# Teoria da Computação

A Tese de Church-Turing

#### Aula 10

Prof. Felipe A. Louza



## Roteiro

- 🚺 Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- 2 A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- Referências

Vamos ver algumas definições alternativas de máquinas de Turing, chamadas de variantes de MTs:

- MTs com mais de uma fita.
- MTs não-determinísticas.

Vamos ver que todas as variantes possuem o mesmo poder computacional:

1

Variantes de MTs podem ser úteis dependendo do problema estudado.

Vamos ver algumas definições alternativas de máquinas de Turing, chamadas de variantes de MTs:

- MTs com mais de uma fita.
- MTs não-determinísticas.

Vamos ver que todas as variantes possuem o mesmo poder computacional:

- Decidem/Reconhecem a mesma classe de linguagens.
- Chamamos esta invariância de robustez

Variantes de MTs podem ser úteis dependendo do problema estudado.

Vamos ver algumas definições alternativas de máquinas de Turing, chamadas de variantes de MTs:

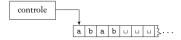
- MTs com mais de uma fita.
- MTs não-determinísticas.

Vamos ver que todas as variantes possuem o mesmo poder computacional:

- Decidem/Reconhecem a mesma classe de linguagens.
- Chamamos esta invariância de robustez.

Variantes de MTs podem ser úteis dependendo do problema estudado.

Por exemplo, no modelo de MT estudado (**MT padrão**), o cursor sempre vai ou para **E** ou para a **D**.



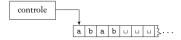
• Vamos propor uma variante que permite que o cursor fique parado.

$$\delta: Q \times \Gamma \to Q \times \Gamma \times \{E, D, P\}$$

- Essa variante permite que as MTs reconheçam linguagens adicionais?
  - A resposta é não

4

Por exemplo, no modelo de MT estudado (**MT padrão**), o cursor sempre vai ou para **E** ou para a **D**.



Vamos propor uma variante que permite que o cursor fique parado.

$$\delta: Q \times \Gamma \to Q \times \Gamma \times \{E, D, P\}$$

- Essa variante permite que as MTs reconheçam linguagens adicionais?
  - A resposta é não.

4

Isso porque podemos "converter" qualquer MT com essa característica para uma **MT padrão**:

• Cada transição  $\delta(q, a) = (p, b, P)$ :

$$\rightarrow q \xrightarrow{a/b, P} p$$

E substituída por um par, com movimentos para a D e para E



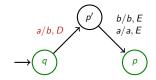
- Logo os dois modelos são equivalentes
  - MT com movimento P → MT padrão; e
    - MT padrão → MT com movimento P (trivial)

Isso porque podemos "converter" qualquer MT com essa característica para uma **MT padrão**:

• Cada transição  $\delta(q, a) = (p, b, P)$ :

$$\rightarrow q$$
  $\xrightarrow{a/b, P} p$ 

• É substituída por um par, com movimentos para a D e para E:



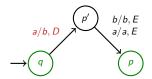
- Logo os dois modelos são equivalentes
  - MT com movimento P → MT padrão; e
  - MT padrão → MT com movimento P (trivial)

Isso porque podemos "converter" qualquer MT com essa característica para uma **MT padrão**:

• Cada transição  $\delta(q, a) = (p, b, P)$ :

$$\longrightarrow q \xrightarrow{a/b, P} p$$

• É substituída por um par, com movimentos para a D e para E:



- Logo os dois modelos são equivalentes.
  - MT com movimento P → MT padrão; e
  - MT padrão → MT com movimento P (trivial).

5

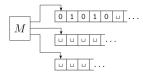
Esse pequeno exemplo mostra a chave para a equivalência entre as variantes de MTs:

• Precisamos mostrar como simular um modelo pelo outro.

## Roteiro

- Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- Referências

Uma MT multifita é como uma MT padrão com k fitas.



- Cada fita tem o seu próprio cursor de leitura/escrita independente.
- Inicialmente,  $w = w_1 w_2 \dots w_n$  aparece na fita 1, e as outras fitas estão em branco.
- A função de transição é redefinida:

$$\delta: Q \times \Gamma^k \to Q \times \Gamma^k \times \{E, D, P\}^k$$

com isso:

$$\delta(q, a_1, a_2, \ldots, a_k) = (p, b_1, b_2, \ldots, b_k, \underbrace{E, D, \ldots, P}_{k})$$

8

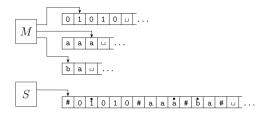
As MTs multifita aparentam ser mais poderosas do que as MTs padrão, mas na verdade não são.

