Teoria da Computação
Indecidibilidade

Leonardo Takuno
{leonardo.takuno@gmail.com}

Centro Universitário Senac

Sumário

Sumário

Paradoxos

Em uma cidade, existe apenas um barbeiro, do sexo masculino. Todo homem deve se manter barbeado, seja indo ao barbeiro ou fazendo ele mesmo. O barbeiro só faz a barba daqueles que não se barbeiam. Quem barbeia o barbeiro?

Máquina de Turing Universal

Sabemos que as linguagens:

$$A_{AFD} = \{\langle B, w\rangle | B \text{ é um AFD que aceita } w\}$$

$$A_{GLC} = \{\langle G, w\rangle | G \text{ é uma GLC que gera } w\}$$

são Turing-decidíveis.
E sobre a linguagem

$$A_{MT} = \{\langle M, w\rangle | M \text{ é uma MT que aceita } w\}.$$

Existe uma máquina de Turing capaz de simular outras Máquinas de Turing ?

Probema de aceitação para Máquinas de Turing

A linguagem

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

é chamada de **problema de aceitação para MT** ou **problema da parada** (*the halting problem*).

Máquina de Turing Universal

Teorema: A linguagem A_{MT} é Turing-reconhecível.

Dada a entrada $\langle M, w \rangle$, onde M é uma MT e w é uma cadeia, podemos simular M sobre w?
Podemos simular via máquina de Turing Universal U.
U = "Sobre a entrada $\langle M, w \rangle$, onde M é uma MT e w é uma cadeia:

1. Simule M sobre a entrada w.
2. Se M em algum momento entra no seu estado de aceitação, *aceite*; se M em algum momento entra em seu estado de rejeição, *rejeite*. "

Problema da Parada

A existência da máquina de Turing Universal U mostra que

$$A_{MT} = \{\langle M, w\rangle | M \text{ é uma MT que aceita } w\}.$$

é Turing-reconhecível, mas também podemos decidí-lo?

- O problema ocorre nos casos em que M não pára sobre um determinado w.
- Veremos que este é um insuperável problema: em geral, não se pode decidir se uma MT irá parar sobre w ou não, assim A_{MT} é indecidível.

Sumário

Problema da Parada

Teorema 4.11: A linguagem

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

é indecidível.

Prova: Por contradição. Assuma que exista um decisor H para a linguagem A_{TM}. Então,

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

Problema da Parada

Construímos uma nova MT D tal que
D = "Sobre a entrada $\langle Q \rangle$ onde Q é uma MT:

1. Execute H sobre a entrada $\langle Q, \langle Q \rangle \rangle$.
2. Faça o oposto da saída de H; se H aceita, rejeite e se H rejeita, aceite."

Agora,

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

Problema da Parada

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	$\cdots$
M_1	*aceite*		*aceite*		
M_2	*aceite*	*aceite*	*aceite*	*aceite*	
M_3					$\cdots$
M_4	*aceite*	*aceite*			
$\vdots$		$\vdots$			

A máquina em uma dada linha aceita a entrada em uma dada coluna.

Problema da Parada

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	$\cdots$
M_1	*aceite*	*rejeite*	*aceite*	*rejeite*	
M_2	*aceite*	*aceite*	*aceite*	*aceite*	$\cdots$
M_3	*rejeite*	*rejeite*	*rejeite*	*rejeite*	
M_4	*aceite*	*aceite*	*rejeite*	*rejeite*	
$\vdots$			$\vdots$		

A entrada i, j é o valor de H sobre a entrada $\langle M_i, \langle M_j \rangle \rangle$.

Problema da Parada

Agora, adicionamos D. Note que D computa o oposto das entradas na diagonal.

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	$\cdots$	$\langle D \rangle$	$\cdots$
M_1	*aceite*	*rejeite*	*aceite*	*rejeite*		*aceite*	
M_2	*aceite*	*aceite*	*aceite*	*aceite*	$\cdots$	*aceite*	$\cdots$
M_3	*rejeite*	*rejeite*	*rejeite*	*rejeite*		*rejeite*	
M_4	*aceite*	*aceite*	*rejeite*	*rejeite*		*aceite*	
$\vdots$			$\vdots$		$\ddots$		
D	*rejeite*	*rejeite*	*aceite*	*aceite*		?	
$\vdots$			$\vdots$				$\ddots$

Problema da Parada

O que acontece quando rodamos D com sua própria descrição $\langle D \rangle$ como entrada ? Nesse caso, obtemos

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

- Independentemente do que D faz, ela é forçada a fazer o oposto.
- Isto é uma contradição. Portanto, nem H nem D pode existir e A_{MT} é indecidível.

