DCC638 - Introdução à Lógica Computacional 2025.1

Estruturas Básicas: Cardinalidade e Enumerabilidade

Área de Teoria DCC/UFMG

Cardinalidade: Introdução

- A cardinalidade de um conjunto finito é o número de seus elementos.
- A cardinalidade de conjuntos finitos é comparável por qual tem mais elementos
- Isto não se aplica a conjuntos infinitos
- Aqui estudaremos as <u>cardinalidades</u> de conjuntos infinitos e como compará-las.
- Em particular, definiremos conjuntos enumeráveis, o objeto de estudo da Matemática Discreta.
- Estes conjuntos estão em contraste com os **conjuntos não-enumeráveis**, objeto de estudo na **Matemática Contínua**.

Cardinalidade: Introdução

A cardinalidade de um conjunto finito é seu número de elementos.

Por exemplo:

- **1** O conjunto finito $A = \{a, b, c\}$ tem cardinalidade |A| = 3.
- Podemos dividir os conjuntos finitos em classes de acordo com sua cardinalidade:
 - a classe de conjuntos com 0 elementos.
 - a classe de conjuntos com 1 elementos,
 - a classe de conjuntos com 2 elementos,
 - . . .
 - a classe de conjuntos com k elementos,
 - ...

Cardinalidade: Introdução

- Mas e quanto a conjuntos infinitos, como \mathbb{N} , \mathbb{Z} e \mathbb{R} ?
- Relembrando: a seguinte afirmação é verdadeira ou é falsa?
 - "O conjunto $\mathbb Z$ dos inteiros é maior que o conjunto $\mathbb N$ dos naturais."
- Há duas possibilidades, ambas não necessariamente intuitivas:
 - <u>Verdadeira</u>: então existe um infinito maior que o outro.
 - <u>Falsa</u>: então um conjunto pode ter a mesma cardinalidade que um de seus subconjuntos próprios

Nesse case $\mathbb Z$ teria a mesma cardinalidade que seu subconjunto próprio $\mathbb N.$

• Investigaremos as diferentes classes de cardinalidade de conjuntos infinitos.

Cardinalidade de conjuntos

• Dados conjuntos A e B quaisquer, dizemos que A tem a **mesma** cardinalidade de B, denotado por

$$|A| = |B|,$$

sse existe uma uma função bijetiva de A para B.

• Esta definição engloba conjuntos tanto finitos como infinitos.

• Um conjunto S é chamado **enumerável** ou **contável** se ele é finito ou se ele possui a mesma cardinalidade que o conjunto dos números naturais \mathbb{N} :

$$|S| = |\mathbb{N}|$$

Caso contrário o conjunto é chamado não-enumerável ou não-contável.

- ullet Logo um conjunto S é enumerável se há uma bijeção entre $\mathbb N$ e S
- Note que prover uma sequência (indexada pelos naturais) de todos os elementos de S:

$$a_0, a_1, a_2, \ldots, a_n, \ldots,$$

define uma bijeção entre $\mathbb N$ e S em que

$$f(0) = a_0, \quad f(1) = a_1, \quad f(2) = a_2, \quad \dots, \quad f(n) = a_n, \quad \dots$$

• Exemplo 1 O conjunto P dos números naturais pares é enumerável?

• Exemplo 1 O conjunto P dos números naturais pares é enumerável?

Solução. Considere a bijeção f entre os naturais e o conjunto P dos pares positivos, definida como

$$f(n)=2n$$
,

e que pode ser ilustrada por

Esta bijeção demonstra que P é enumerável.

Note que esta bijeção é uma maneira de **enumerar** ou **contar** os elementos de P em uma sequência:

$$0, 2, 4, 6, 8, \dots$$

ullet Exemplo 2 ig| O conjunto $\mathbb Z$ de todos os números inteiros é enumerável?

ullet Exemplo 2 O conjunto $\mathbb Z$ de todos os números inteiros é enumerável?