#### Teorema

Toda MT multifita tem uma máquina de Turing padrão que lhe é equivalente.

#### Ideia da Prova:

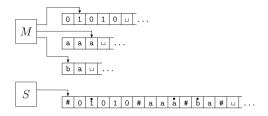
- Mostramos como converter uma MT multifita em uma MT de fita única.
- Seja *M* uma MT multifita e *S* uma MT de fita única.



- Vamos concatenar o conteúdo das k fitas na fita de S com o delimitador  $\# \notin \Gamma$ :
- A posição de cada cursor é representada por um símbolo w (cursores virtuais).

#### Ideia da Prova:

- Mostramos como converter uma MT multifita em uma MT de fita única.
- Seja M uma MT multifita e S uma MT de fita única.



- Vamos concatenar o conteúdo das k fitas na fita de S com o delimitador  $\# \notin \Gamma$ :
- A posição de cada cursor é representada por um símbolo w (cursores virtuais).

## Ideia da Prova (continuação):

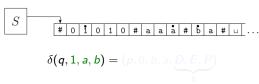
Primeiro colocamos w na fita de S na codificação proposta, isto é:

$$\#\dot{w}_1w_2\ldots w_n\#\dot{\sqcup}\#\dot{\sqcup}\#\ldots\#$$

Para simular

$$\delta(q, a_1, a_2, \ldots, a_k) = (p, b_1, b_2, \ldots, b_k, \underbrace{E, D, \ldots, P}_{k})$$

 A máquina S verifica cada cursor virtual para definir qual transição deve ser aplicada.



## Ideia da Prova (continuação):

Primeiro colocamos w na fita de S na codificação proposta, isto é:

$$\#\dot{w}_1w_2\ldots w_n\#\dot{\sqcup}\#\dot{\sqcup}\#\ldots\#$$

Para simular

$$\delta(q, a_1, a_2, \ldots, a_k) = (p, b_1, b_2, \ldots, b_k, \underbrace{E, D, \ldots, P}_{k})$$

 A máquina S verifica cada cursor virtual para definir qual transição deve ser aplicada.

$$S = \frac{1}{\# 0 \ 1 \ 0 \ 1 \ 0 \ \# \ a \ a \ a \ a \ \# \ b \ a \ \# \ u} \dots$$
$$\delta(q, 1, a, b) = (p, 0, b, a, \underbrace{D, E, P}_{3})$$

## Ideia da Prova (continuação):

Oefinida a transição

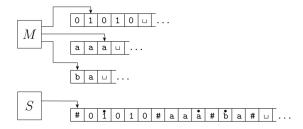
$$\delta(q,1,a,b) = (p,0,b,a,\underbrace{D,E,P}_{k})$$

A máquina S faz uma segunda leitura atualizando a fita.



## Ideia da Prova (continuação):

 Se em algum momento, algum cursor virtual vai parar sobre o i-ésimo #:



- Na fita *i* de *M* ele está em uma posição ⊔.

#### Prova:

- "Sobre a cadeia de entrada  $w = w_1 w_2 \dots w_n$ :
  - Primeiro S (MT padrão) põe sua fita no formato que representa todas as k fitas da MT M.

$$\#\dot{w}_1w_2...w_n\#\dot{\sqcup}\#\dot{\sqcup}\#...\#$$

- ② Para simular um único movimento, S faz uma varredura na sua fita desde o primeiro #, que marca a extremidade esquerda, até o (k+1)-ésimo #, que marca a extremidade direita, de modo a determinar os símbolos sob os cursores virtuais. Então, S faz uma segunda passagem para atualizar as fitas conforme a função de transição de M estabelece.
- Se em algum ponto S move um dos cursores virtuais sobre um #, S desloca o conteúdo da fita, a partir dessa célula até o último #, uma posição para a direita e escreve um símbolo em branco nessa célula da fita. Então ela continua a simulação tal qual anteriormente."

#### Corolário

Uma linguagem é Turing-reconhecível se, e somente se, alguma máquina de Turing multifita a reconhece.