Problema da Parada

Assista:

https://www.youtube.com/watch?v=92WHN-pAFCs

Sumário

Método da Diagonalização

- Veremos agora uma prova construtiva que mostra que algumas linguagens não são computáveis por algoritmos.
- Esta prova mostra que o conjunto de todas as máquinas de Turing é contável ao passo que o conjunto de todas as linguagens é incontável.
- Portanto, existem algumas linguagem que não são reconhecíveis por máquina de Turing.

Conjuntos

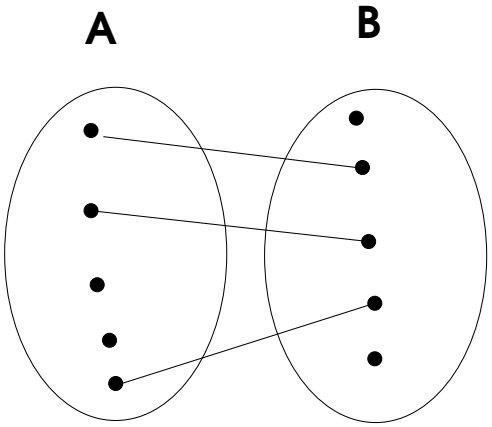
- Georg Cantor (1873).
- Medida do tamanho de conjuntos infinitos.
- Se tivermos dois conjuntos infinitos, como podemos dizer se um é maior que o outro ou se eles têm o mesmo tamanho?

Funções

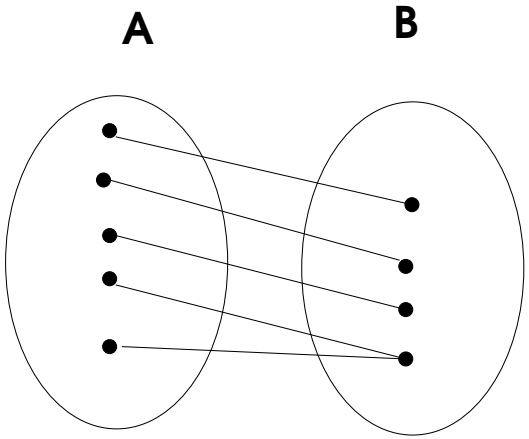
Definição 4.12: Se A e B são conjuntos e uma função $f : A \to B$, dizemos que:

- f é **um-para-um** se $f(a) \neq f(b)$ sempre que $a \neq b$.
- f é **sobrejetora** se para todo $b \in B$ existe um $a \in A$ tal que $f(a) = b$.
- f é **correspondência** se f é tanto um-para-um quanto sobrejetora.

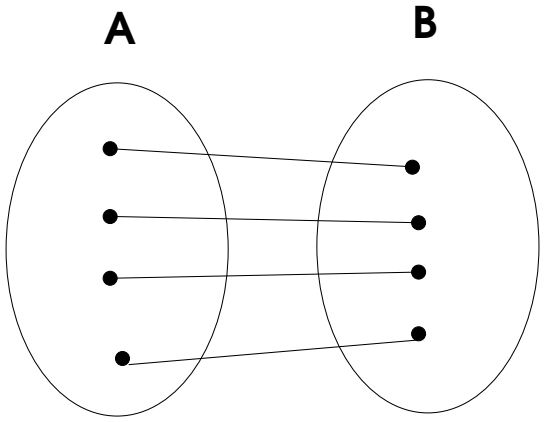
Funções



um–para–um



sobrejetora



correspondência

Funções

Definição: Dois conjuntos A e B são de **mesmo tamanho** se existe uma correspondência $f : A \rightarrow B$.

Definição 4.14: Um conjunto é **contável** se é finito ou tem o mesmo tamanho que $\mathcal{N}$

Método da Diagonalização

Exemplo: $f : \mathcal{N} \to \mathcal{E}$, onde $\mathcal{N}$ é o conjunto dos números naturais e $\mathcal{E}$ é o conjunto dos naturais pares.

- $f(n) = 2n$ é uma correspondência.

