

MAC 414

Autômatos, Computabilidade e
Complexidade

aula 14 — 9/11/2020

O que é Algoritmo?

O que é Algoritmo?

Sequência de instruções que, para cada entrada válida para em um número finito de passos dando uma resposta correspondente à entrada.

O que é Algoritmo?

Sequência de instruções que, para cada entrada válida para em um número finito de passos dando uma resposta correspondente à entrada. Computa uma função.

O que é Algoritmo?

Sequência de instruções que, para cada entrada válida para em um número finito de passos dando uma resposta correspondente à entrada. Computa uma função.

Pode ser escrito em linguagem de programação, como MT, como função recursiva primitiva ou μ -recursiva, outros formalismos.

O que é Algoritmo?

Sequência de instruções que, para cada entrada válida para em um número finito de passos dando uma resposta correspondente à entrada. Computa uma função.

Pode ser escrito em linguagem de programação, como MT, como função recursiva primitiva ou μ -recursiva, outros formalismos.

Tudo simulável por MTs.

Tese de Church-Turing

Algoritmo é o mesmo que uma Máquina de Turing que para sempre.

Tese de Church-Turing

Algoritmo é o mesmo que uma Máquina de Turing que para sempre.

Tese de Church-Turing

Algoritmo é o mesmo que uma Máquina de Turing que para sempre.

*Em particular uma função é **computável** sse for **Turing-computável**.*

Tese de Church-Turing

Algoritmo é o mesmo que uma Máquina de Turing que para sempre.

*Em particular uma função é **computável** sse for **Turing-computável**.*

Tese de Church-Turing

Algoritmo é o mesmo que uma Máquina de Turing que para sempre.

*Em particular uma função é **computável** sse for **Turing-computável**.*

Noção informal \rightarrow definição formal.

Tese de Church-Turing

Algoritmo é o mesmo que uma Máquina de Turing que para sempre.

*Em particular uma função é **computável** sse for **Turing-computável**.*

Noção informal \rightarrow definição formal.

Aceita *porque* todas as tentativas de produzir novas definições recaíram nessa.

Tese de Church-Turing

Algoritmo é o mesmo que uma Máquina de Turing que para sempre.

*Em particular uma função é **computável** sse for **Turing-computável**.*

Noção informal → definição formal.

Aceita *porque* todas as tentativas de produzir novas definições recaíram nessa.

Dá um *caminho* para mostrar que uma dada função *não é computável*.

MT universal

MT universal

Simulador genérico de MTs.

MT universal

Simulador genérico de MTs.

Pode ser pensado como um computador que executa código “escrito em MT”.

MT universal

Simulador genérico de MTs.

Pode ser pensado como um computador que executa código “escrito em MT”.

Entrada: descrição de uma MT \mathcal{M} e uma entrada x para ela.

MT universal

Simulador genérico de MTs.

Pode ser pensado como um computador que executa código “escrito em MT”.

Entrada: descrição de uma MT \mathcal{M} e uma entrada x para ela.

Execução: computa $\mathcal{M}(x)$ (se estiver definido).

MT universal

Simulador genérico de MTs.

Pode ser pensado como um computador que executa código “escrito em MT”.

Entrada: descrição de uma MT \mathcal{M} e uma entrada x para ela.

Execução: computa $\mathcal{M}(x)$ (se estiver definido).

Não pode haver restrição no número de estados de \mathcal{M} ou no tamanho do seu alfabeto.

Convenções

Convenções

Os estados de \mathcal{M} serão numerados como q_0, q_1, \dots, q_n , com $s = q_0$.

Convenções

Os estados de \mathcal{M} serão numerados como q_0, q_1, \dots, q_n , com $s = q_0$.

Seja k um inteiro tal que exista uma representação binária de n em k bits. Vamos codificar o estado q_j por um q seguido da representação de j em k bits. Essa palavra será denotada como “ q_j ”.

Convenções

Os estados de \mathcal{M} serão numerados como q_0, q_1, \dots, q_n , com $s = q_0$.

Seja k um inteiro tal que exista uma representação binária de n em k bits. Vamos codificar o estado q_j por um q seguido da representação de j em k bits. Essa palavra será denotada como “ q_j ”.

Ex: Se $k = 4$, “ q_5 ” = $q0101$.

