mathfrak{c}$ cardinalidade de $\mathbb{R}$ (ou "do contínuo"), página 16

$\text{fix}(g)$ elementos fixados por g, página 100

$\lceil x \rceil$ teto de x, página 2

$\lfloor x \rfloor$ chão de x, página 2

$\left(\!\binom{n}{r}\!\right)$ combinações com repetição, página 28

$\text{orb}_G(x)$ órbita de x, página 99

$\phi(n)$ quantidade de coprimos antes de n, página 43

$\preceq$ relação de ordem, página 9

$\lfloor x \rceil$ inteiro mais próximo de x, página 2

$\left\{ {n \atop k} \right\}$ Número de Stirling, página 57

$\text{stab}_G(x)$ estabilizador, página 99

$\underline{n}$ Conjunto de inteiros de 1 a n, página 10

$A \cap B$ interseção, página 1

$A \cup B$ união, página 1

$A \setminus B$ diferença entre conjuntos, página 1

$A \subseteq B$ A está contido em B, página 1

$A \times B$ produto cartesiano de A e B, página 2

Capítulo 1

Conjuntos e Relações

Este Capítulo trata de conceitos básicos que usamos no resto do texto: conjuntos, relações e grafos.

1.1 Conjuntos

Não definimos conjuntos.

Denotamos conjuntos *usualmente* (mas não sempre) pode letras maiúsculas. O conjunto vazio é normalmente denotado por $\emptyset$, e algumas vezes por $\{\}$.

Definição 1.1. Um *multiconjunto* é um conjunto onde cada elemento pode estar presente mais de uma vez (ou, de forma equivalente, um conjunto onde cada elemento tem um número associado, chamado de *multiplicidade*). ♦

Definição 1.2 (subconjunto)**.** Um conjunto A é *subconjunto* de B se todo elemento de A também pertence a B. Dizemos que A *está contido* em B.

$$A \subseteq B \quad \Leftrightarrow \quad x \in A \Rightarrow x \in B. \qquad \blacklozenge$$

Definição 1.3 (união)**.** A *união* dos conjuntos A e B é o conjunto dos elementos que pertencem a A *ou* a B.

$$A \cup B = \Big\{ x : x \in A \text{ ou } x \in B \Big\}. \qquad \blacklozenge$$

Definição 1.4 (interseção)**.** A *interseção* dos conjuntos A e B é o conjunto dos elementos que pertencem tanto a A como a B.

$$A \cap B = \Big\{ x : x \in A \text{ e } x \in B \Big\}. \qquad \blacklozenge$$

Definição 1.5 (diferença)**.** A *diferença* entre os conjuntos A e B, denotada $A \setminus B$, é igual ao conjunto contendo os elementos de A que não pertencem a B:

$$A \setminus B = \Big\{ x \in A : x \notin B \Big\}.$$

A *diferença simétrica* entre A e B, denotada $A \triangle B$ é o conjunto de elementos que estão em A ou em B, mas não em ambos:

$$A \triangle B = (A \cup B) \setminus (A \cap B). \qquad \blacklozenge$$

Definição 1.6 (complemento)**.** Fixado um conjunto universo U, o *complemento* de A em relação a U, que denotamos A^C, é

$$A^C = U \setminus A. \qquad \blacklozenge$$

Definição 1.7 (produto cartesiano)**.** O *produto cartesiano* de dois conjuntos A e B, denotado $A \times B$, é o conjunto de todos os pares ordenados onde o primeiro elemento pertence a A e o segundo pertence a B – ou seja,

$$A \times B = \{(a, b) : a \in A, b \in B\}. \qquad \blacklozenge$$

Definição 1.8 (cardinalidade)**.** A *cardinalidade* do conjunto A é a quantidade de elementos que pertencem a A. Denotamos a cardinalidade por $|A|$. $\blacklozenge$

Definição 1.9 (inteiro mais próximo (arredondamento))**.** O inteiro mais próximo de x é denotado por $\lfloor x \rceil$. $\blacklozenge$

Definição 1.10 (chão e teto)**.** O *chão* de um número real x é o maior inteiro menor ou igual a x. Denotamos[1] o chão por $\lfloor x \rfloor$.

O *teto* de um número real x é o menor inteiro maior ou igual a x. Denotamos o teto por $\lceil x \rceil$. $\blacklozenge$

Exemplo 1.11. Uma situação em que usamos chão e teto é quando dividimos um conjunto em partes iguais ou tão próximo disso quanto possível.

Quando um conjunto A tiver cardinalidade ímpar, e o dividirmos em duas partes, por exemplo, poredemos ter $A = B \cup C$, com

$$|B| = \left\lceil \frac{|A|}{2} \right\rceil,$$
$$|C| = \left\lfloor \frac{|A|}{2} \right\rfloor.$$

Para tornar o exemplo mais concreto, seja

$$A = \{a, b, c, d, e, f, g\}.$$

Como $|A| = 7$, não temos como dividí-lo em duas partes iguais. Podemos no entanto dividir A em dois subconjuntos de cardinalidades $\lceil 7/2 \rceil = 4$ e $\lfloor 7/2 \rfloor = 3$, como $A' = \{a, c, e, g\}$ e $A'' = \{b, d, f\}$. $\blacktriangleleft$

Definição 1.12 (relação)**.** Uma relação R entre conjuntos A e B é um subconjunto do produto cartesiano $A \times B$. Define-se semelhantemente uma relação entre vários conjuntos A_i como subconjunto do produto cartesiano $A_1 \times A_2 \times \ldots \times A_n$.

Uma relação é, portanto, um conjunto de pares ordenados.

Se um par (x, y) pertence a uma relação R, denotamos xRy. Podemos também denotar $x\overline{R}y$ quando $(x, y) \notin R$. $\blacklozenge$

[1] É também comum denotar chão por $[\![x]\!]$ e teto por $]\!]x[\!]$.

Definição 1.13 (conjunto potência)**.** Seja X um conjunto. Então 2^X é o *conjunto potência*, ou *conjunto das partes* de X:

$$2^x = \{Y : Y \subseteq X\}$$ ♦

Exemplo 1.14. Seja

$$A = \{a, b, c, d\}.$$

Então

$$2^A = \left\{ \begin{array}{c} \emptyset, \\ \{a\},\{b\},\{c\},\{d\}, \\ \{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\},\{c,d\} \\ \{a,b,c\},\{a,b,d\},\{a,c,d\},\{b,c,d\}, \\ \{a,b,c,d\} \end{array} \right\}$$ ◄

O teorema a seguir nos diz porque a nomenclatura 2^X é usada.

Teorema 1.15. *Para qualquer conjunto* X, $|2^X| = 2^{|X|}$.

Definição 1.16 (reflexividade, simetria e transitividade)**.** Uma relação R em um conjunto A é

- *reflexiva* se aRa para todo $a \in A$,
- *simétrica* se aRb implica em bRa para todos $a, b \in A$,
- *transitiva* se aRb e bRc implicam em aRc para todos $a, b, c \in A$. ♦

Exemplo 1.17. A relação $=$ de igualdade entre números é reflexiva, porque $a = a$, simétrica, porque se $a = b$ então $b = a$, e transitiva, porque $a = b$ e $b = c$ implicam em $a = c$. ◄

Teorema 1.18. *Uma relação* R *é transitiva se e somente se* $R \circ R \subseteq R$.

1.2 Grafos

Um *grafo* é uma representação gráfica de uma relação. Informalmente, representamos uma relação R em um conjunto X graficamente da seguinte maneira: os elemenos de X são dispostos como pontos no plano, e quando xRy, desenhamos um traço ligando x a y. Os pontos são chamados de *vértices*, e os traços de *arestas*.

Definição 1.19 (grafo)**.** Um *grafo* é um conjunto de nós ligados por arestas. Formalmente, um grafo é um par (V, E), tal que V é o conjunto de nós (ou *vértices*), e V é um conjunto de arestas.

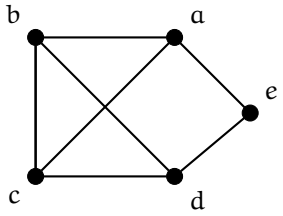
Em um grafo *orientado*, uma aresta sai de um nó origem e chega a um nó destino,. Neste tipo de grafo $E \subseteq V^2$, e uma aresta é um par (v, w).

Em um grafo *não-orientado*, as arestas ligam pares de nós, sem distinção de direção. Nestes grafos, $E \subseteq \left\{\{x, y\} : x, y \in V\right\}$, e uma aresta é um conjunto $\{x, y\}$, com $x, y \in V$. ♦

Exemplo 1.20. Por exemplo, o grafo não-orientado $G = (V, E)$ onde $V = \{a, b, c, d, e\}$ e

$$E = \begin{Bmatrix} \{a, b\}, & \{a, c\}, & \{a, e\}, & \\ \{b, c\}, & \{b, d\}, & \{c, d\}, & \{d, e\} \end{Bmatrix}.$$

é representado graficamente na figura a seguir.

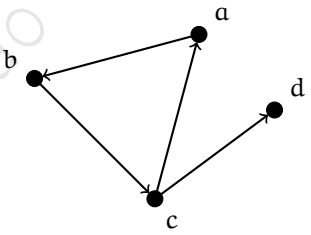


As posições exatas dos nós e arestas não são relevantes; importa apenas quais são os nós, e como cada um deles se relaciona com os outros. ◀

Exemplo 1.21. O grafo orientado $G = (V, E)$, com $V = \{a, b, c, d\}$ e

$$E = \{(a, b), (b, c), (c, a), (c, d)\}$$

é representado graficamente como na figura a seguir.



◀

Definição 1.22 (matriz de adjacência)**.** Seja $G = (V, E)$ um grafo com n vértices. Sem perda de generalidade, presuma que os vértices de G são rotulados como $v_1, v_2, \ldots v_n$. A *matriz de adjacência* de G é uma matriz quadrada de ordem $|V|$ tal que a posição i, j é zero se não há aresta ligando v_i a v_j, e um se há aresta ligando v_i a v_j. Para grafos orientados, a matriz de adjacência M é tal que

$$m_{i,j} = \begin{cases} 0 & se (i, j) \notin E \\ 1 & se (i, j) \in E \end{cases}$$

Para grafos não-orientados a matriz é definida de forma semelhante. ♦

Exemplo 1.23. A matriz de adjacência do grafo não-orientado do exemplo 1.20 é

$$M = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Note que a matriz é simétrica, já que tanto (i, j) como (j, i) representam a mesma aresta em um grafo não-orientado.

Já para o grafo orientado do exemplo 1.21, a matriz de adjacência é

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$ ◀

Definição 1.24 (grafo completo)**.** O grafo com n vértices onde todos os vértices são ligados a todos os outros é chamado de *grafo completo*. ♦

A matriz de equivalência de um grafo completo tem zeros na diagonal e uns em todas as outras entradas.

Definição 1.25 (coloração de arestas)**.** Uma *coloração das arestas* de um grafo G com k cores é uma atribuição de uma das k cores a cada um dos vértices de G. ♦

1.3 Relações de equivalência

Definição 1.26 (relação de equivalência)**.** Uma relação é dita *de equivalência* se é *simétrica*, *reflexiva* e *transitiva*. ♦

Exemplo 1.27. A relação em $\mathbb{R}$ dada por aRb se e somente se $a^2 = b^2$ é uma relação de equivalencia:

- *(reflexiva)*: trivialmente, $a^2 = a^2$.
- *(simétrica)* se $a^2 = b^2$, então $b^2 = a^2$.
- *(transitiva)* se $a^2 = b^2$ e $b^2 = c^2$, temos também trivialmente $a^2 = c^2$. ◀

Exemplo 1.28. Dois triângulos são *congruentes* se os tamanhos de seus lados, quando dispostos em ordem crescente, são iguais.

A congruência de triângulos é uma relação de equivalência no conjunto de todos os triângulos no plano.

- *(reflexiva)*: trivialmente, todo triângulo é congruente a si mesmo.
- *(simétrica)* também trivial: se A é côngruo a B, então B é côngruo a A.

- *(transitiva)* se A é côngruo a B e B é côngruo a C, claramente A é côngruo a C, porque os tamanhos dos lados de todos os tres triângulos são os mesmos.

Dizemos também que dois triângulos são *similares* se seus lados, quando dispostos em ordem crescente, só diferem por um fator constante (ou seja, admitimos também uma mudança de escala). A similaridade de triângulos é uma relação de equivalência.

As relações de congruência e similaridade podem ser generalizadas para quaisquer figuras geométricas, e continuam sendo relações de equivalência. ◀

Exemplo 1.29. Em $\mathbb{R}$, a relação $a\mathrm{R}b$ se e somente se $a - b \in \mathbb{Z}$ é uma relação de equivalência:

- *(reflexiva)* claramente, $a - a = 0 \in \mathbb{Z}$,
- *(simétrica)* se $a - b = c \in \mathbb{Z}$, então $b - a = -c \in \mathbb{Z}$,
- *(transitiva)* se $a - b = k_1 \in \mathbb{Z}$, e $b - c = k_2 \in \mathbb{Z}$, então $a - c = (k_1 + b) - (b - k_2) = k_1 + k_2 \in \mathbb{Z}$. ◀

A definição a seguir é usada como exemplo, mas é suficientemente importante para que a destaquemos.

Definição 1.30 (congruência módulo um inteiro)**.** Sejam $a, b \in \mathbb{Z}$. Dizemos que a é *côngruo a* b *módulo* m se $m|(a-b)$. Isso é o mesmo que dizer que existe um k inteiro tal que $mk = a - b$ – ou seja, o resto de a por m é igual ao resto de b por m. Denotamos $a \equiv b \pmod{m}$. ♦

Exemplo 1.31. A relação de congruência módulo um inteiro é uma relação de equivalência. Para todos $a, b, c, m \in \mathbb{Z}$,

- *(reflexiva)*: trivialmente, $a \equiv a \mod m$, porque $m|(a - a = 0)$.
- *(simétrica)* se $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, porque se $m|(a - b)$, então $m|(b - a)$.
- *(transitiva)* se $m|(a-b)$, e $m|(b-c)$, então $m|[(a-b)+(b-c)]$, e claramente $m|(a - c)$. ◀

Exemplo 1.32. Seja F o conjunto de todas as funções de $\mathbb{R}$ em $\mathbb{R}$. Defina que $f\mathrm{R}g$ se e somente se existe uma constante c tal que $f(x) = g(x) + c$, para todo x. Então R é uma relação de equivalência.

- *(reflexiva)*: $f(x) = f(x) + 0$.
- *(simétrica)* se $f(x) = g(x) + c$, então $g(x) = f(x) + (-c)$.
- *(transitiva)* se $f(x) = g(x) + c_1$ e $g(x) = h(x) + c_2$, então $f(x) = h(x) + c_2 + c_1$. ◀

Exemplo 1.33. No conjunto de todas as funções reais, a relação definida por $f\mathrm{R}g$ se e somente se $f' = g'$ (ou seja, f e g tem a mesma derivada) é uma relação de equivalência. ◀

Definição 1.34 (classe de equivalência)**.** Seja R uma relação de equivalência em um conjunto A. Então a *classe de equivalência* de um elemento $a \in A$ é o conjunto $\{x \in A : xRa\}$. ♦

Exemplo 1.35. Já determinamos que a congruência modulo um m inteiro é uma relação de equivalência. Como o resto da divisão de qualquer inteiro por m só pode estar entre zero e $m-1$, a relação de congruência módulo m define m classes de congruência, que usualmente denotamos $[0]$, $[1]$, ..., $[m-1]$. Por exemplo, se $m = 5$, temos

$$\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}.
\end{aligned}$$ ◀

Exemplo 1.36. Em $\mathbb{Z}^2$, a relação $\sim$, definida por

$$(a, b) \sim (x, y) \Leftrightarrow ay = bx$$

é uma relação de equivalência:

- *(reflexividade)* trivialmente, $(a, b) \sim (a, b)$, já que $ab = ba$.
- *(simetria)* também é trivial: $ab = ba$ implica em $ba = ab$.
- *(transitividade)* queremos mostrar que se

  $$\begin{aligned}(a, b) &\sim (x, y) \\ (x, y) &\sim (p, q)\end{aligned}$$

  então $(a, b) \sim (p, q)$. Usando a definição da relação, o que queremos é provar que se

  $$\begin{aligned}ay &= bx \\ xq &= yp \end{aligned} \tag{1.1}$$

  então

  $$aq = bp \tag{1.2}$$

  É de vital importância observar, no entanto, que não podemos simplesmente dividir um dos lados de qualquer destas equações por uma das variáveis, porque estamos trabalhando com inteiros. Podemos, no entanto, multiplicar $ay = bx$ por q:

  $$ayq = bxq$$

  Podemos substituir qx por yp (equação 1.1):

  $$ayq = ypb$$

Aqui sim, sabemos que ambos os lados da equação são divisíveis por y, e portanto

$$aq = bp,$$

que é o que queríamos mostrar (equação 1.2).

A classe de equivalência $[(a, b)]$ define o número racional que usualmente denotamos por a/b, e a relação $\sim$ define igualdade entre racionais: $(1, 2) \sim (3, 6) \sim (50, 100)$, etc. ◀

Definição 1.37 (partição de conjunto)**.** Uma *partição* de um conjunto A é uma família de conjuntos $A_1, A_2, \ldots, A_n$ tais que

$$\bigcup_{i=1}^{n} A_i = A$$
$$A_i \cap A_j = \emptyset \quad \text{se } i \neq j$$ ♦

Teorema 1.38. *Seja* R *uma relação de equivalência em um conjunto* A*. Então as classes de equivalência definidas por* R *são uma partição de* A*.*

Demonstração. Em primeiro lugar, a união das classes de equivalência resultam em A, porque todo elemento de A pertence a uma classe de equivalência, e não há nas classes qualquer elemento que não pertença a A. Com isso temos $\bigcup_{i=1}^{n} A_i = A$.

Finalmente, mostramos queas classes de equivalência são disjuntas. Suponha que xRy. Mostramos que $[x] \subseteq [y]$. Suponha que $z \in [x]$. Temos então xRz, e por simetria zRx; por transitividade, zRy. Isso implica que $z \in [y]$. Ou seja, todo $z \in [x]$ também está em $[y]$. Usando simetria, fazemos o argumento contrário e temos $[x] = [y]$.

Suponha agora que $x\overline{R}y$. Mostramos agora que $[x] \cap [y] = \emptyset$. Suponha que $z \in [x] \cap [y]$. Então xRz e zRy valem, e portanto também deveria valer xRy – uma contradição. Temos então $[x] \cap [y] = \emptyset$ quando $[x] \neq [y]$. ■

1.4 Relações de ordem

Definição 1.39 (ordem total)**.** Uma relação R em um conjunto A é dita *de ordem total* se

- R é *antissimétrica*, *reflexiva* e *transitiva*,
- Para todos elementos $a, b \in A$, necessariamente aRb ou bRa. ♦

Exemplo 1.40. A relação $\leq$ no conjunto dos números reais é uma ordem total:

- *(antissimétrica)* Se $a \leq b$ e $b \leq a$ então $a = b$,
- *(reflexiva)* $a \leq a$,
- *(transitiva)* $a \leq b$, $b \leq c$ implica em $a \leq c$.

Além disso, para quaisquer dois reais a e b, temos que $a \leq b$ ou $b \leq a$. ◀

Definição 1.41 (ordem parcial)**.** Uma relação R em um conjunto A é dita *de ordem parcial* se R é *antissimétrica*, *reflexiva* e *transitiva*. ♦

Exemplo 1.42. Toda ordem total é também parcial, portanto os exemplos anteriores de ordem total são também exemplos de ordem parcial. ◀

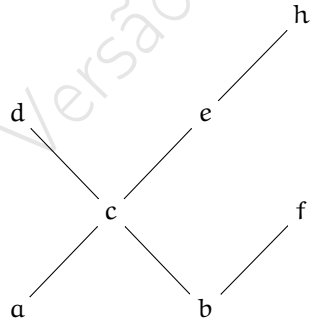
A notação $\preceq$ é normalmente usada para relação de ordem em conjunto parcialmente ordenado.

É comum usar um diagrama para representar relações de ordem parcial. Dada uma relação R em um conjunto X, o *diagrama de Hasse* desta relação é um grafo onde há um vértice para cada elemento de X, e há aresta entre x e y se xRy. Para simplificar o grafo, não são representados os *loops* ($a \preceq a$) e as relações que podem ser deduzidas por transitividade (se $a \preceq b$ e $b \preceq c$, não representamos $a \preceq c$); além disso, não representamos as direções das arestas, e presumimos que todas são orientadas "de baixo para cima".

Exemplo 1.43. No conjunto $\{a, b, c, d, e, f, g\}$, a relação dada por

$$\begin{aligned} a &\preceq c \\ b &\preceq c \\ b &\preceq f \\ c &\preceq d \\ c &\preceq e \end{aligned}$$

é uma ordem parcial. Seu diagrama de Hasse é



◀

Exemplo 1.44. Dados $a, b \in \mathbb{N}$, denotamos por "$a|b$" o fato de a dividir b (ou seja, existe um c tal que $b = ac$). A relação $|$ é uma ordem parcial em $\mathbb{N}$:

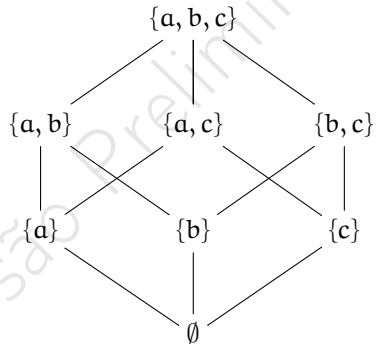
- *(antissimétrica)* Se $a|b$ e $b|a$ então $a = b$, porque $a = bc_1$, $b = ac_2$ implicam em $a = ac_2c_1$, e portanto $c_1 = c_2^{-1}$, mas o único natural com inverso para multiplicação é 1, e $c_1 = c_2 = 1$,
- *(reflexiva)* $a|a$, porque existe $c = 1$ tal que $a = (1)a$,
- *(transitiva)* $a|b$ e $b|c$ implicam e $a|c$.

A relação |, no entanto, *não* é ordem parcial, porque dois números naturais não necssariamente se relacionam desta forma. O exemplo mais claro é possivelmente o de dois números primos: se p e q são primos, $p \nmid q$, e $q \nmid p$. ◀

Exemplo 1.45. Seja 2^X o conjunto das partes de X. Então a relação de inclusão, $\subseteq$, é uma ordem parcial em X, mas *não* é ordem total.

- *(antissimétrica)* se $A \subseteq B$ e $B \subseteq A$, então $A = B$.
- *(reflexiva)* $A \subseteq A$, trivialmente.
- *(transitiva)* $A \subseteq B$ e $B \subseteq C$ implicam em $A \subseteq C$.

Dentre as partes de um conjunto, no entanto, pode haver subcobjuntos que não são se relacionam de nenhuma forma: como exemplo, considere as partes de $\{a, b, c\}$. Podemos ver no diagrama de Hasse que nem todos os pares se relacionam – por exemplo, $\{a, b\} \not\subseteq \{b, c\}$ e $\{b, c\} \not\subseteq \{a, b\}$



◀

Definição 1.46 (ordem lexicográfica)**.** Seja A um conjunto e $\preceq$ uma relação de ordem em A. Sejam $(a_{1,2}), (x_1, x_2) \in A^2$. Dizemos que (a_1, a_2) *precede* (x_1, x_2) *lexicograficamente* se $a_1 \preceq x_1$ ou se $a_1 \approx x_1$ e $a_2 \preceq x_2$.

Sejam $\alpha = (a_1, a_2, \ldots), \beta = (x_1, x_2, \ldots) \in A^n$. Então $\alpha \preceq \beta$ se $a_1 \preceq x_1$ ou se $a_1 \approx x_1$ e $(a_2, \ldots) \preceq (x_2, \ldots)$. ♦

Exemplo 1.47. Seja A o alfabeto da língua Portuguesa. A ordem lexicográfica é a ordem usada em dicionários: "banalidade" $\preceq$ "banana", porque $L \preceq N$. ◀

Denotamos por $\underline{n}$ o conjunto $\{1, 2, \ldots, n\}$.

Exemplo 1.48. Seja $\underline{3}^{\underline{3}}$ o conjunto de todas as 27 funções de $\underline{3}$ em $\underline{3}$. denotaremos cada uma destas funções listando $f(1), f(2), f(3)$. Por exemplo, $(1, 3, 3)$ é uma função.

Listamos todas em ordem lexicográfica. Leia as colunas de cima para baixo pri-

meiro, e da esquerda para a direita depois.

$$\begin{array}{ccc} 111 & 211 & 311 \\ 112 & 212 & 312 \\ 113 & 213 & 313 \\ 121 & 221 & 321 \\ 122 & 222 & 322 \\ 123 & 223 & 323 \\ 131 & 231 & 331 \\ 132 & 232 & 332 \\ 133 & 233 & 333 \end{array}$$

◀

Definição 1.49 (boa ordem)**.** Um conjunto X é *bem-ordenado* com uma relação de ordem $\prec$ se esta for uma relação de ordem parcial, e todo subconjunto não vazio de X tenha um menor elemento. ♦

Exemplo 1.50. O conjunto $\mathbb{N}$ com $\leq$ é bem-ordenado.

Já $\mathbb{Z}$ com $\leq$ não, porque há subconjuntos de $\mathbb{Z}$ onde não haverá menor elemento, como o próprio $\mathbb{Z}$, ou

$$\{x \in \mathbb{Z} \,:\, x < 10\},$$

por exemplo. ◀

Exercícios

Ex. 1 — Verifique que tipo de relação são:

- Em $\mathbb{R}$, $a \sim b$ se $a - b \in \mathbb{Q}$
- Em $\mathbb{R}$, $a \sim b$ se $|a| = |b|$
- Para matrizes quadradas, $A \sim B$ se $\det A = \det B$
- Para matrizes quadradas não-singulares, $\det A \leq \det B$
- Para matrizes quadradas, $A \sim B$ se $\det AB \neq 0$
- Para polinômios com coeficientes em $\mathbb{R}$ e grau no máximo n, $p(x) \sim q(x)$ se $p(x) + q(x) \leq 0$ (para todo x)
- Para polinômios com coeficietnes em $\mathbb{R}$ e grau no máximo n, $p(x) \sim q(x)$ se $p(x) + q(x)$ tem todas as raízes reais.
- Em $\mathbb{R}$, $\alpha \sim \beta$ se $\alpha + \beta = k\pi/2$, para algum $k \in \mathbb{Z}$
- Em $\mathbb{Z}$, $a \sim b$ se ab tem raiz quadrada inteira
- Em $\mathbb{Z}$, $a \sim b$ se $a^2 - b^2$ tem raiz quadrada inteira
- Em $\mathbb{N}$, $a \sim b$ se a tem menos fatores primos (contando as multiplicidades) do que b
- Em $\mathbb{N}$, $a \sim b$ se a se a multiplicidade do menor fator primo de a é menor que a do menor fator primo de b

- Em $\mathbb{N}$, $a \sim b$ definida da seguinte forma: seja d_a a distancia de a até o primo mais próximo de a. Seja d_b a distância de b até o primo mais próximo de b. $a \sim b$ se $d_a \leq d_b$.

Ex. 2 — Seja $\sim$ uma relação em funções reais definida como

$$f \sim g \quad \Leftrightarrow \quad \lim_{x\to\infty} f(x) = \lim_{x\to\infty} g(X) \pm C.$$

Determine se $\sim$ é relação de equivalencia.

Ex. 3 — Construa (parcialmente) o diagrama de Hasse para a relação $|$ em $\mathbb{N}$, dispondo os números com k fatores na k-ésima linha, e assim por diante.

Ex. 4 — Dê uma definição não recursiva para ordem lexicográfica.

Ex. 5 — Seja C o conjunto de todas as circunferências no plano. Mostre diferentes ordens em C, pelo menos uma dela total.

Ex. 6 — Seja E o conjunto de elipses no plano. Mostre pelo menos tres partições de E, explicitando a relação de equivalência que determina cada partição.

Ex. 7 — Fixe um número L natural. Seja $\prec$ definida em qualquer subconjunto de $\mathbb{N}$ da seguinte maneira: $a \preceq b$ se a quantidade de primos entre a e $L/2$ é menor ou igual que a quantidade de primos entre b e $L/2$. A relação $a \prec b$ é ordem total?

Ex. 8 — Seja P um conjunto de proposições $p_1, p_2, \ldots$, e P^* o conjunto de todas as conjunções de proposições em P:

$$P^* = \{p_1, p_2, \ldots, p_n, p_1 \wedge p_2, p_1 \wedge p_3, \ldots, p_2 \wedge p_3, p_2 \wedge p_3, \ldots, P_1 \wedge p_2 \wedge p_3, \ldots\}$$

A relação de implicação $(p_i \to p_j)$ em P^* é de que tipo?

Ex. 9 — Seja $P(n)$ o conjunto de todos os polinômios com grau menor ou igual a n. Claramente pode-se definir uma ordem lexicográfica $\preceq$ em $P(n)$ a partir dos coeficientes dos polinômios. Mostre que, dados dois polinômios $p(.)$ e $q(.)$ em $P(n)$, $p \preceq q$ se e somente se $p(x) \leq q(x), \forall x \in \mathbb{R}$.

Ex. 10 — Mostre uma bijeção entre $\mathbb{Q}$ e $\mathbb{N}$. Que tipo de relação ela é?

