

# Matemática Discreta

Pedro Hokama

## Fontes

- Gomide, Anamaria; Stolfi, Jorge. Elementos de Matematica Discreta para Computação.
- Rosen, Kenneth H. Discrete mathematics and its applications. McGraw-Hill Education, 8th Edition, 2019.

1 / 44

2 / 44

# Cardinalidade de conjuntos

- Anteriormente definimos informalmente a cardinalidade de conjuntos finitos.
- Agora temos condições de dar uma definição mais precisa de cardinalidade, inclusive para conjuntos infinitos.

**Definição:** Sejam  $A$  e  $B$  dois conjuntos. Se existir uma função bijetora  $f : A \rightarrow B$ , então dizemos que  $A$  e  $B$  **tem a mesma cardinalidade**. Denotaremos este fato por  $A \sim B$ .

3 / 44

4 / 44

- Pode-se provar que “ $\sim$ ” é uma **relação de equivalência**. As classes de equivalência da relação “ $\sim$ ” são chamadas de **cardinalidades** ou **números cardinais**.
- A cardinalidade de um conjunto  $A$  é geralmente denotada por  $|A|$  ou  $\#A$ . Portanto temos que  $A \sim B$  se e somente se  $|A| = |B|$ .

5/44

- Portanto a cardinalidade de um conjunto finito pode ser identificada com seu número de elementos.
- Observe que, de acordo com a definição, o conjunto vazio  $\emptyset$  é finito e  $|\emptyset| = 0$ .

7/44

## Conjuntos finitos

- Para cada número natural  $n$  definimos  $I_n = \{i \in \mathbb{N} : i < n\}$ .
- Por exemplo,  $I_5 = \{0, 1, 2, 3, 4\}$ . Um conjunto  $A$  é dito **finito** se existe um número natural  $n$  tal que  $A \sim I_n$ .
- Neste caso, dizemos que  $n$  é o número de elementos de  $A$ .
- É fácil ver que dois conjuntos finitos tem a mesma cardinalidade se e somente se eles tem o mesmo número de elementos.

6/44

## Conjuntos infinitos

- Para certos conjuntos  $A$ , não existe uma bijeção de  $A$  para  $I_n$ , para nenhum  $n \in \mathbb{N}$ .
- Exemplos incluem o próprio conjunto  $\mathbb{N}$ , bem como  $\mathbb{Z}$ ,  $\mathbb{Q}$  e  $\mathbb{R}$ . Dizemos que estes conjuntos são **infinitos**.
- Poderíamos supor que, como no caso dos conjuntos finitos, os subconjuntos próprios de um conjunto infinito  $A$  tem cardinalidades estritamente menores que  $|A|$ .

8/44

- Porém, os exemplos abaixo mostram que isso não é verdade:

**Exemplo:** Seja  $\mathbb{E} \subset \mathbb{N}$  o conjunto dos números naturais **pares**,  $\{2k : k \in \mathbb{N}\}$ . Considere a função  $f : \mathbb{N} \rightarrow \mathbb{E}$  definida por  $f(n) = 2n$ . A função  $f$  é uma bijeção do conjunto dos naturais no conjunto dos números pares. Portanto  $\mathbb{N} \sim \mathbb{E}$  e portanto a cardinalidade de  $\mathbb{N}$  é a mesma que  $\mathbb{E}$ .

9/44

- Ou seja, é possível retirar elementos de um conjunto infinito sem alterar sua cardinalidade.
- Verifica-se que esta é uma propriedade geral de conjuntos infinitos.
- Inclusive, muitos autores usam esta propriedade como definição, dizendo que um conjunto  $A$  é infinito se e somente se ele tem um subconjunto próprio  $B$  tal que  $A \sim B$ .

10/44

- O exemplo anterior foi enunciado pelo matemático alemão David Hilbert (1862–1943) na forma de uma anedota: um hotel com infinitos quartos, todos ocupados, de repente recebe infinitos novos hóspedes, e precisa arrumar quartos para eles.
- Dois outros exemplos importantes serão enunciados.