Solução. A seguinte bijeção demonstra que os inteiros são enumeráveis:

Logo, podemos enumerar os elementos de $\mathbb Z$ na sequência:

$$0, -1, 1, -2, 2, -3, 3, -4, 4, \dots$$

Observação: Note que uma forma explícita para a bijeção $f: \mathbb{Z} \to \mathbb{N}$ dada acima é:

$$f(n) = \begin{cases} 2n, & \text{se } n \ge 0 \\ (-2n) - 1, & \text{se } n < 0 \end{cases}$$

Já um algoritmo para construir a sequência equivalente é:

"Inclua 0 na sequência e então, para cada inteiro positivo n, inclua n na sequência, depois inclua — n."

• Exemplo 3 O conjunto \mathbb{Q}^+ dos racionais positivos é enumerável?

Exemplo 3 O conjunto \mathbb{Q}^+ dos racionais positivos é enumerável?

Solução. Vamos representar o conjunto \mathbb{Q}^+ como uma tabela em que cada linha representa um possível numerador (um natural) e cada coluna representa um possível denominador (um natural positivo). A tabela abaixo mostra uma bijeção entre \mathbb{Q}^+ (frações) e \mathbb{N} (números circulados). (As frações não-simplificadas são redundantes e não entram na bijeção.)

Num./Den.	1	2	3	4	5	
1	1/1 0	1/2 ①	1/3 (4)	1/4 (5)	1/5 10	
2	2/1 (2)	$^{2/_{2}}$	2/3 6	2/4 ×	2/5 ?	
3	3/1 ③	3/2 (7)	3/3 ×	3/4 ?	3/5 ?	
4	4/1 (8)	4/2 ×	4/3 ?	4/4	4/5 ?	

Logo \mathbb{Q}^+ é enumerável:

1, 1/2, 2, 3, 1/3, 1/4, 2/3, 3/2, 4, 5, 1/5, 1/6, 2/5, 3/4, 4/3, 5/2, ...

Exemplo 4 O conjunto $\mathbb Q$ de todos os racionais é enumerável?

ullet Exemplo 4 O conjunto $\mathbb Q$ de todos os racionais é enumerável?

Solução.

(As frações não-simplificadas são redundantes e não entram na bijeção.)

N/D	1	2	3	4	5	
0	0/1 (0)	$0/2_{\times}$	0/3 ×	0/4 ×	0/5 ×	
1	1/1 (1)	1/2 (2)	1/3 (4)	1/4 (7)	$1/_{5?}$	
-1	-1/1 (3)	-1/2 (5)	-1/3 8	-1/4 ?	$-1/_{5?}$	
2	$\frac{2}{1}$ 6	$^{2}/_{2}$ ×	$^{2}/_{3}$?	2/4 ×	$\frac{2}{5}$?	
-2	$\frac{-2}{1}$	$-2/2_{\times}$	-2/3 ?	$-2/4_{\times}$	-2/5 ?	

Logo Q é enumerável.

• Exemplo 4 (Continuação)

<u>Método 2</u>: Considere a seguinte enumeração dos racionais no intervalo [0,1] (em que as frações aparecem em ordem crescente de denominador, depois de numerador, tomando o cuidado de eliminar frações repetidas):

$$0,\,\frac{1}{1},\,\frac{1}{2},\,\frac{2}{2},\,\frac{1}{3},\,\frac{2}{3},\,\frac{3}{3},\,\frac{1}{4},\,\frac{2}{4},\,\frac{3}{4},\,\frac{4}{4},\,\dots$$

Para incluir os racionais maiores que 1, podemos estender a lista acima, listando cada fração inversa após a fração original:

$$0, \frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{1}, \frac{2}{3}, \frac{3}{2}, \frac{1}{4}, \frac{4}{1}, \frac{3}{4}, \frac{4}{3}, \dots$$

Por fim, para obter uma enumeração completa dos racionais \mathbb{Q} , podemos estender a lista acima ao enumerar após cada fração, sua oposta:

$$0,\,\frac{1}{1},\,-\frac{1}{1},\,\frac{1}{2},\,-\frac{1}{2},\,\frac{2}{1},\,-\frac{2}{1},\,\frac{1}{3},\,-\frac{1}{3},\,\frac{3}{1},\,-\frac{3}{1},\,\frac{2}{3},\,-\frac{2}{3},\,\frac{3}{2},\,-\frac{3}{2},\,\frac{1}{4},\,-\frac{1}{4}\,\frac{4}{1},\,-\frac{4}{1},\,\ldots$$

Como obtivemos uma enumeração de \mathbb{Q} , este conjunto é enumerável.