Ex. 11 — Há alguma maneira de ordenar o conjunto dos números complexos, ainda que abrindo mão de algumas de suas características de corpo?

Ex. 12 — Considere o conjunto de todas as sequências de números racionais. Defina a relação R como $(a_n)R(b_n)$ se $\lim_{n\to\infty}(a_n - b_n) = 0$. Que tipo de relação é R?

Capítulo 2

Cardinalidade

Determinar e comparar a cardinalidade de conjuntos finitos é conceitualmente simples: a cardinalidade de um destes conjuntos sempre será um número natural, e a ordem total de $\mathbb{N}$ nos permite facilmente determinar quando um conjunto é "maior" que ourto. Nesta Capítulo tratamos da Cardinalidade de conjuntos, dando ênfase em conjuntos infinitos.

Definição 2.1 (cardinalidade)**.** Dois conjuntos tem a mesma cardinalidade se existe uma bijeção de um deles no outro. ♦

Note que pode haver muitas bijeções entre dois conjuntos. Só precisamos de uma para afirmar que a dardinalidade dos dois é a mesma.

Exemplo 2.2. Os conjuntos $\{0, 1, 2\}$ e $\{a, b, c\}$ tem a mesma cardinalidade, porque existe a bijeção

$$\begin{aligned} f(1) &= a \\ f(2) &= b \\ f(3) &= c \end{aligned}$$

Note que poderíamos ter apresentad qualquer uma das outras cinco bijeções. Mostramos uma em cada coluna da tabela a seguir.

$$\begin{array}{lllll} f(1) = a & f(1) = b & f(1) = b & f(1) = c & f(1) = c \\ f(2) = c & f(2) = a & f(2) = c & f(2) = a & f(2) = b \\ f(3) = b & f(3) = c & f(3) = a & f(3) = b & f(3) = a \end{array}$$

Qualquer uma delas teria sido suficiente para a demonstração. ◄

Escolhemos esta definição, e não uma que fale em "quantidade de elementos", porque usando bijeções poderemos tratar de conjuntos infinitos.

Exemplo 2.3. A cardinalidade de $\mathbb{N}$ é a mesma que a de $\mathbb{Z}$, porque a função $f : \mathbb{N} \to \mathbb{Z}$ a seguir é bijetora:

$$f(n) = (-1)^{n-1} 2 \left\lfloor \frac{n}{2} \right\rfloor.$$

A tabela a seguir mostra alguns valores de f.

n:	1	2	3	4	5	6	7	8	$\cdots$
$f(n)$:	0	1	-1	2	-2	3	-3	4	$\cdots$

◀

Definição 2.4 (infinito)**.** Um conjunto é *infinito* se existe uma bijeção dele em um subconjunto próprio dele mesmo. ♦

Exemplo 2.5. O conjunto $\mathbb{N}$ é infinito, porque $f(n) = 2n$ mapeia $\mathbb{N}$ nos pares, e é bijeção: a inversa é $f^{-1}(m) = n/2$. ◀

Exemplo 2.6. Semelhantemente, o conjunto $[0, 10]$ é infinito, porque $f(x) = x/10$ mapeia $[0, 10]$ e, seu subconjunto $[0, 1]$, e é bijeção: a inversa é $f^{-1}(x) = 10x$. ◀

Definição 2.7 (enumerável)**.** Um conjunto é enumerável se tem a mesma cardinalidade de $\mathbb{N}$, que denotamos $\aleph_0$. ♦

Exemplo 2.8. O conjunto P dos naturais pares é enumerável. Isso porque a bijeção $f : \mathbb{N} \to P$, com $f(n) = 2n$ mostra que ambos tem a mesma cardinalidade. ◀

Teorema 2.9. *$\mathbb{Z}$ é enumerável.*

Demonstração. A demonstração é exposta no exemplo 2.3 ■

Teorema 2.10. *A união de uma quantidade enumerável de conjuntos enumeráveis é enumerável.*

Demonstração. Presumimos que temos $S_1, S_2, \ldots$, uma quantidade enumerável de conjuntos; e que cada S_i é enumerável. Queremos mostrar que

$$S = \bigcup_i S_i = S_1 \cup S_2 \cup S_3 \cup \cdots$$

é enumerável – ou seja, que existe uma bijeção de $\mathbb{N}$ neste conjunto.

Suponha que os elementos de cada S_i sejam s_{ij}:

$$S_i = \{s_{i1}, s_{i2}, s_{i3}, \ldots\}.$$

Para identificar a bijeção, basta dispor os elementos em uma tabela, onde o elemento s_{ij} fica na i-ésima linha e j-ésima coluna (ou seja, os elementos do conjunto S_i ocupam a i-ésima linha):

$$\begin{array}{cccc} s_{11} & s_{12} & s_{13} & \cdots \\ s_{21} & s_{22} & s_{23} & \cdots \\ s_{13} & s_{32} & s_{33} & \\ \vdots & \vdots & & \ddots \end{array}$$

A bijeção é criada percorrendo sequencialmente a tabela na diagonal:

$$\begin{array}{cccccc}
s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\
s_{21} & s_{22} & s_{23} & s_{24} & s_{25} & s_{26} \\
s_{31} & s_{32} & s_{33} & s_{34} & s_{35} & s_{36} \\
s_{41} & s_{42} & s_{43} & s_{44} & s_{45} & s_{46} \\
s_{51} & s_{52} & s_{53} & s_{54} & s_{55} & s_{56} \\
s_{61} & s_{62} & s_{63} & s_{64} & s_{65} & s_{66}
\end{array}$$

Note que há outras maneiras de percorrer a tabela, e portanto há também outras bijeções diferentes. A seguir mostramos mais uma.

$$\begin{array}{cccccc}
s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\
s_{21} & s_{22} & s_{23} & s_{24} & s_{25} & s_{26} \\
s_{31} & s_{32} & s_{33} & s_{34} & s_{35} & s_{36} \\
s_{41} & s_{42} & s_{43} & s_{44} & s_{45} & s_{46} \\
s_{51} & s_{52} & s_{53} & s_{54} & s_{55} & s_{56} \\
s_{61} & s_{62} & s_{63} & s_{64} & s_{65} & s_{66}
\end{array}$$

■

Teorema 2.11. *Sejam* A *e* B *dois conjuntos infinitos e enumeráveis.* $A \times B$ *é enumerável.*

Demonstração. A demonstração é semelhante à usada para união de conjuntos enumeráveis. Basta construir uma tabela onde i é o índice de elementos de A e j o índice de elementos de B:

$$\begin{array}{cccccc}
(a_1, b_1) & (a_1, b_2) & (a_1, b_3) & (a_1, b_4) & (a_1, b_5) & (a_1, b_6) \\
(a_2, b_1) & (a_2, b_2) & (a_2, b_3) & (a_2, b_4) & (a_2, b_5) & (a_2, b_6) \\
(a_3, b_1) & (a_3, b_2) & (a_3, b_3) & (a_3, b_4) & (a_3, b_5) & (a_3, b_6) \\
(a_4, b_1) & (a_4, b_2) & (a_4, b_3) & (a_4, b_4) & (a_4, b_5) & (a_4, b_6) \\
(a_5, b_1) & (a_5, b_2) & (a_5, b_3) & (a_5, b_4) & (a_5, b_5) & (a_5, b_6) \\
(a_6, b_1) & (a_6, b_2) & (a_6, b_3) & (a_6, b_4) & (a_6, b_5) & (a_6, b_6)
\end{array}$$

■

Teorema 2.12. $\mathbb{Q}$ *é enumerável.*

Apresentamos duas demonstrações. Uma usando a propriedade da cardinalidade da união de infinitos enumeráveis, que já demonstramos. A outra consiste na identificação de uma bijeção entre $\mathbb{N}$ e $\mathbb{Q}$.

Demonstração. Para qualquer k, seja

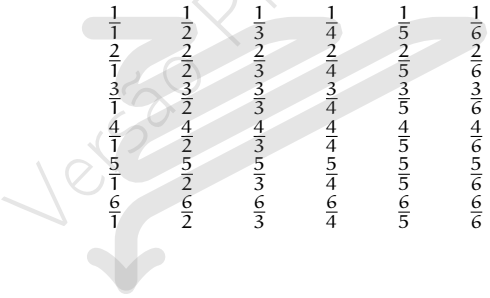
$$Q_k = \bigcup_{i\in\mathbb{Z}} \left\{ \frac{i}{k} \right\} = \left\{ \cdots, -\frac{2}{k}, -\frac{1}{k}, 0, +\frac{1}{k}, +\frac{2}{k}, \cdots \right\}$$

Claramente,

$$\mathbb{Q} = \bigcup_{j\in\mathbb{Z}} Q_j$$

Como $\mathbb{Z}$ é enumerável, a união descrita acima também é. ■

Demonstração. Primeiro provamos que Q^+ é enumerável. Cada racional positivo é a razão de dois naturais (exijimos o denominador diferente de zero). Podemos dispor os racionais em uma tabela, onde as linhas determinam o numerador e as colunas determinam o denominador. Usamos a enumeração em ziguezague, como fizemos para provar que uniões de enumeráveis são enumeráveis.



Pode-se ver que há na tabela elementos repetidos – isto não altera a validade da demonstração, porque conseguimos enumerar um conjunto *no mínimo com a mesma cardinalidade de* $\mathbb{Q}^+$.

Para mostrar que todo o conjunto $\mathbb{Q}$ é enumerável podemos usar o mesmo argumento que usamos ao mostrar que $\mathbb{Z}$ é enumerável. ■

Teorema 2.13. *$\mathbb{R}$ não é enumerável; denotamos $|\mathbb{R}|$ por $\mathfrak{c}$.*

Demonstração. A técnica usada nesta demonstração se chama *diagonalização*[1].

Bastará que provemos que $(0,1)$ não é enuemrável, porque $(0,1) \subseteq \mathbb{R}$, e se $\mathbb{R}$ contém um subconjunto não-enumerável, ele também não pode ser enumerável.

[1] Dizemos também que "usamos o argumento da diagonal". Esta técnica foi descoberta por Georg Cantor.

Cada número em $(0,1)$ é descrito na representação decimal por "$0,\square\square\square\cdots$", onde cada caixa representa um dígito. Assim, o i-ésimo número pode ter seus dígitos enumerados como $d_{i1}, d_{i2}, \ldots$:

$$0, d_{i1}\, d_{i2}\, d_{i3}\, \ldots$$

Suponha que $\mathbb{R}$ seja enumerável. Então poderíamos enumerar todos os reais, um por linha (seja qual for a ordem que escolhamos), como na tabela abaixo.

$$\begin{array}{llllllll}
0, & d_{11} & d_{12} & d_{13} & d_{14} & d_{15} & d_{16} \\
0, & d_{21} & d_{22} & d_{23} & d_{24} & d_{25} & d_{26} \\
0, & d_{31} & d_{32} & d_{33} & d_{34} & d_{35} & d_{36} \\
0, & d_{41} & d_{42} & d_{43} & d_{44} & d_{45} & d_{46} \\
0, & d_{51} & d_{52} & d_{53} & d_{54} & d_{55} & d_{56} \\
0, & d_{61} & d_{62} & d_{63} & d_{64} & d_{65} & d_{66}
\end{array}$$

Esta tabela mostra que há uma *injeção* de $\mathbb{N}$ em $(0,1)$ (logo temos $|\mathbb{N}| \leq |\ (0,1)\ |$). No entanto, para qualquer enumeração como esta é possível mostrar um número em $(0,1)$ que não está na tabela:

- Construa um número x tomando os dígitos da diagonal:

$$0, d_{11}\, d_{22}\, d_{33}\, \ldots$$

- Agora construa x', mudando todos os dígitos de x, de forma que nenhum deles continue igual:

$$0, d'_{11}\, d'_{22}\, d'_{33}\, \ldots$$

$$\begin{array}{llllllll}
0, & d_{11} & d_{12} & d_{13} & d_{14} & d_{15} & d_{16} \\
0, & d_{21} & d_{22} & d_{23} & d_{24} & d_{25} & d_{26} \\
0, & d_{31} & d_{32} & d_{33} & d_{34} & d_{35} & d_{36} \\
0, & d_{41} & d_{42} & d_{43} & d_{44} & d_{45} & d_{46} \\
0, & d_{51} & d_{52} & d_{53} & d_{54} & d_{55} & d_{56} \\
0, & d_{61} & d_{62} & d_{63} & d_{64} & d_{65} & d_{66}
\end{array}$$

O número $x' = 0, d'_{11} d'_{22} d'_{33} \cdots$ não pode estar na primeira linha, porque $d_{11} \neq d'_{11}$; nem na segunda, porque $d_{22} \neq d'_{22}$, e assim por diante: o novo número que construímos é claramente pertencente ao intervalo $(0,1)$, mas não consta na tabela de enumeração.

Como há injeção de $\mathbb{N}$ em $(0,1)$, mas não pode haver bijeção, então $|\mathbb{N}| < |\ (0,1)\ |$. ■

Note que a técnica de diagonalização não pode ser usada para provar que $\mathbb{N}| > |\mathbb{N}|$, porque teríamos que trocar um dígito em cada posição da tabela, obtendo um número com infinitos dígitos – e que portanto não é natural.

Teorema 2.14. *Um subconjunto infinito de um conjunto enumerável é, também, enumerável.*

Teorema 2.15. *Se S é não-enumerável e $S \subseteq A$, então A também é não-enumerável.*

Teorema 2.16. *Para todo conjunto A, $|A| < |2^A|$.*

Demonstração. ■

Ao tentar demonstrar que dois conjuntos tem a mesma cardinalidade, podemos encontrar dificuldades para identificar uma bijeção entre eles. O Teorema de Cantor-Bernstein-Schröeder nos permite usar um caminho mais fácil: se exibirmos uma injeção de A em B e outra, diferente, de B em A, então garantimos a existência de uma bijeção (ainda que não a mostremos explicitamente).

Teorema 2.17 (Cantor-Bernstein-Schröeder)**.** *Se $|A| \leq |B|$ e $|B| \leq |A|$, então $|A| = |B|$.*

Demonstração. ■

Exemplo 2.18. Usaremos o teorema de Cantor-Bernstein-Schröeder para provar que os conjuntos $(0,1)$ e $[0,1]$ tem a mesma cardinalidade. Embora a afirmação pareça óbvia, a bijeção não é. No entanto, conseguiremos duas injeções.

- $|\ (0,1)\ | \leq |\ [0,1]\ |$: trivialmente, $f(x) = x$ é injetora, logo a cardinalidade de $(0,1)$ é menor ou igual que a de $[0,1]$.
- $|\ [0,1]\ | \leq |\ (0,1)\ |$: a função $g : [0,1] \to (0,1)$ a seguir é injetora: mapeamos 0 em 0.1 e 1 em 0.9. Os outros números entre 0 e 1, mapeamos entre 0.1 e 0.9.

  $$g(x) = \frac{1}{10} + \frac{8}{10}x.$$

  A função g é claramente injetora, porque é linear[2]. Além disso, quando definida no domínio $[0,1]$, sua imagem é $\left[\frac{1}{10}, \frac{9}{10}\right]$.

Como temos uma injeção de $(0,1)$ em $[0,1]$ e outra no sentido contrário, o Teorema de Cantor-Bernstein-Schröeder nos garante que os dois conjuntos tem a mesma cardinalidade – e que existe uma bijeção entre eles. O leitor perceberá que encontrar tal bijeção, embora possível, pode ser mais difícil do que apresentar as duas funções injetoras, como fizemos. ◄

Teorema 2.19. $|2^{\mathbb{N}}| = |\mathbb{R}|$.

Demonstração. Sabemos que $|\mathbb{R}| = |\ (0,1)\ |$, portanto só precisamos mostrar que $|2^{\mathbb{N}}| = |\ (0,1)\ |$.

Nas duas funções injetoras que construiremos, usaremos a representação decimal dos números em $(0,1)$. Se $x \in (0,1)$, então

$$x = 0, d_1 d_2 d_3 \ldots$$

[2] Na verdade, afim, porque somamos uma constante ao termo linear.

Definimos uma injeção $f : 2^{\mathbb{N}} \to (0,1)$: um elemento de $2^{\mathbb{N}}$ é um conjunto de números: $\{1,2\}$ e $\{3,9\}$, por exemplo, pertencem a $2^{\mathbb{N}}$.

Para cada $X \in 2^{\mathbb{N}}$,

$$f(X) = 0, d_1 d_2 d_3 \ldots,$$

onde cada dígito é determinado como segue:

$$d_i = \begin{cases} 1 & \text{se } i \in X \\ 0 & \text{se } i \notin X \end{cases}$$

Por exemplo,

$$f(\{1,3,5\}) = 0,10101.$$

Esta função é claramente injetora: se $X, Y \in 2^{\mathbb{N}}$, e $X \neq Y$, então há pelo menos um número natural em X que não está em Y. Isto implica que pelo menos um dígito de $f(X)$ será diferente do seu correspondente em $f(Y)$.

Agora definimos a injeção $g : (0,1) \to 2^{\mathbb{N}}$:

$$g(0, d_1 d_2 d_3 \ldots) = \{10d_1, 10^2 d_2, 10^3 d_3, \ldots\}$$

Como exemplo,

$$\begin{aligned} g(0,2103) &= \left\{10(2),\ 10^2(1),\ 10^3(0),\ 10^4(3)\right\} \\ &= \{20, 100, 0, 30000\}. \end{aligned}$$

Agora que temos as duas funções injetoras f e g, o Teorema de Cantor-Bernstein-Schröeder nos permite afirmar que $|2^{\mathbb{N}}| = |\mathbb{R}|$. ■

2.1 A Hipótese do Contínuo

Sabendo que a cardinalidade de $\mathbb{N}$ é estritamente menor que a de $\mathbb{R}$, surge uma pergunta aparentemente simples, mas cuja resposta mostrou-se extremamente difícil de encontrar: há algum conjunto cuja cardinalidade esteja entre $|\mathbb{N}|$ e $|\mathbb{R}|$? ou seja, existe A tal que

$$\aleph_0 < |A| < \mathfrak{c} \ ?$$

Ou, mudando a notação, "$|\mathbb{N}| < |A| < |\mathbb{R}|$?"

Kurt Gödel mostrou que a hipótese do contínuo não suscitaria contradições na Teoria de Conjuntos de Zermelo-Fraenkel; já Paul Coehn, anos mais tarde, mostrou que a *negação* da hipótese também não gera contradições.

Exercícios

Ex. 13 — Prove que a quantidade de injeções de $\mathbb{N}$ em $\mathbb{Q}$ é infinita.

Ex. 14 — Determine se o conjunto de injeções de $\mathbb{N}$ em $\mathbb{Q}$ é enumerável.

Ex. 15 — Prove que $|\ (0,1)\ | = |\mathbb{R}|$.

Ex. 16 — Mostre que $|\mathbb{R}^n| = |\mathbb{R}|$.

Ex. 17 — Se A é não-enumerável, é verdade que $|A| = |\mathbb{R}|$?

Ex. 18 — Prove que sim ou que não: se S é infinito e enumerável; U é não-enumerável; e $S \subseteq U$, então $U \setminus S$ é não-enumerável.

Capítulo 3

Fundamentos da Contagem: Princípios Aditivo e Multiplicativo

Há dois princípios fundamentais – e extremamente simples – a partir dos quais técnicas de contagem são desenvolvidas.

Definição 3.1 (princípio aditivo)**.** Sejam A e B dois conjuntos finitos. Então $|A \cup B| = |A| + |B|$. ♦

Definição 3.2 (princípio multiplicativo)**.** Sejam A e B dois conjuntos finitos. $|A \times B| = |A||B|$. ♦

Damos agora exemplos de contagem usando estes dois princípios.

Exemplo 3.3. Uma cidade usa 8 dígitos diferentes para representar números de telefone fixo. Quantas linhas telefônicas podem ser representadas?

Temos 8 conjuntos, cada um com 10 elementos. O conjunto de números que podemos representar é o produto cartesiano de todos estes conjuntos, portanto temos

$$10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 10^8$$

números diferentes.

Se quisermos que o primeiro dígito seja diferente de zero, teremos $9 \cdot 10^7$ números. ◄

Exemplo 3.4. Uma cidade usa 9 dígitos para representar números de telefones móveis, sendo que o primeiro sempre deve ser 8 ou 9. A cidade poderá ter, no máximo, $2 \cdot 10^8$ números diferentes para telefones móveis. ◄

Exemplo 3.5. Um sistema computacional usa senhas com 256 bits para controle de acesso. Há um total de 2^{256} senhas possíveis. Se o sistema exigir que o usuário espere

cinco segundos entre uma tentativa e outra, um intruso demoraria $5 \cdot 2^{256}$ segundos para tentar todas as possibilidades se tentar enumeração simples [1]. ◀

Exemplo 3.6. Os nucleotídeos que compões o RNA são adenina (A), guanina (G), citosina (C) e uracila (U). Quão grande, no mínimo, deve ser uma sequência de RNA para representar 1000 indivíduos diferentes?

Cada posição pode conter um dentre 4 nucleotídeos diferentes, portanto uma sequência de tamanho n representa 4^n indivíduos. Precisamos de uma sequência de tamanho $\lceil \log_4 1000 \rceil$. Tomamos o teto porque se calcularmos $\log_4 1000$ obteremos 4.9, que não é inteiro. Uma sequencia menor, de tamanho 4, não será suficiente. Usamos então o teto e temos que a sequencia deve ter tamanho no mínimo igual a 5. ◀

Exemplo 3.7. Computadores usam *endereços IP* para comunicar-se via rede. Cada entidade em uma rede tem um endereço IP. A versão 4 do protocolo que define os endereços IP definia que os endereços teriam que ser formados quatro bytes, que normalmente são descritos em decimal e separados or pontos, como "221.123.4.11". A quantidade de possíveis números IP passou a ser considerada insuficiente: cada byte isolado representa 256 possibilidades diferentes, e portanto temos $256^4 = 4\,294\,967\,296$, pouco mais de quatro bilhões e duzentos mil possíveis números IP. A versão 6 do protocolo IP define endereços com 128 bits, e portanto passa-se a ter 2^{128}, aproximadamente 3.4×10^{38} (um número com trinta e nove dígitos) possíveis endereços. ◀

Exemplo 3.8. Queremos projetar um computador que possa usar 64Gb de memória RAM, sendo que cada posição da memória deve ter o mesmo tamanho que as sequências de bits que representam cada posição. Quanto deve ter cada posição?

$$\begin{aligned} 64\text{Gb} &= 64 \cdot 1024\text{Mb} \\ &= 64 \cdot 1024 \cdot 1024\text{kb} \\ &= 64 \cdot 1024 \cdot 1024 \cdot 1024\text{bytes} \\ &= 64 \cdot 1024 \cdot 1024 \cdot 1024 \cdot 8\text{bits} \\ &= 512 \cdot 1024^3\text{bits}. \end{aligned}$$

Seja t o tamanho de cada palavra, e q a quantidade de bits em cada palavra.

$$(512 \cdot 1024^3) = qt$$

Queremos que os 64Gb sejam endereçaveis por uma palavra, portanto

$$\begin{aligned} \log_2(q) &\leq t \\ q &\leq 2^t \end{aligned}$$

[1] Na verdade, o tempo *esperado* para que o intruso quebre a senha é bem menor que isso.

Assim, temos $qt \leq t2^t$, e

$$\begin{aligned}(512 \cdot 1024^3) &\leq t2^t \\ \log_2(512 \cdot 1024^3/t) &\leq t \\ \log_2(512 \cdot 1024^3) - \log_2(t) &\leq t \\ 39 - \log_2(t) &\leq t \\ t &= \lceil 39 - \log_2(t) \rceil\end{aligned}$$

Podemos escolher $t = 34$. ◀

Exemplo 3.9. Suponha que após um crime ter sido cometido, uma testemunha diga que o criminoso escapou em um veículo, e que se lembra que as placas continham as letras F e C, além de terminar com os números 35. Sabendo que as placas são formadas por três letras seguidas de quatro números, quantos são os carros que podem ter sido usados pelo criminoso?

Contamos dois conjuntos: primeiro, as sequências de quatro dígitos que terminam com 35 são simplesmente as sequências de dois dígitos diferentes. São $10^2 = 100$. Temos também a sequência de letras. Contamos primeiro o caso em que o F aparece antes do C. Há mais uma letra a incluir, que pode ficar antes do F, entre o F e o C, ou depois do C.

$$\_F\_C\_$$

Como há 26 letras e três posições possíveis, temos $3 \cdot 26 = 78$ possibilidades. Como temos que contar também as possibilidades para C antes de F, multiplicamos por 2, e temos 156 possíveis sequências de letras.

Finalmente a quantidade de possíveis placas é $100 \cdot 156 = 15600$. ◀

O próximo exemplo é o primeiro que faz uso do princípio aditivo.

Exemplo 3.10. Contamos o número de anagramas usando as 26 letras do alfabeto que tenham tamanho 3, 5 ou 7: $26^3 + 26^5 + 26^7$. E se exigirmos que as palavras intercalem vogais e consoantes?

Há 5 vogais e 21 consoantes. Para tamanho 3, temos palavras da forma VCV ou CVC. Estes nos dão $(5 \cdot 21 \cdot 5) + (21 \cdot 5 \cdot 21)$ possibilidades. Contando também as possibilidades para 5 e 7, temos

$$\begin{aligned}&(5 \cdot 21 \cdot 5) + (21 \cdot 5 \cdot 21) \\ &+(5 \cdot 21 \cdot 5 \cdot 21 \cdot 5) + (21 \cdot 5 \cdot 21 \cdot 5 \cdot 21) \\ &+(5 \cdot 21 \cdot 5 \cdot 21 \cdot 5 \cdot 21 \cdot 5) + (21 \cdot 5 \cdot 21 \cdot 5 \cdot 21 \cdot 5 \cdot 21) \\ &=(21 \cdot 5^2 + 5 \cdot 21^2) + (21^2 \cdot 5^3 + 21^3 \cdot 5^2) + (21^3 \cdot 5^4 + 21^4 \cdot 5^3) \\ &=(21 \cdot 5^2 + 5 \cdot 21^2) + 5^3 \cdot (21^4 + 21^2) + 21^3(5^4 + 5^2)\end{aligned}$$

possíveis anagramas. ◀

Exemplo 3.11. Um sistema computacional tem controle de acesso com senhas de cinco dígitos alfanuméricos. Isso dá uma quantidade de senhas igual a $(26 + 10)^5 =$

36^5. Se restringirmos as senhas permitidas, exigindo que haja letras e números, teremos menos senhas possíveis. Há 26^5 senhas somente com letras, e 10^5 senhas somente com números. Assim, o total de senhas passaria a ser

$$36^5 - 26^5 - 10^5,$$

um número ainda bastante grande. ◀

Exemplo 3.12. Contaremos a quantidade de divisores do número 75 600.

Fatorando, vemos que

$$75\,600 = 2^4 3^3 5^2 7.$$

Um número inteiro será divisor de 75 600, portanto, se for igual a $2^a 3^b 5^c 7^d$, com

$$\begin{aligned} 0 \leq a \leq 4 \\ 0 \leq b \leq 3 \\ 0 \leq c \leq 2 \\ 0 \leq d \leq 1. \end{aligned}$$

Como todos podem ser zero, há $5 \cdot 4 \cdot 3 \cdot 2$ possibilidades. ◀

Exemplo 3.13. Quantos números de 5 algarismos podemos formar, sendo que a soma do primeiro com o último dígito é par?

Contamos todos os números de 5 dígitos: 10^5. Excluímos: se o primeiro for ímpar e o segundo for par ($5 \cdot 5$), ou o contrário (mais $5 \cdot 5$). Assim,

$$10^5 - 2 \cdot 5^2 \cdot 10^3.$$ ◀

É comum que, ao tentar enumerar os elementos de algum conjunto, contemos a mais para depois descontar. Para isso usamos as formas inversas dos dois princípios básicos de contagem:

- Se há um conjunto que contamos a mais, podemos evidentemente subtraí-lo do total
- Se, *para cada elemento que queríamos contar*, contamos k elementos a mais, dividimos o total por k.

3.1 Permutações

Definição 3.14 (r-permutação)**.** Uma r-*permutação* de n elementos é uma forma de arranjar r desses n elementos em ordem. ♦

Exemplo 3.15. Seja $A = \{a, b, c, d, e\}$. As sequências

$$\begin{aligned} &abced \\ &abcde \\ &baedc \\ &cbade \end{aligned}$$

são 5-permutações de A. Já as sequências

$$\begin{array}{c} acd \\ bde \\ aed \\ bde \end{array}$$

são 3-permutações de A. ◀

Teorema 3.16. *Dado um conjunto A finito, com $|A| = n$, há exatamente $n!/(n-r)!$ r-permutações diferentes dos elementos de A.*

Exemplo 3.17. Seja $A = \{a, b, c, d\}$. Há $4! = 24$ permutações de elementos de A:

abcd	bacd	cabd	dabc
abdc	badc	cadb	dacb
acbd	bcad	cbad	dbac
acdb	bcda	cbda	dbca
adcb	bdac	cdab	dcad
adbc	bdca	cdba	dcda

A quantidade de 2-permutações de A é $4!/2! = 4 \cdot 3 = 12$:

ab	ba	ca	da
ac	bc	cb	db
ad	bd	cd	dc

Já a quantidade de 3-permutações de A é igual a $4!/1! = 4!$, a mesma quantidade de 4-permutações. Isso porque, ao determinarmos os 3 elementos de uma 3-permutação, sobra apenas um para completar uma 4-permutação. ◀

Podemos usar uma definição alternativa: uma r-*permutação* de n elementos é uma função de $\underline{n}$ em $\underline{r}$.