## Roteiro

- Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- 2 A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- Referências

Em uma MT não-determinística, uma computação pode proceder de várias maneiras.

• A função de transição tem a forma:

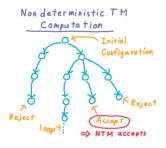
$$\delta: Q \times \Gamma \to 2^{(Q \times \Gamma \times \{L,R\})}$$

ou seja,

$$\delta(\mathbf{q}, \mathbf{a}) = \{(p_i, b_i, \mathbf{D}), (p_i, b_i, \mathbf{E}), \dots\}$$

- Dado um estado e um símbolo de lido:
  - Podemos ir para vários outros estados, escrever diferentes símbolos e mover para diferentes direções.

A computação de uma MT não-determinística é uma árvore cujos ramos correspondem a diferentes computações possíveis.



 A MT não-determinística aceita uma cadeia ✓ se pelo menos um ramo leva ao estado de aceitação.

As MTs não-determinísticas aparentam ser mais poderosas do que as **MTs padrão**, mas na verdade não são.

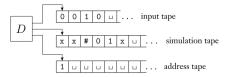
#### Teorema

Toda MT não-determinística tem uma máquina de Turing padrão que lhe é equivalente.

O não-determinísmo não adiciona poder computacional às MTs.

#### Ideia da Prova:

- Mostramos como converter uma MT não-determinística em uma MT multifita.
- Seja N uma MT não-determinística e D uma MT com 3-fitas.



 A MT D simulará todas as possíveis computações não determinísticas.

#### Ideia da Prova:

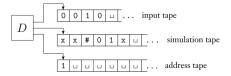
- Mostramos como converter uma MT não-determinística em uma MT multifita.
- Seja N uma MT não-determinística e D uma MT com 3-fitas.



- A MT D simulará todas as possíveis computações não determinísticas.
  - **1** Fita 1: contém a palavra w de entrada  $\leftarrow$  read-only.
  - Fita 2: é a fita de trabalho, mantém uma cópia da fita de N em uma computação de um ramo não-determinístico.
  - Fita 3: guarda a posição de D na árvore de computação.

#### Ideia da Prova:

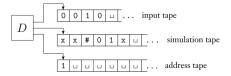
- Mostramos como converter uma MT não-determinística em uma MT multifita.
- Seja N uma MT não-determinística e D uma MT com 3-fitas.



- A MT D simulará todas as possíveis computações não determinísticas.
  - Fita 1: contém a palavra w de entrada  $\leftarrow$  read-only.
  - ② Fita 2: é a fita de trabalho, mantém uma cópia da fita de N em uma computação de um ramo não-determinístico.
  - Fita 3: guarda a posição de D na árvore de computação.

#### <u>Ideia da Prova</u>:

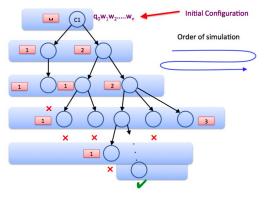
- Mostramos como converter uma MT não-determinística em uma MT multifita.
- Seja N uma MT não-determinística e D uma MT com 3-fitas.



- A MT D simulará todas as possíveis computações não determinísticas.
  - Fita 1: contém a palavra w de entrada  $\leftarrow$  read-only.
  - 2 Fita 2: é a fita de trabalho, mantém uma cópia da fita de *N* em uma computação de um ramo não-determinístico.
  - Sita 3: guarda a posição de D na árvore de computação.

#### Como percorrer a árvore de computações?

Primeiro, vamos enumerar cada nó da árvore: ← nó 2227

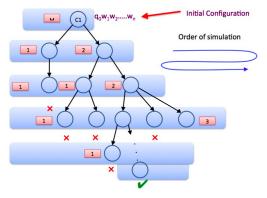


 A MT D simulará cada possível configuração da árvore com uma busca em largura ← nó 223?

Porque busca em profundidade não funciona?

#### Como percorrer a árvore de computações?

Primeiro, vamos enumerar cada nó da árvore: ← nó 222?

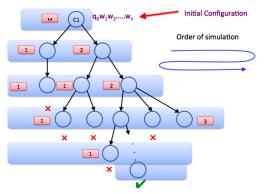


A MT D simulará cada possível configuração da árvore com uma busca em largura ← nó 223?