**Exemplo:** Considere a função  $f : \mathbb{N} \rightarrow \mathbb{Z}$  definida por

$$f(n) = (-1)^n \left\lfloor \frac{n+1}{2} \right\rfloor = \begin{cases} k & \text{se } n \text{ é par } (n = 2k) \\ -(k+1) & \text{se } n \text{ é ímpar } (n = 2k+1) \end{cases} \quad (1)$$

A tabela abaixo ilustra a função  $f$

$n$	0	1	2	3	4	5	6	7...
$f(n)$	0	-1	1	-2	2	-3	3	-4...

Esta função é uma bijeção de  $\mathbb{N}$  para  $\mathbb{Z}$ , e portanto  $\mathbb{N} \sim \mathbb{Z}$ .

11/44

12/44

**Exemplo:** Considere a função  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  definida pela fórmula

$$f(u, v) = \frac{(u + v)(u + v + 1)}{2} + u$$

A tabela ilustra a função  $f$ . Ela associa a cada par  $(u, v)$  um número natural na sequência, segundo diagonais sucessivas.

	$v$					
	0	1	2	3	4	...
0	0	1	3	6	10	...
1	2	4	7	11	...	
$u$ 2	5	8	12	...		
3	9	13	...			
4	14	...				
$\vdots$	$\vdots$					

Verifica-se que esta função é uma bijeção de  $\mathbb{N} \times \mathbb{N}$  para  $\mathbb{N}$ , e portanto  $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ .

13/44

**Exemplo:** Considere a função  $f : [0, 1] \rightarrow [1, 3]$  definida por  $f(x) = 2x + 1$ . Verifica-se que esta função é uma bijeção do intervalo  $[0, 1]$  para o intervalo  $[1, 3]$ , e portanto concluímos que  $[0, 1] \sim [1, 3]$ . Por raciocínio análogo, podemos concluir que todos os intervalos fechados  $[a, b]$  de números reais tem a mesma cardinalidade.

15/44

- Podemos demonstrar também que
  - Teorema:** Para todo inteiro positivo  $n$ ,  $\mathbb{N}^n \sim \mathbb{N}$ .
- A demonstração pode ser feita por indução em  $n$ , usando a função  $f$

$$f(u, v) = \frac{(u + v)(u + v + 1)}{2} + u \quad (2)$$

e a bijeção  $g$  entre os conjuntos  $\mathbb{N}^n$  e  $(\mathbb{N}^{n-1}) \times \mathbb{N}$ , definida por

$$g((a_1, a_2, \dots, a_n)) = ((a_1, a_2, \dots, a_{n-1}), a_n)$$

para toda ênupla  $(a_1, a_2, \dots, a_n)$  em  $\mathbb{N}^n$ .

14/44

**Teorema:** Seja  $X$  um conjunto finito não vazio, e  $X^*$  o conjunto de todas as sequências finitas de elementos de  $X$ , isto é  $X^* = \bigcup_{k \in \mathbb{N}} X^k$ . Então  $X^* \sim \mathbb{N}$ .

**Prova:**

Seja  $m = |X|$ . Note que  $|X^n| = m^n$ . Seja  $f_n$  uma bijeção qualquer do conjunto  $X^n$  para o conjunto  $\{0, 1, \dots, m^n - 1\}$ . Considere a função  $g : X^* \rightarrow \mathbb{N}$ , definida por

$$g(x) = \left( \sum_{k=0}^{n-1} m^k \right) + f_n(x)$$

para todo  $n \in \mathbb{N}$  e toda sequência  $x \in X^n$ .