• Teorema 1: A união de dois conjuntos enumeráveis é enumerável.

• Teorema 1: A união de dois conjuntos enumeráveis é enumerável.

Demonstração. Sejam A e B dois conjuntos enumeráveis.

Então existem:

- uma enumeração $a_0, a_1, a_2, a_3, \ldots$ para A, e
- uma enumeração $b_0, b_1, b_2, b_3, \ldots$ para B.

Podemos construir uma enumeração para $A \cup B$ tomando

$$a_0, b_0, a_1, b_1, a_2, b_2, a_3, b_3 \ldots,$$

com o cuidado de não listar elementos repetidos, i.e., em $A \cap B$.

 Teorema 2: Qualquer subconjunto de um conjunto enumerável é enumerável.

• **Teorema 2:** Qualquer subconjunto de um conjunto enumerável é enumerável.

Demonstração. Dado um conjunto enumerável B, tome $A \subseteq B$. Por hipótese, existe uma enumeração b_0, b_1, b_2, \ldots para B. Eliminando os termos $b_i \notin A$ desta enumeração, obtém-se uma enumeração para A.

• **Corolário:** Se um conjunto B tem um subconjunto $A \subseteq B$ tal que A é não-enumerável, então B é não-enumerável.

Demonstração. Este resultado é apenas a contrapositiva do teorema que diz que qualquer subconjunto de um conjunto enumerável é enumerável.

 Teorema: O conjunto de todos os números reais no intervalo [0,1) não é enumerável.

• **Teorema:** O conjunto de todos os números reais no intervalo [0,1) não é enumerável.

Demonstração. Por contradição, suponha que [0,1) seja enumerável. Então, por definição de enumerabilidade, existe uma lista $r_0, r_1, r_2, \ldots, r_i, \ldots$ em que constam todos os elementos de [0,1).

Esta lista pode ser representada por uma matriz, em que cada linha representa um número real em [0,1), ordenada de acordo com a enumeração acima, e cada coluna representa os dígitos decimais deste número.

Mais precisamente, já que cada r_i nesta lista pertence ao intervalo [0,1), podemos escrever

$$r_i=0\,,\,r_{i0}\,r_{i1}\,r_{i2}\,\ldots\,r_{ij}\,\ldots,$$

onde r_{ij} é o j-ésimo dígito decimal do número r_i .

• Demonstração (Continuação).

Esta tabela tem o formato abaixo:

Enumeração	0° dec.	1° dec.	2° dec.		j-ésimo dec.	
<i>r</i> ₀	<i>r</i> ₀₀	<i>r</i> ₀₁	<i>r</i> ₀₂		r_{0j}	
r_1	<i>r</i> ₁₀	r_{11}	<i>r</i> ₁₂		r_{1j}	
r_2	<i>r</i> ₂₀	<i>r</i> ₂₁	<i>r</i> ₂₂		r_{2j}	
:	:	:	:	٠.	•	:
r_i	r _{i0}	r_{i1}	r_{i2}		r _{ij}	
:	:	:	:	:	•	٠

Demonstração (Continuação).

Esta tabela tem o formato abaixo:

Enumeração	0° dec.	1° dec.	2° dec.		j-ésimo dec.	
<i>r</i> ₀	<i>r</i> ₀₀	<i>r</i> ₀₁	<i>r</i> ₀₂		r_{0j}	
r_1	<i>r</i> ₁₀	<i>r</i> ₁₁	<i>r</i> ₁₂		r_{1j}	
<i>r</i> ₂	<i>r</i> ₂₀	<i>r</i> ₂₁	<i>r</i> ₂₂		r_{2j}	
•	:	:	:	٠.	: :	:
r_i	r _{i0}	r_{i1}	r_{i2}		r _{ij}	
:	:	:	:	:	:	٠.

Se encontrarmos um número $r_{\alpha} \in [0,1)$ que não esteja listado nesta tabela, chegamos a uma contradição com a hipótese de que a lista está completa.