Muitas vezes representamos uma permutação como

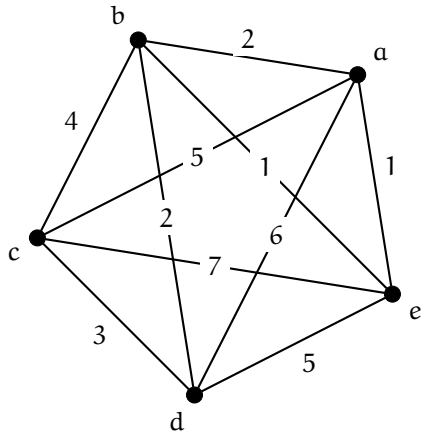
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

onde a linha superior corresponde à ordem anterior dos elementos, e a inferior à ordem imposta pela permutação.

Exemplo 3.18. Um estacionamento tem no total n vagas, uma para cada funcionário. Dessas vagas, somente as quatro vagas de diretores são demarcadas. De quantas maneiras é possível estacionar os carros de todos os funcionários?

Para os diretores, temos $4!$. Para os outros funcionários, $(n-4)!$. Temos portanto $4!(n-4)!$ possibilidades. ◀

Exemplo 3.19. Há n cidades ligadas por estradas, e sabemos o custo de transporte entre cada par de cidades. Isto pode ser representado como um grafo com pesos nas arestas, como na figura a seguir, que dá um exemplo com 5 cidades.



Queremos calcular a maneira mais econômica de percorrer todas as cidades, sem passar por nenhuma delas mais de uma vez, exceto a primeira (que deve ser também a última). Este problema é chamado de *problema do caixeiro viajante*, ou TSP[2].

A quantidade de maneiras diferentes em que podemos percorrer as cidades é exatamente $n!$, já que cada permutação das cidades nos dá um novo percurso. ◀

Exemplo 3.20. Um conjunto X tem 100 elementos. A quantidade de tuplas de tamanho 5 que podemos formar com elementos de X, sem repetição, é

$$\frac{100!}{95!} = 100 \cdot 99 \cdot 98 \cdot 97 \cdot 96.$$ ◀

3.1.1 Com repetições

Se permitirmos repetições de elementos sem limite de reposição, ao invés de termos $(n-1)$ possibilidades para o segundo elemento, $(n-2)$ para o terceiro, etc, teremos sempre n elementos a escolher, portanto há

$$n^r$$

permutações possíveis.

3.1.2 Com objetos idênticos

O número de r-permutações de n objetos, sendo que n_1 deles são de um mesmo tipo; n_2 de um outro tipo, etc, e n_k de um k-ésimo tipo, tais que $n_1 + n_2 + \cdots + n_k = n$, é dado pelo *coeficiente multinomial*

$$\binom{n}{n_1 \quad n_2 \quad \cdots \quad n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

[2] *Travelling Salesperson Problem* em Inglês.

3.2 Combinações

Definição 3.21 (r-combinação)**.** Uma r-*combinação* de n elementos é um subconjunto dos n elementos, tendo tamanho r. ♦

Em outras palavras, uma r-combinação de n elementos é uma seleção de r desses n elementos, sem que importe a ordem.

Teorema 3.22. *O número de combinações diferentes com r elementos escolhidos de um conjunto de tamanho n é*

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Demonstração. O número de r-permutações de n elementos é $n!/(n-r)!$. Cada subconjunto de r elementos foi contado $r!$ vezes (porque cada uma das ordens possíveis foi contabilizada). Assim, para obter o número de r-combinações, basta dividir por $r!$, obtendo a fórmula no enunciado. ■

Exemplo 3.23. Queremos testar a interação entre 8 medicamentos diferentes, quando 3 deles são administrados simultaneamente de cada vez. Queremos portanto testar

$$\binom{8}{3} = \frac{8!}{3!(8-3)!} = 56$$

combinações diferentes de medicamentos. ◄

Exemplo 3.24. Em um estoque há n dispositivos, e r destes tem defeito. Os dispositivos são selecionados aleatoriamente, um a um, para uso. Em quantas das possíveis sequências de uso dois dispositivos defeituosos *não* são selecionados consecutivamente?

Para obter uma sequência sem dois dispositivos defeituosos seguidos, teríamos que obter, entre cada dois funcionais, no máximo um defeituoso. Há $n-m$ dispositivos bons, e $n-m+1$ "espaços" entre eles na sequência de uso. Assim, queremos saber de quantas maneiras os m dispositivos ruins podem ocupar esses espaços[3]:

$$\binom{n-m+1}{m}.$$ ◄

Suponha que queiramos saber quantas soluções existem para a equação

$$x_1 + x_2 + x_3 = 5$$

Sabemos que o valor de cada variável poderá estar entre 1 e 3, e que devem somar 5. Uma maneira simples de encontrar a solução é escrever 5 como a soma de vários uns:

$$1 + 1 + 1 + 1 + 1 = 5$$

[3] Ou seja, a probabilidade de dois defeituosos consecutivos é

$$\frac{n! - \binom{n-m+1}{m}}{n!}$$

e dividir os uns entre x_1, x_2, e x_3 – o que podemos fazer incluindo marcadores que separam a sequência de uns em tres partes. Por exemplo,

$$\overbrace{1}^{x_1}\Big|\overbrace{+1+1}^{x_2}\Big|\overbrace{+1+1}^{x_3} = 5$$

representa $x_1 = 1$, $x + 2 = 2$ e $x_3 = 2$. As duas marcas podem ser inseridas entre um dígito 1 e outro, e portanto há 4 posições para elas. Queremos saber portanto de quantas maneiras podemos selecionar 2 das 4 posições, ou

$$\binom{4}{2} = 6.$$

Generalizando este raciocínio para n variáveis chegamos ao teorema a seguir, cuja demonstração é pedida no exercício 26.

Teorema 3.25. *O número de soluções para a equação $x_1 + x_2 + \cdots + x_n = k$ com todos os x_i inteiros positivos ($x_i > 0$) é igual a*

$$\binom{k-1}{n-1}.$$

Mais ainda, o número de soluções inteiras não negativas ($x_i \geq 0$) é

$$\binom{n+k-1}{k}$$

3.2.1 Com repetições

Definição 3.26 (r-combinação)**.** Uma r-*combinação com repetições* de um conjunto A é um multiconjunto de r elementos, todos pertencentes a A. ♦

Exemplo 3.27. Seja $A = \{a, b, c, d\}$. A seguir temos todas as 3-combinações com repetições de elementos de A (lembramos que permitimos repetições, mas a ordem de apresentação dos elementos não importa).

$\{a, b, c\}$	$\{a, a, b\}$	$\{b, b, c\}$	$\{c, c, d\}$	$\{a, a, a\}$
$\{a, b, d\}$	$\{a, a, c\}$	$\{b, b, d\}$	$\{d, d, a\}$	$\{b, b, b\}$
$\{a, c, d\}$	$\{a, a, d\}$	$\{c, c, a\}$	$\{d, d, b\}$	$\{c, c, c\}$
$\{b, c, d\}$	$\{b, b, a\}$	$\{c, c, b\}$	$\{d, d, c\}$	$\{d, d, d\}$

◀

Teorema 3.28. *Seja A um conjunto com n elementos. Então a quantidade de r-combinações de elementos de A é*

$$\left(\!\!\binom{n}{r}\!\!\right) = \binom{n+r-1}{r}$$

Demonstração. Seja A tal que $|A| = n$. Os multiconjuntos de tamanho r, com elementos de A podem ser enumerados da seguinte forma: para cada elemento de $a_i \in A$,

criamos uma variável x_i que determina o número de vezes que a_i aparece no multiconjunto. Como temos exatamente r elementos, então

$$a_1 + a_2 + \cdots + a_n = r,$$

onde $a_i \geq 0$. Queremos portanto a quantidade de soluções para esta equação, que já sabemos ser igual a

$$\left(\!\!\binom{n}{r}\!\!\right) = \binom{n+r-1}{r}. \qquad \blacksquare$$

3.2.2 Triângulo de Pascal

O exercício 27 pede a demonstração do teorema 3.29.

Teorema 3.29 (identidade de Pascal)**.** *Para todo* $n \in \mathbb{N}$ *e* $1 \leq k \leq n$*,*

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

Se dispusermos, uma linha de cada vez, todos os $\binom{n}{i}$, com $0 \leq i \neq n$, teremos

$$\begin{array}{ccccccc}
\binom{0}{0} & & & & & & \\
\binom{1}{0} & \binom{1}{1} & & & & & \\
\binom{2}{0} & \binom{2}{1} & \binom{2}{2} & & & & \\
\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & & & \\
\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & & \\
\vdots & & & & & \ddots &
\end{array}$$

Mas usando a identidade de Pascal, percebemos que o valor de $\binom{n}{r}$ é dado pela tabela a seguir, conhecida por *triângulo de Pascal*.

		r				
		0	1	2	3	4	
	0	1					
	1	1	1				
n	2	1	2	1			
	3	1	3	3	1		
	4	1	4	6	4	1	
	⋮	⋮					⋱

Podemos, na verdade, dispor os elementos do triângulo de Pascal de diferentes ma-

neiras na forma de matriz, definindo assim *matrizes de Pascal* de ordem n:

$$B_{i,j} = \binom{i-1}{j-1}, \text{se } i \geq j.$$
$$C_{i,j} = \binom{i+j-1}{j-1}$$
$$P_{i,j} = \binom{j-1}{i-1}, \text{se } j \geq i.$$

Assim, temos

$$P_4 = \begin{pmatrix} \binom{0}{0} & \binom{1}{1} & \binom{2}{2} & \binom{3}{3} \\ \binom{1}{0} & \binom{2}{1} & \binom{3}{2} & \binom{4}{3} \\ \binom{2}{0} & \binom{3}{1} & \binom{4}{2} & \binom{5}{3} \\ \binom{3}{0} & \binom{4}{1} & \binom{5}{2} & \binom{6}{3} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{pmatrix}.$$

$$B_4 = \begin{pmatrix} \binom{0}{0} & 0 & 0 & 0 \\ \binom{1}{0} & \binom{1}{1} & 0 & 0 \\ \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & 0 \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{pmatrix}.$$

$$C_4 = B_4^T = \begin{pmatrix} \binom{0}{0} & \binom{1}{1} & \binom{2}{0} & \binom{3}{0} \\ 0 & \binom{1}{1} & \binom{2}{1} & \binom{3}{1} \\ 0 & 0 & \binom{2}{2} & \binom{3}{2} \\ 0 & 0 & 0 & \binom{3}{3} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Além de P_n serem evidentemente simétrica, as matrizes de Pascal tem diversas propriedades interessantes. Listamos a seguir algumas delas.

Teorema 3.30. *Para todo* $n \in \mathbb{N}$, $\det B_n = \det C_n = 1$.

Demonstração. Segue trivialmente se observarmos que as diagonais de B_n e C_n só contém uns. ■

Teorema 3.31. *Para todo* $n \in \mathbb{N}$, $B_n C_n = P_n$, *e* $C_n B_n = |(P_n)^{-1}|$.

Exemplo 3.32. Verificamos aqui que $B_4 C_4 = P_4$.

$$B_4 C_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{pmatrix}.$$ ◀

Corolário 3.33. *Para todo* $n \in \mathbb{N}$, $\det P_n = \det P_n^{-1} = 1$.

Teorema 3.34. *A inversa de* B_n *é igual a* B_n, *exceto por seus elementos terem sinais alternados abaixo da diagonal; o mesmo vale para* C_n.

Corolário 3.35. *A decomposição LU de* P_n *é* (B_n, C_n).

O triângulo de Pascal tem uma grande quantidade de propriedades interessantes – boa parte delas pode ser encontrada no livro de Bondarenko [Bon92].

3.3 Coeficientes binomiais

Teorema 3.36. *Sejam x e y pertencentes a um corpo, e n um inteiro positivo. Então*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

Demonstração. Considere os coeficientes possíveis para $x^{n-k}y^k$, para um k fixo.

A expressão $(x+y)^n = (x+y)(x+y)\cdots$ terá termos $x^{n-i}y_i$, mas com i variando somente entre 0 e n. Para cada termo da expansão, escolhemos $n-i$ vezes a variável x e i vezes a variável y. Há $\binom{n}{i}$ maneiras de fazê-lo, por isso $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i$. ■

Exemplo 3.37.

$$\begin{aligned}(x+y)^6 =& \binom{6}{0}x^6 + \binom{6}{1}x^5y + \binom{6}{2}x^4y^2 \\ &+ \binom{6}{3}x^3y^3 + \binom{6}{4}x^2y^4 + \binom{6}{5}xy^5 + \binom{6}{6}y^6 \\ =& x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y\end{aligned}$$ ◄

3.4 Aproximações para $n!$ e $\binom{n}{k}$

A função fatorial permeia toda a Combinatória. Como seu cálculo é demorado se usarmos a definição, damos aqui uma fórmula para aproximar $n!$.

Definição 3.38 (aproximação de Stirling para $n!$)**.** A *aproximação de Stirling* para o fatorial é

$$s_n = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n. \tag{3.1}$$

♦

O teorema a seguir justifica o uso desta aproximação. A demonstração, no entanto, requer ferramental que não pretendemos apresentar neste texto.

Teorema 3.39. *Seja s_n definido como na equação 3.1. Então*

$$\lim_{n\to\infty} \frac{n!}{s_n} = 1.$$

Além de $n!$, podemos querer aproximar $\binom{n}{k}$.

Teorema 3.40. *para todos n e k naturais,*

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

Teorema 3.41. *Para qualquer n natural,*

$$\binom{2n}{n} \approx \frac{2^{2n}}{\sqrt{\pi n}}.$$

3.5 Teorema binomial generalizado

O teorema binomial nos dá a expansão de $(a+b)^k$ para k inteiro, e é evidente que seria interessante generalizá-lo para qualquer expoente real.

Teorema 3.42. *Para quaisquer $k \in \mathbb{N}$ e $x \in (-1,1)$,*

$$\begin{aligned}(1+x)^r &= 1 + rx + \frac{r(r-1)}{2!}x^2 + \frac{r(r-1)(r-2)}{3!}x^3 + \cdots + \frac{r(r-1)\cdots(r-k+1)}{k!}x^k + \cdots \\ &= \sum_{k=0}^{\infty} \frac{r(r-1)\cdots(r-k+1)}{k!}x^k\end{aligned}$$

Demonstração. Basta tomar a expansão de Taylor de $(1-x)^r$ em zero. ■

Denotamos, para $r \in \mathbb{R}$ e $k \in \mathbb{Z}$,

$$\binom{r}{k} = \frac{r(r-1)\cdots(r-k+1)}{k!}$$

Exemplo 3.43.

$$\begin{aligned}\binom{-\sqrt{3}}{4} &= \frac{-\sqrt{3}(-\sqrt{3}-1)(-\sqrt{3}-2)(-\sqrt{3}-3)}{4!} \\ &= \frac{7\sqrt{3}+12}{4\sqrt{3}} \\ &= \sqrt{3} + \frac{7}{4}.\end{aligned}$$

◄

Como consequência, temos o teorema a seguir.

Teorema 3.44. *Para $r, k \in \mathbb{N}$,*

$$\binom{-r}{k} = (-1)^k \left(\!\!\binom{r}{k}\!\!\right).$$

Consequentemente, $\left|\binom{-r}{k}\right| = \left(\!\!\binom{r}{k}\!\!\right)$.

Para r inteiro negativo, podemos obter os valores de $\binom{r}{k}$ usando a identidade de Pascal. Com isso também obtemos os valores de $\left(\!\!\binom{r}{k}\!\!\right)$. Por exemplo,

$$\begin{array}{l|l|l}
\left(\!\!\binom{-1}{0}\!\!\right) = (-1)^0\left(\!\!\binom{1}{0}\!\!\right) = +1 & \left(\!\!\binom{-1}{0}\!\!\right) = (-1)^0\left(\!\!\binom{1}{0}\!\!\right) = +1 & \left(\!\!\binom{-1}{0}\!\!\right) = (-1)^0\left(\!\!\binom{1}{0}\!\!\right) = +1 \\
\left(\!\!\binom{-2}{1}\!\!\right) = (-1)^1\left(\!\!\binom{1}{1}\!\!\right) = -1 & \left(\!\!\binom{-2}{1}\!\!\right) = (-1)^1\left(\!\!\binom{1}{1}\!\!\right) = -2 & \left(\!\!\binom{-2}{1}\!\!\right) = (-1)^1\left(\!\!\binom{1}{1}\!\!\right) = -3 \\
\left(\!\!\binom{-3}{2}\!\!\right) = (-1)^2\left(\!\!\binom{1}{2}\!\!\right) = +1 & \left(\!\!\binom{-3}{2}\!\!\right) = (-1)^2\left(\!\!\binom{1}{2}\!\!\right) = +3 & \left(\!\!\binom{-3}{2}\!\!\right) = (-1)^2\left(\!\!\binom{1}{2}\!\!\right) = +6 \\
\left(\!\!\binom{-4}{3}\!\!\right) = (-1)^3\left(\!\!\binom{1}{3}\!\!\right) = -1 & \left(\!\!\binom{-3}{3}\!\!\right) = (-1)^3\left(\!\!\binom{1}{2}\!\!\right) = -4 & \left(\!\!\binom{-4}{3}\!\!\right) = (-1)^3\left(\!\!\binom{1}{2}\!\!\right) = -10 \\
\vdots & \vdots & \vdots
\end{array}$$

Podemos portanto expandir o triângulo de Pascal, criando uma parte "superior", incluindo linhas com índice negativo.

		k					
		0	1	2	3	4	
	⋮	⋮					
	−3	1	−3	6	−10	15	⋯
	−2	1	−2	3	−4	5	⋯
	−1	1	−1	1	−1	1	⋯
	0	1					
	1	1	1				
n	2	1	2	1			
	3	1	3	3	1		
	4	1	4	6	4	1	
	⋮	⋮					⋱

Exemplo 3.45 (aproximação de raiz quadrada)**.** O teorema binomial generalizado nos dá imediatamente um método para calcular raízes de números reais entre 0 e 2: basta computar $(1+x)^{1}/k$, com $x \in (-1,1)$. Podemos também usar o mesmo método para calcular raízes de *qualquer* número real.

Como exemplo, calcularemos a raiz quadrada de 40.

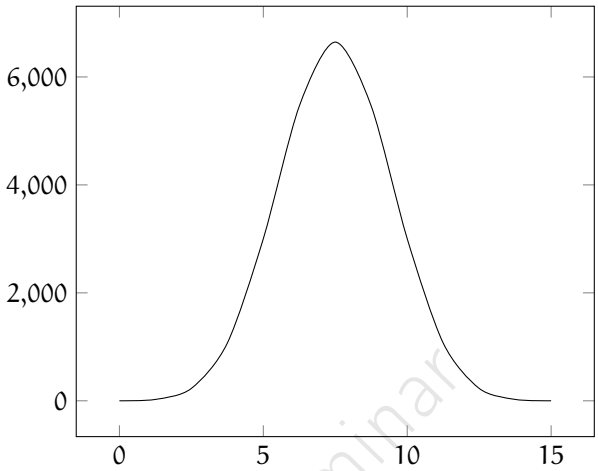
$$\begin{aligned}\sqrt{40} &= \sqrt{36+4} && \text{(36: quadrado perfeito abaixo de 40)}\\ &= \sqrt{36\left(1+\frac{4}{36}\right)}\\ &= 6\sqrt{1+\frac{1}{9}}.\end{aligned}$$

Como $|1/9| < 1$, podemos usar o teorema binomial generalizado.

$$\begin{aligned}\sqrt{40} &= 6\sqrt{1+\frac{1}{9}}\\ &= 6\left[1+\frac{1}{2}\left(\frac{1}{9}\right)\right.\\ &+ \frac{(1/2)(1/2-1)}{2!}\left(\frac{1}{9}\right)^2\\ &+ \frac{(1/2)(1/2-1)(1/2-2)}{3!}\left(\frac{1}{9}\right)^3\\ &+ \frac{(1/2)(1/2-1)(1/2-2)(1/2-3)}{4!}\left(\frac{1}{9}\right)^4\\ &\left.+ \frac{(1/2)(1/2-1)(1/2-2)(1/2-3)(1/2-4)}{5!}\left(\frac{1}{9}\right)^5+\cdots\right]\end{aligned}$$

O valor da aproximação com cinco termos (ou seja, contando até $(1/9)^4$) é 6.324552..., bastante próximo de $\sqrt{40} = 6.3245553\ldots$ ◀

A figura a seguir mostra uma aproximação contínua do gráfico de $\binom{15}{x}$, com x variando de 0 a 15.



3.6 Problemas de ocupação: objetos e locais distinguíveis

3.7 Problemas de ocupação: objetos indistinguíveis, locais distinguíveis

Exercícios

Ex. 19 — Quantos anagramas existem para a palavra "CAPOTE"?

Ex. 20 — Quantas colorações de arestas com k cores existem para um grafo $G = (V, E)$?

Ex. 21 — Um sistema usa senhas que podem variar entre 8 e 10 caracteres. O sistema exige que as senhas tenham pelo menos dois dígitos, duas letras, e dois caracteres especiais, que podem ser ponto (.), traço (-) ou barra (/). Quantas são as senhas possíveis sem as restrições e quantas são com as restrições? [há oficialmente 26 letras em nosso alfabeto]

Ex. 22 — Se placas de carro são representadas por k letras e $k + 1$ números, quanto deve valer k para que possamos representar 10 milhões de carros?

Ex. 23 — Quantos vetores binários de tamanho n existem com média estritamente acima de 0.5?

Ex. 24 — (Difícil) Nos items que seguem considere matrizes cujas entradas são números entre zero e dez.

- Quantas matrizes quadradas de ordem n existem onde uma e apenas uma linha é multiplo de outra?
- Quantas matrizes quadradas de ordem n existem com posto $n-1$? E com posto exatamente $n-k$? E quantas existem com posto *no mínimo* $n-k$
- Quantas matrizes quadradas de ordem n singulares e não singulares existem?

Ex. 25 — Calcule

$$\sum_{k=0}^{n} \binom{n}{k}.$$

Ex. 26 — Prove o teorema 3.25.

Ex. 27 — Prove o teorema 3.29.

Ex. 28 — Prove o teorema binomial usando indução.

Ex. 29 — Mostre a expansão de

a) $(1+x)^n$

b) $(x+y)^n(x-y)^n$

c) $(x+y)^n(x-y)^n(-x+y)^n$

d) $(x+y+z)^n$

e) $(x_1+x_2+\cdots+x_k)^n$

f) $\left(\sum_{i=1}^{k}(-1)^i x_i\right)^n$

Ex. 30 — O teorema binomial pode ser usado para calcularmos a expansão de $(A+B)^n$, onde $n \in \mathbb{N}$ e A, B são matrizes quadradas? Porque?

Ex. 31 — Aproxime $\sqrt[3]{50}$ usando o teorema binomial generalizado. Use quatro termos na aproximação.

Ex. 32 — Qual é o número de relações diferentes que podemos definir em um conjunto de tamanho n?

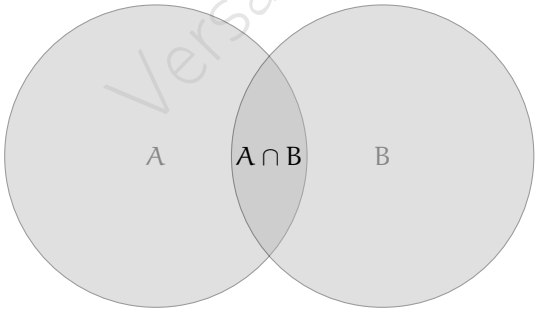
Capítulo 4

Princípio da Inclusão e Exclusão

Este Capítulo versa sobre o problema de determinar a cardinalidade da união de diversos conjuntos não disjuntos, sabendo as cardinalidades das interseções entre os conjuntos.

Está claro, inicialmente, que para quaisquer dois conjuntos A e B,

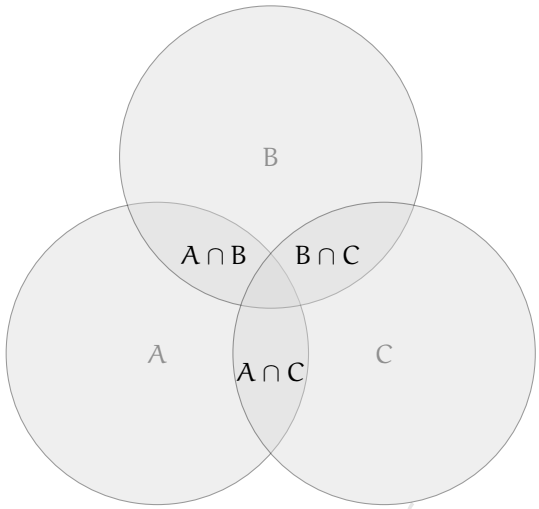
$$|A \cup B| = |A| + |B| - |A \cap B|.$$



Tendo tres conjuntos e usando raciocínio semelhante,

$$\begin{aligned} |A \cup B \cup C| = {} & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C|, \end{aligned}$$

como é possível verificar facilmente a partir da figura a seguir.



Generalizando para n conjuntos, observamos que

$$\begin{aligned}|A_1 \cup A_2 \cup \cdots A_n| = {} & |A_1| + |A_2| + \cdots + |A_n| \\ & - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_{n-1} \cap A_n| \quad \text{(2-combinações)} \\ & + |A_1 \cap A_2 \cap A_3| + \cdots |A_{n-2} \cap A_{n-1} \cap A_n| \\ & \qquad \text{(3-combinações)} \\ & \vdots \\ & \pm |A_1 \cap \cdots A_n|. \qquad \text{(interseção de todos)}\end{aligned}$$

Tomamos primeiro os conjuntos isolados e somamos suas cardinalidades; depois subtraímos as 2-combinações; somamos as 3-combinações; e assim por diante. Listamos as r-combinações, com r variando de 1 a n. Quando r é ímpar, somamos, e quando é par, subtraímos (ou seja, somamos $(-1)^r$ vezes as cardinalidades).

Podemos expressar este processo informalmente da seguinte forma.

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^k \underbrace{\sum \left|\bigcap A_i\right|}_{\text{todas k-combinações}}$$

O teorema 4.1 expressa com rigor esta idéia.

Teorema 4.1. *Sejam $A_1, A_2, \ldots, A_n$ conjuntos finitos. Então*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \binom{n}{k}} \left|\bigcap_{i \in I} A_i\right|,$$

onde $\binom{n}{k}$ é o conjunto de combinações de k elementos de $\underline{n}$.

Demonstração. Seja x um elemento qualquer da união dos conjuntos. Este elemento deve ser contado uma vez na união de todos os conjuntos.

Presuma que x está nos conjuntos $A_1, A_2, \ldots, A_k$, mas não nos outros conjuntos $A_{k+1}, \ldots, A_n$.

x está em todas as interseções envolvendo *apenas* conjuntos $A_1, \ldots, A_k$, e em nenhuma das outras interseções. Assim, x está em todas as tuplas de j elementos, com j variando de 1 a k. Para cada j há $\binom{k}{j}$ interseções, portanto x aparece em

$$k + \binom{k}{2} + \binom{k}{3} + \cdots + \binom{k}{k}$$

interseções. No entanto, cada interseção, ao ser somada na fórmula, é multiplicada por $(-1)^{j-1}$, e portanto x contribui para a contagem

$$k - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k-1}\binom{k}{k}$$

vezes. Esta quantidade é igual a um, e portanto cada elemento x é contabilizado exatamente uma vez. ■

Exemplo 4.2. Para determinar quantos múltiplos de 5 e de 11 existem entre 1 e 2000, calculamos:

- $2000/5 = 400$ múltiplos de 5,
- $\lfloor 2000/11 \rfloor = 181$ múltiplos de 11.

No entanto, calculamos duas vezes cada número que é múltiplo de 5 e também de 11 – ou seja, múltiplos de 55. Descontamos então estes números (há $\lfloor 2000/55 \rfloor = 36$ deles) e temos

$$400 + 181 - 36 = 545$$

múltiplos de 5 e de 11 entre 1 e 2000. ◄

Exemplo 4.3. Há 2700 pessoas em um vilarejo. Destas, $3/4$ cometeram alguma infração de transito no último ano. $1/3$ é réu em processo civil e $1/5$ tem algum tipo de pendência com o fisco. Sabe-se que o número de pessoas que é réu e que também tem problemas com o fisco é 300; que o número de infratores de transito que são réus é 400; e também que a quantidade de infratores em débito com o fisco é 100. Quantos cidadãos tem os tres tipos de problema?

