MT universal e linguagens não-enumeráveis

Luís Felipe

UFF

21 de Junho de 2023

Luís Felipe
21/06/23

O problema da parada

- Vamos mostrar que EXISTE um problema algoritmicamente insolúvel, reconhecível mas não decidível.

- Vamos ver que o problema de determinar se uma MT aceita uma determinada cadeia de entrada é insolúvel.

- Vamos chamá-lo de $A_{MT} = \{\langle M, w\rangle \mid M$ é uma MT e M aceita $w\}$

Luís Felipe
21/06/23

O resultado

Teorema. A_{MT} é indecidível.

Algumas Considerações:

- Antes de provarmos o Teorema, observemos que A_{MT} é Turing-reconhecível.
- De fato, vamos construir uma MT $\mathcal{U}$ que simule uma MT qualquer.
- Esta máquina é chamada de MT universal.
  - Pausa para entendermos melhor uma MT universal.

Luís Felipe
21/06/23

MT universal

- MT universal $\mathcal{U}$: MT capaz de simular qualquer outra MT.
  - $\mathcal{U}$ deve receber como entrada o programa da máquina que está sendo simulada.
  - Para isso, precisamos ser capazes de descrever o alfabeto, o conjunto de estados e as transições de uma máquina de Turing qualquer a partir do alfabeto de $\mathcal{U}$.

- Se podemos enxergar uma máquina de Turing como um modelo formal de um algoritmo, podemos enxergar a máquina de Turing universal como um modelo formal de um computador programável.
  - Ou seja, um computador que pode executar qualquer algoritmo, desde que receba o conjunto de instruções deste algoritmo.

Luís Felipe
21/06/23

Como obter uma MT universal

Seja M a MT a ser simulada em $\mathcal{U}$. Assuma que em M há:

- n estados; alfabeto da fita Σ_M com m símbolos.

Considere $\mathcal{U}$ da seguinte forma:

- Alfabeto da entrada: $\Sigma_{\mathcal{U}} = \{0, 1, \sigma, q, X, Y, Z, \#, a, b\}$.
- Alfabeto da fita: $\Sigma_{\mathcal{U}} \cup \{\triangleright, \sqcup\}$
- As transições de M são feitas na fita de $\mathcal{U}$ enumerando (separadamente) os símbolos e os estados de M no sistema unário (nesse sistema, n é representado por 0^n).
  - Na fita de $\mathcal{U}$, símbolos de M possuem prefixo σ e estados de M possuem prefixo q.
  - Setas $\rightarrow$ e $\leftarrow$ são representados como símbolos de M.
- Reserve $m + 3$ casas na fita de $\mathcal{U}$ para cada símbolo de M
  - 1^a casa: σ. 2^a casa em diante: codificação de tamanho $m + 2$.
  - Codificações: $\triangleright$ em 01^{m+1}; $\leftarrow$ em $0^2 1^m$; $\rightarrow$ em $0^3 1^{m-1}$; r-ésimo símbolo em $0^r 1^{m+2-r}$.
- Reserve $n + 1$ casas na fita de $\mathcal{U}$ para cada estado de M
  - 1^a casa: q. 2^a casa em diante: codificações, r-ésimo estado em $0^r 1^{n-r}$.

Luís Felipe

21/06/23

Continuação da codificação de M em $\mathcal{U}$

Vamos preparar a fita de $\mathcal{U}$ com os dados de M.

- Seja $\delta(q_i, \sigma_j) = (q_r, \sigma_s)$ em M. Codifique-a como S_t na fita de $\mathcal{U}$ da seguinte forma:

X	q	0^i	1^{n-i}	σ	0^j	1^{m+2-j}	q	0^r	1^{n-r}	σ	0^s	1^{m+2-s}	X

- 0^i representa i posições na fita com 0's. O mesmo para os demais símbolos.

Descrição completa de M com entrada w na fita de $\mathcal{U}$:

$\triangleright$	X	S_1	X	S_2	$\cdots$	S_t	Y	Q	Z	σ	u_1	σ	u_2	$\#$	u_3	$\cdots$

- Até Y: descrição de M, $\langle M \rangle$
- $Q = q0^i1^{n-i}$ é o estado em que M se encontra no momento atual da computação
- Após Q: descrição de w, $\langle w \rangle$. u_i representa cada símbolo escrito em unário e precedido de σ.
- $\#$ marca o símbolo atual lido por M na simulação de $\mathcal{U}$.
  - No início da computação de $\mathcal{U}$, Q é preenchido com o estado inicial de M e o símbolo $\#$ fica antes do símbolo u_1 associado ao primeiro símbolo de w.