Convenções

Convenções

Análogo para letras:

Convenções

Análogo para letras:

$\hat{\Sigma} = \Sigma \cup \{\sqcup, \triangleright, \leftarrow, \rightarrow\} = \{\sigma_0, \dots, \sigma_m\}$, onde $\sqcup, \triangleright, \leftarrow, \rightarrow$ recebem os números de 0 a 3.

Convenções

Análogo para letras:

$\hat{\Sigma} = \Sigma \cup \{\sqcup, \triangleright, \leftarrow, \rightarrow\} = \{\sigma_0, \dots, \sigma_m\}$, onde $\sqcup, \triangleright, \leftarrow, \rightarrow$ recebem os números de 0 a 3.

Seja ℓ um inteiro tal que exista uma representação binária de m em ℓ bits. Vamos codificar σ_j por um a seguido da representação de j em ℓ bits. Essa palavra será denotada como " a_j ".

Convenções

Análogo para letras:

$\hat{\Sigma} = \Sigma \cup \{\sqcup, \triangleright, \leftarrow, \rightarrow\} = \{\sigma_0, \dots, \sigma_m\}$, onde $\sqcup, \triangleright, \leftarrow, \rightarrow$ recebem os números de 0 a 3.

Seja ℓ um inteiro tal que exista uma representação binária de m em ℓ bits. Vamos codificar σ_j por um a seguido da representação de j em ℓ bits. Essa palavra será denotada como " a_j ".

Ex: Se $\ell = 4$, " \leftarrow " = $a0010$.

Convenções

Análogo para letras:

$\hat{\Sigma} = \Sigma \cup \{\sqcup, \triangleright, \leftarrow, \rightarrow\} = \{\sigma_0, \dots, \sigma_m\}$, onde $\sqcup, \triangleright, \leftarrow, \rightarrow$ recebem os números de 0 a 3.

Seja ℓ um inteiro tal que exista uma representação binária de m em ℓ bits. Vamos codificar σ_j por um a seguido da representação de j em ℓ bits. Essa palavra será denotada como " a_j ".

Ex: Se $\ell = 4$, " \leftarrow " = $a0010$.

Se $x \in \hat{\Sigma}^*$, " x " é a concatenação dos códigos das suas letras.

Convenções

Análogo para letras:

$\hat{\Sigma} = \Sigma \cup \{\sqcup, \triangleright, \leftarrow, \rightarrow\} = \{\sigma_0, \dots, \sigma_m\}$, onde $\sqcup, \triangleright, \leftarrow, \rightarrow$ recebem os números de 0 a 3.

Seja ℓ um inteiro tal que exista uma representação binária de m em ℓ bits. Vamos codificar σ_j por um a seguido da representação de j em ℓ bits. Essa palavra será denotada como " a_j ".

Ex: Se $\ell = 4$, " \leftarrow " = $a0010$.

Se $x \in \hat{\Sigma}^*$, " x " é a concatenação dos códigos das suas letras.

Se a única letra de verdade é a , ela tem número 4 e " $\triangleright aa \sqcup a$ " = $\underbrace{a001} \underbrace{a100} \underbrace{a100} \underbrace{a000} \underbrace{a100}$.

Convenções

Convenções

A codificação de \mathcal{M} , denotada " \mathcal{M} " é concatenação de todas as quádruplas (q, σ, p, τ) tais que $\delta(q, \sigma) = (p, \tau)$, onde

Convenções

A codificação de \mathcal{M} , denotada " \mathcal{M} " é concatenação de todas as quádruplas (q, σ, p, τ) tais que $\delta(q, \sigma) = (p, \tau)$, onde

$$"(q, \sigma, p, \tau)" = \# "q" " \sigma " "p" " \tau " .$$

Convenções

A codificação de \mathcal{M} , denotada " \mathcal{M} " é concatenação de todas as quádruplas (q, σ, p, τ) tais que $\delta(q, \sigma) = (p, \tau)$, onde

$$“(q, \sigma, p, \tau)” = \# “q” “\sigma” “p” “\tau”.$$

Quádruplas em ordem lexicográfica (conveniência).