16/44

Em particular,

$$\begin{array}{llll} \text{se } x \in X^0 & \text{então } g(x) = f_0(x) & = 0; \\ \text{se } x \in X^1 & \text{então } g(x) = 1 + f_1(x) & \in \{1, \dots, 1 + (m - 1)\}; \\ \text{se } x \in X^2 & \text{então } g(x) = 1 + m + f_2(x) & \in \{1 + m, \dots, 1 + m + (m^2 - 1)\}; \\ \text{se } x \in X^3 & \text{então } g(x) = 1 + m + m^2 + f_3(x) & \in \{1 + m + m^2, \dots, 1 + m + m^2 + (m^3 - 1)\}; \end{array}$$

e assim por diante. Pode-se ver que a função  $g$  é uma bijeção de  $X^*$  para  $\mathbb{N}$ , e portanto  $X^* \sim \mathbb{N}$ .

**Exemplo:** Todo subconjunto  $A$  de  $\mathbb{N}$  é contável. Se  $A$  é finito, ele é contável. Se  $A$  não é finito, considere a função bijetora  $f : A \rightarrow \mathbb{N}$  onde  $f(a)$  é número de elementos de  $A$  que são menores que  $a$ , para todo  $a \in A$ .

**Exemplo:** Se  $B$  é um conjunto contável, todo subconjunto  $C \subseteq B$  é contável. Para provar este fato, considere uma bijeção  $f$  de  $\mathbb{N}$  para  $B$ . Seja  $A$  o subconjunto  $f^{-1}(C)$  de  $\mathbb{N}$ . Pelo exemplo acima,  $A$  é contável. A restrição de  $f$  a  $A$  é uma bijeção de  $A$  para  $C$ , e portanto  $C$  também é contável.

## Conjuntos enumeráveis e contáveis

- Um conjunto é dito **enumerável** se ele tem a mesma cardinalidade dos números naturais.
- Dizemos que um conjunto é **contável** se ele é finito ou enumerável.
- Observe que um conjunto  $A$  é enumerável se, e somente se é possível listar os elementos do conjunto como uma sequência infinita  $a_0, a_1, a_2, \dots$ ; isto é, podemos indexá-los pelos números naturais.

- Conjuntos contáveis podem ser combinados de diversas maneiras e ainda continuam contáveis.
- Pode-se provar que a união de dois conjuntos contáveis é um conjunto contável.
- Por indução, o mesmo vale para a união de qualquer número finito de conjuntos contáveis. Mais ainda:

**Teorema:** Seja  $X$  um conjunto enumerável cujos elementos são conjuntos enumeráveis, disjuntos dois a dois. A união de todos os elementos de  $X$  é enumerável.

- Usando este resultado, pode-se provar que, se  $X$  é um conjunto contável cujos elementos são conjuntos contáveis (não necessariamente disjuntos), a união de todos os elementos de  $X$  é contável.

21 / 44

## Cardinalidade dos números reais

- Em vista dos exemplos acima, poderíamos ser levados a acreditar que todos os conjuntos infinitos têm a mesma cardinalidade, ou seja, que existe apenas um tipo de “infinito”.
- Essa conjectura foi derrubada pelo matemático Georg Cantor em 1879, que mostrou que os conjuntos  $\mathbb{N}$  e  $\mathbb{R}$  tem cardinalidades diferentes. Este fato decorre do seguinte teorema:

22 / 44

**Teorema:** O intervalo aberto

$(0, 1) = \{ x \in \mathbb{R} : 0 < x < 1 \}$  não é contável.

**Prova:** O conjunto  $(0, 1)$  não é finito, portanto precisamos demonstrar apenas que ele não é enumerável. Seja  $f$  uma função qualquer de  $\mathbb{N}$  para  $(0, 1)$ . Para cada número real  $f(i)$ , considere uma representação decimal infinita  $a_i = 0, a_{i0}a_{i1}a_{i2} \dots$  do mesmo. Temos então uma lista infinita de seqüências infinitas de algarismos

$$\begin{aligned} f(0) &= a_0 = 0, a_{00}a_{01}a_{02} \dots \\ f(1) &= a_1 = 0, a_{10}a_{11}a_{12} \dots \\ f(2) &= a_2 = 0, a_{20}a_{21}a_{22} \dots \\ &\vdots \end{aligned}$$

Observe que alguns números reais tem duas representações. Por exemplo, o número  $1/4$  pode ser escrito como  $0,250000 \dots$  ou  $0,249999 \dots$ . Se  $f(i)$  é um destes números, escolhemos para  $a_i$  qualquer das duas representações, arbitrariamente.