Temos

$$|T| = \frac{3}{4}2700 = 2025,$$
$$|C| = \frac{1}{3}2700 = 900,$$
$$|F| = \frac{1}{5}2700 = 540.$$

As interseções são:

$$|T| \cap |C| = \frac{3}{4}2700 = 400,$$
$$|T| \cap |F| = \frac{1}{3}2700 = 100,$$
$$|C| \cap |F| = \frac{1}{5}2700 = 300.$$

A quantidade que se quer é $|T \cap C \cap F|$. Pelo princípio da inclusão e exclusão,

$$2700 = (2025 + 900 + 540) - (400 + 100 + 300) + x,$$

e portanto o número procurado é $x = 35$. ◀

4.1 Permutações caóticas

Definição 4.4 (permutação caótica)**.** Uma *permutação caótica* é uma permutação que não deixa nenhum elemento em sua posição original – ou seja, a permutação tem como entrada uma tupla $(x_1, x_2, \ldots, x_n)$ e como saída $(y_1, y_2, \ldots, y_n)$ tal que $x_i \neq y_i$ para todo i. ♦

Exemplo 4.5. A permutação

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix},$$

apresentada na página 25, é caótica. Já a permutação

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

não é caótica, porque não modifica o elemento na segunda posição. ◀

Teorema 4.6. *A quantidade de permutações caóticas com n elementos, denotada por $!n$, é*

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

Demonstração. Seja P_i o conjunto das permutações que preservam a i-ésima posição. As permutações caóticas devem excluir as permutações em todos os P_i's. No entanto, as interseções entre os P_i não são vazias. Usamos portanto o princípio da inclusão e exclusão: retiramos de $n!$ (quantidade total de permutações) aquelas que pertencem

a algum P_i.

$$\begin{aligned} !n = n! &- \sum_i |P_i| \\ &+ \sum_{i\neq j} |P_i \cap P_j| \\ &- \sum_{i\neq j\neq k} |P_i \cap P_j \cap P_k| \\ &+ \vdots \\ &+ (-1)^n |P_1 \cap \cdots \cap P_n|. \end{aligned}$$

A quantidade de termos nos somatórios desta fórmula é

$$\begin{aligned} n \text{ em } &\sum_i \\ \binom{n}{2} \text{ em } &\sum_{i\neq j} \\ \binom{n}{3} \text{ em } &\sum_{i\neq j\neq k} \\ &\vdots \\ \binom{n}{n} = 1 \text{ na } &\text{última linha.} \end{aligned}$$

Note que o tamanho de $|P_i|$ deve ser $(n-1)!$, porque mantemos fixa a posição i e contamos as permutações dos outros elementos. Usando o mesmo raciocínio para os outros conjuntos na fórmula, temos

$$\begin{aligned} |P_i| &= (n-1)! \\ |P_i \cap P_j| &= (n-2)! \\ |P_i \cap P_j \cap P_k| &= (n-3)! \\ &\vdots \\ |P_1 \cap \cdots \cap P_n| &= (n-n)! = 1 \end{aligned}$$

Nos falta somente substituir estes valores na fórmula:

$$\begin{aligned} !n &= n! - n(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \cdots + (-1)^n 1 \\ &= n! - \frac{n!}{1!} + \frac{n!}{2!(n-2)!}(n-2)! - \frac{n!}{3!(n-3)!}(n-3)! + \cdots + (-1)^n \frac{n!}{n!} \\ &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \cdots + (-1)^n \frac{n!}{n!} \\ &= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right). \end{aligned}$$

■

O próximo teorema mostra uma surpreendente relação entre o número e e a quantidade de permutações caóticas, e nos dá uma outra maneira de calcular $!n$.

Teorema 4.7. *Para todo* $n \in \mathbb{N}^+$,

$$!n = \left\lfloor \frac{n!}{e} \right\rceil.$$

Demonstração. Para $n = 1$ e $n/2$ pode-se verificar facilmente que $\lfloor n!/e \rceil = 1$

Para $n > 2$, basta mostrar que $|!n - n!/e| < 1/2$. A expansão de Taylor para e^x é

$$e^x = \frac{x^0}{0!} + \frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots,$$

e que portanto

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots$$

Calculamos

$$\begin{aligned}
\left|!n - \frac{n!}{e}\right| &= \left|n!(1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + (-1)^n \frac{1}{n!}) - n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots)\right| \\
&= \left|n! \sum_{i=0}^{n} \frac{(-1)^i}{i!} - n! \sum_{i=0}^{\infty} \frac{(-1)^i}{i!}\right| \\
&= \left|n! \sum_{i=n+1}^{\infty} \frac{(-1)^i}{i!}\right| \\
&\leq n! \left(\sum_{i=n+1}^{\infty} \frac{1}{i!}\right) \\
&= \sum_{i=n+1}^{\infty} \frac{n!}{i!} \\
&= \sum_{i=1}^{\infty} \frac{n!}{(n+i)!} \\
&= \frac{1}{(n+1)} + \frac{1}{(n+1)(n+2)} + \cdots \\
&\leq \sum_{i=1}^{\infty} \frac{1}{(n+1)^i} \\
&= \frac{1}{n} \\
&< \frac{1}{2}.
\end{aligned}$$

■

Exemplo 4.8. O número de permutações caóticas com 10 elementos é

$$\begin{aligned}
!n &= n!\left(1+\sum_{i=1}^{n}\frac{(-1)^i}{i!}\right)\\
&= n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\cdots+\frac{1}{10!}\right)\\
&= 10!\left(\frac{16481}{44800}\right)\\
&= 1334961.
\end{aligned}$$

Usando a forma fechada obtemos o mesmo valor,

$$!n = \left\lfloor\frac{10!}{e}\right\rceil = \left\lfloor\frac{3628800}{e}\right\rceil = \lfloor 1334960.916\ldots\rceil = 1334961. \qquad \blacktriangleleft$$

4.2 $\phi(n)$: contando co-primos

Definição 4.9 (função $\phi(n)$ (tociente))**.** Dado um número natural $n \geq 1$, $\phi(n)$ é a quantidade de números entre 1 e n que são co-primos com n. ♦

Exemplo 4.10. $\phi(10) = 4$, porque são coprimos com dez os números 1, 3, 7, e 9. ◀

Exemplo 4.11. Para todo primo p, $\phi(p) = p - 1$, já que p é coprimo com qualquer número natural – inclusive os menores que p. ◀

Teorema 4.12. *Seja n um inteiro cuja fatoração em primos é*

$$n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\ldots p_k^{a_s}$$

Então

$$\phi(n) = n\prod\left(1-\frac{1}{p_i}\right).$$

Demonstração. Sejam $p_1, p_2, \ldots, p_s$ os fatores primos de n. Sejam D_i os conjuntos de divisores de n:

$$\begin{aligned}
D_1 &= \{qp_1 : q \in \mathbb{N}\}\\
D_2 &= \{qp_2 : q \in \mathbb{N}\}\\
&\vdots\\
D_s &= \{qp_s : q \in \mathbb{N}\}
\end{aligned}$$

A quantidade que queremos é

$$\begin{aligned}
\phi(n) &= |\underline{n}| - \left|\bigcup D_i\right|\\
&= n - \left(\sum_i |D_i| - \sum_{i\neq j}|D_i \cap D_j| + \cdots + (-1)^s|A_1 \cap \cdots \cap A_n|\right).
\end{aligned}$$

Observamos que

$$|A_i| = \frac{n}{p_i},$$
$$|A_i \cap A_j| = \frac{n}{p_i p_j},$$

e de maneira geral,

$$|A_i \cap \cdots \cap A_q| = \frac{n}{p_i \cdots p_q}.$$

Assim,

$$\begin{aligned}\phi(n) &= n - \sum_i \frac{n}{p_i} + \sum_{i\neq j} \frac{n}{p_i p_j} - \sum_{i\neq j\neq k} \frac{n}{p_i p_j p_k} + \cdots + (-1)^s \frac{n}{p_1 p_2 \cdots p_s} \\ &= n\left(1 - \sum_i \frac{1}{p_i} + \sum_{i\neq j} \frac{1}{p_i p_j} - \sum_{i\neq j\neq k} \frac{1}{p_i p_j p_k} + \cdots + (-1)^s \frac{1}{p_1 p_2 \cdots p_s}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right).\end{aligned}$$

■

Exemplo 4.13. Seja $n = 2004$. Sua fatoração é

$$n = 2^2 \cdot 3 \cdot 167,$$

portanto

$$\begin{aligned}\phi(n) &= 2004\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{167}\right) \\ &= 2004\left(\frac{166}{501}\right) \\ &= 664.\end{aligned}$$

◀

4.3 Contagem de funções sobrejetoras

Exercícios

Ex. 33 — Se $|A| = 5$, $|B| = 10$, $|C| = 4$, $|A \cap B| = 3$, $|A \cap C| = 1$, $|B \cap C| = 2$, e $|A \cap B \cap C| = 1$, quantos elementos tem $|A \cup B \cup C|$?

Ex. 34 — Quantos números entre 1 e 3000 são divisíveis por 11, 14 ou 6?

Ex. 35 — Demonstre o teorema 4.1 por indução.

Ex. 36 — Mostre que o teorema 4.1, que enuncia o princípio da inclusão e exclusão, pode ser reescrito da seguinte forma, mais compacta[1].

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\emptyset \neq I \subseteq \underline{n}} (-1)^{|I|-1} \left|\bigcap_{i \in I} A_i\right|.$$

[1] De acordo com Matousek Nesetril [MN98] (p. 88), esta é a "mais curta e quase diabólica forma de descrever o princípio da inclusão e exclusão".

Capítulo 5

Funções Geradoras

Neste Capítulo usamos operações em séries de potências (polinômios com infinitos termos) em processos de contagem.

Definição 5.1 (série de potências)**.** Uma *série formal de potências* é uma soma de infinitos termos

$$a_0 + a_1 x + a_2 x^2 + \cdots,$$

ou

$$\sum_{n=0}^{\infty} a_n x^n.$$

Cada série formal de potências representa unicamente a sequência de seus coeficientes (a_n). ♦

Por ora não nos interessará se uma dada série de potencias converge ou não[1].

Nas próximas seções apresentamos as funções geradoras ordinárias, que usaremos na contagem de objetos quando a ordem não importa, e funções geradoras exponenciais, usadas na contagem de objetos cuja ordem é relevante.

5.1 Funções geradoras ordinárias

Estamos interessados na representação da sequencia de coeficientes de uma série de potências. A forma $\sum_n a_n x^n$ nos dá uma representação compacta dessa sequencia.

[1] Mesmo assim observamos que

- Toda série de potências converge para $x = 0$, e
- Toda série de potências converge se $|x| < 1$ e os coeficientes são limitados ($|a_n| < M$ ara algum $M \in \mathbb{R}$).

Definição 5.2 (função geradora ordinária)**.** Seja (a_n) uma sequência. A *função geradora ordinária* de (a_n) é a série formal de potências

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Denotamos por $[x^n]A(x)$ o coeficiente de x^n em $A(x)$. ♦

Exemplo 5.3. Na função geradora

$$A(x) = 1 + x + x^2 + x^3 + \cdots$$

temos $[x^3]A(x) = 3$, e de maneira geral, $[x^n]A(X) = x$, ou seja, a sequencia representada é $a_n = 1$, cujos termos são

$$(1, 1, 1, \ldots).$$

Para $x \in (-1, 1)$, esta série converge para

$$\frac{1}{1-x},$$

por isso dizemos que $\frac{1}{1-x}$ é a função geradora da sequência $a_n = 1$. ◄

Exemplo 5.4. A função geradora

$$C(x) = (1 + x)^n$$

nos dá os coeficientes binomiais de $\binom{n}{0}$ até $\binom{n}{n}$.

$$\begin{aligned}(1+x)^n &= \binom{n}{0}1^n x^0 + \binom{n}{1}1^{n-1}x + \binom{n}{2}1^{n-2}x^2 + \cdots + \binom{n}{n}1^0 x^n \\ &= 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + x^n,\end{aligned}$$

ou seja, $[x^k]C(x) = \binom{n}{k}$.

Dizemos que $(1 + x)^n$ *é a função geradora ordinária para o problema de determinar a quantidade de combinações* $\binom{n}{k}$. ◄

Exemplo 5.5. Verificamos agora a sequencia gerada pela função geradora

$$\frac{1}{\sqrt{1-4x}}.$$

Usamos o teorema binomial generalizado,

$$(1+z)^r = \sum_{i=0}^{\infty} \binom{r}{i} z^i,$$

com $z = -4x$ e $r = -1/2$.

$$\begin{aligned}(1-4x)^{-1/2} &= \sum_{i=0}^{\infty} \binom{-1/2}{i} (-4x)^i \\ &= \sum_{i=0}^{\infty} \overbrace{\frac{(-1/2)(-1/2-1)\cdots(-1/2-i+1)}{i!}}^{*} \underbrace{(-1)^i}_{**} 4^i x^i.\end{aligned}$$

Na fração $(-1/2)(-1/2-1)\cdots(-1/2-i+1)$, marcado com $(*)$, podemos verificar que todos os fatores, $(-1/2)$, $(-1/2-1)$, $(-1/2-2)$, etc, são menores que zero. De $1/2$ até $1/2-i+1$ há $i+2$ fatores, portanto o sinal deste produto será $(-1)^{i+2}$. Como este é também o sinal de $(-1)^i$, marcado com $(**)$, teremos sempre dois números de mesmo sinal sendo multiplicados. O resultado será sempre positivo. Assim,

$$\begin{aligned}(1-4x)^{-1/2} &= 1 + \sum_{i=1}^{\infty} \frac{(1/2)(3/2)(5/2)\cdots((2i-1)/2)}{i!} 4^i x^i \\ &= 1 + \sum_{i=1}^{\infty} \frac{1\cdot 3\cdot 5\cdots(2i-1)}{\underbrace{2\cdot 2\cdot 2\cdots 2}_{i \text{ ocorrencias de } 2}} \left(\frac{1}{i!}\right) 4^i x^i \\ &= 1 + \sum_{i=1}^{\infty} \frac{1\cdot 3\cdot 5\cdots(2i-1)}{2^i i!} 4^i x^i \\ &= 1 + \sum_{i=1}^{\infty} \frac{1\cdot 3\cdot 5\cdots(2i-1)}{i!} 2^i x^i \\ &= 1 + \sum_{i=1}^{\infty} \frac{1\cdot 3\cdot 5\cdots(2i-1)[i!2^i]}{i!i!} x^i \\ &= 1 + \sum_{i=1}^{\infty} \frac{1\cdot 3\cdot 5\cdots(2i-1)[2\cdot 4\cdot 6\cdots 2i]}{i!i!} x^i \\ &= 1 + \sum_{i=1}^{\infty} \frac{2i!}{i!i!} x^i \\ &= \sum_{i=0}^{\infty} \binom{2i}{i} x^i.\end{aligned}$$

Assim, $(1-4x)^{-1/2}$ gera a sequencia

$$\binom{0}{0}, \binom{2}{1}, \binom{4}{2}, \cdots, \binom{2n}{n}, \cdots \qquad \blacktriangleleft$$

Para resolver problemas usando funções geradoras, precisaremos realizar operações com elas. O teorema a seguir lista algumas destas operações.

Teorema 5.6. *Sejam* (a_n) *e* (b_n) *sequências com funções geradoras* $A(x)$ *e* $B(x)$*. Então*

i) $A(x) + B(x)$ *é função geradora para* $(a_n) + (b_n)$*, que é igual a*

$$a_0b_0 + a_1b_1 + a_2b_2 + \cdots$$

ii) $kA(x)$ *é função geradora para* $k(a_n)$*,*

$$ka_0, ka_1, ka_2, \ldots$$

iii) $A(x)B(x)$ *é função geradora para* (c_n)*, onde*

$$c_n = \sum_{\substack{i,j\geq 0 \\ i+j=n}} a_ib_j.$$

Esta sequencia é

$$\begin{aligned} &a_0b_0, \\ &a_0b_1 + a_1b_0, \\ &a_0b_2 + a_1b_1 + a_2b_0, \\ &a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \\ &\vdots \end{aligned}$$

Exemplo 5.7. Queremos encontrar a função geradora para

$$(0, 0, 1, 1, 1, \ldots).$$

Esta sequencia se parece com a sequência $(0, 1, 1, 1, \ldots)$ do exemplo 5.3, que é $\frac{1}{1-x}$.

Aqui observamos que se multiplicarmos uma sequencia inteira por x, cada termo a_kx^k passa a ser $a_kxx^k = a_kx^{k+1}$, e portanto o coeficiente a_k passa a ser o coeficiente de x^{k+1}. Usando este fato percebemos que para transformar $1+x+x^2+x^3+\cdots$ em $0 + 0x + 0x^2 + x^3 + x^4 + \cdots$, basta multiplicar por x^2. A função geradora que queremos é, portanto,

$$x^2\left(\frac{1}{1-x}\right) = \frac{x^2}{1-x}. \qquad \blacktriangleleft$$

O exemplo anterior mostra que algumas operações nas funções geradoras tem efeito simples e bem definido na sequencia de coeficientes.

Exemplo 5.8. Determinaremos a função geradora da sequencia

$$0, \frac{1}{2!}, \left(1 + \frac{1}{3!}\right), \frac{1}{4!}, \frac{1}{5!}, \cdots$$

Esta sequencia se parece com e^x, exceto pelo coeficiente de x^3. Sua função geradora é, claramente,

$$e^x + x^3. \qquad \blacktriangleleft$$

Exemplo 5.9. Considere a série de potências

$$A(x) = \frac{1}{1-x^2}.$$

Obteremos sua sequência de coeficientes. Conhecemos uma função geradora bastante parecida com esta,

$$B(x) = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots,$$

que gera a sequência $(1, 1, 1, \ldots)$.

A diferença entre as duas está somente na troca de x por x^2 – ou seja, se subtituirmos x por x^2 em $B(x)$ obteremos $A(x)$:

$$B(x^2) = \frac{1-(x^2)}{=}A(x).$$

Já podemos desta forma identificar os coeficientes de $A(x)$:

$$A(x) = B(x^2) = 1 + x^2 + x^4 + x^6 + \cdots,$$

e a sequência gerada é $(1, 0, 1, 0, \ldots)$. ◀

5.1.1 Aplicações em contagem

Damos a seguir um exemplo de uso de funções geradoras na resolução de um problema simples.

O exemplo a seguir é extremamente importante, porque explicita a intuição a respeito do mecanismo que usamos para realizar contagem com funções geradoras.

Exemplo 5.10. Suponha que queiramos escolher selecionar objetos de dois tipos, sendo que os objetos de cada tipo são indistinguíveis entre si, e sem que importa a ordem em que são apresentados. Chamaremos o primeiro tipo de T_1, o segundo de T_2.

Suponha que haja a seguinte restrição: podemos usar no máximo três objetos do tipo T_1, e mo máximo dois objetos do tipo T_2.

Ob;servamos que ao multiplicar dois monômios ax^p e bx^q, obtemos $(ab)x^{p+q}$ – os coeficientes são multiplicados, e os expoentes somados. Se representarmos objetos do tipo T_1 e T_2 por

$$T_1 : (t_1x^0 + t_1x^1 + t_1x^2 + t_1x^3)$$
$$T_2 : (t_2x^0 + t_2x^1 + t_2x^2),$$

podemos multiplicar os dois polinômios e observar que ao multiplicar, por exemplo, o termo t_1x^3 pelo termo t_2x^1, obteremos $t_1t_2x^4$. Usamos uma analogia e dizemos que tínhamos dois objetos do tipo t_1 e um do tipo t_2, totalizando tres de ambos os tipos. Mas há outra maneira de obter o mesmo resultado: multiplicamos t_1x^2 por

t_2x^2, obtendo também $t_1t_2x^4$. Na verdade, estas são as únicas maneiras de obtermos x^4:

$$(t_1x^3)(t_2x^1) = (t_1t_2)x^4$$
$$(t_1x^2)(t_2x^2) = (t_1t_2)x^4.$$

Podemos obter x^3 de tres maneiras:

$$(t_1x^3)(t_2x^0) = x^3$$
$$(t_1x^2)(t_2x^1) = x^3$$
$$(t_1x^1)(t_2x^2) = x^3.$$

Mas, se fizermos $t_1 = t_2 = 1$, os coeficientes de x^4 e x^3 na multiplicação dos dois polinômios nos darão exatamente a quantidade de maneiras diferentes para obter 4 objetos, sendo entre 0 e 3 do tipo t_1 e entre 0 e 2 do tipo t_2. Explicitamos a multiplicação dos dois polinômios, com coeficientes unitários:

$$1 + 2x + 3x^2 + 3x^3 + 2x^4 + x^5.$$

Ou seja, há uma única maneira de selecionar cinco objetos, dadas as restrições (3 de t_1 e 2 de t_2); duas de selecionar quatro objetos; tres de selecionar tres objetos, e assim por diante. ◀

Teorema 5.11. *A quantidade de maneiras distinguíveis de escolher* k *objetos de tipos* $1 \dots q$*, sendo que os objetos do mesmo tipo são nidistinguíveis, e sem que importe a ordem, é* $[x^k]G(X)$*, onde*

$$G(x) = (1+x+x^2+\cdots+x^{n_1})(1+x+x^2+\cdots+x^{n_2})\cdots(1+x+x^2+\cdots+x^{n_q}),$$

e n_i *é a quantidade disponível de objetos do tipo* i*.*

Exemplo 5.12. De quantas maneiras é possível alocar cinco tipos diferentes de atividades para 10 pessoas?

Podemos ter de zero a dez pessoas em cada atividade. Representamos, para cada uma das atividades, o coeficiente de x^k como a quantidade de pessoas na k-ésima atividade.

$$1 + x + x^2 + \ldots + x^{10}$$

Para cinco atividades, queremos o coeficiente de x^{10} em

$$(1 + x + x^2 + \ldots + x^{10})^5.$$

Mas

$$1 + x + x^2 + \ldots = \frac{1}{1-x},$$

retiramos os termos excedentes $x^{11} + \cdots$,

$$\begin{aligned}(1 + x + x^2 + \ldots + x^{10}) &= \left(\frac{1}{1-x}\right) - x^{11}\left(\frac{1}{1-x}\right)\\ &= \frac{1-x^{11}}{1-x}.\end{aligned}$$

Assim, temos

$$(1+x+x^2+\ldots+x^{10})^5 = \left(\frac{1-x^{11}}{1-x}\right)^5 = (1-x^{11})^5(1-x)^{-5}.$$

O coeficiente de x^{10} em $(1-x^{11})^5$ é zero, porque os produtos sempre envolvem um ou potências de grau maior que dez (o binômio tem somente 1 e x^{11}). Por isso só procuramos o coeficiente em $(1-x)^{-5}$. Como

$$(1-x)^{-5} = \sum_{i=0}^{\infty} \binom{-5}{k} (-x)^i,$$

o coeficiente procurado é $\binom{-5}{10}$. Sabemos que

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

e portanto temos

$$\binom{-5}{10} = (-1)^{10}\binom{5+10-1}{10} = \binom{14}{10} = 1001.$$

Este problema poderia ter sido resolvido de maneira mais rápida observando que o que se pede é uma quantidade de combinações com elementos idênticos, dada pela forma fechada $\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}$. No entanto, é relevante por ser um exemplo simples de aplicação de funções geradoras. ◀

Exemplo 5.13. De quantas maneira é possível fazer doze pontos jogando quatro dados diferentes (a ordem dos dados não importa)?

Cada dado nos dá um número entre 1 e 6, portanto a função geradora para o número de pontos é

$$\begin{aligned} G(x) &= (x+x^2+\cdots+x^6)^4 \\ &= \left(x(1+x+\cdots+x^5)\right)^4 \\ &= x^4(1+x+\cdots+x^5)^4 \\ &= x^4\left(\frac{1}{1-x} - \frac{x^6}{1-x}\right) \\ &= x^4\left(\frac{1-x^6}{1-x}\right)^4 \\ &= x^4(1-x^6)^4(1-x)^{-4}. \end{aligned}$$

Sabemos que x^4 soma 4 aos coeficientes do resto da expressão, portanto procuramos o coeficiente de x^8 em $(1-x^6)^4(1-x)^{-4}$. Verificamos que

$$(1-x^6)^4 = 1 - 4x^6 + 6x^{12} - 4x^{18} + x^{24}.$$

Podemos formar x^8 de duas maneiras:

i) Usando o termo 1 de $(1-x^6)^4$. Neste caso queremos o coeficiente de x^8 em $(1-x)^{-4}$

ii) Usando o termo $-4x^6$ de $(1-x^6)^4$. Neste caso queremos o coeficiente de x^2 em $(1-x)^{-4}$.

Calculamos:

$$\begin{aligned}[x^8](1-x)^{-4} &= 165\\ [x^2](1-x)^{-4} &= 10.\end{aligned}$$

Assim, a quantidade buscada é $164-4(10)=125$. ◀

Exemplo 5.14 (soluções inteiras de equação linear com coeficientes unitários)**.** Já sabemos como computar a quantidade de soluções inteiras positivas para

$$a_1+a_2+a_3=10.$$

A quantidade é

$$\left(\!\!\binom{3}{10}\!\!\right)=66,$$

que também podemos calcular usando funções geradoras. Para escolher 10 objetos de tres tipos, a_1, a_2 e a_3, havendo estoque ilimitado de cada um, a função geradora é

$$\begin{aligned}G(x) &= (1+x+x^2+\cdots)(1+x+x^2+\cdots)(1+x+x^2+\cdots)\\ &= (1-x)^{-3}.\end{aligned}$$

Calculamos $[x^{10}]G(x)$, que é $\binom{-3}{10}=66$.

Agora tomamos uma versão modificada do problema, onde exigimos que todos $a_i \geq 2$.

A função geradora que nos dará a solução é

$$G(x)=(x^2+x^3+\cdots)^3.$$

Queremos $[x^{10}]G(x)$.

Usamos novamente a função geradora $(1-x)^{-1}$:

$$\begin{aligned}x^2+x^3+\cdots &= x^2(1+x+x^2+\cdots)\\ &= \frac{x^2}{1-x}.\end{aligned}$$

Assim, queremos o coeficiente de x^{10} em

$$\left(\frac{x^2}{1-x}\right)^3=\frac{x^6}{(1-x)^3}=(x^6)(1-x)^{-3}.$$

O efeito de multiplicar qualquer série de potência por x^6 será o de somar seis a todos os expoentes. Assim, podemos simplesmente procurar o coeficiente de x^4 em $(1-x)^{-3}$, que é

$$\binom{-3}{4} = 15.$$

O leitor pode querer verificar a listagem das quinze soluções abaixo (em ordem lexicográfica).

$$\begin{array}{lll} 2,2,6 & 3,2,5 & 4,3,3 \\ 2,3,5 & 3,3,4 & 4,4,2 \\ 2,4,4 & 3,4,3 & 5,2,3 \\ 2,5,3 & 3,5,2 & 5,3,2 \\ 2,6,2 & 4,2,4 & 6,2,2 \end{array}$$

◀

Exemplo 5.15.

$$\frac{x}{(1-x)^2} = \sum_{n\geq 1} nx^n$$

$$\frac{x}{1-cx} = \sum_{n\geq 0} c^n x^n$$

◀

5.2 Funções geradoras exponenciais

Definição 5.16 (função geradora exponencial)**.** Seja (a_n) uma sequência. A *função geradora exponencial* de (a_n) é a série formal de potências

$$A(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Denotamos por $n![x^n]A(x)$ o coeficiente de $(x^n/n!)$ em $A(x)$. ♦

Exemplo 5.17. Seja

$$A(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

Esta é uma função geradora exponencial para a sequência $(1, 1, 1, \ldots)$ – ou seja, $n![x^n]A(X) = 1$ para todo n.

Denotamos esta função geradora por e^x, porque é o valor para o qual ela converge.

◀

5.2.1 Aplicações em contagem

Sabemos como usar funções geradoras para contar as combinações de vários tipos de objetos. Para obter as quantidades de permutações formadas com esses objetos, só precisaríamos multiplicar por $n!$.