Vamos construir r_{α} , dígito decimal a dígito decimal, definindo cada dígito $r_{\alpha j}$ na posição j como:

$$r_{\alpha j} = (r_{jj} + 1) \operatorname{mod} 10 ,$$

em que $x \mod y$ é o resto da divisão do inteiro x pelo inteiro y.

Demonstração (Continuação).

Enumeração	0° dec.	1° dec.	2° dec.	 i-ésimo dec.	
<i>r</i> ₀	r 00	<i>r</i> ₀₁	r ₀₂	 <i>r</i> 0 <i>i</i>	
<i>r</i> ₁	r ₁₀	(r ₁₁)	<i>r</i> ₁₂	 r_{1i}	
<i>r</i> ₂	r ₂₁	r ₃₁	(r ₂₂)	 <i>r</i> _{2<i>i</i>}	
:	:	:	:	 :	
r_i	r_{i0}	r_{i1}	r_{i2}	 (r_{ii})	
:	:	:	:	 :	
r_{α}		$\binom{r_{11}+1}{\operatorname{mod} 10}$	$\frac{(\mathit{r}_{22}+1)}{\bmod 10}$	 $(r_{ii}+1) \ oxdots 10$	•••

Mas note que o número r_{α} não pode estar na lista, pois ele é diferente de todos os demais números da lista: para qualquer r_i na lista, o i-ésimo dígito de r_{α} é diferente do i-ésimo dígito de r_i , logo temos que $r_{\alpha} \neq r_i$.

Logo, a lista não pode estar completa, pois r_{α} não se encontra nela, e chegamos a uma contradição.

• Corolário: O conjunto $\mathbb R$ não é enumerável.

Demonstração. Como $[0,1)\subseteq\mathbb{R}$ e [0,1) não é enumerável, segue, pelo Teorema 2, que \mathbb{R} não é enumerável.

 O método usado no resultado anterior para demonstrar a não-enumerabilidade de um conjunto é conhecido como método de diagonalização de Cantor, devido ao matemático Georg Cantor, que o inventou.

Apêndice - O Teorema de Schröder-Bernstein

Ordenando cardinalidades

• O conceito de cardinalidade pode ser usado para comparar conjuntos de tamanhos diferentes.

- Formalmente, sejam A e B dois conjuntos quaisquer.
 - A tem cardinalidade menor ou igual à cardinalidade de B, denotado por

$$|A| \leq |B|$$
,

see existe uma função injetiva de A para B.

• A tem cardinalidade menor que a de B, denotado por

sse $|A| \leq |B|$ mas $|A| \neq |B|$.

O Teorema de Schröder-Bernstein

 Algumas vezes é difícil encontrar uma bijeção entre dois conjuntos que queremos demonstrar ter a mesma cardinalidade.

Nestes casos o seguinte resultado pode ser útil.

• Teorema de Schröder-Bernstein: Se A e B são conjuntos tais que

$$|A| \le |B|$$
 e $|B| \le |A|$,

então

$$|A| = |B|$$
.

Em outras palavras, se existe uma função injetiva f de A para B e existe uma função injetiva g de B para A, então existe uma função bijetiva de A para B.

O Teorema de Schröder-Bernstein

• Exemplo 5 Mostre que |(0,1)| = |(0,1]|.

Solução. Note que não é de imediatamente evidente como encontrar uma bijeção entre (0,1) e (0,1].

Entretanto, podemos usar o teorema de Schröder-Bernstein, e encontrar uma função injetiva f de (0,1) para (0,1], e outra função injetiva g de (0,1] e (0,1), concluindo assim que ambos os conjuntos têm a mesma cardinalidade.

• Primeiro, encontrar uma função um-para-um de (0,1) para (0,1] é simples. Uma vez que $(0,1)\subseteq (0,1]$, podemos definir

$$f(x) = x$$
.

 Em seguida, encontrar uma função um-para-um de (0,1] para (0,1) também não é difícil. A função

$$g(x)=\frac{x}{2}$$

é claramente injetiva e mapeia (0,1] para $(0,1/2] \subset (0,1]$.