Convenções

A codificação de \mathcal{M} , denotada " \mathcal{M} " é concatenação de todas as quádruplas (q, σ, p, τ) tais que $\delta(q, \sigma) = (p, \tau)$, onde

$$“(q, \sigma, p, \tau)” = \# “q” “\sigma” “p” “\tau”.$$

Quádruplas em ordem lexicográfica (conveniência).

Note que não é preciso dizer quem é s , já que por convenção ele é $q00\dots 0$.

Convenções

A codificação de \mathcal{M} , denotada " \mathcal{M} " é concatenação de todas as quádruplas (q, σ, p, τ) tais que $\delta(q, \sigma) = (p, \tau)$, onde

$$“(q, \sigma, p, \tau)” = \# “q” “\sigma” “p” “\tau”.$$

Quádruplas em ordem lexicográfica (conveniência).

Note que não é preciso dizer quem é s , já que por convenção ele é $q00\dots0$.

Nem H , já que esses são os estados que não aparecem como primeira componente de nenhuma quádrupla

Example 5.2.1: Consider the Turing machine $M = (K, \Sigma, \delta, s, \{h\})$, where $K = \{s, q, h\}$, $\Sigma = \{\sqcup, \triangleright, a\}$, and δ is given in this table.

state, symbol	δ
s, a	(q, \sqcup)
s, \sqcup	(h, \sqcup)
s, \triangleright	(s, \rightarrow)
q, a	(s, a)
q, \sqcup	(s, \rightarrow)
q, \triangleright	(q, \rightarrow)

(s, a, q, \sqcup)

state/symbol	representation
s	$q00$
q	$q01$
h	$q11$
\sqcup	$a000$
\triangleright	$a001$
\leftarrow	$a010$
\rightarrow	$a011$
a	$a100$

Example 5.2.1: Consider the Turing machine $M = (K, \Sigma, \delta, s, \{h\})$, where $K = \{s, q, h\}$, $\Sigma = \{\sqcup, \triangleright, a\}$, and δ is given in this table.

state, symbol	δ
s a	(q, \sqcup)
s \sqcup	(h, \sqcup)
s \triangleright	(s, \rightarrow)
q a	(s, a)
q \sqcup	(s, \rightarrow)
q \triangleright	(q, \rightarrow)

state/symbol	representation
s	$q00$
q	$q01$
h	$q11$
\sqcup	$a000$
\triangleright	$a001$
\leftarrow	$a010$
\rightarrow	$a011$
a	$a100$

" \mathcal{M} " = $\#q00a100q01a000\#q00a000q11a000$
 $\#q00a001q00a011\#q01a100q00a011$
 $\#q01a000q00a011\#q01a001q01a011.$

A máquina universal \mathcal{U}

A máquina universal \mathcal{U}

Descrição funcional:

Se \mathcal{M} é uma MT e w é uma entrada válida para \mathcal{M} ,
então:

$$\mathcal{U}(\underbrace{\underbrace{\text{"}\mathcal{M}\text{"}}_{\text{M}} \underbrace{\text{"}w\text{"}}_{\text{w}}) = \underbrace{\text{"}\mathcal{M}(w)\text{"}}_{\text{Resultado}}.$$

"Resultado do símbolo"

A máquina universal \mathcal{U}

Descrição funcional:

Se \mathcal{M} é uma MT e w é uma entrada válida para \mathcal{M} , então:

$$\mathcal{U}(\langle \mathcal{M} \rangle w) = \mathcal{M}(w).$$

Em particular, se (\mathcal{M}, w) não para, \mathcal{U} com a entrada acima também não.

A máquina universal \mathcal{U}

Descrição funcional:

Se \mathcal{M} é uma MT e w é uma entrada válida para \mathcal{M} , então:

$$\mathcal{U}(\langle \mathcal{M} \rangle w) = \mathcal{M}(w).$$


Em particular, se (\mathcal{M}, w) não para, \mathcal{U} com a entrada acima também não.

Vamos descrever \mathcal{U} como MT de três fitas. A \mathcal{U} de verdade é a MT que simula essa daí.

Inicialização

1 Entrada: $\triangleright \mathcal{U} \mathcal{M} \mathcal{W}$

Inicialização

- 1 Entrada: $\triangleright \sqcup "M" "w"$ 
- 2 Copie "M" para a fita 2, apagando da 1, junto com $\triangleright \sqcup$. Cursor 2 para a esquerda.