Teorema 5.18. *A quantidade de maneiras distinguíveis de escolher* k *objetos de tipos* $1 \dots q$*, sendo que os objetos do mesmo tipo são indistinguíveis, onde a ordem importa, é* $n![x^k]G(x)$*, onde*

$$G(x) = \left(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n_1}}{n_1!}\right)\left(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n_2}}{n_2!}\right)\cdots\left(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n_q}}{n_q!}\right),$$

e n_i *é a quantidade disponível de objetos do tipo* i*.*

Exemplo 5.19. Contamos a quantidade de palavras de quatro letras que podemos construir com a, b, c sendo que podemos usar

a 3 vezes,
b 2 vezes,
c 1 vez.

$$\begin{aligned} G(x) &= \left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!}\right)\left(1 + x + \frac{x^2}{2!}\right)(1 + x) \\ &= 1 + 3x + 4x^2 + \frac{19}{6}x^3 + \frac{19}{12}x^4 + \frac{x^5}{2} + \frac{x^6}{12} \end{aligned}$$

Queremos os coeficientes de $\frac{x!}{n!}$, por isso reorganizamos o polinômio de forma que todos os termos tenham $n!$ no denominador.

$$E(X) = 1 + 3\frac{x}{1!} + 8\frac{x^2}{2!} + 19\frac{x^3}{3!} + 38\frac{x^4}{4!} + 60\frac{x^5}{5!} + 60\frac{x^6}{6!},$$

e nossa resposta está no coeficiente de $x^4/4!$, ou seja, 38. ◀

5.3 Ocupação: objetos distinguíveis, locais distinguíveis

Teorema 5.20. *A quantidade de maneiras possíveis de organizar* n *objetos diferentes em* k *locais diferentes, sem que nenhum lugar fique vazio é dada por*

$$T(n,k) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n.$$

Demonstração. Suponha que o i-ésimo objeto seja posto no local $L(i)$. Uma maneira de organizar os objetos em locais será dada pela sequência $L(1), L(2), \dots, L(n)$, que é uma n-permutação do conjunto $\{1, 2, \dots, k\}$ de locais. Para um número fixo k de locais, a função geradora para $T(n,k)$ é

$$G(x) = \left(x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)^k = (e^x - 1)^k,$$

e portanto

$$T(n,k) = n![x^n]G(x).$$

Pelo teorema binomial,

$$G(x) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i e^{(k-i)x}.$$

Substituímos $(k-i)x$ na expansão de e^x e a usamos na fórmula acima, obtendo

$$\begin{aligned} G(x) &= \sum_{i=0}^{k} \binom{k}{i} (-1)^i \sum_{n=0}^{\infty} \frac{1}{n!} (k-i)^n x^n \\ &= \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n. \end{aligned}$$

O coeficiente $n![x^n]G(x)$ é

$$T(n,k) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n. \qquad \blacksquare$$

Exemplo 5.21. A quantidade de maneiras de organizar 10 objetos diferentes em 4 gavetas é

$$\begin{aligned} T(10,5) &= \sum_{i=0}^{4} (-1)^i \binom{4}{i} (4-i)^{10} \\ &= \binom{4}{0} 4^{10} - \binom{4}{1} 3^{10} + \binom{4}{2} 2^{10} - \binom{4}{3} 1^{10} + \binom{4}{4} 0^{10} \\ &= (1)4^{10} - (4)3^{10} + (6)2^{10} - (4) + 0 \\ &= 818520. \end{aligned}$$ ◀

Teorema 5.22. *A quantidade de maneiras possíveis de organizar* n *objetos diferentes em* k *locais diferentes, podendo haver locais vazios é*

$$k^n.$$

Exemplo 5.23. A quantidade de maneiras de organizar 10 objetos diferentes em 4 gavetas, podendo haver gavetas vazias, é

$$4^{10} = 1048576.$$ ◀

5.4 Ocupação: objetos distinguíveis, locais indistinguíveis

Teorema 5.24. *A quantidade de maneiras possíveis de organizar* n *objetos diferentes em* k *locais indistinguíveis, sem que nenhum lugar fique vazio é chamada de* número de Stirling

do segundo tipo, *dado por*

$$S(n,k) = \left\{ {n \atop k} \right\} = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n.$$

Demonstração. A única diferença entre $T(n,k)$ e $S(n,k)$ é que os locais são indistinguíveis. Assim, $T(n,k) = k!S(n,k)$, e a validade do teorema segue trivialmente. ■

A notação $\{ {n \atop k} \}$ sugere algo relacionado a conjuntos. E de fato, separar objetos distinguíveis em locais indistinguíveis é o mesmo que separar elementos de um conjunto em subconjuntos. Assim, $\{ {n \atop k} \}$ é a quantidade de maneiras diferentes de dividir um conjunto em subconjuntos.

Exemplo 5.25. A quantidade de maneiras de particionar o conjunto $\{v, w, x, y, z\}$ em dois subconjuntos, nenhum vazio, é

$$\begin{aligned} \left\{ {5 \atop 2} \right\} &= \frac{1}{2!} T(5,2) \\ &= \frac{1}{2!} \left(\binom{2}{2} 2^5 - 2 \binom{2}{1} 1^5 \right) \\ &= 30/2! \\ &= 15. \end{aligned}$$

◀

Teorema 5.26. *A quantidade de maneiras possíveis de organizar n objetos diferentes em k locais indistinguíveis, podendo haver locais vazios é dada por*

$$\sum_{i=1}^{k} \left\{ {n \atop i} \right\}.$$

Demonstração. Temos $\{ {n \atop 1} \}$ possibilidades usando apenas um local, deixando os outros $k-1$ vazios; $\{ {n \atop 2} \}$ usando dois locais, e assim por diante. Disso segue trivialmente o enunciado do teorema. ■

Exemplo 5.27. A quantidade de maneiras de particionar o conjunto $\{v, w, x, y, z\}$ em dois subconjuntos, contando subconjuntos vazios, é

$$\begin{aligned} \left\{ {5 \atop 2} \right\} + \left\{ {5 \atop 1} \right\} &= 15 + T(5,1) \\ &= 15 + \frac{1}{1!} \binom{1}{1} 1^5 \\ &= 15 + 1 \\ &= 16. \end{aligned}$$

◀

5.5 Funções geradoras em Probabilidade

Definição 5.28 (função geradora de probabilidade)**.** ♦

Definição 5.29 (função geradora de momentos)**.** ♦

5.6 Uma lista de funções geradoras

Esta seção traz uma lista de funções geradoras e suas sequências. O exercício 40 pede a demonstração de corretude delas.

Funções geradoras ordinárias:

$(1,1,1,\ldots,1,\ldots)$	$\frac{1}{1-x}$	$\sum_{i\geq 0} x^i$
$(0,1,2,3,\ldots,n,\ldots)$	$\frac{x}{(1-x)^2}$	$\sum_{i\geq 1} ix^i$
$(0,0,\ldots,\binom{n}{m},\ldots)$	$\frac{x^m}{(1-x)^{m+1}}$	$\sum_{i\geq m} \binom{i}{m}x^i$
$(1,\binom{m}{1},\binom{m}{2},\ldots,\binom{m}{n},\ldots)$	$(1+x)^m$	$\sum_{i\geq 0} \binom{m}{i}x^i$
$(0,1,0,1,\ldots,\frac{1-(-1)^n}{2},\ldots)$	$\frac{1}{1-x^2}$	$\sum_{i\geq 0} x^{2n}$
$(1,k,k^2,k^3,\ldots,k^n,\ldots)$	$\frac{1}{1-kx}$	$\sum_{i\geq 0} k^i x^i$
$(0,1,\frac{1}{2},\frac{1}{3},\ldots,\frac{1}{n},\ldots)$	$\ln\frac{1}{1-x}$	$\sum_{i\geq 1} \frac{x^i}{i}$

Funções geradoras exponenciais:

$(1,1,1,\ldots,1,\ldots)$	e^x	$\sum_{i\geq 0} \frac{x^i}{i!}$
$(0,1,2,3,\ldots,n,\ldots)$	xe^x	$\sum_{i\geq 1} \frac{x^i}{(i-1)!}$
$(1,2,6,24,120,\ldots,n!,\ldots)$	$\frac{1}{1-x}$	$\sum_{i\geq 0} \frac{i!x^i}{i!}$

5.7 Leitura adicional

Um estudo mais detalhado de funções geradoras pode ser encontrado no livro de Herbert Wilf [Wil05], e no de Flajolet e Sedgewick [SF96]. Tópicos mais avançados são discutidos no livro de Goulden e Jackson [GJ04]. Usando Análise Complexa no estudo de funções geradoras (ao tomá-las como funções complexas), chega-se ao que se chama Combinatória Analítica, cuja referencia básica é o livro de Flajolet e Sedgewick [FS09].

Exercícios

Ex. 37 — Qual é a sequencia da função geradora ordinária $e^x + x^2 - x^3$?

Ex. 38 — Qual é a função geradora ordinária de

i)	$a_k = \frac{1}{k} + 1$	v)	$a_k = k^k$
ii)	$a_k = \frac{1}{2k}$	vi)	$a_k = F_k$
iii)	$a_k = 2k^3$	vii)	$a_k = 2k$
iv)	$a_k = \frac{k}{2}$	viii)	$a_k = \frac{k+1}{2}$
ix)	$a_k = (-1)^k$	x)	$a_k = k - 1$
xi)	$a_k = \lfloor \frac{k}{2} \rfloor$		

(F_k é o k-ésimo número de Fibonacci)

Ex. 39 — No exemplo 5.10, o que estaríamos contando se tivéssemos usado $t_1 \neq t_2$? Por exemplo, $t_1 = 2$ e $t_2 = 3$?

Ex. 40 — Mostre que as tabelas da seção 5.6 estão corretas.

Capítulo 6

Partições de um Inteiro

Definição 6.1 (partição de um inteiro)**.** Uma *partição* de um inteiro não negativo n é uma representação de n como soma de outros inteiros não negativos, sem que importe a ordem. Denotamos a quantidade de partições diferentes de um inteiro por $p(n)$. Definimos que $p(0) = 1$. ♦

Exemplo 6.2. O inteiro 5 pode descrito como

$$\begin{aligned} 5 &= 5 \\ &= 4 + 1 \\ &= 3 + 2 \\ &= 3 + 1 + 1 \\ &= 2 + 2 + 1 \\ &= 2 + 1 + 1 + 1 \\ &= 1 + 1 + 1 + 1 + 1, \end{aligned}$$

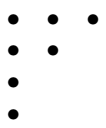
e portanto $p(5) = 7$. ◄

6.1 Diagramas de Ferrers

Uma partição de um inteiro pode ser representada como um diagrama.

Definição 6.3 (diagrama de Ferrers)**.** Seja $a_1 + a_2 + \cdots + a_k$ uma partição de um inteiro n. O *diagrama de Ferrers* desta partição consiste de linhas preenchidas com pontos, uma linha por elemento da partição, e em cada linha i, a quantidade de pontos é igual ao elemento a_i que ela representa. ♦

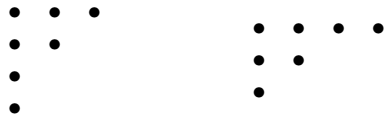
Exemplo 6.4. Por exemplo, o diagrama de Ferrers para a partição $7 = 3+2+1+1$ é



◄

Definição 6.5 (partição conjugada)**.** A *partição conjugada* de uma partição é obtida lendo as colunas do diagrama de Ferrers como se fossem linhas. ♦

Exemplo 6.6. A partição conjugada de $7 = 3 + 2 + 1 + 1$ é $7 = 4 + 2 + 1$, porque o diagrama de Ferrers da primeira partição, quando "transposto", resulta no da segunda.



◄

Teorema 6.7. *Para todo inteiro* n, $p_m(n) = q_m(n)$.

Demonstração. Segue diretamente da noção de partição conjugada: para cada partição contada em $p_m(n)$, há uma conjugada em $q_m(n)$. ■

6.2 Funções geradoras para partições

Nesta seção obteremos funções geradoras para diversas quantidades de partições de inteiros.

Definição 6.8 (produto infinito)**.** Definimos o *produto infinito* de uma sequência (a_n) como

$$\prod_{i=0}^{\infty} a_i = \lim_{n\to\infty} \prod_{i=0}^{n} a_i$$

se o limite existe e é diferente de zero. Se o limite é zero ou não existe, dizemos que o produto é divergente. ♦

Teorema 6.9. *Para todo* $x \in (-1, +1)$,

$$\sum_{n=0}^{\infty} p_m(n) x^n = \prod_{i=1}^{m} \frac{1}{1-x^i},$$

ou seja,

$$p_m(n) = [x^n] \left(\prod_{i=1}^{m} \frac{1}{1-x^i} \right).$$

Demonstração. Primeiro observamos que

$$\begin{aligned}
\prod_{i=1}^{m} \frac{1}{1-x^i} = \left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^2}\right)\cdots\left(\frac{1}{1-x^m}\right) \\
&= (1 + x + x^2 + x^3 + x^4 + \cdots) \\
&\quad \cdot (1 + x^2 + x^{2\cdot 2} + + x^{2\cdot 3} + x^{2\cdot 4} + \cdots) \\
&\quad \vdots \\
&\quad \cdot (1 + x^m + x^{m\cdot 2} + x^{m\cdot 3} + x^{m\cdot 4} + \cdots).
\end{aligned}$$

Cada fator, portanto, será $(1 + x^k + x^{2k} + x^{3k} + \cdots)$. Se multiplicarmos e reorganizarmos os termos, escrevendo os de grau i na i-ésima linha, teremos

$$\begin{aligned}\prod_{i=1}^{m} \frac{1}{1-x^i} & \\ &= 1 && (x^0)\\ &+ x^1 \\ &+ x^2 + x^{2\cdot 1} \\ &+ x^3 + x^{2+1} + x^{3\cdot 1} \\ &+ x^4 + x^{3+1} + x^{2\cdot 2} + x^{2+2\cdot 1} + x^{4\cdot 1} \\ &\ \ \vdots\end{aligned}$$

Para cada limha i, podemos ver uma bijeção entre expoentes e partições de i. ■

Teorema 6.10. *Para todo $x \in (-1, +1)$,*

$$p(n) = [x^n]\left(\prod_{i=1}^{\infty} \frac{1}{1-x^i}\right).$$

Teorema 6.11. *A quantidade de partições de um inteiro n em que as partes são todas diferentes, mas nenhuma parte tem mais que m elementos, é*

$$p_m^d(n) = [x^n]\left(\prod_{i=1}^{m}(1+x^i)\right).$$

A quantidade de partições de um inteiro n em que as partes são todas diferentes é

$$p^d(n) = [x^n]\left(\prod_{i=1}^{\infty}(1+x^i)\right).$$

Demonstração.

$$\begin{aligned}\prod_{i=1}^{m}(1+x^i) &= (1+x)(1+x^2)\cdots(1+x^m) \\ &= 1 + x + x^2 + (x^{2+1} + x^3) + (x^4 + x^{3+1}) + (x^5 + x^{4+1} + x^{3+2}) + \cdots\end{aligned}$$

O termo x^n aparecerá na soma tantas vezes quantas for possível expressar n como soma de m inteiros distintos.

O mesmo argumento pode ser repetido para $p^d(n)$, sem restrição de tamanho nas partições, apenas usando o produtório infinito ao invés do produtório até m. ■

Teorema 6.12. *A quantidade de partições de um inteiro n em partes ímpares é igual a*

$$p^i(n) = [x^n]\left(\prod_{i=1}^{\infty} \frac{1}{(1-x^{2n-1})}\right)$$

Demonstração. A função geradora para o número de partições de n é

$$\prod_{i=1}^{\infty} \frac{1}{1-x^i}.$$

Se removermos os fatores onde x aparece como potência par, teremos apenas os coeficientes para as partições de tamanho ímpar. ■

Teorema 6.13 (Euler)**.** *Para todo natural* n*,*

$$p^d(n) = p^i(n).$$

Demonstração. Provamos que as funções geradoras são iguais.

$$\begin{aligned}
\prod_{i=1}^{\infty}(1+x^i) &= \prod_{i=1}^{\infty} \frac{(1+x^i)(1-x^i)}{(1-x^i)} \\
&= \prod_{i=1}^{\infty} \frac{1-x^{2i}}{1-x^i} \\
&= \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots} \\
&= \prod_{i=1}^{\infty} \frac{1}{1-x^{2i-1}}.
\end{aligned}$$

■

6.3 Fórmula exata para $p(n)$

Obter o coeficiente de x^n na função geradora de $p(n)$ ou em outros produtórios infinitos é, de maneira geral, difícil, e não tentaremos fazê-lo. Há, no entanto, uma fórmula para o número de partições de um inteiro, dada por Hardy e Ramanujan, que reproduzimos aqui

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{i=1}^{\infty} A_i(n)\sqrt{i} \left(\frac{d}{dx} \frac{\operatorname{senh}\left(\frac{\pi}{i}\sqrt{\frac{2}{3}\left(x-\frac{1}{24}\right)}\right)}{\sqrt{x-\frac{1}{24}}} \right)_{x=n},$$

com

$$A_i(n) = \sum_{\substack{0\le h\le k-1 \\ (h,k)=1}} \omega_{h,k} e^{-2\pi i n h/k}$$

onde os $\omega_{h,k}$ são raizes da unidade.

6.4 Estimativa para $p(n)$

Calcular $p(n)$ de maneira exata pode tomar muito tempo. O teorema a seguir, que enunciamos sem demonstração, determina limites superior e inferior para $p(n)$.

Teorema 6.14. *Para todo* $n \geq 4$*,*

$$2^{\sqrt{n}} < p(n) < \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

A estimativa, no entanto, não é muito justa, como podemos notar tomando $n = 100$:

$$2^{\sqrt{100}} < p(100) < \exp\left(\pi\sqrt{\frac{2(100)}{3}}\right)$$
$$1024 < 190569292 < 13806585290.37873$$

Teorema 6.15. *Para todo* $n \geq 0$*,*

$$p(n) \leq F_{n+1},$$

sendo F_i *o* i*-ésimo número de Fibonacci.*

Teorema 6.16 (Hardy/Ramanujan)**.** *Quando* $n \to \infty$*,*

$$p(n) \approx \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}.$$

Exemplo 6.17. Temos $p(200) \approx 3.9 \times 10^{12}$, e

$$\frac{1}{4(200)\sqrt{3}} e^{\pi\sqrt{2(200)/3}} = 4.1 \times 10^{12}.$$ ◀

6.5 Problemas de ocupação (objetos e locais indistinguíveis)

Nesta seção mostramos como usar partições de inteiros em contagem.

- A quantidade de maneiras diferentes de dispor n objetos indistinguíveis em k locais indistinguíveis, sem que locais fiquem vazios, é dada pelo número de partições de n em k partes.
- A quantidade de maneiras diferentes de dispor n objetos indistinguíveis em k locais indistinguíveis, permitindo lugares vazios, é dada pelo número de partições de n em k ou menos partes.

6.6 Alguns fatos sobre partições

Teorema 6.18. *A quantidade de partições de* n *onde* $k \leq n$ *aparece é igual a* $p(n-k)$*.*

Demonstração. Para cada partição de n onde k aparece, podemos remover k obtendo uma partição de $n-k$. Da mesma forma, para cada partição de $n-k$, podemos adicionar o elemento k, obtendo uma partição de n. Assim estabelecemos uma bijeção, e as duas quantidades são iguais. ■

Teorema 6.19. *Para todo* $n \in \mathbb{N}$,

$$q_2(n) = \left\lfloor \frac{n}{2} \right\rfloor.$$

6.7 Leitura adicional

A teoria de partições faz parte da teoria aditiva de números (em contraste com a teoria multiplicativa de números, onde primalidade e divisibilidade são tópicos centrais). Introduções à teoria de partições de inteiros são dadas nos livros de Goerge Andrews [And94] e de Niven, Zuckerman e Montgomery [NSM91] (este último contém uma demonstração do teorema 6.14).

Exercícios

Ex. 41 — Ache as partições conjugadas de

i) $6 = 3+1+1+1$

ii) $10 = 3+2+2+1+1+1$

iii) $15 = 10+4+1$

Ex. 42 — Represente as partições de um inteiro n como uma matriz $M(n)$: cada linha contém os elementos de uma partição, começando da esquerda e listando os elementos seguintes à direita. As linhas devem ficar em ordem lexicográfica. Quais são o posto, determinante e traço de $M(n)$? (Demonstre)

Ex. 43 — Liste as partições de 6.

Ex. 44 — Use funções geradoras para encontrar $p(15)$.

Ex. 45 — Determine a função geradora para o número de partições de um inteiro cuja maior parte é k (o coeficiente de x^n deve ser o número de partições de n onde a maoir das partes é k).

Ex. 46 — Mostre que a quantidade de divisores de n é ímpar se e somente se n é quadrado perfeito.

Capítulo 7

Recorrências

Neste Capítulo examinamos *relações de recorrência*, que são descrições finitas para sequências numéricas infinitas.

7.1 Definição e classificação

Começamos definindo relações de recorrência.

Definição 7.1 (relação de recorrência)**.** Uma *relação de recorrência* é uma definição recursiva de uma sequência, ou seja uma definição que inclui a definição de a_n usando termos anteriores a a_n:

$$a_n = f(a_1, \ldots, a_{n-1}).$$

Uma relação de recorrência é *de ordem* k se a_n depende de a_{n-k}, mas não de termos anteriores a a_{n-k}.

Se são definidos valores para pontos isolados,

$$\begin{aligned} a_0 &= z, \\ a_1 &= z', \\ &\vdots \end{aligned}$$

estes são chamados de *valores iniciais*, ou *condições iniciais*. ♦

Definição 7.2 (recorrência linear e homogênea)**.** Uma relação de recorrência é *linear* se é da forma

$$a_n = \sum_{i=1}^{n-1} c_i a_i + g(n),$$

e *homogênea* se $g(n) = 0$. ♦

Exemplo 7.3. A função fatorial pode ser definida recursivamente. A sequência onde $a_n = n!$ é dada pela relação de recorrência

$$\begin{aligned} a_0 &= 1 \\ a_n &= n a_{n-1}. \end{aligned}$$

◀

Exemplo 7.4. Suponha que precisemos de um algoritmo para localizar um elemento em um vetor ordenado. O algoritmo ingênuo para este problema é pesquisar, da primeira até a última posição do vetor, pelo elemento procurado. Na pior das hipóteses – ou seja, no *pior caso* – o elemento será encontrado na última posição pesquisada (ou não será encontrado em nenhuma das posições), e teremos que realizar n comparações.

Podemos usar um algoritmo melhor para isso. Como sabemos que o vetor está ordenado, começamos comparando x com a posição

$$\left\lfloor \frac{n}{2} \right\rfloor$$

do vetor. Se o elemento naquela posição for maior que x, descartamos a metade à direita e reiniciamos a busca nos $\left\lfloor \frac{n}{2} \right\rfloor$ elementos à esquerda. O mesmo vale quando o elemento é menor que x: descartamos a primeira metade do vetor, e recomeçamos com os $\left\lceil \frac{n}{2} \right\rceil$ elementos à direita. A intuição nos diz que este algoritmo é mais eficiente que o anterior. Seu tempo de execução é dado pela relação de recorrência

$$\begin{aligned} t_1 &= 1 \\ t_n &= 1 + t_{\lfloor n/2 \rfloor}. \end{aligned}$$

◀

Exemplo 7.5. Para resolver o problema das torres de Hanoi, há um algoritmo bastante conhecido:

- Mova $n-1$ discos de A para B
- Mova 1 disco de A para C
- Mova $n-1$ discos de B para C

Deste algoritmo deduzimos que a quantidade de movimentos necessários para mover n discos de uma haste a outra é dada pela relação de recorrência

$$\begin{aligned} h_1 &= 1 \\ h_n &= 2h_{n-1} + 1. \end{aligned}$$

Esta recorrência é não-homogênea, linear, de ordem um e com coeficientes constantes. ◀

Exemplo 7.6. Os números de Fibonacci são definidos pela relação de recorrência

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2}. \end{aligned}$$

Esta recorrência é linear, homogênea, e de ordem dois, com coeficientes constantes. ◀

Exemplo 7.7. Usaremos retas para dividir o plano em regiões. As retas não são paralelas, e a interseção de quaisquer três retas sempre será vazia.

Com nenhuma reta, temos uma região (o plano inteiro). Com uma reta, temos duas regiões. Denotaremos por r_n o número de regiões em que o plano é dividido por n retas.

Quanto já temos $n-1$ retas, e portanto r_{n-1} regiões, a n-ésima reta cruzará todas as outras. E para cada outra reta que cruzar, criará uma nova região. Assim, r_n é dado pela relação de recorrência

$$\begin{aligned} r_0 &= 1 \\ r_n &= r_{n-1} + n - 1. \end{aligned}$$

Esta relação de recorrência é linear e não homogênea, de ordem um. ◀

Exemplo 7.8. Juros compostos podem ser definidos da seguinte maneira:

- Começamos com um montante inicial p
- A cada período, aplicamos uma taxa j sobre o montante do período anterior.

Isto pode ser resumido da seguinte forma:

$$\begin{aligned} v_0 &= p \\ v_n &= v_{n-1} + jv_{n-1} \end{aligned}$$

A segunda equação é uma equação recorrente linear (porque a j é constante) e homogênea. ◀

Exemplo 7.9. O problema a seguir é conhecido como *problema de Josephus*.

Há n homens dispostos em círculo, e pretende-se eliminar $n-1$ deles, ficando apenas um sobrevivente. O método para eliminar os $n-1$ homens é o seguinte: os homens são numerados de 1 a n. Depois, elimina-se cada k-ésimo homem a partir do primeiro (ou seja, o de índice k, o de índice $2k$, etc), até que sobre apenas um homem. ◀

Exemplo 7.10. Para realizar a intercalação de dois vetores de tamanho $n/2$ precisamos de n comparações.

O mergesort divide o vetor em dois, chama a si mesmo recursivamente em dois vetores de tamanho $n/2$, e finalmente intercala os dois vetores. A equação de recorrência que determina o número de comparações feita pelo mergesort é, portanto,

$$\begin{aligned} t_1 &= 1 \\ t_n &= 2t_{n/2} + n. \end{aligned}$$

Esta recorrência é linear e não homogênea. ◀

O teorema a seguir explicita o que é intuitivamente claro: uma relação de recorrencia de ordem k precisa de k valores iniciais. O exercício 56 pede a demonstração.

Teorema 7.11. *Uma equação recorrente de ordem k acompanhada de k valores iniciais define unicamente uma sequência (a_n).*

Se a equação estiver acompanha de de menos de k valores iniciais, haverá mais de uma sequência satisfazendo a relação de recorrência.

Se a equação estiver acompanhada de mais de k valores iniciais, então uma de duas situações ocorrerá: ou a recorrência não determinará nenhuma sequência; ou ela determinará uma única sequência. No segundo caso, um dos valores iniciais poderá ser descartado, e a relação de recorrência continuará representando a mesma sequência.

7.2 Solução de recorrências lineares de ordem um

Recorrências de ordem um são usualmente fáceis de resolver.

O teorema 7.12 é um dos resultados mais simples que podemos explicitar. Sua demonstração é pedida no exercício 53.

Teorema 7.12. *A forma fechada para a recorrencia $a_n = ka_{n-1}$ é*

$$a_n = a_0 k^n.$$

Exemplo 7.13. A recorrência para juros compostos é

$$\begin{aligned} v_0 &= p \\ v_n &= v_{n-1} + jv_{n-1}, \end{aligned}$$

onde p é o valor principal, j são os juros (juros de 2% são descritos como 0.02, por exemplo), e v_n é o montante no n-ésimo período.

Podemos escrever a equação recorrente como $v_n = (1+j)v_{n-1}$, e portanto

$$v_n = p(1+j)^n.$$ ◀

Teorema 7.14. *A recorrencia linear de primeira ordem*

$$\begin{aligned} a_0 &= k_0 \\ a_n &= q_n a_{n-1} + k_n, \end{aligned}$$

onde $k_0, \ldots, k_n, q_1, \ldots, q_n$ são constantes, tem como solução

$$\begin{aligned} a_n &= k_n + \sum_{0 \le i \le n} k_i (q_{i+1} q_{i+2} \cdots q_n) \\ &= k_n + \sum_{0 \le i \le n} \left(k_i \prod_{m=i+1}^{n} q_m \right). \end{aligned}$$

Demonstração. A demonstração é por indução em n.

A base pode ser verificada trivialmente para $n = 0$.

Para o passo, presumimos que

$$a_n = k_n + \sum_{0 \le i \le n} \left(k_i \prod_{m=i+1}^{n} q_m \right).$$

Para a_{n+1}, temos

$$\begin{aligned} a_{n+1} &= q_{n+1}a_n + k_{n+1} \\ &= k_{n+1} + q_{n+1}\left\{k_n + \sum_{0\le i\le n}\left(k_i \prod_{m=i+1}^{n} q_m\right)\right\} \\ &= k_{n+1} + q_{n+1}k_n + q_{n+1}\sum_{0\le i\le n}\left(k_i \prod_{m=i+1}^{n} q_m\right) \\ &= k_{n+1} + \sum_{0\le i\le n+1}\left(k_i \prod_{m=i+1}^{n+1} q_m\right) \end{aligned}$$

■

Teorema 7.15. *Se a sequencia x_n é solução da recorrencia $a_n = f(n)a_{n-1}$, então a troca de variáveis $a_n = x_n b_n$ transforma a recorrencia*

$$a_n = f(n)a_{n-1} + g(n)$$

em

$$b_n = b_{n-1} + g(n)\left(\frac{1}{x_{n-1}f(n-1)}\right)$$

Exemplo 7.16. Seja

$$\begin{aligned} a_0 &= 2 \\ a_n &= 2a_{n-1} + 2^{n-1} \end{aligned}$$

A recorrência

$$\alpha_n = 2\alpha_{n-1}$$

admite como solução $x_n = 2^{n-1}$. Assim, podemos substituir

$$a_n = 2^{n-1}b_n,$$

e chegamos em

$$\begin{aligned} a_n &= 2a_{n-1} + 2^{n-1} \\ 2^{n-1}b_n &= 2\left(2^{n-2}b_{n-1}\right) + 2^{n-1} \\ 2^{n-1}b_n &= 2^{n-1}b_{n-1} + 2^{n-1} \\ b_n &= b_{n-1} + 1. \end{aligned}$$

◄

7.3 Solução de recorrencias lineares homogêneas

Observando a definição dada no início do Capítulo, percebemos que uma equação de recorrência *linear homogênea de ordem* k *com coeficientes constantes* pode ser posta na forma

$$c_0 f_n + c_1 f_{n-1} + c_2 f_{n-2} + \cdots + c_k f_{n-k} = 0,$$

com todos os c_i constantes.