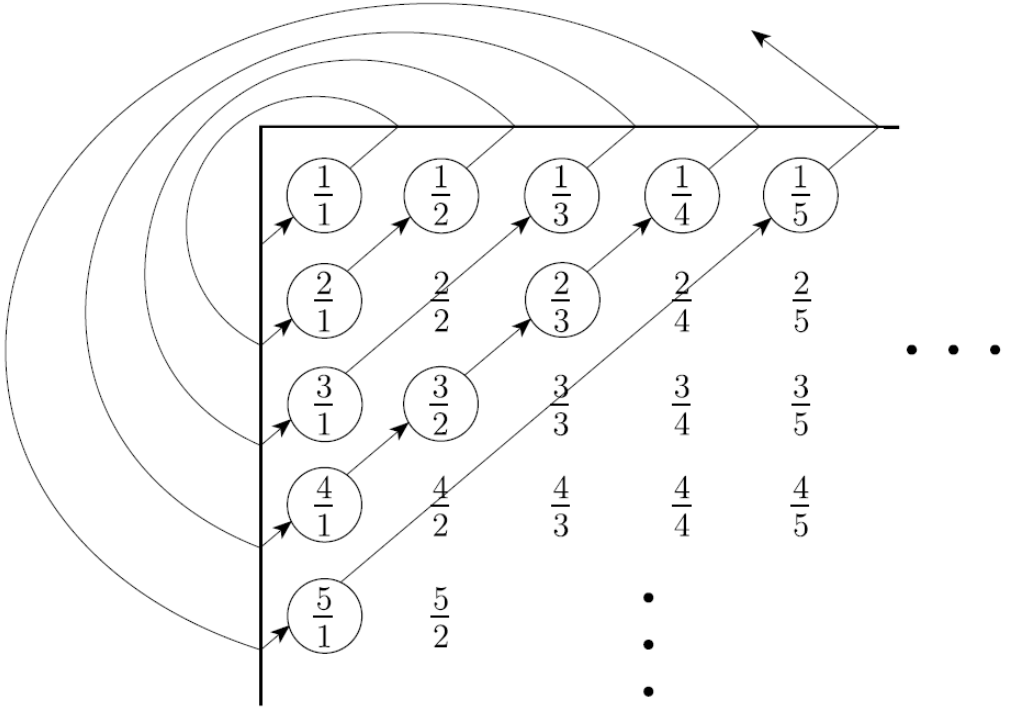
n	$f(n)$
1	2
2	4
3	6
$\vdots$	$\vdots$

Portanto, declaramos que estes dois conjuntos são do mesmo tamanho.

Método da Diagonalização

Teorema: Seja $Q = \{\frac{m}{n} | m, n \in \mathcal{N}\}$ o conjunto dos números racionais positivos, Q é contável.

Idéia da prova:



Cadeias sobre um alfabeto

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

Prova:

- Seja $C_i \in \Sigma^*$ o conjunto de todas as cadeias de comprimento i. Note que $|C_i| = k^i$, onde k é o tamanho do alfabeto Σ.
- Faça uma lista que contém os elementos de C_0 seguidos pelos elementos de C_1, seguidos por elementos de C_2, assim por diante.
- Faça $f(n) =$"a $(n+1)-$ésima cadeia dessa lista" $\forall n \in \mathcal{N}$.
- Note que f é bijetora: duas posições diferentes possuem cadeias diferentes e toda cadeia será listada. $\square$

Cadeias sobre um alfabeto

$\Sigma = \{0, 1\}$

0	ε
1	$0, 1$
2	$00, 01, 10, 11$
3	$000, 001, 010, 011, 100, 101, 111$
4	$0000, 0001 \cdots, 1111$
$\vdots$	$\ddots$

Máquinas de Turing

Teorema: O conjunto de todas as máquinas de Turing é contável.

Prova

- Qualquer TM M pode ser codificada com uma string $\langle M \rangle$ sobre um alfabeto Σ.
- Seja $\langle M \rangle^*$ o conjunto de todas as descrições de MT válidas.
- Sabemos que Σ^* é contável e $\langle M \rangle^* \subseteq \Sigma^*$, logo, $\langle M \rangle^*$ é contável. $\square$

Conjuntos incontáveis

- Alguns conjuntos não podem ser mapeados por bijeção ao conjunto $\mathcal{N}$.
- Tais conjuntos são incontáveis.

Método da Diagonalização

Teorema 4.17: Seja $\mathcal{R}$ o conjunto dos números reais, $\mathcal{R}$ é incontável.