Apêndice -O Teorema de Cantor

O Teorema de Cantor

- Cantor produziu várias contribuições importantes para a matemática.
- Seu método de diagonalização é utilizado em vários resultados fundamentais em ciência da computação.
- Uma das contribuições mais relevantes de Cantor foi mostrar que existem infinitos de tamanhos diferentes.
- Mas Cantor foi além: ele generalizou o método da diagonalização para mostrar que existem conjuntos de cardinalidade ainda maior que a dos reais.

Existe um número infinito de infinitos diferentes, cada um maior que o outro!

O Teorema de Cantor

• <u>Teorema</u> (Teorema de Cantor) Dado qualquer conjunto A, seu conjunto potência $\mathcal{P}(A)$ tem cardinalidade maior:

$$|A| < |\mathcal{P}(A)|.$$

Demonstração.

Primeiro vamos mostrar que a cardinalidade de A não pode ser maior que a de seu conjunto potência $\mathcal{P}(A)$.

Para isto, basta notar que existe uma função injetiva $f:A\to \mathcal{P}(A)$ definida como $f(a)=\{a\}$ para todo $a\in A$. Logo, $\mathcal{P}(A)$ tem pelo menos tantos elementos quando A.

O segundo passo da demonstração é mostrar que a cardinalidade de A não pode igual à de seu conjunto potência $\mathcal{P}(A)$.

Para isto, vamos mostrar que nenhuma função f de um conjunto A para seu conjunto potência $\mathcal{P}(A)$ pode ser bijetiva.

O Teorema de Cantor

• Demonstração. (Continuação)

Por contradição, assuma que exista uma bijeção f entre A e $\mathcal{P}(A)$.

Considere o conjunto

$$B = \{a \in A \mid a \notin f(a)\}.$$

Como $B \in \mathcal{P}(A)$, então deve existir um $x \in A$ tal que f(x) = B, uma vez que f é bijetiva.

Há duas possibilidades a se considerarem:

- Se $x \in B$, então $x \notin f(x)$, ou seja, $x \notin B$, o que é uma contradição.
- Se $x \notin B$, então $x \in f(x)$, ou seja, $x \in B$, o que é uma contradição.

Logo, f não é uma função sobrejetiva, e chegamos a uma contradição.

Para concluir, note que como mostramos que $|A| \leq |\mathcal{P}(A)|$ e que $|A| \neq |\mathcal{P}(A)|$, podemos concluir que $|A| < |\mathcal{P}(A)|$.

Apêndice -O Hotel de Hilbert

• Exemplo 6 Imagine um hotel com infinitos quartos acomodando infinitos hóspedes, de modo que cada quarto esteja ocupado por um único hóspede.

Suponha que um novo hóspede chegue ao hotel procurando por um quarto.

É possível acomodar este novo hóspede em algum quarto, sem expulsar nenhum hóspede que já estava no hotel?

• Exemplo 6 Imagine um hotel com infinitos quartos acomodando infinitos hóspedes, de modo que cada quarto esteja ocupado por um único hóspede.

Suponha que um novo hóspede chegue ao hotel procurando por um quarto.

É possível acomodar este novo hóspede em algum quarto, sem expulsar nenhum hóspede que já estava no hotel?

Solução.

- Se o hotel tivesse um número finito de quartos, a resposta seria negativa...
 Mas o Hotel de Hilbert tem infinitos quartos... E o infinito é bizarro!
- Podemos acomodar o novo hóspede se fizermos cada hóspede em um quarto n mudar-se para o quarto n+1:
 - o hóspede do quarto 1 muda-se para o quarto 2,
 - o hóspede do quarto 2 muda-se para o quarto 3,
 - o hóspede do quarto 3 muda-se para o quarto 4,
 - etc...

Assim podemos acomodar o novo hóspede no quarto 1!

• Exemplo 7 Imagine ainda o mesmo hotel com infinitos quartos acomodando infinitos hóspedes, estando um hóspede em cada quarto.

Suponha que é alta-estação, e um ônibus trazendo um número infinito de hóspedes chega ao hotel, todos procurando por um quarto.

É possível acomodar todos os infinitos hóspedes, um em cada quarto, sem expulsar nenhum hóspede que já estava no hotel?

• Exemplo 7 Imagine ainda o mesmo hotel com infinitos quartos acomodando infinitos hóspedes, estando um hóspede em cada quarto.

