O problema da Parada

Suponha que A_{MT} seja Turing-decidível.

Seja H um decisor para A_{MT}.

Assim, $$H(\langle M, w\rangle) = \begin{cases} \text{aceite} & \text{se } M \text{ aceita } w \\ \text{rejeite} & \text{se } M \text{ não aceita } w \end{cases}$$

Construa uma nova máquina D da seguinte forma:

D = "Sobre a entrada $\langle M \rangle$:
(1) Execute H sobre $\langle M, \langle M \rangle\rangle$.
(2) Se H aceita, rejeite. Caso contrário, aceite."

$$D(\langle M \rangle) = \begin{cases} \text{aceite} & \text{se } M \text{ não aceita } \langle M \rangle \\ \text{rejeite} & \text{se } M \text{ aceita } \langle M \rangle \end{cases}$$

Na tabela a seguir, a entrada i, j é aceita se M_i aceita $\langle M_j \rangle$:

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	...
M_1	aceita		aceita		
M_2	aceita	aceita	aceita	aceita	
M_3					...
M_4	aceita	aceita			
⋮			⋮		

Na tabela a seguir, a entrada i, j é o resultado de H sobre a entrada $\langle M_i, \langle M_j \rangle \rangle$:

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	...	$\langle D \rangle$
M_1	aceita	rejeita	aceita	rejeita		
M_2	aceita	aceita	aceita	aceita		
M_3	rejeita	rejeita	rejeita	rejeita	...	
M_4	aceita	aceita	rejeita	rejeita		
⋮			⋮			
D	rejeita	rejeita	aceita	aceita	..	?

$$H(\langle M, w \rangle) = \begin{cases} \text{aceite} & \text{se } M \text{ aceita } w \\ \text{rejeite} & \text{se } M \text{ não aceita } w \end{cases}$$

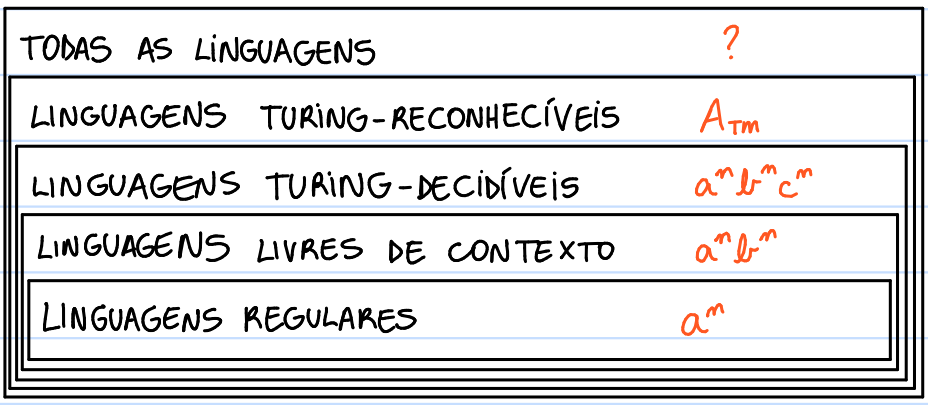
$$D(\langle M \rangle) = \begin{cases} \text{aceite} & \text{se } M \text{ não aceita } \langle M \rangle \\ \text{rejeite} & \text{se } M \text{ aceita } \langle M \rangle \end{cases}$$

D aparece na tabela, pois é uma máquina de Turing.
O que acontece quando rodamos D com a sua própria descrição?

$$D(\langle M \rangle) = \begin{cases} \text{aceite} & \text{se } M \text{ não aceita } \langle M \rangle \\ \text{rejeite} & \text{se } M \text{ aceita } \langle M \rangle \end{cases}$$

Independente do que D faz, ela é forçada a fazer o oposto, o que é uma contradição!
Então nem D e nem H podem existir.

TEOREMA: A_{MT} é indecidível.