Prova:

- Suponha que $\mathcal{R}$ é contável. Então existe uma correspondência f entre $\mathcal{N}$ e $\mathcal{R}$.

n	$f(n)$
1	$3,14159...$
2	$55,55555...$
3	$0,12345...$
4	$0,500000...$
$\vdots$	$\vdots$

Método da Diagonalização

... continuação

- Agora obtemos um $x \in \mathcal{R}$ que não é pareada com qualquer elemento de $\mathcal{N}$.
- Escolha o *i-ésimo* dígito fracionário de x diferente do dígito da *i-ésima* fração.

n	$f(n)$
1	$3,\underline{1}4159...$
2	$55,5\underline{5}555...$
3	$0,12\underline{3}45...$
4	$0,500\underline{0}00...$
$\vdots$	$\vdots$

Ex: $x = 0,4641....$ Então, $x \neq f(n)$ para todo n. Logo $\mathcal{R}$ é incontável.$\square$

Uma prova construtiva

Teorema: O conjunto de todas as seqüências binárias infinita é incontável.

Prova: Prova por contradição. Defina uma correspondência $f : \mathcal{N} \to \mathcal{B}$, onde $\mathcal{N}$ são os números naturais e $\mathcal{B}$ é o conjunto de todas as seqüências binárias infinitas. Então,

n	$f(n)$
1	0100111 ...
2	11111000 ...
3	10110010 ...
$\vdots$	$\vdots$
k	0010 ... 0_k ...
$\vdots$	$\vdots$

Uma prova construtiva

Então,

n	$f(n)$
1	0100111 ...
2	11111000 ...
3	1011001 ...
$\vdots$	$\vdots$
k	0010 ... 0_k ...
$\vdots$	$\vdots$

Podemos construir uma seqüência binária que difere de todas as seqüências enumeradas pelo menos em 1 bit.

Uma prova construtiva

... continuação

n	$f(n)$
1	$\underline{0}100111\ \ldots$
2	$1\underline{1}111000\ \ldots$
3	$10\underline{1}1001\ \ldots$
$\vdots$	$\vdots$
k	$0010\ \ldots\ \underline{0}_k\ \ldots$
$\vdots$	$\vdots$

exemplo: $x = 100...1....$

- Para qualquer valor de k construímos uma sequência que diferen no valor de $f(k)$ no $k-$ésimo bit.
- Portanto, existem elementos em $\mathcal{B}$ que não são imagens de f. Isto significa nossa hipótese de que f é uma correspondência incorreta.$\square$

Uma prova construtiva

Teorema: O conjunto de todas as linguagens $\mathcal{L}$ sobre o alfabeto $\Sigma_{0,1}$ é incontável.

Prova:

- Mostramos uma correspondência $f : \mathcal{L} \rightarrow \mathcal{B}$, onde $\mathcal{L}$ é o conjunto de todas as linguagens e $\mathcal{B}$ é o conjunto de sequências binárias infinitas.
- Para cada linguagem $A \in \mathcal{L}$ podemos construir um único elemento em $\mathcal{B}$.
- Seja $\Sigma^* = \{s_1, s_2, s_3, ...\}$. O *i-ésimo* bit da **seqüência característica** de A é 1 se $s_i \in A$ e 0 se $s_i \notin A$.

Uma prova construtiva

Teorema: O conjunto de todas as linguagens $\mathcal{L}$ sobre o alfabeto $\Sigma_{0,1}$ é incontável.

Exemplo: se A fosse a linguagem de todas as cadeias começando com 0 sobre o alfabeto $\{0, 1\}$, sua seqüência característica $\mathcal{X}_A$ seria

$$\begin{array}{lcccccccccc} \Sigma^* & = \{ & \varepsilon, & 1, & 00, & 01, & 10, & 11, & 000, & 001, & ...\} \\ \mathcal{A} & = \{ & , & , & 00, & 01, & , & , & 000, & 001, & ...\} \\ \mathcal{X}_{\mathcal{A}} & = \{ & 0\ , & 0, & 1, & 1, & 0, & 0, & 1, & 1\ , & ...\} \end{array}$$

A função $f : \mathcal{L} \to \mathcal{B}$, onde $f(A)$ é a seqüência característica de A, é um-para-um e sobrejetora e, portanto, uma correspondência. Conseqüentemente, como $\mathcal{B}$ é incontável, $\mathcal{L}$ também é incontável.$\square$

Uma prova construtiva

Corolário 4.18: Algumas linguagens não são Turing-reconhecíveis.

Prova: Observe que o conjunto de Máquinas de Turing é contável e da prova anterior segue que o conjunto de todas as linguagens é incontável. Assim, não conseguimos construir uma correspondência entre o conjunto de todas as linguagens e o conjunto de máquinas de Turing.
Portanto, existem algumas linguagens que não são reconhecidas por Máquina de Turing. □

Sumário

Linguagem Turing-irreconhecível

- A demonstração apresentada anteriormente mostra que A_{MT} é indecidível.
- No entanto, sabemos que A_{MT} é Turing-reconhecível.
- Agora apresentaremos uma linguagem que não é sequer Turing-reconhecível.
- Segue como consequência do Teorema 4.22, a seguir.