Luís Felipe
21/06/23

Processamento de $\mathcal{U}$

- Primeiramente, verifique se a fita de $\mathcal{U}$ descreve M.
  - Varre a fita a partir de $\triangleright$ se os X's, q's, σ's, Y's e Z's estão posicionados nas posições corretas.
  - Precisa ver também se o comprimento de cada string está de acordo conforme codificação devida.
- Simule $\mathcal{U}$ em 3 etapas:
  1. No início, cabeçote sobre $\triangleright$. Então, vá até o trecho S da 4-upla associado ao par (Q, τ). Q é o estado representado entre Y e Z; τ é o símbolo representado na fita à direita do Z que se inicia com a marcação $\#$.
     - Enquanto busca (Q, τ), $\mathcal{U}$ troca 0's e 1's por a's e b's (da esq. p/ dir.), resp. Assim, sabemos até onde a busca foi feita.
     - Se encontrar, faça as alterações devidas. Senão, o estado atual de M é final. Assim, $\mathcal{U}$ entra em um estado final, que faz a máquina parar.
  2. O estado seguinte ao atual na transição de M a partir de (Q, τ) é copiado entre Y e Z. Além disso, os 0's e 1's associados a Q são trocados por a's e b's, resp.
  3. $\mathcal{U}$ volta para $\triangleright$, trocando a's e b's por 0's e 1's, resp. Agora, $\mathcal{U}$ está pronta para recomeçar.

Luís Felipe
21/06/23

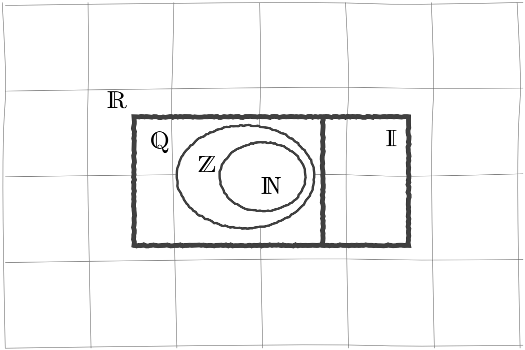
O que fazer com MT universal

- Considerando
  $A_{MT} = \{\langle M, w\rangle \mid M$ é uma MT e M aceita $w\}$
- $U =$ Sobre a entrada $\langle M, w\rangle$, onde M é uma MT e w é uma cadeia:
  - Simule M sobre w
  - Se M em algum momento entra em um estado de aceitação, aceite.
  - Se M em algum momento entra em seu estado de rejeição, rejeite.
- U pode entrar em loop? Quando?
- Se M entra em loop, U entra em loop.
- Note que U não decide A_{MT}.
- Se houvesse uma forma de saber se M está em loop, então poderíamos rejeitar a entrada.
- Por isso, este problema é chamado de Problema da Parada.

Luís Felipe
21/06/23

Método da Diagonalização

- Descoberto por Georg Cantor em 1873
  - que estava preocupado em medir os tamanhos de conjuntos infinitos
  - Existem conjuntos infinitos de tamanhos diferentes ou todos têm o mesmo tamanho???



Luís Felipe
21/06/23

A tal da bijeção

- Uma função é injetora se ela nunca mapeia dois elementos do domínio no mesmo elemento do contradomínio.
- Uma função é sobrejetora quando todo elemento do contradomínio é imagem de algum elemento do domínio.
- Uma função é bijetora quando é injetora e sobrejetora ao mesmo tempo.
- Assim, se A é o domínio de uma função bijetora e B o seu contradomínio, então $|A| = |B|$.
- Há, portanto, uma correspondência entre os elementos de A e B.
- Ou seja, eles poderiam ser emparelhados.

Luís Felipe

21/06/23

Exemplo

- Considere o conjunto dos números naturais e seja P o conjunto dos números naturais pares.
- Note que, embora P seja subconjunto próprio de $\mathbb{N}$, P e $\mathbb{N}$ podem ser emparelhados.

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

- $f(n) = 2n$, onde $n \in \mathbb{N}$ é bijetora.
- Isso não é estranho??
  - P é, intuitivamente, menor que $\mathbb{N}$ devido a sua condição de subconjunto próprio.

Luís Felipe
21/06/23

Conjuntos enumeráveis

Um conjunto é enumerável se é finito ou se existe uma bijeção entre ele e $\mathbb{N}$.

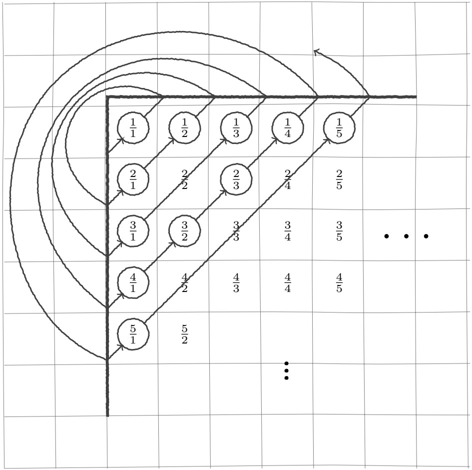
Exemplo:

- O conjunto $\mathbb{Q}_+^* = \{\frac{m}{n} \mid m, n \in \mathbb{N}\}$ tem uma bijeção com $\mathbb{N}$?