Inicialização



- 1 Entrada: $\triangleright \sqcup$ "M" "w"
- 2 Copie "M" para a fita 2, apagando da 1, junto com $\triangleright \sqcup$. Cursor 2 para a esquerda.
- 3 Escreva "s" na fita 3. Cursor 3 para a esquerda.

Inicialização

- 1 Entrada: $\triangleright \sqcup \mathcal{M} \sqcup w$
- 2 Copie \mathcal{M} para a fita 2, apagando da 1, junto com $\triangleright \sqcup$. Cursor 2 para a esquerda.
- 3 Escreva s na fita 3. Cursor 3 para a esquerda.
- 4 Escreva $\triangleright \sqcup$ à esquerda da fita 1, e desloque w para encostar. Fita 1 contém $\triangleright \sqcup w$. Cursor 1 no início do \sqcup mais esquerda.

0000 - 0



Operação

Operação

Simulação de um passo de \mathcal{M} .

Invariantes:

- 1 Fita 1 contém a codificação da fita de \mathcal{M} , com cursor na posição correspondente.

Operação

Simulação de um passo de \mathcal{M} .

Invariantes:

- 1 Fita 1 contém a codificação da fita de \mathcal{M} , com cursor na posição correspondente.
- 2 Fita 2 contém " \mathcal{M} ", cursor à esquerda.

Operação

Simulação de um passo de \mathcal{M} .

Invariantes:

- 1 Fita 1 contém a codificação da fita de \mathcal{M} , com cursor na posição correspondente.
- 2 Fita 2 contém " \mathcal{M} ", cursor à esquerda.
- 3 Fita 3 contém a codificação do estado atual, cursor à esquerda.

O passo:

O passo:

Seja x o conteúdo da fita 3 e y a codificação de caractere começando pelo cursor da fita 1.

O passo:

Handwritten notes:
~ a 0 0 1 1 ~
a 1 0 0 0
~ ~ ~ a 1 0 0 0

Seja x o conteúdo da fita 3 e y a codificação de caractere começando pelo cursor da fita 1.

Procura na fita 2 o texto $\#xy$.

- Se achou, mude o estado registrado na fita 3, conforme a 3ª componente da quádrupla, e opere a fita 1 conforme a 4ª. Volte cursores 2 e 3 para a esquerda.

Handwritten notes:
→ .. a 1 0 0 0
L
~

O passo:

Seja x o conteúdo da fita 3 e y a codificação de caractere começando pelo cursor da fita 1.

Procura na fita 2 o texto $\#xy$.

- Se achou, mude o estado registrado na fita 3, conforme a 3ª componente da quádrupla, e opere a fita 1 conforme a 4ª. Volte cursores 2 e 3 para a esquerda.
- Se não achou, pare. A fita 3 indica um estado de parada de \mathcal{M} .

O passo:

Seja x o conteúdo da fita 3 e y a codificação de caractere começando pelo cursor da fita 1.

Procura na fita 2 o texto $\#xy$.

- Se achou, mude o estado registrado na fita 3, conforme a 3ª componente da quádrupla, e opere a fita 1 conforme a 4ª. Volte cursores 2 e 3 para a esquerda.
- Se não achou, pare. A fita 3 indica um estado de parada de \mathcal{M} .

O passo:

Seja x o conteúdo da fita 3 e y a codificação de caractere começando pelo cursor da fita 1.

Procura na fita 2 o texto $\#xy$.

- Se achou, mude o estado registrado na fita 3, conforme a 3ª componente da quádrupla, e opere a fita 1 conforme a 4ª. Volte cursores 2 e 3 para a esquerda.
- Se não achou, pare. A fita 3 indica um estado de parada de \mathcal{M} .

O invariante claramente se mantém. Assim, \mathcal{U} para com “ x ” na fita 1 sse (\mathcal{M}, w) para com x na fita.

Relembrando

$L \subseteq \Sigma^*$ é:

Relembrando

$L \subseteq \Sigma^*$ é:

Recursiva: se existe uma MT \mathcal{M} que para sempre, computando 0 ou 1, e tal que para todo x , $\mathcal{M}(x) = 1$ sse $x \in L$.

Relembrando

$L \subseteq \Sigma^*$ é:

Recursiva: se existe uma MT \mathcal{M} que para sempre, computando 0 ou 1, e tal que para todo x , $\mathcal{M}(x) = 1$ sse $x \in L$.