Exemplo 7.17. A equação

$$a_n = 2a_{n-1} - 3a_{n-4}$$

pode ser reescrita como

$$a_n - 2a_{n-1} + 3a_{n-4} = 0.$$ ◀

Lema 7.18. *Se as sequências (x_n) e (y_n) satisfazem uma equação de recorrência linear homogênea, então qualquer combinação linear $\alpha x + \beta y$ também satisfaz a mesma equação.*

Demonstração.

$$\sum c_i x_i = 0 = \sum c_i y_i$$

implica que

$$\alpha \sum c_i x_i = \alpha 0 = \beta 0 = \beta \sum c_i y_i.$$ ■

Exemplo 7.19. Sejam

$$(x_n) = 1, 2, 4, 8, 16, \ldots$$
$$(y_n) = 3, 6, 12, 24, 48, \ldots$$

Notamos que as duas sequências satisfazem a equação recorrente

$$a_n = 2a_{n-1},$$

já que $x_k = 2x_{k-1}$ e $y_k = 2y_{k-1}$. Então tanto (x_n) como (y_n) são duas soluções diferentes para a equação. Pelo Lema 7.18, a combinação linear

$$2(x_n) + (y_n) = 5, 10, 20, 40, 80, \ldots$$

também satisfaz a mesma equação. ◀

7.3.1 Matriz associada

Definição 7.20 (Matriz associada a equação de recorrência)**.** Uma equação de recorrência linear de ordem k

$$a_n = c_1 a_{n-1} + c_2 a_{n-1} + \cdots + c_k a_{n-k}$$

pode ser descrita em forma de matriz:

$$\overbrace{\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ 0 & 0 & 0 & \ddots & \\ \vdots & & & & 1 \\ c_k & c_{k-1} & c_{k-2} & \cdots & c_1 \end{pmatrix}}^{C} \begin{pmatrix} a_n \\ a_{n+1} \\ a_{n+2} \\ \vdots \\ a_{n+k} \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ a_{n+2} \\ a_{n+3} \\ \vdots \\ a_{n+k+1} \end{pmatrix}$$

À matriz C damos o nome de *matriz associada* à equação de recorrência (a_n). ♦

Exemplo 7.21. A recorrencia

$$a_n = 3a_{n-1} - 2a_{n-2}$$

tem matriz associada

$$\begin{pmatrix} 0 & 1 \\ -2 & 3 \end{pmatrix},$$

e polinômio característico

$$p(x) = x^2 - 3x + 2. \quad \blacktriangleleft$$

Exemplo 7.22. A recorrencia

$$b_n = 2b_{n-1} - 3b_{n-3}$$

x tem matriz associada

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -3 & 0 & 2 \end{pmatrix},$$

e polinômio característico

$$p(x) = x^3 - 2x^2 + 3. \quad \blacktriangleleft$$

Exemplo 7.23. A recorrencia

$$e_n = 16e_{n-4}$$

tem matriz associada

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 16 & 0 & 0 & 0 \end{pmatrix},$$

e polinômio característico

$$p(x) = x^4 - 16. \quad \blacktriangleleft$$

Enunciamos lemas e teoremas que permitirão encontrar a forma fechada para recorrências lineares homogêneas.

Lema 7.24. *Seja* C *a matriz associada à equação de recorrência da sequência* a_n*. O polinômio característico de* C *é*

$$\lambda^k + c_k\lambda^{k-1} + c_{k-1}\lambda^{k-2} + \cdots + c_2\lambda + c_1.$$

C *não tem autovalores zero, e para qualquer autovalor* λ *de* C, $a_n = \lambda^n$ *é solução da recorrência.*

Teorema 7.25. *Seja*

$$a_n = c_1 a_{n-1} + \cdots + c_{n-k}a_{n-k}$$

uma equação recorrente linear homogênea de ordem k *com* polinômio característico

$$p(x) = x^k + c_1 x^{k-1} + \cdots + c_{k-1}x + c_k.$$

Se o polinômio característico tem k *raízes distintas* $r_1, \ldots, r_k$ *(ou seja, não tem raízes repetidas), então uma sequência* (x_n) *satisfaz a equação se e somente se*

$$x_n = b_1 r_1^n + \cdots + b_k r_k$$

onde os b_i *são constantes.*

Demonstração. Pelo teorema fundamental da álgebra, o polinômio característico (que tem grau k) tem k raízes, e portanto

$$p(x) = \prod_{i=1}^{k} (x - r_i),$$

com $p(r_i) = 0$.

Mas se para qualquer raiz, $p(r_i) = 0$, então $x = r_i$ é solução para a recorrência. Além disso, pelo Lema 7.24, r_i^n também é solução. Como combinações lineares de soluções também são soluções, temos a solução

$$f_n = c_1 r_1^n + c_2 r_2^n + \cdots + c_k r_k^n. \qquad \blacksquare$$

Como normalmente temos k valores iniciais, podemos aplicar o Teorema 7.25 para construir um sistema com k equações e k variáveis,

$$\begin{aligned} f_1 &= c_1 r_1^1 + c_2 r_2^1 + \cdots + c_k r_k^1 \\ f_2 &= c_1 r_1^2 + c_2 r_2^2 + \cdots + c_k r_k^2 \\ &\vdots \\ f_k &= c_1 r_1^k + c_2 r_2^k + \cdots + c_k r_k^k, \end{aligned}$$

obtendo assim a forma fechada (as variáveis neste sistema são os c_i).

Exemplo 7.26. Considere a recorrência

$$\begin{aligned} a_1 &= 3 \\ a_2 &= 4 \\ a_n &= a_{n-1} + 2a_{n-2} \end{aligned}$$

O polinômio característico é

$$x^2 - x - 2 = (x - 2)(x + 1),$$

com raízes 2 e -1. A solução para a recorrência é

$$a_n = c_1 (2)^n + c_2 (-1)^n.$$

Para a_1, e a_2 temos

$$\begin{aligned} c_1(2) + c_2(-1) &= 3 \\ c_1(2)^2 + c_2(-1)^2 &= 4 \end{aligned}$$

e portanto

$$c_1 = \frac{7}{6}, \quad c_2 = -\frac{2}{3}.$$

Finalmente,

$$a_n = \frac{7}{6}2^n - \frac{2}{3}(-1)^n,$$

e temos uma forma fechada para a_n. ◄

Exemplo 7.27. Considere a sequência de Fibonacci,

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2}. \end{aligned}$$

Reescrevemos a equação,

$$F_n - F_{n-1} - F_{n-2} = 0,$$

e obtemos o polinômio característico

$$x^2 - x - 1,$$

que tem as raízes

$$\frac{1-\sqrt{5}}{2}, \quad \frac{1+\sqrt{5}}{2}.$$

A solução para a recorrência deve ser

$$F_n = c_1\left(\frac{1-\sqrt{5}}{2}\right)^n + c_2\left(\frac{1+\sqrt{5}}{2}\right)^n.$$

Substituimos e resolvemos o sistema para F_0 e F_1,

$$\begin{aligned} c_1\left(\frac{1-\sqrt{5}}{2}\right)^0 + c_2\left(\frac{1+\sqrt{5}}{2}\right)^0 &= 0 \\ c_1\left(\frac{1-\sqrt{5}}{2}\right)^1 + c_2\left(\frac{1+\sqrt{5}}{2}\right)^1 &= 1, \end{aligned}$$

ou

$$\begin{aligned} c_1 + c_2 &= 0 \\ c_1\left(\frac{1-\sqrt{5}}{2}\right) + c_2\left(\frac{1+\sqrt{5}}{2}\right) &= 1, \end{aligned}$$

e obtemos

$$c_1 = -\frac{1}{\sqrt{5}} \quad c_2 = \frac{1}{\sqrt{5}},$$

e portanto

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right],$$

que é a forma fechada para o n-ésimo número de Fibonacci. ◀

Exemplo 7.28. A recorrência a seguir, pequena e com apenas coeficientes inteiros, é bastante interessante.

$$\begin{aligned} t_0 &= 0 \\ t_1 &= 1 \\ t_n &= 2t_{n-1} - 2t_{n-2} \end{aligned}$$

Reescrevemos a recorrência,

$$t_n - 2t_{n-1} + 2t_{n-2} = 0,$$

e identificamos a equação característica,

$$1x^2 - 2x + 2 = 0.$$

Ao resolver esta equação obtemos raízes complexas $1-i$ e $1+i$. A solução da recorrência será

$$t_n = c_1(1-i)^n + c_2(1+i)^n.$$

Para t_0 e t_1,

$$\begin{aligned} c_1 + c_2 &= 0 \\ c_1(1-i) + c_2(1+i) &= 1 \end{aligned}$$

A solução para o sistema é

$$c_1 = \frac{i}{2}, \quad c_2 = -\frac{i}{2},$$

e a forma geral da recorrência é

$$t_n = \frac{i}{2}(1-i)^n - \frac{i}{2}(1+i)^n.$$

Pode-se mostrar que

$$t_n = \sqrt{2^n}\,\mathrm{sen}\left(\frac{n\pi}{4}\right). \quad ◀$$

7.3.2 Raízes múltiplas

Considere a recorrência

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 5 \\ a_n &= 4a_{n-1} - 4a_{n-2}. \end{aligned}$$

Reescrevendo obtemos $a_n - 4a_{n-1} + 4a_{n-2}$. A equação característica é

$$x^2 - 4x + 4 = 0,$$

que tem suas duas raízes iguais a 2. Não podemos aplicar diretamente o método do polinômio característico. Se tentarmos, veremos que não há solução da forma $a_n = c2^n$ para a_1.

Teorema 7.29. *Se o polinômio característico de uma recorrencia linear homogenea tem uma raiz* r *com multiplicidade* k*, então*

$$a_n = r^n, \quad a_n = nr^n, \quad a_n = n^2r^n, \quad \cdots, \quad a_n = n^{k-1}r^n$$

satisfazem a equação de recorrencia.

Combinações lineares de soluções são soluções, e isso significa que podemos usar, no exemplo inicial,

$$a_n = (c_1)2^n + (c_2)n2^n.$$

Para obter c_1 e c_2, resolvemos

$$\begin{aligned} c_1 + (c_2)(0)(2^0) &= 2 \qquad (c_1 = 2) \\ c_1 2^1 + c_2(1)(2^1) &= 5 \end{aligned}$$

e obtemos

$$c_1 = 2 \quad c_2 = \frac{1}{2}.$$

Finalmente, podemos escrever a forma fechada para a_n:

$$\begin{aligned} a_n &= 2(2^n) + \frac{1}{2}n2^n \\ &= 2^{n+1} + n2^{n-1}. \end{aligned}$$

Exemplo 7.30. Determinaremos a forma fechada para a recorrência a seguir, de ordem tres.

$$\begin{aligned} a_0 &= 3 \\ a_1 &= 12 \\ a_2 &= 30 \\ a_n &= -3a_{n-1} + 4a_{n-3} \end{aligned}$$

A equação característica é

$$x^3 + 3x^2 - 4 = 0.$$

Fatorando, temos

$$(x+2)^2(x-1),$$

e portanto as raízes são 1 e -2. Tendo somente duas raízes, presumimos que a solução é da forma

$$a_n = (c_1)1^n + (c_2)(-2)^n + (c_3)n(-2)^n.$$

$$\begin{aligned} a_0: &\quad (c_1)1^0 + (c_2)(-2)^0 + (c_3)0(-2)^0 = 3 \\ a_1: &\quad (c_1)1^1 + (c_2)(-2)^1 + (c_3)1(-2)^1 = 12 \\ a_2: &\quad (c_1)1^2 + (c_2)(-2)^2 + (c_3)2(-2)^2 = 30 \end{aligned}$$

Obtemos

$$c_1 = 10 \quad c_2 = -7 \quad c_3 = 6.$$

Então,

$$a_n = (10)1^n - 7(-2)^n + 6n(-2)^n. \qquad \blacktriangleleft$$

7.3.3 Diagonalização da matriz associada

O Teorema 7.31 nos dá outro método, que é mais geral (que não depende das raízes serem distintas) e conceitualmente mais elegante, para resolver recorrências lineares homogêneas.

Teorema 7.31. *Seja C uma matriz associada a uma relação de recorrência de ordem k. Se C é diagonalizável, sejam P e P^{-1} as matrizes de mudança de base tais que $D = P^{-1}CP$ é diagonal. Seja Z o vetor coluna com os valores iniciais da recorrência,*

$$Z = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ \vdots \\ z_k \end{pmatrix}.$$

A forma fechada para o n-ésimo termo da recorrência é dada pela primeira entrada do vetor

$$PD^{n-1}P^{-1}Z.$$

Exemplo 7.32. Considere novamente a recorrência do exemplo 7.26:

$$\begin{aligned} a_1 &= 3 \\ a_2 &= 4 \\ a_n &= a_{n-1} + 2a_{n-2} \end{aligned}$$

A matriz associada é

$$\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}.$$

Diagonalizando A, temos

$$A = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{3} \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}.$$

Temos portanto,

$$\begin{aligned} a_n &= PD^{n-1}P^{-1}Z \\ &= \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}^{n-1} \frac{1}{3} \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} \\ &= \frac{7}{6}2^n - \frac{2}{3}(-1)^n. \end{aligned}$$

◀

7.4 Equações lineares não homogêneas

Teorema 7.33. *Seja $p(n)$ um polinômio de grau g, z uma constante, e*

$$a_n = A_1 a_{n-1} + A_2 a_{n-2} + \ldots + A_k a_{n-k} + p(n)z^n$$

uma relação de recorrência, com a equação característica sem o termo dependente de n (ou seja, com a equação característica da recorrencia homogenea associada) igual a

$$x^k + A_1 x^{k-1} + \cdots + A_k = 0.$$

Se esta equação for multiplicada por $(x - z)^{g+1}$, obtém-se outra equação com raízes r_1, r_2, ... Então existem c_i tais que $a_n = c_i r_i^n$ é solução para a recorrência, assim como no caso homogêneo. Se r_i tem multiplicidade m, aplica-se o teorema 7.29.

Exemplo 7.34. Resolvemos inicialmente uma recorrência linear não-homogênea de ordem um.

$$\begin{aligned} a_0 &= 2 \\ a_n &= \frac{a_{n-1}}{2} + 3^n \end{aligned}$$

Temos $p(n) = 0$, e $z(n) = 3^n$. A equação característica da recorrência homogênea associada é

$$x - \frac{1}{2} = 0.$$

Multiplicamos por $(x - 3)$, obtendo

$$x(x-3) - \frac{x-3}{2} = 0,$$

com raízes

$$r_1 = 3 \quad r_2 = \frac{1}{2}$$

As soluções serão da forma

$$a_n = c_1(3)^n + c_2\left(\frac{1}{2}\right)^n.$$

No entanto, temos duas constantes para determinar (c_1 e c_2), mas só temos um valor inicial ($a_0 = 2$). Resolvemos este problema calculando a_1:

$$a_1 = \frac{a_0}{2} + 3^1 = 4$$

Agora podemos resolver o sistema:

$$\begin{aligned} a_0: \quad & c_1 + c_2 = 2 \\ a_1: \quad & c_1(3) + c_2(1/2) = 4 \end{aligned}$$

determinando as constantes

$$c_1 = \frac{6}{5} \quad c_2 = \frac{4}{5}$$

Já temos portanto a forma fechada para a recorrência:

$$a_n = \frac{6}{5}(3)^n + \frac{4}{(5)2^n}.$$ ◀

Exemplo 7.35. Nem toda recorrência não-homogênea pode ser resolvida de forma simples. Em alguns casos, no entanto, é possível encontrar a forma fechada com relativa facilidade.

Considere a seguinte relação de recorrência linear não-homogênea de ordem 3.

$$\begin{aligned} b_0 &= 4 \\ b_1 &= 2 \\ b_2 &= 3 \\ b_n &= -b_{n-1} + 4b_{n-2} + 4b_{n-3} + n \end{aligned}$$

Podemos escrever o termo dependente de n como $(n^1)(1^n)$, e portanto o teorema 7.33 se aplica. O polinômio é de grau um, portanto a equação característica será multiplicada por $(x-1)^1$.

A equação característica da homogênea associada é

$$x^3 + x^2 - 4x - 4 = 0$$

Multiplicamos por $(x-1)$, e obtemos

$$\begin{aligned} (x^4 - x^3) + (x^3 - x^2)(-4x^2 + 4x)(-4x - 4) &= 0 \\ x^4 - 5x^2 + 4 &= 0 \end{aligned}$$

Para resolver a equação do quarto grau[1], fazemos $y = x^2$,

$$y^2 - 5y + 4 = 0$$

[1] Há forma fechada para as soluções de uma equação do quarto grau, mas não a usaremos.

e obtemos $y = 1, y = 4$. Ao desfazer a troca de variáveis, conseguimos a solução para a equação quártica original:

$$x_1 = 1 \quad x_2 = -1 \quad x_3 = 2 \quad x_4 = -2$$

As soluções da recorrencia devem ser da forma

$$b_n = c_1(1)^n + c_2(-1)^n + c_3(2)^n_+ c_4(-2)^n$$

Precisamos de quatro valores iniciais. Calculamos b_3, que ainda não temos:

$$\begin{aligned} b_0 &= 4 \\ b_1 &= 2 \\ b_2 &= 3 \\ b_3 &= -3 + 4(2) + 4(4) + 3 = 24 \end{aligned}$$

O sistema a ser resolvido é

$$\begin{aligned} c_1 + c_2 + c_3 + c_4 &= 4 \\ c_1 - c_2 + 2c_3 + -2c_4 &= 2 \\ c_1 + c_2 + 4c_3 + 4c_4 &= 3 \\ c_1 - c_2 + 8c_3 + -8c_4 &= 24 \end{aligned}$$

Temos finalmente

$$c_1 = -\frac{1}{2} \quad c_2 = \frac{29}{6} \quad c_3 = \frac{5}{3} \quad c_4 = -2$$

E a forma fechada para b_n é

$$b_n = -\frac{1}{2} + \frac{29}{6}(-1)^n + \frac{5}{3}(2^n) - 2(-2)^n. \qquad \blacktriangleleft$$

7.5 Troca de variáveis

Em diversas situações, uma troca de variáveis pode tornar muito mais fácil a obtenção de forma fechada para uma recorrência.

Exemplo 7.36. Considere a recorrência do algoritmo para as torres de Hanói:

$$\begin{aligned} h_1 &= 1 \\ h_n &= 2h_{n-1} + 1. \end{aligned}$$

Somamos 1 a ambos os lados da equação recorrente, obtendo

$$\begin{aligned} h_n + 1 &= 2h_{n-1} + 2 \\ h_n + 1 &= 2(h_{n-1} + 1) \end{aligned}$$

Agora fazemos uma troca de variáveis: seja $f_n = h_n + 1$. então a recorrencia passa a ser

$$\begin{aligned} f_1 &= 2 \\ f_n &= 2f_{n-1}, \end{aligned}$$

ou seja, temos uma PG de razão 2 e termo inicial $f_1 = 2$. A solução é

$$f_n = 2^n,$$

e portanto

$$h_n = 2^n - 1.$$ ◀

Exemplo 7.37. Considere a equação recorrente

$$a_n = \sqrt{a_{n-1}\, a_{n-2} \ldots a_{n-k}}.$$

Seja $b_n = \ln a_n$. Então a solução da equação recorrente

$$b_n = \frac{b_{n-1} + b_{n-2} + \cdots + b_{n-k}}{2}$$

nos dá também uma solução para a equação original. ◀

7.6 Funções geradoras

Para encontrar uma forma fechada para o n-ésimo termo de uma sequência (a_n), podemos tentar usar a função geradora da sequência. Por exemplo,

$$\begin{aligned} a_0 &= 1 \\ a_n &= 3a_{n-1} \end{aligned}$$

A função geradora ordinária da sequência (a_n) é

$$A(x) = \sum_{i=0}^{\infty} a_i x^i.$$

Muliplicamos a equação $a_n = 3a_{n-1}$ por x_n e depois somamos para todos os valores para os quais a recorrência vale (de zero a ∞):

$$\sum_{i=0}^{\infty} a_{i+1} x^i = 3 \sum_{i=0}^{\infty} a_i x^i$$

$$\begin{aligned} \sum_{i=0}^{\infty} a_{i+1} x^i &= a_1 + a_2 x + a_x x^2 \cdots \\ &= x^{-1} \left(a_1 x + a_2 x^2 + a_3 x^3 + \cdots \right) \\ &= x^{-1} \left(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots \right) - x^{-1} a_0 \\ &= x^{-1} (A(x) - a_0). \end{aligned}$$

Substituindo, temos

$$x^{-1}(A(x) - a_0) = 3A(x)$$

e encontramos

$$A(x) = \frac{a_0}{1-3x}.$$

Como $a_0 = 1$,

$$A(x) = \frac{1}{1-3x}.$$

Como já sabemos que esta é a função geradora para 3^n, temos $[x^n]A(x) = 3^n$, e

$$a_n = 3^n.$$

Exemplo 7.38. Considere a recorrencia

$$a_0 = 1$$
$$a_{n+1} = 2a_n + 2^n$$

Continuando,

$$\sum_{i=0}^{\infty} a_{i+1}x^i = 2\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} 2^i x^i.$$

Ou seja,

$$\frac{A(x) - a_0}{x} = 2A(x) + \sum_{i=0}^{\infty}(2x)^i$$
$$\frac{A(x) - 1}{x} = 2A(x) + \sum_{i=0}^{\infty}(2x)^i$$

A função geradora de 2^i é $1/(1-2x)$, portanto

$$\frac{A(x) - 1}{x} = 2A(x) + \frac{1}{1-2x}$$

Reescrevemos em função de $A(x)$:

$$A(x) = \frac{1}{1-2x} + \frac{x}{(1-2x)^2}$$
$$[x^n]A(x) = 2^n + [x^n]\left(\frac{x}{(1-2x)^2}\right)$$

Sabemos que

$$\frac{x}{(1-x)^2} = \sum_{i\geq 1} nx^n,$$

portanto o termo de grau n nesta função geradora é $n(2x)^n = n2^n x^n$. Assim,

$$[x^n]A(x) = 2^n + n2^n$$

E finalmente podemos escrever

$$a_n = (n+1)2^n.$$ ◀

7.7 Divisão e conquista

Algoritmos de divisão e conquista normalmente rem seu tempo de execução descrito por recorrências da forma

$$t_n = At_{n/B} + f(n)$$

Uma técnica útil em muitas recorrencias deste tipo é a troca de variáveis. Seja $s_k = t_{B^k}$. Então

$$\begin{aligned} S_k = t_{B^k} &= AT_{B^k/N} + f(B^k) \\ &= AT_{B^{k-1}} + f(B^k) \\ &= AS_{k-1} + f(B^k), \end{aligned}$$

que é uma recorrência linear. Depois de resolvê-la, podemos desfazer a troca de variáveis. No entanto, esta recorrência nos dará apenas os valores de t_{B^k}. Para t_n, onde n não é potência de B, a recorrência não é válida.

Exemplo 7.39. A recorrência que dá o tempo da busca binária é

$$\begin{aligned} t_1 &= 1 \\ t_n &= t_{\lfloor n/2 \rfloor} + 1, \end{aligned}$$

com $A = 1$, $B = 2$ e $f(n) = 1$.

Seja $S_k = t_{2^k}$. Então

$$\begin{aligned} S_1 &= 2 && (2^0 = 1 = t_1) \\ S_k &= S_{k-1} + 1. \end{aligned}$$

A solução para esta recorrência é $S_n = n + 1$. Desfazendo a troca de variáveis,

$$\begin{aligned} t_{2^n} &= n + 1 \\ t_n &= \log_2(n), \end{aligned}$$

que é a quantidade de comparações necessária no pior caso da busca binária *para potencias de* 2, porque usamos $S_k = t_{2^k}$. O leitor pode facilmente perceber que para $n \neq 2^k$ a solução que encontramos não é válida, já que teríamos número não inteiro, a sequência original é inteira. ◀

Exemplo 7.40. A recorrencia que dá o tempo de execução do *mergesort* é

$$\begin{aligned} t_1 &= 1 \\ t_n &= 2t_{\lfloor n/2 \rfloor} + n, \end{aligned}$$

com $A = 2$, $B = 2$ e $f(n) = n$.

Seja $S_k = t_{2^k}$. Então

$$\begin{aligned} S_1 &= 4 && (S_1 = t_2 = 4) \\ S_k &= 2S_{k-1} + 2^k. \end{aligned}$$

A recorrência agora é linear, e sua solução é

$$S_n = 2^n(n+1)$$

Temos portanto

$$\begin{aligned} S_n = t_{2^n} &= 2^n(n+1) \\ t_n &= 2^{\log_2(n)}(\log_2(n)+1) && (n \to \log(n)) \\ t_n &= n\log_2(n) + n \end{aligned}$$

que é a quantidade de comparações feitas pelo *mergesort* no pior caso, *quando* n *é potência de* 2. ◀

7.8 Demonstrando que uma solução candidata é correta

Muitas vezes, a partir de observação podemos chegar a uma "provável" forma fechada para uma recorrência. Se tivermos uma forma candidata à forma geral para o n-ésimo termo de uma recorrência, podemos provar por indução a validade da forma.

Exemplo 7.41. Considere a seguinte recorrência não linear.

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 3 \\ a_n &= a_{n-1}a_{n-2} \end{aligned}$$

Expandimos a sequencia para alguns valores, e obtemos

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 3 \\ a_2 &= 2 \cdot 3 \\ a_3 &= 2 \cdot 3^2 \\ a_4 &= 2^2 \cdot 3^3 \\ a_5 &= 2^3 \cdot 3^5 \\ a_6 &= 2^4 \cdot 3^6. \end{aligned}$$

Aparentemente, para $n > 1$ temos $a_n = 2^{F_{n-2}} \cdot 3^{F_{n-1}}$. Tentaremos provar por indução que esta de fato é a forma fechada para a sequência.

Nossa hipotese de indução diz que para $k < n$,

$$a_k = 2^{F_{k-2}} \cdot 3^{F_{k-1}}$$

Temos portanto

$$\begin{aligned} a_n &= a_{n-1}a_{n-2} \\ &= \left(2^{F_{n-3}} \cdot 3^{F_{n-2}}\right)\left(2^{F_{n-4}} \cdot 3^{F_{n-3}}\right) && \text{(hipótese de indução)} \\ &= 2^{F_{n-3}+F_{n-4}}3^{F_{n-3}F_{n-2}} \\ &= 2^{F_{n-2}}3^{F_{n-1}}. && \text{(definição de } F_n\text{)} \end{aligned}$$

Assim, provamos que a sequência é dada por

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 3 \\ a_n &= 2^{F_{n-2}}3^{F_{n-1}}. \end{aligned}$$

Claramente, a demonstração pode ser adaptada de forma trivial para diferentes valores iniciais (seja por exemplo $a_0 = x$ e $a_1 = y$), resultando em

$$\begin{aligned} a_0 &= x \\ a_1 &= y \\ a_n &= x^{F_{n-2}}y^{F_{n-1}}. \end{aligned}$$ ◀

Exercícios

Ex. 47 — Determine a recorrência para juros simples, e a resolva.

Ex. 48 — Resolva as recorrências

a)

$$\begin{aligned} a_1 &= 1 \\ a_n &= \sqrt{n} + n a_{n-1} \end{aligned}$$

b)

$$\begin{aligned} a_0 &= x \\ a_1 &= y \\ a_n &= a_{n-1}/a_{n-2} \end{aligned}$$

Ex. 49 — Prove que F_n é exatamente o número de maneiras diferentes de escrever n como soma de uns e dois:

$$\begin{aligned} 1 &= 1, F_1 = 1 \\ 2 &= 2, F_2 = 1 \\ 3 &= 1+2 = 1+1+1, F_3 = 2 \\ 4 &= 2+2 = 2+1+1 = 1+1+1+1, F_4 = 3 \end{aligned}$$

Ex. 50 — Denotamos por F_n o n-éesimo número de Fibonacci. Prove que

a) $F_n^2 - F_{n+1}F_{n-1} = (-1)^n$, para $n \geq 1$

b) $\sum_{i=0}^{n} F_i = F_{n+1} - 1$

c) $F_{n-1}^2 + F_n^2 = F_{2n}$, $\quad F_{n-1}F_n + F_nF_{n+1} = F_{2n+1}$

Ex. 51 — Mostre que F_n é composto para qualquer n ímpar maior que 3.

Ex. 52 — Seja F_n o n-ésimo número de Fibonacci.

a) Há n objetos organizados em uma fila. Prove que a quantidade de diferentes maneiras de escolher um subconjunto destes objetos, sem usar dois consecutivos, é F_{n+1}.

b) Se os $n > 2$ objetos são organizados em círculo, de diferentes maneiras de escolher um subconjunto destes objetos, sem usar dois consecutivos? (Responda em termos de F_n, F_{n-1}, etc).

Ex. 53 — Prove o teorema 7.12.

Ex. 54 — Determine a forma fechada da sequência semelhante à de Fibonacci, mas com $F_0 = 2$ e $F_1 = 3$.

Ex. 55 — Podemos retroceder a sequência de Fibonacci, para números menores que zero, de forma que continue valendo tanto a definição recursiva como a forma fechada que encontramos?

Ex. 56 — Demonstre o teorema 7.11.

Ex. 57 — Dê a solução da recorrência

$$\begin{aligned} a_0 &= e^3 \\ a_1 &= e^4 \\ a_n &= \sqrt[3]{a_{n-1}a_{n-2}^2}. \end{aligned}$$

Capítulo 8

Princípio da Casa dos Pombos

O *princípio da casa dos pombos* é uma afirmação aparentemente evidente e inocente, mas com aplicações surpreendentes. O princípio é enunciado no teorema 8.1, e sua generalização no teorema 8.17. O restante deste Capítulo contém exemplos de aplicação.