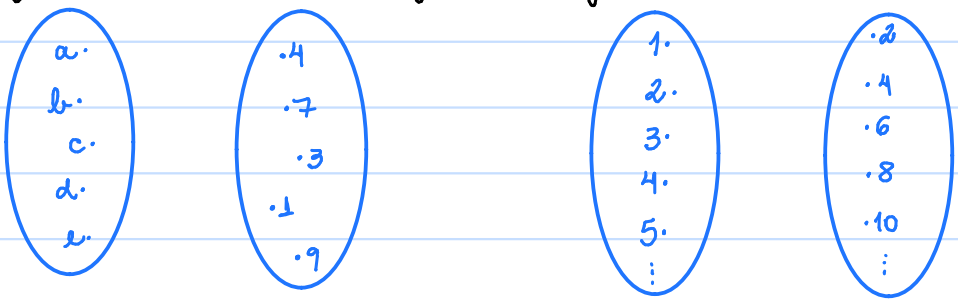


Outro problema indecidível: verificar corretude de software. Dada a especificação de um programa e a especificação do que ele deveria fazer, não é possível decidir se ele o faz.

22) O MÉTODO DA DIAGONALIZAÇÃO

Teoria dos conjuntos

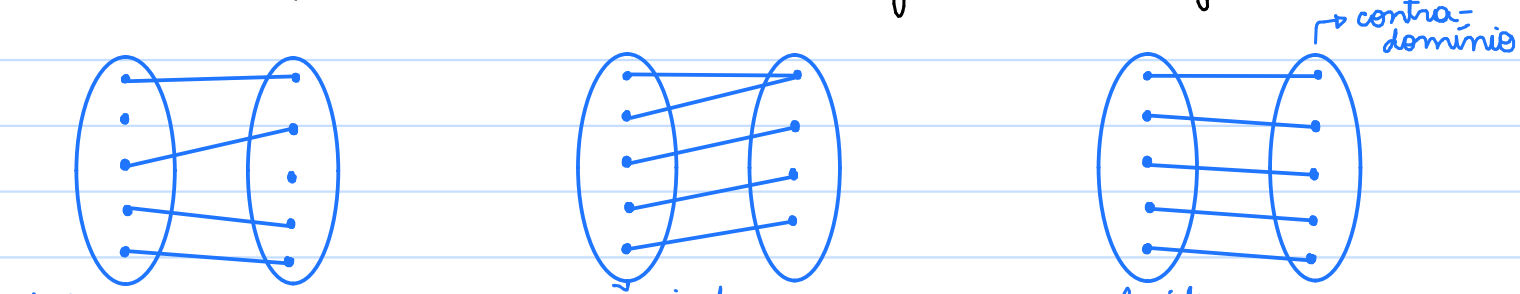
→ 1873, Georg Cantor: dois conjuntos infinitos têm o mesmo tamanho?



Funções

DEFINIÇÃO: Se A e B são conjuntos e $f: A \to B$, dizemos que f é

- INJETORA (UM-PARA-UM) se $f(x) \neq f(y)$ sempre que $x \neq y$.
- SOBREJETORA se $\forall z \in B \ \exists x \in A$ tal que $z = f(x)$.
- BIJETORA (CORRESPONDÊNCIA) se é injetora e sobrejetora



injetora
não sobrejetora

não injetora
sobrejetora

bijetora

Conjuntos

DEFINIÇÃO: Dois conjuntos A e B têm o mesmo tamanho se existe uma bijeção / correspondência $f: A \to B$.

DEFINIÇÃO: Um conjunto A é contável se:

- é finito, ou
- tem o mesmo tamanho que $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Números pares

TEOREMA: O conjunto $P = \{0, 2, 4, 6, 8, \dots\}$ dos números naturais pares é contável.

DEMONSTRAÇÃO: Vamos mostrar que $f(n) = 2n$ é uma bijeção entre $\mathbb{N}$ e P.
Para $n, m \in \mathbb{N}$, com $n \neq m$, claramente $2n \neq 2m$, o que implica $f(n) \neq f(m)$. Logo, f é injetora.

Seja $a \in P$. Então existe $k \in \mathbb{N}$ tal que $a = 2k$. Mas então $f(k) = a$. Logo, f é sobrejetora.