Recursivamente enumerável: se existe uma MT \mathcal{M} tal que $L = \{x \mid (\mathcal{M}, x) \text{ para}\}$.

Relembrando

$L \subseteq \Sigma^*$ é:

Recursiva: se existe uma MT \mathcal{M} que para sempre, computando 0 ou 1, e tal que para todo x , $\mathcal{M}(x) = 1$ sse $x \in L$.

Recursivamente enumerável: se existe uma MT \mathcal{M} tal que $L = \{x \mid (\mathcal{M}, x) \text{ para}\}$.

Relembrando

$L \subseteq \Sigma^*$ é:

Recursiva: se existe uma MT \mathcal{M} que para sempre, computando 0 ou 1, e tal que para todo x , $\mathcal{M}(x) = 1$ sse $x \in L$.

Recursivamente enumerável: se existe uma MT \mathcal{M} tal que $L = \{x \mid (\mathcal{M}, x) \text{ para}\}$.

Fato: toda linguagem recursiva é recursivamente enumerável.

Timeout

Timeout

A linguagem $H = \{ \langle M \rangle \langle w \rangle \mid M \text{ é MT, } (M, w) \text{ para} \}$
é semi-decida por \mathcal{U} , logo é recursivamente
enumerável. É recursiva?

Timeout

A linguagem $H = \{ \langle \mathcal{M} \rangle \langle w \rangle \mid \mathcal{M} \text{ é MT, } (\mathcal{M}, w) \text{ para} \}$ é semi-decida por \mathcal{U} , logo é recursivamente enumerável. É recursiva?

Problema: \mathcal{M} pode ficar rodando indefinidamente.

Timeout

A linguagem $H = \{ \langle M \rangle \langle w \rangle \mid M \text{ é MT, } (M, w) \text{ para} \}$ é semi-decida por \mathcal{U} , logo é recursivamente enumerável. É recursiva?

Problema: M pode ficar rodando indefinidamente.

Truque padrão: parar o programa se passar do tempo.

Timeout

A linguagem $H = \{ \langle \mathcal{M} \rangle \langle w \rangle \mid \mathcal{M} \text{ é MT, } (\mathcal{M}, w) \text{ para} \}$ é semi-decida por \mathcal{U} , logo é recursivamente enumerável. É recursiva?

Problema: \mathcal{M} pode ficar rodando indefinidamente.

Truque padrão: parar o programa se passar do tempo.

Prop: A linguagem

$\{ \langle \mathcal{M} \rangle \langle w \rangle, (n)_2 \mid \mathcal{M} \text{ é MT, } n \in \mathbb{N}, (\mathcal{M}, w) \text{ para em até } n \text{ passos} \}$ é recursiva.

Timeout

A linguagem $H = \{ \langle M \rangle \langle w \rangle \mid M \text{ é MT, } (M, w) \text{ para} \}$ é semi-decida por \mathcal{U} , logo é recursivamente enumerável. É recursiva?

Problema: M pode ficar rodando indefinidamente.

Truque padrão: parar o programa se passar do tempo.

Prop: A linguagem

$\{ \langle M \rangle \langle w \rangle, (n)_2 \mid M \text{ é MT, } n \in \mathbb{N}, (M, w) \text{ para em até } n \text{ passos} \}$ é recursiva.

Dem: Modifique \mathcal{U} para contar passos e parar se passou o tempo.

O problema da parada

Desejo: um programa **Para** (Q, x) que, dado o código de um programa Q e uma entrada x para ele, decide se Q pára dada a entrada x , devolvendo 0 ou 1.

O problema da parada

Desejo: um programa **Para** (Q, x) que, dado o código de um programa Q e uma entrada x para ele, decide se Q para dada a entrada x , devolvendo 0 ou 1.

Se existisse, existiria este programa:

```
diagonal ( $Q$ )  
  while Para ( $Q, Q$ );
```

O problema da parada

Desejo: um programa **Para** (Q, x) que, dado o código de um programa Q e uma entrada x para ele, decide se Q para dada a entrada x , devolvendo 0 ou 1.

Se existisse, existiria este programa:

diagonal (Q)

while **Para** (Q, Q);

diagonal (**diagonal**) para?