8.1 Forma simples do princípio da casa dos pombos

Teorema 8.1 (princípio da casa dos pombos)**.** *Se há* $n+1$ *pombos e* n *casas, pelo menos dois pombos ocuparão a mesma casa.*

Este princípio pode ser declarado de outra maneira[1], como no teorema 8.2.

Teorema 8.2 (princípio da casa dos pombos)**.** *Se* $|A| > |B|$*, não exite função injetora de* A *em* B*.*

Exemplo 8.3. Em um grupo de 13 pessoas há necessariamente duas que fazem aniversário no mesmo mês: há 12 meses no ano, e não haveria meses suficientes para que todos os 13 tivessem aniversários em meses diferentes. ◀

Exemplo 8.4. Em uma metrópole com um milhão de habitantes há duas pessoas, não carecas, que tem a mesma quantidade de fios de cabelo.

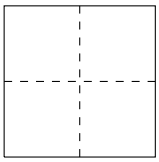
Presumimos que menos da metade da população é careca. Assim, temos pelo menos 500 001 pessoas com cabelo.

Uma pessoa tem no máximo 500 000 fios de cabelo. Como há mais de 500 000 pessoas com cabelo na metrópole, haverá duas pessoas com o mesmo número de fios. ◀

Exemplo 8.5. Se cinco pontos são dispostos dentro de um quadrado de lado 1, então há dois pontos para os quais a distância é menos que $\frac{\sqrt{2}}{2}$.

Dividimos o quadrado em quatro outro quadrados de lado $1/2$.

[1] Ou ainda, trocando pombos por casas (buracos), há a versão politicamente incorreta, "Se você atirar e acertar $n+1$ balas em n pombos, haverá pelo menos um pombo com mais de um buraco".



Há quatro quadrados pequenos e cinco pontos, portanto deve haver algum quadrado pequeno com dois pontos. Se dois pontos estão em um quadrado de lado $1/2$, então a distância entre eles não pode ser maior do que a diagonal desse quadrado, que mede $\frac{\sqrt{2}}{2}$. ◀

Exemplo 8.6. Em um grafo não-dirigido conexo com mais de um vértice e sem *loops*, há dois vértices com o mesmo grau.

Um vértice pode estar ligado, no máximo, a $n-1$ outros vértices, portanto o grau de um vértice pode ser qualquer número entre 1 e $n-1$. Há $n-1$ graus possíveis.

Como há n vértices e $n-1$ possibilidades para grau, existem dois vértices com o mesmo grau. ◀

Exemplo 8.7. Em uma lista qualquer de $k+1$ números $a_1, a_2, \ldots, a_{k+1}$, haverá pelo menos dois números a_i e a_j tais que $(a_i - a_j)|k$.

O resto da divisão por k pode ser $0, 1, \ldots, k-1$ (portanto há k possíveis restos). No entanto, temos $k+1$ números, portanto há dois números com o mesmo resto:

$$\begin{aligned} a_i &= c_i k + r \\ a_j &= c_j k + r \end{aligned}$$

Mas

$$a_i - a_j = c_i k + r - c_j k - r = (c_i - c_i)k,$$

divisível por k. ◀

Exemplo 8.8. Dados $n+1$ números inteiros entre 1 e $2n$, haverá dois números x e y tais que $x = 2^k y$.

Fatore o número 2 de cada um dos $n+1$ números tanto quanto possível. Com isso cada um será da forma $a2^k$, com a ímpar. Então para cada número fatorado, a pode ser um dentre os n números $1, 3, 5, \ldots, 2n-1$. Há portanto n possibilidades de a para $n+1$ números, e dois terão o mesmo fator a:

$$x = a2^q \quad y = a2^r$$

Então, supondo $q > r$, temos

$$\frac{x}{y} = \frac{a2^q}{a2^r} = 2^{q-r}.$$ ◀

Exemplo 8.9. Neste exemplo mostramos uma aplicação do princípio da casa dos pombos em uma demonstração relacionada a compressão de dados.

Definição 8.10. Um *algoritmo de compressão de dados* pode ser visto como uma função cuja entrada é uma sequência de M bits, e cuja saída é uma sequência de $n \leq M$ bits. ♦

Teorema 8.11. *Seja* C *um algoritmo de compressão de dados sem perda de informação. Então existe pelo menos uma entrada que* C *não poderá comprimir, nem mesmo em um bit.*

Demonstração. Há 2^M entradas possíveis, e cada entrada é mapeada em uma saída diferente. Se n fosse estritamente menor que M, teríamos $2^n < 2^M$, menos saídas do que entradas. Pelo princípio da casa dos pombos, portanto, deve haver alguma saída com tamanho igual a M. ■

Este exemplo é um de vários relacionados à Teoria da Informação. ◄

Exemplo 8.12. Um *gerador de bits pseudoaleatórios* é uma função G que tem como entrada uma sequencia de n bits e como saída outra sequência, de $M > n$ bits. Idealmente, o conjunto de possíveis saídas do gerador deve ter distribuição uniforme sobre o as possíveis sequências de M bits.

Teorema 8.13. *Não existe gerador de bits pseudoaleatórios cuja saída tenha distribuição uniforme.*

Demonstração. Para que a saída tivesse distribuição uniforme, cada uma das 2^M saídas teria que ser gerada por uma entrada diferente. Mas há apenas $2^n < 2^M$ entradas, portanto teríamos que ter duas saídas para a mesma entrada – impossível. Assim, há saídas que não serão geradas, e a distribuição das sequências de saída não pode ser uniforme. ■

Dada a restrição imposta por este teorema, em Criptografia define-se o objetivo de construir geradores pseudoaleatórios cujas saídas sejam *indistinguíveis* de bits aleatórios por algoritmos eficientes. ◄

Exemplo 8.14. Um mágico entrega um baralho a uma pessoa, que poderá embaralhá-lo como quiser. Esta pessoa retirará cinco cartas do baralho e as entregará ao assistente do mágico. O assistente escolhe quatro cartas e as mostra, em uma certa ordem, ao mágico – mas o mágico não vê a quinta carta, e mesmo assim, ele declara seu valor e naipe.

Determinando o naipe: esta á a parte fácil. Como há quatro naipes possíveis e cinco cartas, haverá duas delas com o mesmo naipe (apica-se o princípio da casa dos pombos). O assistente esconde uma das duas cartas e posiciona a outra em primeiro lugar, de forma que o mágico saiba o naipe da carta escondida.

Determinando o valor da carta: damos às cartas os valores A $= 1, 2, 3 \ldots,$ 10, J $= 11$, Q $= 12$, K $= 13$. Dispomos os 13 números em círculo. A distância para a frente entre dois números a, b, que denotamos por $\mathrm{df}(ab)$, é a quantidade a quantidade de passos necessários, no sentido do relógio, para chegar de a até b.

Para quaisquer dois números a e b, temos que $\mathrm{df}(a, b) \leq 6$ ou $\mathrm{df}(b, a) \leq 6$. Para que as duas distâncias fossem maiores que 6, seria necessário haver $7+7 = 14$ valores diferentes para as cartas de baralho (aplica-se o princípio da casa dos pombos).

Sejam a e b as duas cartas com mesmo naipe, com $\mathrm{df}(a, b) \leq 6$. O assistente mostrará ao mágico a, e não b, de forma que o mágico saiba que a distância da primeira carta em sua mão e a carta secreta seja menor que seis.

O assistente também ajusta a ordem das três últimas cartas mostradas ao mágico para que contenham uma codificação da distância entre a e b – que sabemos ser no

máximo seis. Determine uma ordem total para as cartas (por exemplo, a ordem lexicográfica por valor e naipe). O assistente então apresenta as cartas em diferentes ordens a fim de comunicar diferentes números. Suponha que a ordem seja $c_1 \prec c_2 \prec c_3$. Então a distancia poderia ser comunicada da seguinte forma:

$$\begin{array}{ll} c1, c2, c3 & 1 \\ c1, c3, c2 & 2 \\ c2, c1, c3 & 3 \\ c2, c3, c1 & 4 \\ c3, c2, c1 & 5 \\ c3, c1, c2 & 6 \end{array}$$

◀

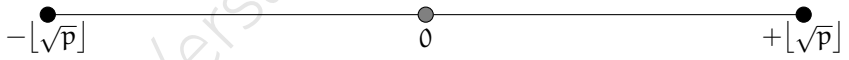
Exemplo 8.15. O princípio da casa dos pombos pode ser usado para demonstrar o teorema de Fermat sobre a soma de quadrados (8.16).

Teorema 8.16. *Todo número primo* p *tal que* $p \equiv 1 \pmod 4$ *pode ser escrito como a soma dos quadrados de dois inteiros.*

Demonstração. Para primos da forma $p \equiv 1 \pmod 4$, existe x inteiro tal que $x^2 = -1 \pmod p$ (a demonstração será omitida aqui).

Se existirem u e v inteiros tais que $u + vx \equiv 0 \pmod p$, com $0 < |u| \leq \sqrt{p}$ e $0 < |v| \leq \sqrt{p}$, então $u^2 + v^2 \equiv 0 \pmod p$, e $0 < u^2 + v^2 \leq 2p$.

Mostramos então que u e v devem existir. Suponha que não. Considere todos os pares (u, v) diferentes de $(0, 0)$ tais que $-\sqrt{p} \leq u, v \leq \sqrt{p}$. Existem $(2\lfloor\sqrt{p}\rfloor + 1)^2$ possibilidades para estes números, contando $(0, 0)$.



Descontando, temos $(2\lfloor\sqrt{p}\rfloor + 1)^2 - 1$ destes pares (note que excluímos $(0, 0)$, mas não os pares $(u, 0)$ e $(0, v)$). Este número é portanto a quantidade de números da forma $u + vx$ (estes são os pombos). Mas existem somente $p - 1$ possibilidades para o resto da divisão por p (estas são as casas), portanto deve existir pares $(u, v) \neq (t, w)$ tais que

$$u + vx \equiv t + vw \pmod p.$$

Mas isso implica que o par $(u - t, v - w)$ satisfaz

$$(u - t) + (v - w)x \equiv 0 \pmod p,$$

e havíamos presumido que tal par não existe. Chegamos a um absurdo, e concluímos a demonstração. ■

◀

8.2 Generalização do princípio da casa dos pombos

Teorema 8.17 (princípio generalizado da casa dos pombos)**.** *Se n objetos são dispostos em m lugares, haverá pelo menos um lugar com no mínimo $\lceil n/m \rceil$ objetos.*

Demonstração. Suponha que todos os lugares tem menos de $\lceil n/m \rceil$ objetos, ou seja, cada lugar tem no máximo $\lceil n/m \rceil - 1$ objetos. Então a quantidade máxima de objetos seria

$$\begin{aligned} M &< m\left(\left\lceil \frac{n}{m} \right\rceil - 1\right) \\ &< m\left(\left(\frac{n}{m} + 1\right) - 1\right) \\ &= m\frac{n}{m} = n. \end{aligned}$$

■

Exemplo 8.18. Em um grupo de 100 pessoas haverá no mínimo

$$\left\lceil \frac{100}{12} \right\rceil = 9$$

pessoas que fazem aniversário no mesmo mês. ◄

Exemplo 8.19. Pode-se usar o princípio generalizado da casa dos pombos para demonstrar o teorema de Erdös-Szekeres (8.20).

Teorema 8.20 (de Erdös-Szekeres)**.** *Em uma sequência de $mn + 1$ números diferentes, existe uma subsequência crescente de tamanho $m + 1$ ou uma subsequência decrescente de tamanho $n + 1$.*

Demonstração. Seja $A = \{a_k\}_k = 1^{k=mn+1}$ a sequência. Seja ℓ_i o tamanho da maior subsequência de A começando em a_i.

Há $mn + 1$ inteiros positivos $\ell_1, \ell_2, \ldots, \ell_{mn+1}$. Se existe j tal que $\ell_j \geq m + 1$ então existe subsequência de tamanho $m + 1$ começando em a_j – a subsequência de que trata o enunciado do teorema.

Suponha então que não existe j tal que $\ell_j \geq m + 1$ – ou seja, $\ell_i \leq m$ para todo i.

Temos portanto $mn+1$ números ℓ_i, que devem ser postos nos "lugares" $1, 2, \ldots, m$. Pelo princípio generalizado da casa dos pombos, um dos lugares contém pelo menos

$$\left\lceil \frac{mn+1}{m} \right\rceil = n + 1$$

números. Em outras palavras, há $n+1$ subsequências crescentes com o mesmo comrimento, e portanto existem $n+1$ índices $i_1, \ldots, i_{n+1}$ tais que $\ell_{i_1} = \ell_{i_2} = \cdots = \ell_{i_{n+1}}$.

Agora, suponha que a subsequência crescente começando em a_{i_2} seja $a_{i_2} < \ldots < a_{i_k}$, e que $a_{i_1} < a_{i_2}$. Então existiria uma sequência

$$a_{i_1} < a_{i_2} < \ldots < a_{i_k}$$

crescente com tamanho $n + 1$. O mesmo vale para todos os outros $a_{i_\square}$. Então temos

$$a_{i_1} > a_{i_2} > \cdots > a_{i_{n+1}}.$$

Repetindo o argumento trocando subsequências crescentes por decrescentes, completa-se a demonstração. ■

◀

Exercícios

Ex. 58 — Sete dardos são arremessados contra um alvo de raio 10. Mostre que haverá dois dardos entre os quais a distância será menor que 10.

Ex. 59 — Prove que dados n números inteiros $a_1, a_2, \ldots, a_n$, existem inteiros j e k, com $1 \leq j < k \leq n$ tais que

$$n|(a_j + a_{j+1} + \ldots + a_k).$$

Ex. 60 — Suponha que tenhamos escolhido cinco pontos no plano, sendo que todos tem coordenadas inteiras. Mostre que há pelo menos um par de pontos tal que o ponto médio entre eles também tem coordenadas inteiras.

Ex. 61 — Em um poliedro qualquer, há duas faces com o mesmo número de arestas.

Ex. 62 — Dados quaisquer quatro pontos em um círculo de raio unitário, há pelo menos dois deles entre os quais a distância é menor que $\sqrt{2}$.

Ex. 63 — Se escolhermos quaisquer $n+1$ números do conjunto $\underline{2n} = \{1, 2, \ldots, 2n\}$, haverá dentre os $n+1$ números escolhidos, dois coprimos.

Ex. 64 — Dados cinco pontos na superfície de uma esfera, pode-se dividí-la em duas metades de forma que um hemisfério contenha quatro deles.

Ex. 65 — Se as casas de um tabuleiro de xadrez de tamanho $n \times n$ forem numeradas de 1 a n^2, haverá duas casas adjacentes com números que diferem em no mínimo n – independente da ordem em que os números tenham sido atribuídos às casas.

Capítulo 9

Teoria da Contagem de Pólya

9.1 Grupos

Para chegarmos ao lema de Burnside e ao teorema de enumeração de Pólya será necessário detalhar alguns teoremas em grupos.

Definição 9.1 (grupo)**.** Um grupo é um conjunto não-vazio G associado a uma operação $\cdot : G \times G \to G$ tendo as propriedades listadas a seguir.

- **Associatividade:** para todos $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Existencia de neutro:** Deve haver um elemento neutro $e \in G$ para a operação de grupo: $\exists e \in G : \ a \cdot e = e \cdot a = a$.
- **Existencia de inverso:** Para todo $a \in G$, há um *inverso* $a' \in G$ tal que $a \cdot a' = a' \cdot a = e$.

Se a operação do grupo for comutativa ($ab = ba$ para todos $a, b \in G$), dizemos que o grupo é *comutativo* (ou *abeliano*).

A quantidade de elementos no grupo G é chamada de *ordem* de G, que denotamos por $|G|$. ♦

Observe que para termos um grupo a operação deve ser $\cdot : G \times G \to G$. Isso significa que ela deve sempre resultar em um elemento do grupo (damos a esta propriedade da operação o nome de *fechamento*).

Exemplo 9.2. O conjunto dos inteiros com a operação usual de soma é um grupo: a soma é associativa; existe o elemento neutro zero; e todo inteiro x tem um inverso $-x$.

Já o conjunto dos inteiros com a operação de multiplicação não é um grupo: o elemento neutro deve ser 1, e somente ele tem inverso – para todos os outros o inverso seria $1/x$, que não é inteiro. ◄

Exemplo 9.3. Dado um inteiro positivo n, o conjunto de matrizes quadradas de ordem n não singulares com a operação usual de multiplicação de matrizes é um grupo.

Em primeiro lugar, verificamos o fechamento: o produto de duas matrizes quadradas não singulares é outra matriz quadrada não singular. Além disso, observamos que o produto de matrizes é associativo. A matriz identidade funciona como elemento neutro para multiplicação, e toda matriz não singular tem inversa. ◀

Exemplo 9.4. O conjunto $\{1, 2, 3, 4\}$ com a operação de grupo sendo a multiplicação módulo 5, ou seja,

$$a \cdot b = ab \pmod 5,$$

é um grupo. Primeiro, verificamos o fechamento. Temos números de 1 a 4, e ao multiplicá-los nunca teremos um múltiplo de 5, portanto nunca teremos zero. A operação também não resultará em número maior que 4.

A multiplicação é associativa; existe um elemento neutro, 1: para todo x, temos $1x = x1 = x \pmod 5$.

Finalmente, todo elemento tem inverso:

$$\begin{aligned}(1 \cdot 1) &\pmod 5 = 1\\ (2 \cdot 3) &\pmod 5 = 1\\ (3 \cdot 2) &\pmod 5 = 1\\ (4 \cdot 4) &\pmod 5 = 1\end{aligned}$$

Temos portanto um grupo. O mesmo vale se trocarmos 5 por qualquer primo: o conjunto $\{1, 2, \ldots, p-1\}$ com a operação de multiplicação módulo p será um grupo. ◀

Definição 9.5 (subgrupo)**.** Se $H \subset G$ e H é um grupo com a mesma operação de G, então H é *subgrupo* de G. ♦

Exemplo 9.6. O conjunto dos inteiros pares é subgrupo do grupo dos inteiros: o zero continua sendo neutro, a soma de dois pares é par (e portanto a operação não resulta em alguém fora do conjunto), e todo par x tem um inverso $-x$ que também é par. ◀

Exemplo 9.7. O conjunto D de matrizes quadradas diagonais não singulares de ordem n é subgrupo do grupo M de matrizes quadradas singulares de ordem n.

Primeiro, $D \subset M$. Além disso, notamos que

- O produto de duas matrizes diagonais é diagonal;
- O produto de matrizes é associativo;
- A identidade é diagonal;
- Toda matriz diagonal tem inversa diagonal. ◀

Definição 9.8 (classe lateral)**.** Seja G um grupo e H subgrupo de G. Um subconjunto

$$gH = \{g.h | h \in H\},$$

onde $g \in G$, é chamado de *classe lateral à esquerda de* H *em* G.

De forma simétrica define-se a classe lateral à direita Hg. ♦

Exemplo 9.9. Seja D_n^I o grupo das matrizes diagonais ímpares não singulares de ordem n (os elementos na diagonal são todos ímpares), com a operação usual de multiplicação. Seja

$$Q = 4\mathcal{I} = \begin{pmatrix} 4 & 0 & 0 & \cdots & 0 \\ 0 & 4 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & & \\ 0 & 0 & \cdots & & 4 \end{pmatrix}.$$

Então o conjunto

$$QD_n^I = \{QA | A \in D_n^I\}$$

é uma classe lateral à esquerda de D^I em D_n. Esta classe lateral contém as matrizes múltiplas de 4. ◀

Teorema 9.10 (Lagrange)**.** *Se* G *é um grupo finito e* H *subgrupo de* G*, então a ordem de* H *divide a ordem de* G*, e a quantidade de classes laterais esquerdas distintas de* H *em* G *é*

$$\frac{|G|}{|H|}.$$

Demonstração. Considere a função $f : H \to xH$, definida como $f(h) = xh$. Ela é uma bijeção entre H e xH, portanto para todo x

$$|xH| = |H|.$$

Como G é a união *disjunta* das classes laterais à esquerda,

$$G = x_1H \cup x_2H \cup \cdots \cup x_nH,$$

com $n = |G|$, temos $|G| = |H|\,c$, onde c é a quantidade de classes laterais. ■

Exemplo 9.11. ◀

9.2 Ações de grupo, Lema de Burnside

Definição 9.12 (grupo de permutações)**.** Seja G, grupo e n um inteiro positivo. Denotamos por S_n o grupo formado por todas as permutações de n elementos, com a operação de composição. ♦

Exemplo 9.13. Seja $n = 3$. Temos $3! = 6$ permutações que compõem o conjunto S_3:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

A primeira delas, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, é o elemento neutro. ◀

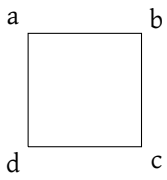
Definimos a seguir o conceito de *ação de grupo*[1]. Uma ação de grupo é um mapeamento de um grupo G em um grupo de permutações S_n. Note que não exigimos que o mapeamento seja injetivo nem sobrejetivo.

Definição 9.15 (ação de grupo)**.** Seja G um grupo e X um conjunto com $|X| = n$. Uma *ação* de G em X é uma função $f : G \to S_n$ tal que[2]

$$f(g(x)) = (fg)(x).$$

Dizemos que G é um grupo *agindo em* X. ♦

Exemplo 9.16. Seja Q um quadrado com cantos rotulados a, b, c, d:



Podemos representar o quadrado pela sequência de cantos, (abcd). Considere as seguintes ações sobre um quadrado:

- Identidade (e), que pode ser descrita como a permutação de cantos $\left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right)$
- Rotação no sentido horário, que pode ser descrita como a permutação de cantos $\left(\begin{smallmatrix}1&2&3&4\\4&1&2&3\end{smallmatrix}\right)$. Denotamos esta permutação por $\curvearrowright$.
- Rotação no sentido anti-horário, que pode ser descrita como a permutação de cantos $\left(\begin{smallmatrix}1&2&3&4\\2&3&4&1\end{smallmatrix}\right)$. Denotamos esta permutação por $\curvearrowleft$.

Estas tres rotações (ou permutações) e suas aplicações em sequência formam um grupo, que age sobre todos os quadrados possíveis: A identidade é o elemento neutro, e toda sequencia de rotações tem inversa, já que pode-se rotacionar nas duas direções. O grupo é finito, como podemos ver:

$$G = \{\curvearrowright, \curvearrowright\curvearrowright, \curvearrowleft, e\}.$$

Note que há muitas sequencias equivalentes: $\curvearrowright\curvearrowright = \curvearrowleft\curvearrowleft$, $e = \curvearrowright\curvearrowleft = \curvearrowright\curvearrowright\curvearrowright\curvearrowright$, por exemplo.

Também é importante observar que nem todas as 4! permutações dos cantos estão presentes. ◀

[1] A seguinte definição, também usualmente encontrada, é equivalente à que damos.

Definição 9.14 (ação de grupo)**.** Seja G um grupo e X um conjunto. Uma *ação* de G em X é uma função $f : G \times X \to X$ tal que

- f(e,x)=x para todo $x \in X$,
- f(g,f(h,x)) = f(gh,x) para todos $g, h \in G$. ♦

[2] Ou seja, é um *homomorfismo* de G em S_n.

Suponha que temos um grupo agindo em um conjunto X. Será útil definir o conjunto de elementos de X que podem resultar da aplicação de uma ação de G. Esta é a *órbita* do elemento.

Definição 9.17 (órbita)**.** Seja G um grupo finito agindo em um conjunto X. A *órbita* de x em G, denotada por $\text{orb}_G(x)$, é

$$\text{orb}_G(x) = \{g \cdot x | g \in G\}. \qquad \blacklozenge$$

Observe que se $g, h \in G$, gx está na órbita de x, mas isso implica que ggx, ghx, ... também estarão, porque gg e gh, ... também pertencem ao grupo.

Exemplo 9.18. Considere o grupo de rotações já dado agindo sobre o conjunto de todos os quadrados com rótulos nos cantos, onde os rótulos podem ser a, b, c, d, permitindo com repetições (há $4^4 = 256$ destes quadrados). A órbita do quadrado $abcd$ é o conjunto de quatro quadrados

$$\{abcd, bcda, cdab, dabc\}$$

Já a órbita do quadrado $abab$ é o conjunto de dois quadrados

$$\{abab, baba\}. \qquad \blacktriangleleft$$

Definição 9.19 (estabilizador)**.** Seja G um grupo finito agindo em um conjunto X. O *estabilizador de* x, denotado $\text{stab}_G(x)$, é o conjunto de elementos de g que fixam x, ou seja,

$$\text{stab}_G(x) = \{g \in G | g \cdot x = x\}. \qquad \blacklozenge$$

Exemplo 9.20. A identidade fixa todos os quadrados. A permutação $\curvearrowright\curvearrowright$ fixa os quadrados $abab$, $baba$, $acac$, etc, da forma "XYXY". Qualquer permutação fixa os quadrados com todos rótulos iguais, $aaaa$, $bbbb$, etc.

Claramente, $\text{stab}_G(aaaa)$ é igual a G. Já $\text{stab}_G(abab)$ é igual a $\{e, \curvearrowright\curvearrowright\}$. Finalmente, $\text{stab}_G(abcd)$ é igual a $\{e\}$. $\blacktriangleleft$

Quando temos um grupo agindo em um conjunto, as órbitas são classes de equivalênca, e portanto podemos particionar o grupo em órbitas. O exercício 70 pede a demonstração deste fato, enunciado na proposição 9.21.

Proposição 9.21. *Seja* G *um grupo finito aginto em um conjunto* X*. Defina que um elemento* $y \in X$ *é* alcançavel em um passo *a partir de outro elemento* $x \in X$ *se existe algum* $g \in G$ *tal que* $gx = y$*. A relação alcançável é uma relação de equivalência, as classes de equivalência definidas por ela são as órbitas de seus elementos.*

Lema 9.22. $\text{stab}_G(x)$ *é subgrupo de* G*.*

Teorema 9.23 (da órbita e do estabilizador)**.** *Seja* G *um grupo agindo em um conjunto* X*. Então, para todo* $x \in X$*,*

$$|G| = |\text{orb}_G(x)| \, |\text{stab}_G(x)|.$$

Demonstração. Pelo teorema de Lagrange, a quantidade de classes laterais à esquerda de $\text{stab}_G(x)$ é

$$\frac{|G|}{|\text{stab}_G(x)|}.$$

Nos falta apenas mostrar que o número de classes laterais à esquerda de $\text{stab}_G(x)$ é igual a $|\text{orb}_G(x)|$.

Sejam $g, h \in G$, e suponha que $g\,\text{stab}_G(x) = h\,\text{stab}_G(x)$. Então $g^{-1}g\,\text{stab}_G(x) = (g^{-1}h)\,\text{stab}_G(x)$, e temos

$$\text{stab}_G(x) = (g^{-1}h)\,\text{stab}_G(x),$$

portanto $g^{-1}h \in \text{stab}_G(x)$. Mas se $(g^{-1}h)x = x$, então $g = h$.

Da mesma foram, $g = h$ implica que $g\,\text{stab}_G(x) = h\,\text{stab}_G(x)$, portanto temos uma bijeção entre as classes laterais à esquerda de $\text{stab}_G(x)$ e os elementos de $\text{orb}_G(x)$, concluindo a demonstração. ■

9.2.1 Lema de Burnside

Sabemos que ações de grupo definem relações de equivalência, particionando o conjunto. O lema de Burnside nos permite, havendo um grupo agindo sobre um conjunto, calcular a quantidade de classes de equivalencia definidas pelas ações de grupo. No contexto do exemplo do quadrado com cantos rotulados, podemos contar a quantidade de qudrados diferentes, *independente de rotação*.

Definição 9.24. Seja G um grupo finito agindo em um conjunto X. Para todo $g \in G$, a quantidade de elementos de X que g não modifica é denotada por $\text{fix}(g)$, ou seja,

$$\text{fix}(g) = \big|\{x \in X | g \cdot x = x\}\big|. \quad \blacklozenge$$

Lema 9.25 (de Burnside)**.** *Se G é um grupo finito agindo em um conjunto X, a quantidade de órbitas de G em X é*

$$\frac{1}{|G|}\sum_{g\in G} |\,\text{fix}(g)|.$$

Demonstração. Seja n a quantidade de pares (g, x), com $g \in G$ e $x \in X$ e $gx = x$. Se fixarmos g, o número de pares desta forma é exatamente $\text{fix}_G(g)$. Assim,

$$n = \sum_{g\in G} |\,\text{fix}_G(g)|.$$

Agora, se fixarmos x, temos

$$n = \sum_{x\in X} |\,\text{stab}_G(x)|.$$

Sabemos que se x e y estão na mesma órbita, então $\text{orb}_G(x) = \text{orb}_G(y)$, e $\text{stab}_G(x) = \text{stab}_G(y)$. Então escolhemos um x e usamos o teorema da órbita e estabilizador para calcular a seguinte soma sobre todo y na órbita de x:

$$\sum_{y\in \text{orb}_G(x)} |\,\text{stab}_G(y)| = |\,\text{orb}_G(x)|\,|\,\text{stab}_G(x)| = |G|.$$

Das equações já apresentadas nesta demonstração, concluimos que

$$n = \sum_{g \in G} |\operatorname{fix}_G(g)| = \sum_{x \in X} |\operatorname{stab}_G(x)| = |G|k,$$

onde k é a quantidade de órbitas. ■

Exemplo 9.26. A quantidade de permutações no grupo é 4. Para cada uma das rotações, temos

$$\begin{aligned} |\operatorname{fix}(e)| &= 256 \\ |\operatorname{fix}(\curvearrowright)| &= 4 \\ |\operatorname{fix}(\curvearrowright\curvearrowright)| &= 4^2 = 16 \\ |\operatorname{fix}(\curvearrowleft)| &= 4 \end{aligned}$$

assim, a quantidade de órbitas (ou seja, de quadrados realmente diferentes, independente de rotação) é

$$\frac{1}{|G|} \sum_{g \in G} |\operatorname{fix}(g)| = \frac{1}{4}(256 + 4 + 16 + 4) = 70. \quad \blacktriangleleft$$

9.3 Teorema de Enumeração de Pólya

George Pólya conseguiu uma generalização do teorema de Burnside, conhecida como o *teorema de enumeração de Pólya*.