Suponha que é alta-estação, e um ônibus trazendo um número infinito de hóspedes chega ao hotel, todos procurando por um quarto.

É possível acomodar todos os infinitos hóspedes, um em cada quarto, sem expulsar nenhum hóspede que já estava no hotel?

Solução.

- Sim! Podemos acomodar os infinitos hóspedes assim se fizermos cada hóspede em um quarto n mudar-se para o quarto 2n:
 - o hóspede do quarto 1 muda-se para o quarto 2,
 - o hóspede do quarto 2 muda-se para o quarto 4,
 - o hóspede do quarto 3 muda-se para o quarto 6,
 - etc...

• Exemplo 7 Imagine ainda o mesmo hotel com infinitos quartos acomodando infinitos hóspedes, estando um hóspede em cada quarto.

Suponha que é alta-estação, e um ônibus trazendo um número infinito de hóspedes chega ao hotel, todos procurando por um quarto.

É possível acomodar todos os infinitos hóspedes, um em cada quarto, sem expulsar nenhum hóspede que já estava no hotel?

Solução.

- Sim! Podemos acomodar os infinitos hóspedes assim se fizermos cada hóspede em um quarto n mudar-se para o quarto 2n:
 - o hóspede do quarto 1 muda-se para o quarto 2,
 - o hóspede do quarto 2 muda-se para o quarto 4,
 - o hóspede do quarto 3 muda-se para o quarto 6,
 - etc...

Assim todos os quartos ímpares ficam vagos, e podemos acomodar os infinitos novos hóspedes nos quartos ímpares!

• Exemplo 8 Imagine ainda o mesmo hotel com infinitos quartos acomodando infinitos hóspedes, estando um hóspede em cada quarto.

Agora imagine que cheguem ao hotel um número infinito de ônibus, cada ônibus com um número infinito de hóspedes procurando por um quarto.

É possível acomodar todos os novos hóspedes no hotel, sem expulsar nenhum hóspede que já estava no hotel?

Solução.

Desafio para o(a) estudante!

(Dica: é possível!)

Uma Consequência de Não-Enumerabilidade: Funções Não-Computáveis

Uma consequência de não-enumerabilidade: Funções não-computáveis

Uma função é computável se existe um algoritmo que computa seus valores.
 Caso contrário ela é não-computável.

 Usando o que vimos nesta aula, vamos mostrar um resultado que revolucionou a Matemática no século XX (e tornou Turing famoso):
 Existem funções não-computáveis!

Uma consequência de não-enumerabilidade: Funções não-computáveis

• **Proposição 1.** O conjunto de todos os algoritmos que podem ser escritos em uma dada linguagem é enumerável.

Demonstração.

De acordo com o que vimos nesta aula, as seguintes afirmações são válidas:

- a) O conjunto de todas as strings que podem ser geradas é enumerável: podemos listar todas strings em ordem alfabética, da menor para a maior, produzindo assim uma enumeração.
- b) O conjunto de todos os algoritmos que podem ser escritos em uma dada linguagem (C, Java, Python, etc...) é um subconjunto do conjunto de todas as strings que podem geradas.
- c) Qualquer subconjunto de um conjunto enumerável é também enumerável.

Juntando as observações (a), (b) e (c) acima, obtemos o resultado proposto.

Uma consequência de não-enumerabilidade: Funções não-computáveis

• **Proposição 2.** O conjunto de todas as funções tendo como domínio os naturais e co-domínio o conjunto $\{0,1,2,3,4,5,6,7,8,9\}$ não é enumerável.

Demonstração. Considere nossa demonstração de que o conjunto dos reais no intervalo [0,1) não é enumerável. Cada linha r_i da tabela pode ser vista como uma função dos naturais para $\{0,1,2,3,4,5,6,7,8,9\}$. Mais precisamente, cada r_i pode ser visto como a função que mapeia o natural j ao dígito r_{ij} . Mas como nós mostramos que o conjunto de r_i 's é não-enumerável, então o número de funções é também não-enumerável.

 Das Proposições 1 e 2 acima, podemos concluir que existem mais funções do que algoritmos, o que implica que existem funções que não são computáveis.

Em outras palavras:

Existem problemas computacionais para os quais não há algoritmos!