Porque busca em profundidade não funciona?

#### Como percorrer a árvore de computações?

Primeiro, vamos enumerar cada nó da árvore: ← nó 222?

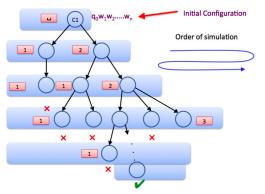


 A MT D simulará cada possível configuração da árvore com uma busca em largura

Porque busca em profundidade não funciona?

#### Como percorrer a árvore de computações?

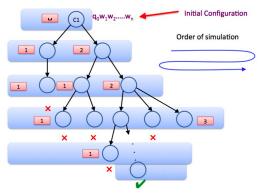
Primeiro, vamos enumerar cada nó da árvore: ← nó 222?



 A MT D simulará cada possível configuração da árvore com uma busca em largura ← nó 223?

#### Como percorrer a árvore de computações?

Primeiro, vamos enumerar cada nó da árvore: ← nó 222?

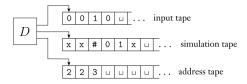


 A MT D simulará cada possível configuração da árvore com uma busca em largura ← nó 223?

Porque busca em profundidade não funciona?

## Ideia da Prova (continuação):

• A 3ª fita indica qual o ramo de computação de *N* estamos simulando atualmente, e utiliza a 2ª fita (de trabalho).



Para simular a busca em largura o endereço é incrementado:

### Ideia da Prova (continuação):

 A 3ª fita indica qual o ramo de computação de N estamos simulando atualmente, e utiliza a 2ª fita (de trabalho).

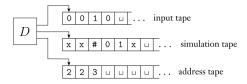


- Para simular a busca em largura o endereço é incrementado:
  - ① Suponha que o número máximo de filhos na árvore é b=3
  - A máquina considera as seguintes configurações

 $1, 2, 3, 11, 12, 13, 21, 22, 23, \ldots, 111, 112, 113, \ldots 221, 222, 223, 231\ldots$ 

### Ideia da Prova (continuação):

 A 3ª fita indica qual o ramo de computação de N estamos simulando atualmente, e utiliza a 2ª fita (de trabalho).



- Para simular a busca em largura o endereço é incrementado:
  - **1** Suponha que o número máximo de filhos na árvore é b=3
  - A máquina considera as seguintes configurações:

 $1,2,3,11,12,13,21,22,23,\dots,111,112,113,\dots 221,222,223,231\dots$ 

### Ideia da Prova (continuação):

• A 3ª fita indica qual o ramo de computação de N estamos simulando atualmente, e utiliza a 2ª fita (de trabalho).

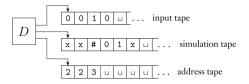


- Para simular a busca em largura o endereço é incrementado:
  - **1** Suponha que o número máximo de filhos na árvore é b = 3
  - A máquina considera as seguintes configurações:

 $1, 2, 3, 11, 12, 13, 21, 22, 23, \dots, 111, 112, 113, \dots 221, 222, 223, 231\dots$ 

### Ideia da Prova (continuação):

 A 3ª fita indica qual o ramo de computação de N estamos simulando atualmente, e utiliza a 2ª fita (de trabalho).

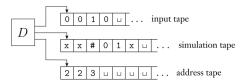


- Para simular a busca em largura o endereço é incrementado:
  - **1** Suponha que o número máximo de filhos na árvore é b = 3
  - A máquina considera as seguintes configurações:

```
1, 2, 3, 11, 12, 13, 21, 22, 23, \ldots, 111, 112, 113, \ldots 221, 222, 223, 231 \ldots
```

### Ideia da Prova (continuação):

 A 3ª fita indica qual o ramo de computação de N estamos simulando atualmente, e utiliza a 2ª fita (de trabalho).

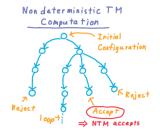


- Para simular a busca em largura o endereço é incrementado:
  - **1** Suponha que o número máximo de filhos na árvore é b = 3
  - A máquina considera as seguintes configurações:

```
1, 2, \textcolor{red}{3}, \textcolor{blue}{11}, \textcolor{blue}{12}, \textcolor{blue}{13}, \textcolor{blue}{21}, \textcolor{blue}{22}, \textcolor{blue}{23}, \ldots, \textcolor{blue}{111}, \textcolor{blue}{112}, \textcolor{blue}{113}, \ldots \textcolor{blue}{221}, \textcolor{blue}{222}, \textcolor{blue}{223}, \textcolor{blue}{231} \ldots
```

### Ideia da Prova (continuação):

 Se em algum momento, um ramo alcança o estado q<sub>aceita</sub>, então a MT D aceita w √.