23 / 44

24 / 44

Todos os outros números reais tem uma, e apenas uma, representação decimal. Observe também que as sequências  $0,000000\dots$  e  $0,999999\dots$  representam os números 0 e 1, respectivamente, e portanto não estão no intervalo aberto  $(0, 1)$ . Porém, exceto por esses dois casos, toda representação decimal infinita que começa com 0,  $\dots$  representa algum número real no intervalo  $(0, 1)$ .

25 / 44

Uma vez que  $b$  não termina nem em infinitos zeros nem em infinitos noves, o número  $b^*$  tem apenas essa representação, e portanto ele é diferente do número real  $f(i)$ , para todo  $i$  em  $\mathbb{N}$ .

Concluimos que nenhuma função  $f$  de  $\mathbb{N}$  para  $(0, 1)$  pode ser sobrejetora. Logo  $(0, 1)$  não é enumerável.  $\square$

27 / 44

Considere agora a representação decimal infinita  $b = 0, b_0 b_1 b_2 \dots$  onde

$$b_i = \begin{cases} 4 & \text{se } a_{ii} \neq 4 \\ 5 & \text{se } a_{ii} = 4 \end{cases}$$

A representação infinita  $b$  não aparece na lista acima, pois ela difere de cada  $a_i$  na posição  $i$  depois da vírgula. Como  $b$  usa apenas algarismos 4 e 5 depois da vírgula, o número real  $b^*$  que ela representa não é nem 0 nem 1, e portanto está no intervalo aberto  $(0, 1)$ .

26 / 44

- A técnica usada nesta demonstração para encontrar o contra exemplo  $b^*$  é conhecida como **método da diagonalização** (ou **método da diagonalização de Cantor**).
- Este método é muito usado em lógica matemática e na teoria da computação.

28 / 44

- Não é difícil encontrar uma bijeção entre o intervalo aberto  $(0, 1)$  e o conjunto dos números reais  $\mathbb{R}$ . Portanto, em vista do teorema anterior a cardinalidade de  $\mathbb{R}$  é estritamente maior que a cardinalidade de  $\mathbb{N}$ . Na verdade, pode-se demonstrar que

$$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}| \quad (3)$$

29 / 44

- Em particular, para quaisquer conjuntos  $A, B$  tais que  $A \subseteq B$ , a função identidade  $I_A$  é uma função injetora de  $A$  para  $B$ ;
- portanto concluímos que  $A \subseteq B$  implica  $A \leq B$ . Em particular,  $A \leq A$  para qualquer conjunto  $A$ ; ou seja,  $\leq$  é uma relação reflexiva.
- Prova-se também que, se  $A \leq B$  e  $B \leq C$ , então  $A \leq C$ ; isto é,  $\leq$  é transitiva.
- Finalmente, prova-se que, se  $A \leq B$  e  $B \leq A$ , então  $A \sim B$  (isto é,  $A$  e  $B$  tem a mesma cardinalidade).

31 / 44

## Comparação de cardinalidades

- Sejam  $A$  e  $C$  conjuntos. Definimos a relação  $C$  **domina**  $A$  e escrevemos  $A \leq C$  se existe um conjunto  $B$  tal que  $A \sim B$  e  $B \subseteq C$ .
- Em outras palavras,  $A \leq C$  se e somente se existe uma função injetora de  $A$  para  $C$ .