  - Sim. Para mostrar isso, vamos construir uma matriz infinita contendo todos os elementos de $\mathbb{Q}_+^*$
  - linha i: todos os elementos com numerador i
  - coluna j: todos os elementos com denominadores j
  - Como formar uma lista a partir da matriz para emparelhar com $\mathbb{N}$?
    - Seria uma boa ideia começar a lista com os elementos da primeira linha? NÃO. Nunca alcançaríamos a linha 2.
  - A ideia é listar os elementos nas diagonais, pulando as repetições.

Luís Felipe
21/06/23

Diagrama



Assim, ao o elemento $\frac{1}{1}$ estaria mapeado em 1, o elemento $\frac{2}{1}$ em 2, $\frac{1}{2}$ em 3 e assim sucessivamente.

Luís Felipe
21/06/23

E os Reais?

Seria possível utilizar essa mesma estratégia com os Reais?
Teorema. $\mathbb{R}$ é não-enumerável.
Ideia: Vamos mostrar que não existe bijeção com $\mathbb{N}$. Mais precisamente, vamos exibir um número real que não tem mapeamento em $\mathbb{N}$. Suponha por absurdo que $\mathbb{R}$ seja enumerável. Então existe uma bijeção f que emparelha todo elemento de $\mathbb{N}$ com todo elemento de $\mathbb{R}$. Vamos construir o número real $x, 0 < x < 1$ da seguinte forma:

n	$f(n)$
1	$3,\underline{1}4578\ldots$
2	$1,7\underline{8}8555\ldots$
3	$0,57\underline{5}543\ldots$
4	$0,876\underline{2}01\ldots$
$\vdots$	$\vdots$

Obtenha para i-ésimo dígito de x algum dígito diferente do i-ésimo fracionário de $f(i)$:

$x = 0,3531\ldots$

Se x estivesse na tabela, então x estaria numa posição n. Porém na n-ésima posição fracionária de x está um dígito distinto do de x. Absurdo.

Luís Felipe
21/06/23

A conta não fecha

- Segue do teorema anterior que nem toda linguagem é Turing-reconhecível

  - Vamos ver que Σ^* é enumerável.
  - Vamos ver que o conjunto de todas as linguagens é não-enumerável enquanto que o conjunto das MT's é enumerável.
    - Parênteses: Não acham estranho?! Uma linguagem é um subconjunto de Σ^*.
    - Σ^* é enumerável e o conjunto de todas as linguagens é não-enumerável.
    - Na verdade, de Análise Matemática, temos que se X for um conjunto infinito, então $\mathcal{P}(X)$ será um conjunto não-enumerável.
  - Como cada MT pode reconhecer uma única linguagem, a conta não fecha.
  - Logo, existem linguagens que não são Turing-reconhecíveis.

Luís Felipe
21/06/23

Nem tudo é Turing-reconhecível

Corolário. Existem linguagens que não são Turing-reconhecíveis.

Ideia: Para mostrar que o conjunto de MTs é enumerável vamos observar 2 aspectos:

1. Cada MT M tem uma codificação em uma string $\langle M \rangle$
2. O conjunto Σ^* é enumerável.
   - Basta notar que o número de cadeias de tamanho i é finito
   - Assim, podemos fazer uma lista com as cadeias de tamanho $0, 1, 2, 3$ etc.
   - Claramente temos uma bijeção com $\mathbb{N}$
   - Dentre todas as cadeias de Σ^*, existem as que não são codificações de MT.
   - Logo, temos uma lista com todas as MTs

Luís Felipe
21/06/23

Ideia - Continuação

Ideia (cont.): Resta, portanto, mostrar que o conjunto das linguagens é não-enumerável. Para tal, note que:

1. O conjunto de todas as sequências binárias infinitas, $\mathcal{B}$ é não-enumerável. (Prova semelhante à prova de que $\mathbb{R}$ é não enumerável)
2. Para mostrar que o conjunto de todas as linguagens $\mathcal{L}$ é não-enumerável, vamos fazer uma correspondência com $\mathcal{B}$
3. Seja $A \in \mathcal{L}$. A será mapeada em $\mathcal{B}$ através de sua sequência característica. Observe o exemplo:

Luís Felipe
21/06/23

Exemplo

A é a linguagem de todas as cadeias que começam por 0.

$$\begin{array}{lclcccccccccc} \Sigma^\star & = & \{ & \varepsilon, & 0, & 1, & 00, & 01, & 10, & 11, & 000, & 001, & \ldots & \} \\ A & = & \{ & & 0, & & 00, & 01, & & & 000, & 001, & \ldots & \} \\ \chi_A & = & & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \ldots & \end{array}$$

A função que leva $\mathcal{L}$ em $\mathcal{B}$ tal que $f(A)$ é a sequência característica de A, $A \in \mathcal{L}$ é bijetora. Logo, $\mathcal{L}$ é não-enumerável.

Assim, temos mais linguagens do que MTs para reconhecê-las.