\rightarrow $\text{Para}(d, d) = 1$
 \leftarrow $\text{Para}(d, d) = 0$

O problema da parada

Formalizando: vamos provar que

$H = \{ \langle M \rangle w \mid M \text{ é MT, } (M, w) \text{ para} \}$
não é recursiva.

O problema da parada

Formalizando: vamos provar que

$H = \{ \langle M \rangle w \mid M \text{ é MT, } (M, w) \text{ para} \}$
não é recursiva.

Se fosse, então

$D = \{ \langle M \rangle \mid (M, \langle M \rangle) \text{ para} \}$
também seria.

$L(M) = D$ *ba?!*

$N: \underline{D} \cup \bar{D} \rightarrow \underline{D} \cup \bar{D}$

O problema da parada

Formalizando: vamos provar que

$H = \{ \text{"M"}w \mid \text{M é MT, } (\text{M}, w) \text{ para} \}$
não é recursiva.

Se fosse, então

$D = \{ \text{"M"} \mid (\text{M}, \text{"M"}) \text{ para} \}$
também seria.

M

Então, o complemento \bar{D} também seria:

$\bar{D} = \{ x \mid x \text{ não codifica MT,} \}$
ou $x = \text{"M"} \text{ e } (\text{M}, x) \text{ não para}$

M̂



O problema da parada

Formalizando: vamos provar que

$H = \{ \text{"M"}w \mid \text{M é MT, } (M, w) \text{ para} \}$
não é recursiva.

Se fosse, então

$D = \{ \text{"M"} \mid (M, \text{"M"}) \text{ para} \}$
também seria.

Então, o complemento \bar{D} também seria:

$\bar{D} = \{ x \mid x \text{ não codifica MT,} \}$
ou $x = \text{"M"} \text{ e } (M, x) \text{ não para}$

Mas \bar{D} nem recursivamente enumerável é!

$\{x \mid (N, x) \text{ para}\}$
 \hookrightarrow
 $\mathcal{L}(N) = \bar{D}$
 $(N, \text{"N"})$
"N" $\in \bar{D}$?
 $\notin \bar{D}$

O problema da parada

Teorema

O problema da parada é indecidível.

O problema da parada

Teorema

O problema da parada é indecidível.

Teorema

A família das linguagens recursivas é subconjunto próprio das recursivamente enumeráveis.

O problema da parada

Teorema

O problema da parada é indecidível.

Teorema

A família das linguagens recursivas é subconjunto próprio das recursivamente enumeráveis.

Teorema

O conjunto das linguagens recursivamente enumeráveis não é fechado por complemento.

Enumeração

Enumeração

Uma linguagem L é **Turing-enumerável** se existe uma MT M com um estado especial **print** tal que

$$L = \{ w \mid (s, \triangleright \underline{\quad}) \vdash_M^* (\text{print}, \triangleright \underline{\quad} w) \}.$$

Teorema

Uma linguagem é Turing-enumerável sse ela for recursivamente enumerável.

km: Blá!

Enumeração

Uma linguagem L é **Turing-enumérável** se existe uma MT M com um estado especial **print** tal que

$$L = \{ w \mid (s, \triangleright \underline{\quad}) \vdash_M^* (\text{print}, \triangleright \underline{\quad} w) \}.$$

Teorema

Uma linguagem é Turing-enumérável sse ela for recursivamente enumerável.

Enumeração

Uma linguagem L é **Turing-enumerável** se existe uma MT M com um estado especial **print** tal que

$$L = \{w \mid (s, \triangleright \underline{\quad}) \vdash_M^* (\text{print}, \triangleright \underline{\quad} w)\}.$$

Teorema

Uma linguagem é Turing-enumerável sse ela for recursivamente enumerável.

Uma linguagem L é **lexicograficamente Turing-enumerável** se existe uma MT que a enumera em ordem lexicográfica.

Teorema

Uma linguagem L é lexicograficamente Turing-enumerável sse for recursiva.

Se L é R.E., então o T.E.

$$M \text{ t.q. } L = \{x \mid (M, x) \text{ para}\}$$

$$M' \quad L = \{x \mid \exists n \text{ } (M, x, n) \text{ para em } \leq n \text{ passos}\}$$

gerar sistematicamente pares (x, n)