Linguagem Turing-irreconhecível

Teorema 4.22: Uma linguagem é decidível sse ela é Turing-reconhecível e co-Turing-reconhecível

Em outras palavras, uma linguagem é decidível exatamente quando ela e seu complmento são ambas Turing-reconhecíveis.

Linguagem Turing-irreconhecível

Teorema 4.22: Uma linguagem é decidível sse ela é Turing-reconhecível e co-Turing-reconhecível

Prova:
($\Rightarrow$)

- Se A for decidível, então A e $\overline{A}$ são Turing-Reconhecíveis.
- Qualquer linguagem decidível é Turing-Reconhecível;
- O complemento de uma linguagem decidível é também decidível.

Linguagem Turing-irreconhecível

Teorema 4.22: Uma linguagem é decidível sse ela é Turing-reconhecível e co-Turing-reconhecível

($\Leftarrow$)

- Se tanto A quanto $\overline{A}$, fazemos M_1 ser o reconhecedor para A e M_2 o reconhecedor para $\overline{A}$. Construa M um decisor para A.

  $M =$ "Sobre a entrada w:

  1. Execute M_1 e M_2, sobre a entrada w em paralelo.
  2. Se M_1 aceita, aceite; se M_2 aceita, rejeita.

  M sempre pára, portanto é um decisor. Logo A é decidível.

Linguagem Turing-irreconhecível

Corolário 4.23: A linguagem $\overline{A_{MT}}$ não é Turing-reconhecível.

Prova: Por contradição. Observe que A_{MT} é indecidível. Além disso, observe que A_{MT} é Turing-reconhecível. Agora, assuma que that $\overline{A_{MT}}$ é também Turing-reconhecível. Verifique que a string w, ou é um elemento de A_{MT}, ou um elemento de $\overline{A_{MT}}$ podemos contruir o seguinte decisor para A_{MT}.

Linguagem Turing-irreconhecível

Seja $M1$ e $M2$ reconhecedores para A_{MT} e $\overline{A_{MT}}$, respectivamente:
M = "Sobre a entrada w, onde w é uma string:

1. Execute $M1$ e $M2$ em paralelo sobre w.
2. Se $M1$ aceita, aceite; se $M2$ aceita, rejeite."

Note que esta máquina é um decisor pois irá parar sobre toda entrada w. Note também, que este decisor contradiz nosso teorema que A_{MT} é indecidível. Portanto, nossa hipótese que $\overline{A_{MT}}$ é Turing-reconhecível deve estar errada. Isto mostra que $\overline{A_{MT}}$ não é Turing-reconhecível.□

Exercícios

1) Mostre que o conjunto dos números naturais pares $\{2, 4, 6, \cdots\}$ e o conjunto dos números naturais ímpares $\{1, 3, 5, \cdots\}$ têm o mesmo tamanho.

Exercícios (Solução)

Basta realizar o seguinte emparelhamento (função bijetora) entre os dois conjuntos:

Pares	Ímpares
0	1
2	3
4	5
6	7
8	9
10	11
...	...

A função que mapeia os pares nos ímpares é dada por $f : \mathit{pares} \rightarrow \mathit{impares}$, $f(x) = x + 1$ que, claramente, é uma função bijetora (gráfico é uma reta)

Exercícios

2) Mostre que o conjunto dos números inteiros $\mathcal{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ é contável.

Exercícios

2) Mostre que o conjunto dos números inteiros $\mathcal{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ é contável.
Prova: Vamos mostrar que

$$f(n) = \begin{cases} \frac{n}{2} & \text{se n é par} \\ \frac{-(n+1)}{2} & \text{se n é ímpar} \end{cases}$$

é uma bijeção de $\mathcal{N}$ para $\mathcal{Z}$
Sejam $m, n \in \mathcal{N}$ com $n \neq m$. Se ambas tem a mesma paridade, 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 $\frac{n}{2} \neq \frac{-(m+1)}{2}$. (injetora)

Exercícios

... continuação

Seja $z \in \mathcal{Z}$. Se $z \geq 0$, então $2z$ é um número natural par tal que $f(2z) = z$. Se $z < 0$, então $-(2z + 1)$ é um número ímpar tal que $f(-(2z + 1)) = z$. (sobrejetora). $\square$