CQD

Números inteiros

TEOREMA: O conjunto $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ dos números inteiros é contável.

DEMONSTRAÇÃO: Vamos mostrar que $f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{n+1}{2} & \text{se } n \text{ é ímpar} \end{cases}$ é uma bijeção de $\mathbb{N}$ para $\mathbb{Z}$.
Sejam $n, m \in \mathbb{N}$, com $n \neq m$. Se ambos têm a mesma paridade, então claramente $f(n) \neq f(m)$, pois $\frac{n}{2} \neq \frac{m}{2}$ e $-\frac{n+1}{2} \neq -\frac{m+1}{2}$. Caso contrário, suponha s.p.g que n é par e m é ímpar. Também claramente $f(n) \neq f(m)$, pois $\frac{n}{2} \neq -\frac{m+1}{2}$ (sinal diferente). Logo, f é injetora.
Seja $z \in \mathbb{Z}$. Se $z \geq 0$, então $2z$ é um número natural par e $f(2z) = z$. Se $z < 0$, então $-(2z+1)$ é um número natural ímpar e $f(-(2z+1)) = z$. Logo, f é sobrejetora. CQD

Cadeias sobre um alfabeto

TEOREMA: O conjunto Σ^* é contável, para qualquer Σ.

DEMONSTRAÇÃO: Seja $C_i \subseteq \Sigma^*$ o conjunto com todas as cadeias de comprimento i. Note que $|C_i| = |\Sigma|^i$.

Faça uma lista que contém os elementos de C_0 seguidos pelos elementos de C_1, seguidos por C_2, e assim por diante.

Faça $f(n) =$ "a $(n+1)$-ésima cadeia dessa lista" $\forall n \in \mathbb{N}$.

Note que f é bijetora: duas posições diferentes possuem cadeias diferentes e toda cadeia será listada. CQD

0	ε
1	0, 1
2	00, 01, 10, 11
3	000, 001, 010, 011, 100, 101, 110, 111
4	0000, 0001, 0010, ..., 1111
⋮	⋮

Números racionais

TEOREMA: O conjunto $\mathbb{Q}_+ = \left\{ \frac{m}{n} : m \in \mathbb{N} \text{ e } n \in \mathbb{N}^* \right\}$ dos números racionais não negativos é contável.

n \ m	1	2	3	4	5	6	7	...
0	0/1	0/2	0/3	0/4	0/5	0/6	0/7	
1	1/1	1/2	1/3	1/4	1/5	1/6	1/7	...
2	2/1	2/2	2/3	2/4	2/5	2/6	2/7	
3	3/1	3/2	3/3	3/4	3/5	3/6	3/7	...
4	4/1	4/2	4/3	4/4	4/5	4/6	4/7	
5	5/1	5/2	5/3	5/4	5/5	5/6	5/7	...
6	6/1	6/2	6/3	6/4	6/5	6/6	6/7	
⋮		⋮		⋮		⋮		⋱

Números racionais

TEOREMA: O conjunto $\mathbb{Q}_+ = \{ \frac{m}{n} : m \in \mathbb{N} \text{ e } n \in \mathbb{N}^* \}$ dos números racionais não negativos é contável.

DEMONSTRAÇÃO: Seja $P_i = \{ \frac{0}{i+1}, \frac{1}{i}, \frac{2}{i-1}, \frac{3}{i-2}, \dots, \frac{i}{1} \}$, para $i = 0, 1, 2, \dots$.

Note que $\mathbb{Q}_+ = P_0 \cup P_1 \cup P_2 \cup \dots$, pois qualquer $\frac{m}{n} \in \mathbb{Q}_+$ pertence ao conjunto P_j com $j = m + n - 1$.

Faça uma lista que contém os elementos de P_0 seguidos pelos elementos de $P_1 \setminus P_0$, seguidos pelos elementos de $P_2 \setminus (P_1 \cup P_0)$, e assim sucessivamente. Faça $f(n) =$ "o $(n+1)$-ésimo número dessa lista."