**Exemplo:** Seja  $\mathbb{C}$  o conjunto dos números primos, e  $\mathbb{M}$  o conjunto dos quadrados perfeitos,  $\{n^2 : n \in \mathbb{N}\}$ . Observe que a função  $f$  de  $\mathbb{C}$  para  $\mathbb{M}$  definida por  $f(p) = p^2$  é uma função injetora. Portanto, concluímos que  $\mathbb{C} \leq \mathbb{M}$ .

30 / 44

- Pode-se verificar também que se  $A \sim A'$ ,  $B \sim B'$ , e  $A \leq B$ , então  $A' \leq B'$ . Portanto a relação  $\leq$  entre conjuntos depende apenas de suas cardinalidades, e não dos conjuntos em si.
- Podemos então substituir  $\leq$  por uma relação entre cardinalidades. Em vista das propriedades acima, esta é uma relação de ordem total, que denotaremos por  $\leq$ . Ou seja, dizemos **a cardinalidade de  $A$  é menor ou igual à de  $C$** , e escrevemos  $|A| \leq |C|$ , se e somente se  $A \leq C$ .

32 / 44

- Se  $|A| \leq |B|$ , mas  $|A| \neq |B|$ , dizemos que a cardinalidade de  $A$  é estritamente menor que a cardinalidade de  $B$ , e denotamos esse fato por  $|A| < |B|$ .
- Para conjuntos finitos, a relação de ordem  $\leq$  entre cardinalidades coincide com a relação  $\leq$  entre números naturais.

33 / 44

- É fácil ver também que a cardinalidade de um conjunto finito é sempre maior que a cardinalidade de qualquer subconjunto próprio.
- Ou seja, para qualquer conjunto finito  $A$  e qualquer conjunto  $B$ , temos  $B \subset A \rightarrow |B| < |A|$ .

34 / 44

## Teorema de Cantor

- Cantor mostrou também o seguinte resultado importante:
  - Teorema:** Para todo conjunto  $A$ ,  $|A| < |\mathbb{P}(A)|$ .
- Dito de outra forma, todo conjunto (finito ou infinito) tem mais subconjuntos do que elementos.
- Este resultado é óbvio para conjuntos finitos, pois se  $|A| = n$  então  $|\mathbb{P}(A)| = 2^n$  e  $2^n > n$  para todo  $n \in \mathbb{N}$ .
- A contribuição de Cantor foi mostrar que o resultado vale também para conjuntos infinitos.

35 / 44

**Teorema:** Para todo conjunto  $A$ ,  $|A| < |\mathbb{P}(A)|$ .

**Prova:** Sejam  $A$  um conjunto e  $f$  uma função qualquer de  $A$  para  $\mathbb{P}(A)$ , ou seja, uma função  $f$  que a cada elemento  $a \in A$  associa um subconjunto  $f(a) \subseteq A$ . Vamos mostrar que  $f$  não pode ser uma bijeção de  $A$  para  $\mathbb{P}(A)$ .

Observe que o elemento  $a$  pode pertencer ou não ao subconjunto  $f(a)$ . Considere agora o seguinte conjunto:

$$X = \{ a \in A : a \notin f(a) \}$$

36 / 44

$$X = \{ a \in A : a \notin f(a) \}$$

Observe que  $X$  é um subconjunto de  $A$ , logo  $X \in \mathbb{P}(A)$ . Porém, para todo  $a \in A$ , temos  $f(a) \neq X$ , pois se  $a \in f(a)$  então  $a \notin X$ , e se  $a \notin f(a)$  então  $a \in X$ . Portanto  $f$  não é sobrejetora em  $\mathbb{P}(A)$ . Concluimos que, para qualquer conjunto  $A$ , não existe nenhuma bijeção de  $A$  para  $\mathbb{P}(A)$ ; ou seja, estes dois conjuntos não tem a mesma cardinalidade.