Caso contrário, D rejeita w e fica em loop (continua a simulação).

#### Prova:

- "Sobre a cadeia de entrada  $w = w_1 w_2 \dots w_n$ :
  - 1 Inicialmente, a fita 1 contém a entrada w e as fitas 2 e 3 estão vazias.
  - 2 Copie a fita 1 para a fita 2.
  - 3 Use a fita 2 para simular N com a entrada w sobre um ramo de sua computação não-determinística. Antes de cada passo de N, consulte o próximo símbolo na fita 3 para determinar qual escolha fazer entre aquelas permitidas pela função de transição de N. Se não restam mais símbolos na fita 3, ou se essa escolha não-determinística for inválida, aborte esse ramo indo para o passo (4). Também vá para o passo (4) se uma configuração de rejeição for encontrada. Se uma configuração de aceitação for encontrada, aceite a entrada ✓.
  - Substitua a cadeia na fita 3 pela próxima cadeia na ordem lexicográfica. Simule o próximo ramo da computação de N indo para o passo (2)."

#### MTs multifita

#### Corolário

Uma linguagem é Turing-reconhecível se, e somente se alguma máquina de Turing não-determinística a reconhece.

### Roteiro

- Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- 2 A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- Referências

Vimos diferentes variantes das **MT-padrão**, todas equivalentes em poder.

- Muitos outros modelos para computação têm sido propostos, alguns similares a MTs, outros nem tanto.
- Todos compartilham a característica essencial das máquinas de Turing:

acesso irrestrito a memória ilimitada

### Todos os modelos com essas caracteríticas são equivalentes em poder<sup>1</sup>.

- Similar ao que vemos entre linguagens de programação
  - Todo programa que pode ser escrito em Python, pode ser escrito em Java, C++, ....
- Esta equivalência entre modelos de computação tem uma implicação profunda para o conceito de "computação":

Muito embora possamos imaginar modelos de computação diferentes, a classe de algoritmos que eles descrevem permanece a mesma.

28

<sup>&</sup>lt;sup>1</sup>Desde que eles não façam coisas absurdas, como executar uma sequência infinita de tarefas em um único passo.

Todos os modelos com essas caracteríticas são equivalentes em poder<sup>1</sup>.

- Similar ao que vemos entre linguagens de programação.
  - Todo programa que pode ser escrito em Python, pode ser escrito em Java, C++, ....
- Esta equivalência entre modelos de computação tem uma implicação profunda para o conceito de "computação":

Muito embora possamos imaginar modelos de computação diferentes, a classe de algoritmos que eles descrevem permanece a mesma.

<sup>&</sup>lt;sup>1</sup>Desde que eles não façam coisas absurdas, como executar uma sequência infinita de tarefas em um único passo.

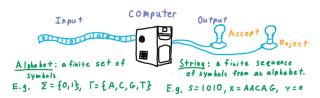
Todos os modelos com essas caracteríticas são equivalentes em poder<sup>1</sup>.

- Similar ao que vemos entre linguagens de programação.
  - Todo programa que pode ser escrito em Python, pode ser escrito em Java, C++, ....
- Esta equivalência entre modelos de computação tem uma implicação profunda para o conceito de "computação":

Muito embora possamos imaginar modelos de computação diferentes, a classe de algoritmos que eles descrevem permanece a mesma.

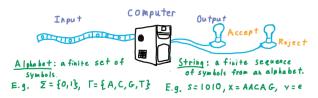
<sup>&</sup>lt;sup>1</sup>Desde que eles não façam coisas absurdas, como executar uma sequência infinita de tarefas em um único passo.

Podemos comparar MTs com os computadores que usamos no dia a dia.



- Embora esses modelos pareçam bem diferentes, eles aceitam a mesma classe de linguagens.
  - Não é difícil ver que um computador pode simular uma MT<sup>2</sup>.
  - Mais interessante é mostrar que uma MT consegue fazer tudo que um computador faz.