Note que f é bijetora: duas posições diferentes contêm dois racionais diferentes e todo elemento de $\mathbb{Q}_+$ está na lista.

CQD

Máquinas de Turing

TEOREMA: O conjunto $T = \{ M : M \text{ é uma máquina de Turing} \}$ é contável.

DEMONSTRAÇÃO: Toda $M \in T$ possui uma codificação em cadeia $\langle M \rangle$ sobre algum alfabeto Σ.

Como Σ^* é contável e $\{ \langle M \rangle : M \in T \} \subseteq \Sigma^*$, então T é contável.

CQD

Existem infinitos infinitos

→ Alguns conjuntos infinitos são maiores do que $\mathbb{N}$.

→ São chamados incontáveis.

- Para eles, não haverá bijeção possível.

Números reais

TEOREMA: O conjunto $\mathbb{R}$ dos números reais é incontável.

DEMONSTRAÇÃO: Suponha que $\mathbb{R}$ é contável. Então existe uma bijeção $f: \mathbb{N} \to \mathbb{R}$.

$$
\begin{aligned}
f(0) &= 2,7182818\ldots \\
f(1) &= 1,1415926\ldots \\
f(2) &= 0,4142135\ldots \\
f(3) &= 2,6180339\ldots \\
f(4) &= 0,5000000\ldots \\
&\vdots
\end{aligned}
$$

Seja x um número real entre 0 e 1 tal que $x \neq f(0)$ pois a 1ª casa decimal de x é diferente da 1ª casa decimal de $f(0)$.
Também $x \neq f(1)$, pois a 2ª casa decimal deles difere.
De forma geral, $x \neq f(i)$, pois a $(i+1)$-ésima casa decimal de x difere da de $f(i)$, $\forall\, i \geq 0$.
Mas então não existe $n \in \mathbb{N}$ tal que $x = f(n)$, o que é uma contradição com f ser bijetora.
Logo, f não existe. CQD

Outros exemplos

TEOREMA: O conjunto $\mathcal{B} = \{ s : s \text{ é seq. binária infinita} \}$ é incontável.

TEOREMA: O conjunto $\mathcal{P}(A)$ é incontável para qualquer conjunto A infinito.

Subconjuntos

TEOREMA: Se $A \subseteq B$ e B é contável, então A é contável.

TEOREMA: Se $A \subseteq B$ e A é incontável, então B é incontável.
(contrapositiva)

23) LINGUAGENS INDECIDÍVEIS E IRRECONHECÍVEIS

Outra forma de provar decidibilidade

TEOREMA: Uma linguagem é decidível se e somente se ela e seu complemento são Turing-reconhecíveis.

DEMONSTRAÇÃO: ($\Rightarrow$) Seja L linguagem decidível.
Toda linguagem decidível é Turing-reconhecível.
Linguagens decidíveis são fechadas sob complemento.
Então L e $\overline{L}$ são Turing-reconhecíveis.

($\Leftarrow$) Sejam L e $\overline{L}$ Turing-reconhecíveis.
Sejam M_L e $M_{\overline{L}}$ reconhecedores de L e $\overline{L}$, respectivamente.
Construa M tal que:

M = "Sobre uma entrada w:
(1) Execute M_L e $M_{\overline{L}}$ sobre w em paralelo.
(2) Se M_L aceita, aceite. Se $M_{\overline{L}}$ aceita, rejeite."

Note que para toda cadeia w, $w \in L$ ou $w \in \overline{L}$. Logo, M_L ou $M_{\overline{L}}$ aceita w. Como M para sempre que M_L ou $M_{\overline{L}}$ aceita, sabemos que M sempre para. Logo, M é decisora. Como M aceita quando $w \in L$ e rejeita quando $w \in \overline{L}$ ($w \notin L$), então M decide L.