37 / 44

Por outro lado, observe que existe uma bijeção de qualquer conjunto  $A$  para o conjunto  $A' = \{ \{a\} : a \in A \}$ , que é um subconjunto de  $\mathbb{P}(A)$ . Isto mostra que  $|A| \leq |\mathbb{P}(A)|$ . Juntando estes dois resultados, concluímos que  $|A| < |\mathbb{P}(A)|$ . □  
Em particular, a cardinalidade de  $\mathbb{P}(\mathbb{N})$  é estritamente maior que a de  $\mathbb{N}$ .

38 / 44

## A hipótese do contínuo

- Depois de mostrar que  $|\mathbb{P}(\mathbb{N})| = |\mathbb{R}|$ , Cantor conjecturou em 1878 que não é possível definir um conjunto com cardinalidade entre  $|\mathbb{N}|$  e  $|\mathbb{R}|$  — isto é, estritamente maior que  $\mathbb{N}$  mas estritamente menor que  $\mathbb{R}$ .

39 / 44

- Esta conjectura ficou conhecida como a **hipótese do contínuo**, e ficou aberta até 1963, quando Paul Cohen (baseado em um teorema provado por Kurt Gödel em 1939) mostrou que, com os axiomas usuais da teoria dos conjuntos, não é possível demonstrar nem essa afirmação nem sua negação.
- Ou seja, pode-se supor que tais conjuntos existem, ou que não existem — e, nos dois casos, nunca se chegará a uma contradição.

40 / 44

## Cardinalidade e Computabilidade

- Os conceitos de cardinalidade de conjuntos infinitos permitem responder a questão: “toda função pode ser computada?”.
- Observamos que qualquer programa de computador, pode ser visto como uma sequência finita de caracteres.

**Teorema:** O conjunto de todos os programas em uma dada linguagem de programação é contável.

41 / 44

Seja  $f$  a função com domínio  $S$  definida da seguinte maneira: para cada  $a \in S$ ,  $f(a) = f_a$  é a função de  $\mathbb{N}$  para  $\mathbb{N}$  que associa cada natural  $n$  com o dígito  $a_n$  de  $a$ . Note que  $f_a$  é um elemento de  $\mathcal{F}$ .

A função  $f$  é injetora; pois, se  $f_x = f_y$ , cada dígito decimal de  $x$  é igual ao dígito decimal correspondente de  $y$ , portanto  $x = y$ . Portanto  $f$  é uma bijeção entre  $S$  e o conjunto  $\mathcal{G} = \text{Img}(f) \subset \mathcal{F}$ .

Vimos que  $S$  não é enumerável. Concluimos que  $\mathcal{F}$  tem um subconjunto que não é enumerável. Portanto  $\mathcal{F}$  não é enumerável.  $\square$

43 / 44

Por outro lado, temos também o seguinte fato:

**Teorema:** O conjunto  $\mathcal{F}$  de todas as funções de  $\mathbb{N}$  para  $\mathbb{N}$  não é enumerável.

**Prova:**

Seja  $S$  o intervalo  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ . Como visto anteriormente, todo número  $a$  nesse conjunto pode ser representado na notação decimal por uma sequência infinita  $0, a_1 a_2 \dots a_n \dots$  onde cada  $a_i$  é um algarismo (um inteiro) entre 0 e 9.

42 / 44

- Diz-se que uma função  $f : \mathbb{N} \rightarrow \mathbb{N}$  é **computável** em uma dada linguagem se existe um programa nessa linguagem que, para todo  $x \in \mathbb{N}$ , devolve  $f(x)$  quando seu dado de entrada é  $x$ .
- Seja  $C$  o conjunto de todas as funções computáveis de uma dada linguagem. Mostramos que  $|C| \leq |\mathbb{N}|$ . Por outro lado mostramos que  $|\mathcal{F}| > |\mathbb{N}|$ . Logo, concluímos que existem funções de  $\mathbb{N}$  para  $\mathbb{N}$  que não são computáveis.

44 / 44