Uma descrição básica do teorema de Pólya é dada por Fred Roberts e Barry Tesman [RT09].

Exercícios

Ex. 66 — Determine onde está o erro: *Damos um contraexemplo, provando que o teorema de Lagrange não vale. Seja* $\mathbb{Z}_5 = \{1, \ldots, 4\}$ *o grupo de inteiros módulo* 5 *e* $\mathbb{Z}_7 = \{1, \ldots, 6\}$ *o grupo de inteiros módulo* 7*. Em ambos os conjuntos a operação é a de multiplicação modular, e* $\mathbb{Z}_5 \subset \mathbb{Z}_7$ *(é subgrupo). Temos* 4 *elementos em* $\mathbb{Z}_5$ *e* 6 *elementos em* $\mathbb{Z}_7$*. No entanto,* $4 \nmid 6$*, contrariando o teorema de Lagrange.*

Ex. 67 — Na demonstração do Lema de Burnside, dissemos que

$$n = \sum_{g \in G} |\operatorname{fix}_G(g)| = \sum_{x \in X} |\operatorname{stab}_G(x)| = |G|k,$$

A quantidade de órbitas deve ser portanto igual a

$$\frac{1}{|G|} \sum_{x \in X} |\operatorname{stab}_G(x)|$$

Calcule a quantidade de órbitas dos quadrados usando esta fórmula (você deve chegar também em 70 órbitas).

Ex. 68 — Seja P o conjunto de todos os pentágonos com vértices pintados usando duas cores, e G um grupo contendo todas as rotações possíveis nesses pentágonos. Conte as órbitas.

Ex. 69 — Refaça o exemplo dos quadrados dado no texto usando, além das rotações, reflexões em torno das duas diagonais.

Ex. 70 — Prove a proposição 9.21.

Capítulo 10

O Método Probabilístico

Damos o nome de *método probabilístico* ao uso de argumentos probabilísticos em contagem e demonstrações de existência em Combinatória. Muito simplificadamente, o método pode ser descrito da seguinte maneira. Suponha que queiramos demonstrar que uma determinada estrutura com certas propriadades existe – um subgrafo de um grafo com alguma característica especial ou um subconjunto de um conjunto, por exemplo. Construimos um experimento aleatório, gerando estruturas de acordo com alguma distribuição, e criamos uma variável aleatória relacionada à existência daquela de nosso interesse (o subgrafo, conjunto, etc) – por exemplo, "seja X a variável aleatória que representa o evento 'o grafo gerado é bipartido'". A partir daí, podemos usar propriedades dessa variável aleatória para demonstrar a existência da estrutura, ou mesmo determinar limites para a sua quantidade.

Este Capítulo apresenta apenas exemplos básicos de uso do método probabilístico.

10.1 Primeiro Momento (esperança)

A primeira característica que usaremos é a esperança (ou "primeiro momento de probabilidade"). Nosso uso da esperança no método probabilístico é resumido no Lema 10.1

Lema 10.1. *Seja X uma variável aleatória. Há pelo menos um ponto no espaço amostral tal que $X \geq \mathbb{E}[X]$, e pelo menos um ponto tal que $X \leq \mathbb{E}[X]$.*

O primeiro exemplo é a demonstração de existência de certos subconjuntos de conjuntos de inteiros.

Definição 10.2 (conjunto livre de soma)**.** Um conjunto A de inteiros não-nulos é *livre de soma* se para todos $a, b \in A$, $a + b \notin A$. ♦

Teorema 10.3. *Todo conjunto A de inteiros não-nulos tem um subconjunto livre de soma de tamanho $\geq |A|/3$.*

Demonstração. Denote $n = |A|$. Seja $m = \max\{|x| : x \in A\}$ (o maior valor absoluto de elementos de A).

Escolha um número primo $p = 3k + 2$, que seja maior que $2m$.

Seja $C = \{k + 1, k + 2, \ldots, 2k + 1\}$. Este conjunto é livre de soma, porque se $a, b \in C$, então $2k + 2 \leq a + b$, e isto vale também para $a + b \pmod p$.

Observe que $|C| = k + 1$, e

$$\frac{|C|}{p-1} = \frac{k+1}{3k+2} > \frac{1}{3}.$$

Agora escolhemos aleatoriamente um elemento $1 \leq x < p$, com distribuição uniforme, e definimos que

$$d_i = xa_i \pmod p.$$

Como $1 \leq x < p$, também teremos $1 \leq d_i < p$, ou seja, nenhum d_i será zero (tanto x como a_i são diferentes de zero, e nenhum deles é divisível por p). Assim,

$$\Pr[d_i \in C] = \frac{|C|}{p-1} > \frac{1}{3}.$$

Isso significa que *a esperança da quantidade de elementos* d_i *que pertencem a* C *é maior que* $n/3$. Assim, deve existir um $1 \leq x < p$ e $B \subseteq A$ com $|B| > n/3$ tais que para todo $b \in B$, $xb \pmod p \in C$.

O conjunto B é livre de soma: se houvesse $a, b, c \in B$ tais que $a + b \equiv c \pmod p$, então teríamos $xa + xb \equiv xc \pmod p$, e C não seria livre de soma – o que contradiz o que já havíamos determinado. ■

O próximo exemplo é a determinação de limite inferior para números de Ramsey.

Definição 10.4 (Número de Ramsey)**.** Dado um inteiros positivos k, ℓ, o menor inteiro n tal que existe um grafo completo com n vértices que, quando colorido com duas cores, sempre conterá um subgrafo completo com k vértices e todas as arestas de uma cor ou um subgrafo completo com ℓ vértices com todas as arestas da outra cor.

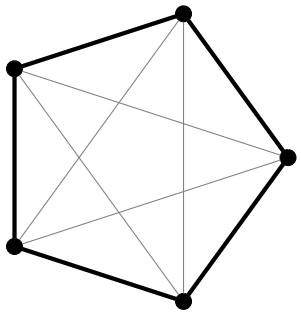
Denotamos o número de Ramsey por $R(k, \ell)$, e quando $k = \ell$, denotamos simplesmente $R(k)$. ♦

Define-se similarmente números de Ramsey para várias cores, que são denotados por $R(k_1, k_2, \ldots, k_m)$.

Exemplo 10.5. Temos $R(2) = 2$. O grafo completo com dois vértices, K_2, é mostrado abaixo.

Trivialmente este grafo, ao ser colorido, sempre terá ele mesmo como subgrafo de tamanho 2 com uma única cor. ◄

Exemplo 10.6. Já $R(3)$ é igual a seis, porque há uma coloração para a qual o grafo completo K_5 não contém subgrafos completos de tamanho 3 com todas as arestas da mesma cor:



Já no grafo K_6, toda coloração resultará necessariamente em um subgrafo completo de tamanho 3 com todas as arestas da mesma cor. ◀

Teorema 10.7. *para todo inteiro positivo* k*,*

$$R(k) \geq 2^{k/2}.$$

Demonstração. Atribua as duas cores a todas as arestas aleatoriamente: cada aresta é pintada de vermelho com probabilidade $1/2$ e de preto com probabilidade $1/2$, sendo que a escolha da cor de cada aresta independe das escolhas das outras.

Seja $x_1, \ldots, x_k$ um subconjunto dos vértices do grafo. A probabilidade de cada x_i estar ligado a todo x_j por aresta vermelha é $2^{-\binom{k}{2}}$. A esperança para o número de subgrafos com k vértices contendo apenas arestas da mesma cor é

$$2^{1-\binom{k}{2}}\binom{n}{k}.$$

Se este valor for menor que um, então deve ser possível que não haja tais subgrafos, e este valor é menor que um quando

$$n < 2^{k/2},$$

portanto para $n \geq 2^{k/2}$ sempre deve existir tal conjunto, e $R(k) \geq 2^{k/2}$. ■

Também pode-se mostrar, usando argumentos não probabilísticos, que $R(k) \leq 2^{2k}$.

O último exemplo desta seção trata da cardinalidade de certas famílias de conjuntos. Provaremos o teorema de Erdös-Ko-Rado.

Definição 10.8 (família intersectante de conjuntos)**.** Uma família F de conjuntos é *intersectante* se para todos $A, B \in F$, $A \cap B \neq \emptyset$. ♦

Usaremos o Lema 10.9, cuja demonstração é pedida no exercício 73.

Lema 10.9. *Considere* $X = \{0, 1, \ldots, n-1\}$ *com a operação de adição módulo* n*. Seja* $A_s = \{s, s+1, \ldots, s+(k-1)\} \subseteq X$*, para todo* $s < n$*. Então, para* $n \geq 2k$*, qualquer família* $F \subseteq \binom{X}{k}$ *contém pelo menos* k *do sconjuntos* A_s*.*

Teorema 10.10 (de Erdös-Ko-Rado)**.** *Seja* X *um conjunto, tal que* $|X| = n$*, e* $k \in \mathbb{N}$ *tal que* $n \geq 2k$*. Seja também* F *uma família intersectante de* k*-subconjuntos de* X *(ou seja,* $F \subseteq \binom{X}{k}$*). Então*

$$|F| \leq \binom{n-1}{k-1}.$$

Demonstração. Sem perda de generalidade, presumimos que $X = \{0, 1, 2, \ldots, n-1\}$. Seja $\sigma : X \to X$ uma permutação. Denotamos por $\sigma(A_s)$ o conjunto

$$\sigma(A_S) = \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}.$$

O efeito de σ em A_s é somente o de renomear os elementos. Desta forma, o Lema 10.9 nos garante que no máximo k desses n conjuntos está em F.

Se escolhermos aleatoriamente s e σ,

$$\Pr[\sigma(A_s) \in F] \leq \frac{k}{n}. \tag{10.1}$$

Mas escolher A_s desta forma é o mesmo que escolher aleatoriamente um conjunto de k elementos de X, portanto

$$\Pr[\sigma(A_s) \in F] = \frac{|F|}{\binom{n}{k}}$$

$$\binom{n}{k} \Pr[\sigma(A_s) \in F] = |F| \tag{10.2}$$

De 10.1 e 10.2, segue o resultado:

$$|F| \leq \binom{n}{k}\frac{k}{n} = \binom{n-1}{k-1}.$$ ■

Exemplo 10.11. Seja $A = \{1, 2, 3, 4, 5, 6\}$. Temos $|A| = n = 6$. Escolhemos agora $k = 3$. Qualquer família de subconjuntos intersectante de A terá no máximo

$$\binom{n-1}{k-1} = \binom{5}{2} = 10$$

conjuntos. ◀

Uma extensa discussão do método probabilístico pode ser encontrada no livro de Noga Alon e Joel Spencer [AS08].

10.2 Linearidade da esperança

Em diversos problemas de contagem onde aplicamos o método probabilístico, podemos usar diferentes fatos a respeito das variáveis aleatórias que identificamos. Nesta seção damos como exemplo a linearidade da esperança.

Sabemos que o conjunto de todas as variáveis aleatórias reais em um espaço amostral é um espaço vetorial. Ao aplicar o método probabilístico, podemos usar seguinte Lema 10.12, que nos garante que a esperança é um operador linear nesse espaço.

Lema 10.12. *A esperança é um operador linear, ou seja, para quaisquer variáveis aleatórias* X *e* Y *e constante* $c \in \mathbb{R}$*,*

$$\mathbb{E}[X+Y] = \mathbb{E}[X] + \mathbb{E}[Y]$$
$$\mathbb{E}[cX] = c\mathbb{E}[X].$$

Demonstração. Verificamos a soma:

$$\begin{aligned}
\mathbb{E}[X+Y] &= \sum_x \sum_y (x+y)\Pr[X=x, Y=y] \\
&= \sum_x x \sum_y \Pr[X=x, Y=y] + \sum_y y \sum_x \Pr[X=x, Y=y] \\
&= \sum_x x \Pr[x] + \sum_y y \Pr[x] \\
&= \mathbb{E}[X] + \mathbb{E}[Y].
\end{aligned}$$

Para a multiplicação,

$$\mathbb{E}[cX] = \sum_x cx \Pr[x] = c\mathbb{E}(X). \qquad \blacksquare$$

A demonstração que damos para o Teorema 10.13 usa a linearidade da esperança.

Teorema 10.13. *Seja* $G = (V, E)$ *um grafo com* n *vértices e* k *arestas. Então há um subgrafo bipartido de* G *com no mínimo* $k/2$ *arestas.*

Demonstração. Seja $B = V - A$. Uma aresta (a, b), com $a \in A$ e $b \in B$, cruza A e B. O número destas arestas (cruzando A e B) é dado pela variável aleatória

$$C = \sum_{x,y \in E} C_{x,y},$$

onde $C_{a,b}$ é uma variável aleatória valendo um se (x, y) cruza A e B e zero em caso contrário. A esperança desta variável é

$$\begin{aligned}
\mathbb{E}[C_{x,y}] &= \Pr[x \in B, y \in A] + \Pr[x \in A, y \in B] \\
&= \Pr[x \in B]\Pr[y \in A] + \Pr[x \in A]\Pr[y \in B] \\
&\qquad \text{(eventos são independentes)} \\
&= 1/2.
\end{aligned}$$

Como a esperança é linear,

$$\mathbb{E}[C] = \sum_{x,y \in E} \mathbb{E}[C_{x,y}] = k/2.$$

Assim, existe pelo menos uma escolha A que nos dá pelo menos $\geq k/2$ arestas cruzando as duas partes.

Para este A que identificamos, remova as arestas que *não* cruzam A e B. O resultado é bipartido (porque só restaram as arestas cruzando A e B) e tem pelo menos $k/2$ arestas. $\blacksquare$

10.3 Segundo momento (variância)

Lema 10.14 (desigualdade de Chebyshev)**.** *Seja* X *uma variável aleatória com variância finita. Então, para todo* $t > 0$*,*

$$\Pr\Big[\ |X - \mathbb{E}[X]|\ \geq\ t\Big] \leq \frac{\mathrm{Var}[X]}{t^2}.$$

Em nosso próximo exemplo, usaremos o método do segundo momento paradeterminar o limite inferior para um coeficiente binomial. Quando Na expansão de qualquer binômio $(x+y)^{2m}$, o maior coeficiente será sempre o do meio, que é igual a $\binom{2m}{m}$. Por exemplo, na expansão de $(x+y)^6$, o maior coeficiente é $\binom{6}{3} = 20$:

$$(x+y)^6 = x^6 + 6x^5y^2 + 15x^4y^2 + \mathbf{20}x^3y^3 + 15x^2y^4 + 6xy^5 + 1y^6$$

O coeficiente para o qual determinaremos o limite inferior é exatamente este, $\binom{2m}{m}$.

Teorema 10.15. *Para todo* $m \geq 1$*,*

$$\binom{2m}{m} \geq \frac{2^{2m}}{2+4\sqrt{m}}$$

Demonstração. Defina um experimento aleatório onde $2m$ moedas são jogadas. Cada moeda dá origem a uma variável aleatória X_i. Temos portanto $2m$ variáveis aleatórias $X_1, X_2, \ldots, X_{2m}$, independentes, tais que

$$\Pr[X_i = 1] = 1/2$$
$$\Pr[X_i = 0] = 1/2.$$

Definimos agora a variável $X = X_1 + X_2 + \cdots + X_m$. A esperança e a variância de X são

$$\mathbb{E}[X] = m$$
$$\mathrm{Var}[X] = \frac{m}{2}.$$

A desigualdade de Chebyshev com $t = \sqrt{m}$ nos dá

$$\Pr\Big[|X - m| < \sqrt{m}\Big] \geq \frac{1}{2}.$$

Dado um k tal que $|k| < \sqrt{m}$, a probabilidade de X assumir o valor $m+k$ é

$$\Pr\Big[X = m+k\Big] = \binom{2m}{m+k}\frac{1}{2^{2m}},$$

mas como $\binom{2m}{m}$ é o maior coeficiente, então temos

$$\begin{aligned}\Pr\Big[X = m+k\Big] &= \binom{2m}{m+k}\frac{1}{2^{2m}} \\ &\leq \binom{2m}{m}\frac{1}{2^{2m}},\end{aligned}$$

e finalmente temos

$$\begin{aligned}\frac{1}{2} &\leq \sum |k| < \sqrt{m}\Pr\left[X = m + k\right] \\ &\leq (2\sqrt{m}+1)\binom{2m}{m}\frac{1}{2^{2m}},\end{aligned}$$

terminando a demonstração. ■

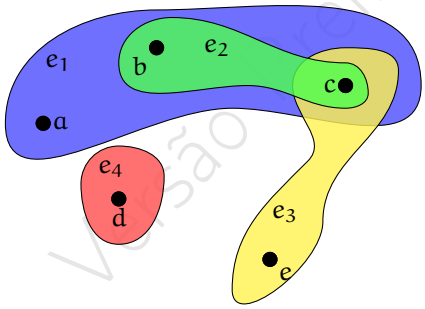
Exercícios

Ex. 71 — Seja $G = (V, E)$ um grafo aleatório. Calcule o número de vértices isolados em G.

Ex. 72 — Um *hipergrafo* é um par (V, E), onde V é um conjunto de vértices, e E é um conjunto de arestas. Uma aresta pode ligar mais de dois vértices: $E \subseteq 2^V$.
Por exemplo, o hipergrafo

$$\begin{aligned}V &= \{a, b, c, d, e\} \\ E &= \Big\{\{a, b, c\}, \{b, c\}, \{c, e\}, \{d\}\Big\}\end{aligned}$$

pode ser representado como na figura a seguir.



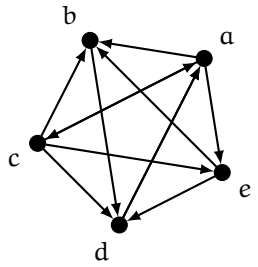
Um hipergrafo é k-uniforme se cada aresta conecta exatamente k vértices. Dizemos também que um hipergrafo é *bipartido* se seu conjunto de vértices pode ser dividido em dois conjuntos, V_1 e V_2, de forma que em cada V_i não haja dois vértices ligados pela mesma aresta. No exemplo dado anteriormente, vemos trivialmente que o hipergrafo é bipartido, porque podemos separar V em $V_1 = \{d\}$ e $V_2 = \{a, b, c, e\}$.
Seja G um hipergrafo k-uniforme. com menos de 2^{k-1} hiperarestas. Então G é bipartido.

Ex. 73 — Prove o Lema 10.9 (não é necessário usar o método probabilístico).

Ex. 74 — Prove o Teorema de Legendre, usando o método probabilístico: *Seja* p *um número primo. A potência de* p *na fatoração de* $n!$ *é*

$$\sum_{k\geq 1}\left\lfloor\frac{n}{p^k}\right\rfloor.$$

Ex. 75 — Seja G um grafo não-orientado completo. Um *torneio* é um grafo orientado obtido a partir de G escolhendo uma direção para cada aresta. A idéia é modelar um torneio competitivo, onde cada aresta representa um competidor vencendo outro. A figura a seguir mostra um torneio com cinco vértices.



Note que há um ciclo dirigido com n (5) arestas no grafo: $acebda$.
Prove, usando o método probabilístico, que para qualquer $n \geq 3$ existe um torneio com n vértices e pelo menos $(n-1)!2^{-n}$ ciclos dirigidos com n arestas.

Ex. 76 — Refaça o Exercício 75, mas considerando ciclos de qualquer tamanho.

Ex. 77 — Dado um $n \geq 3$, é sempre possível obter um torneio onde não há ciclos de tamanho n? E torneios onde não há ciclos de nenhum tamanho?

Ex. 78 — Considere o problema da satisfatibilidade booleana (SAT) com n cláusulas e k variáveis. Prove que existe uma valoração que satisfaz pelo menos $n(1-2^{-k})$ cláusulas.

Apêndice A

Dicas e Respostas

Resp. (Ex. 15) — Defina a bijeção $f : \mathbb{R} \to (0, \infty)$, com $f(x) = 2^x$. Depois mostre que $|(0, \infty)| = |(0, 1)|$.

Resp. (Ex. 16) — Prove primeiro que $|\mathbb{R}^2| = |\mathbb{R}|$, depois proceda por indução na dimensão.

Resp. (Ex. 17) — Não: use $2^{\mathbb{R}}$ e o Teorema 2.16.

Resp. (Ex. 19) — $6!$

Resp. (Ex. 20) — A cada aresta podem ser atribuídas k cores, portanto temos $k^{|E|}$ colorações possíveis.

Resp. (Ex. 22) — Com k letras e $k+1$ dígitos representamos $(26^k)(10^{k+1})$. Queremos

$$\begin{aligned} 26^k 10^{k+1} &\geq 10^7 \\ 26^k 10^k 10 &\geq 10^7 \\ 260^k &\geq 10^6 \\ k &\geq \lceil \log_{260}(10^6) \rceil \end{aligned}$$

Percebemos que $260^2 = 67600$, $260^3 = 17576000$, portanto precisamos de $k \geq 3$.

Resp. (Ex. 25) — 2^n.

Resp. (Ex. 28) — Use a identidade de Pascal no passo de indução.

Resp. (Ex. 30) — Não, porque o produto de matrizes não é comutativo. Dadas A e B,

$$(A+B)^2 = AA + AB + BA + BB,$$

mas como AB não necessariamente é igual a BA, não podemos abreviar esta forma como $A^2 + 2AB + B^2$.

Resp. (Ex. 32) — Consideramos relações não necessariamente simétricas. Para o conjunto vazio, uma relação (a relação vazia). Para n elementos, a quantidade é 2^{1+n^2}.

Resp. (Ex. 33) — $5 + 10 + 4 - 3 - 1 - 2 + 1 = 14$.

Resp. (Ex. 38) — (i) $-\ln(1-x)$ (ii) $\frac{2}{2-x}$ (iii) $(1-2x)^{-1}$ (iv) $(2x^2-4x+2)^{-1}$ (v) $\frac{x(x+1)}{(1-x)^3}$ (vii) $\frac{2x}{x^2-2x+1}$ (viii) $\frac{x}{x^4-2x^2+1}$ (ix) $(1+x)^{-1}$

Resp. (Ex. 42) — (Dica) O posto é n, o determinante é zero, e o traço é $n+1$, para todo n.

Resp. (Ex. 47) — $v_n = v_{n-1} + jv_0$. $v_n = v_0 + nj(v_0)$.

Resp. (Ex. 48) — (a) $\sqrt{n} + \sum_{i=2}^{n} n\sqrt{n-1}$

Resp. (Ex. 51) — Pelo exercício 50(c), temos $F_{2n+1} = F_n(F_{n-1} + F_{n+1})$, e se $n > 1$, os dois fatores são maiores que um.

Resp. (Ex. 52) — (a) Por indução. Se $g(n)$ é este número, temos para base:

$$g(1) = 2 = F_2$$
$$g(2) = 3 = F_3$$

Para $n > 2$, presumimos que $g(n-1) = F_n$.
Separamos as possibilidades em:

i) as que usam o último objeto

ii) as que não usam o último objeto

Nas do tipo (i) o penúltimo não pode ser usado, portanto elas somam $g(n-2)$ possíveis escolhas.

Nas do tipo (ii) podemos usar o penúltimo, logo temos $g(n-1)$ escolhas. Assim, temos

$$g(n) = g(n-1) + g(n-2) = F_n + F_{n-1} = f_{n+1}$$

(b) Considere uma posição qualquer no círculo. Se está desocupada, podemos quebrar o círculo naquela posição e temos uma linha com $n-1$ posições, donde podemos selecionar objetos de $g(n-1) = F_n$ maneiras.
Se a posição está ocupada, seus vizinhos estão desocupados, e (com $n > 2$) podemos remover esta posição e os dois vizinhos. Temos portanto $g(n-3) = F_{n-2}$ possibilidades.
Assim, há $F_n + F_{n-2}$ possibilidades.

Resp. (Ex. 55) — Sim:

$$\begin{aligned} F_{-4} &= -3 \\ F_{-3} &= 2 \\ F_{-2} &= -1 \\ F_{-1} &= 1 \\ F_0 &= 0 \\ F_1 &= 1 \\ F_2 &= 1 \\ F_3 &= 2 \\ F_3 &= 3 \end{aligned}$$

Ou seja, se $k > 0$, $F_{-k} = (-1^{k+1})F_k$.
A relação $F_n = F_{n-1} + F_{n-2}$ continua valendo, assim como a forma fechada (prove esta última parte!)

Resp. (Ex. 57) — Faça $b_n = \ln(a_n)$. A solução é

$$a_n = \sqrt[5]{\exp(18 - 3(-2/3)^n)}.$$

Resp. (Ex. 66) — As operações nos dois grupos são diferentes: multiplicar $\pmod 5$ não é o mesmo que multiplicar $\pmod 7$, portanto $\mathbb{Z}_5$ *não* é subgrupo de $\mathbb{Z}_7$.

Resp. (Ex. 67) — A tabela a seguir lista os quadrados, sua quantidade, a quantidade de estabilizadores e a lista de estabilizadores.

quadrados	qtde	$\lvert \mathrm{stab}_G \rvert$	stab_G
XXXX	4	4	G
XYXY	12	2	$e, \curvearrowright\curvearrowright$
resto	240	1	e

Temos então que a quantidade de órbitas é

$$\frac{1}{|G|}\sum_{x\in X}|\operatorname{stab}_G(x)| = \frac{1}{4}(4\cdot 4 + 12\cdot 2 + 240) = \frac{280}{4} = 70.$$

Resp. (Ex. 70) — Os elementos na órbita de x são todos alcançáveis entre si através de uma única operação do grupo: x alcança a si mesmo porque $ex = x$, onde e é o elemento neutro. Todo outro elemento da órbita alcança x porque se $gx = y$, então $g^{-1}y = x$. E todos $y, z \neq x$ alcançam um ao outro porque se $gy = x$ e $hz = x$, então $(gh^{-1})y = z$.

Resp. (Ex. 72) — (Dica) Releia o Teorema 10.7.

Resp. (Ex. 75) — Comece com K_n, e gere aleatoriamente orientações para as arestas. A probabilidade de $v_1, v_2, \ldots, v_n$ ser um ciclo orientado é $1/2^n$, porque dependemos da orientação de n arestas. Em seguida, considere que existem $(n-1)!$ permutações dos vértices, portanto há $(n-1)!$ sequências que poderiam ou não formar ciclos. Seja X_i a variável aleatória que indica que a i-ésima permutação de vértices é um ciclo ($X_i = 1$ se a permutação é ciclo, $X_i = 0$ se não é). Temos $\mathbb{E}[X] - 1/2^n$. O número total esperado de ciclos é

$$\begin{aligned}\mathbb{E}\left[\sum_i X_i\right] &= \sum_i \mathbb{E}[X_i] \\ &= (n-1)!(1/2^n).\end{aligned}$$

Como a esperança para o total de ciclos é $(n-1)!(1/2^n)$, deve haver um torneio com pelo menos esse número de ciclos.

Ficha Técnica

Este texto foi produzido inteiramente em LaTeX em sistema Linux. Os diagramas foram criados sem editor gráfico, usando diretamente o pacote Tikz. O ambiente Emacs foi usado para edição do texto LaTeX.

Bibliografia

[And94] George Andrews. *Number Theory*. Dover, 1994. ISBN: 978-0-486-68252-5.

[AS08] Noga Alon e Joel H. Spencer. *The Probabilistic Method*. 3ª ed. Wiley, 2008. ISBN: 978-0470170205.

[Bon92] Boris A. Bondarenko. *Generalized Pascal Triangles and Pyramids, Their Fractals, Graphs, and Applications*. Fibonacci Assn, 1992. ISBN: 978-5648007383.

[FS09] Philppe Flajolet e Robert Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009. ISBN: 978-0-521-89806-5.

[GJ04] Ian P. Goulden e David M. Jackson. *Combinatorial Enumeration*. Dover, 2004. ISBN: 978-0-486-43597-8.

[MN98] Jiri Matousek e Jaroslav Nesetril. *Invitation to Discrete Mathematics*. Oxford, 1998. ISBN: 0-19-850208-7.

[NSM91] Ivan Niven, Herbert S. Suzkerman e Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. Wiley, 1991. ISBN: 978-0471625469.

[RT09] Fred S. Roberts e Barry Tesman. *Applied Combinatorics*. 2ª ed. CRC Press, 2009. ISBN: 978-1-4200-9982-9.

[SF96] Robert Sedgewick e Philppe Flajolet. *An Introduction to the Analysis of Algorithms*. Addison Wesley, 1996. ISBN: 0-201-40009-X.

[Wil05] Herbert S. Wilf. *Generatingfunctionology*. 3ª ed. A K Peters/CRC Press, 2005. ISBN: 978-1568812793.

Índice Remissivo