CQD

Propriedades de fechamento

→ Linguagens Turing-decidíveis são fechadas sob
- união
- concatenação
- estrela
- complemento
- interseção

Existem problemas que não são decidíveis

PROB: Dados uma MT e uma cadeia, ela a aceita?
EQUIV: $A_{MT} = \{\langle M, w\rangle : M \text{ é MT que aceita } w\}$

PROB: Dado um polinômio sobre múltiplas variáveis, ele possui raiz inteira?
EQUIV: $R_{INT} = \{\langle p\rangle : p \text{ é um polinômio com uma raiz inteira}\}$

> Não é possível criar um algoritmo que resolva esses problemas!! Eles são *insolúveis*.

A_{TM} é Turing-reconhecível

U = "Sobre a entrada $\langle M, w\rangle$, onde M é MT e w é cadeia:
(1) Simule M sobre w.
(2) Se M aceita, aceite. Se M rejeita, rejeite."

R_{INT} é Turing-reconhecível

P = "Sobre a entrada $\langle p\rangle$, onde p é um polinômio:
(1) Para cada valor da seqüência 0, 1, -1, 2, -2, 3, -3...
Calcule p com esse valor em x
Se deu 0, aceite.
(2) Rejeite."

→ Todo problema que não é decidível pode ser reconhecido?

→ Existem problemas *irreconhecíveis*?

Existem problemas irreconhecíveis?

TEOREMA: Algumas linguagens são Turing-irreconhecíveis.

DEMONSTRAÇÃO: Seja $\mathcal{L}$ o conjunto de todas as linguagens sobre Σ.
Seja $\Sigma^* = \{w_1, w_2, w_3, \dots\}$.
Para qualquer $A \in \mathcal{L}$, definimos a sequência característica de A como sendo a sequência binária χ_A em que o i-ésimo bit é 1 se $s_i \in A$ e 0 se $s_i \notin A$.

$\Sigma = \{a, b\}$
$\Sigma^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, aba, \dots\}$
$A = \{\quad b, \quad ab, \quad bb, \quad aab, \quad \dots\}$
$\chi_A = 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0$

Note que $\chi_A \in \mathcal{B}$, onde $\mathcal{B}$ é o conjunto das sequências binárias infinitas, o qual é incontável.
Note ainda que $f(A) = \chi_A$ é uma bijeção de $\mathcal{L}$ em $\mathcal{B}$: duas linguagens diferentes têm sequências características diferentes e toda sequência binária infinita descreve uma linguagem.
Logo, $\mathcal{L}$ é incontável.
Porém, o conjunto das máquinas de Turing é contável.
Portanto, existem linguagens para as quais não há máquinas de Turing que as reconheça.

CQD

Uma linguagem Turing-irreconhecível

TEOREMA: $\overline{A_{TM}}$ é Turing-irreconhecível.

DEMONSTRAÇÃO: Como A_{TM} é Turing-reconhecível, se $\overline{A_{TM}}$ também fosse, deveríamos ter A_{TM} decidível, o que não é o caso.

CQD

$$A_{TM} = \{\langle M, w\rangle : M \text{ é MT que aceita } w\}$$

Existem problemas que não são decidíveis

→ Todo problema que não é decidível pode ser reconhecido?
$\overline{A_{TM}}$ não é decidível pois, se fosse, A_{TM} seria.

→ Existem problemas irreconhecíveis?
Sim, um número infinitamente incontável

Propriedades de fechamento

→ Linguagens Turing-reconhecíveis são fechadas sob
- união
- concatenação
- estrela
- interseção

TODAS AS LINGUAGENS			$\overline{A_{TM}}$
LINGUAGENS TURING-RECONHECÍVEIS	A_{TM}	R_{INT}	PCP
LINGUAGENS TURING-DECIDÍVEIS	$\{a^n b^n c^n : n \geq 0\}$		$\{0^p : p \text{ é primo}\}$
LINGUAGENS LIVRES DE CONTEXTO	$\{a^n b^n : n \geq 0\}$		$\{ww^R : w \in \{0,1\}^*\}$
LINGUAGENS REGULARES	$\{a^n : n \geq 0\}$		$\{0^p : p \text{ é par}\}$

POST CORRESPONDENCE PROBLEM