Podemos comparar MTs com os computadores que usamos no dia a dia.

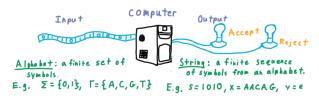


- Embora esses modelos pareçam bem diferentes, eles aceitam a mesma classe de linguagens.
  - Não é difícil ver que um computador pode simular uma MT<sup>2</sup>.
  - Mais interessante é mostrar que uma MT consegue fazer tudo que um computador faz.

29

<sup>&</sup>lt;sup>2</sup>Considerando que a memória do computador é suficientemente grande para todos os problemas (mas não infinita).

Podemos comparar MTs com os computadores que usamos no dia a dia.



- Embora esses modelos pareçam bem diferentes, eles aceitam a mesma classe de linguagens.
  - Não é difícil ver que um computador pode simular uma MT<sup>2</sup>.
  - Mais interessante é mostrar que uma MT consegue fazer tudo que um computador faz.

Considerando que a memória do computador é suficientemente grande para todos os problemas (mas não infinita)

Para isso, vamos definir um modelo de computador:

- Memória:
  - Sequência indefinidamente longa de palavras, cada qual com um endereço.
- Programa:
  - Está armazenado em algumas das palavras da memória;
  - Cada palavra representa uma instrução simples:
    - read, write, load, store, ...
  - Cada instrução envolve um número limitado (finito) de palavras
  - Cada instrução altera o valor de no máximo uma palavra
- Contador de instruções (program counter)
  - Registrador especial que indica a próxima instrução a ser executada

Para isso, vamos definir um modelo de computador:

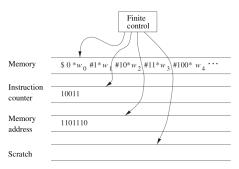
- Memória:
  - Sequência indefinidamente longa de palavras, cada qual com um endereço.
- Programa:
  - Está armazenado em algumas das palavras da memória;
  - Cada palavra representa uma instrução simples:
    - read, write, load, store, ...
  - Cada instrução envolve um número limitado (finito) de palavras
  - Cada instrução altera o valor de no máximo uma palavra
- Contador de instruções (program counter)
  - Registrador especial que indica a próxima instrução a ser executada

Para isso, vamos definir um modelo de computador:

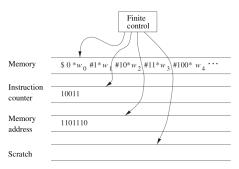
- Memória:
  - Sequência indefinidamente longa de palavras, cada qual com um endereço.
- Programa:
  - Está armazenado em algumas das palavras da memória;
  - Cada palavra representa uma instrução simples:
    - read, write, load, store, ...
  - Cada instrução envolve um número limitado (finito) de palavras
  - Cada instrução altera o valor de no máximo uma palavra
- Ontador de instruções (program counter):
  - Registrador especial que indica a próxima instrução a ser executada.

Para isso, vamos definir um modelo de computador:

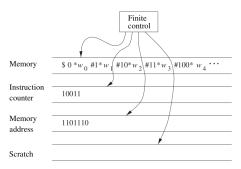
- Memória:
  - Sequência indefinidamente longa de palavras, cada qual com um endereço.
- Programa:
  - Está armazenado em algumas das palavras da memória;
  - Cada palavra representa uma instrução simples:
    - read, write, load, store, ...
  - Cada instrução envolve um número limitado (finito) de palavras
  - Cada instrução altera o valor de no máximo uma palavra
- Ontador de instruções (program counter):
  - Registrador especial que indica a próxima instrução a ser executada.



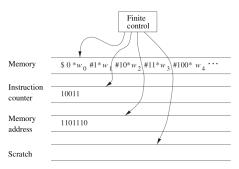
- Ciclo de instruções do computador:
  - A MT procura na fita 1 o local apontado pelo conteúdo da fita 2.
  - ② Interpreta o conteúdo da instrução
  - Se a instrução usa o valor de um endereço, copiamos para a fita 3
  - A MT então executa a instrução usando o rascunho.
  - A MT incrementa o conteúdo da fita 2 e recomeça o ciclo.



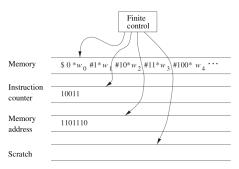
- Ciclo de instruções do computador:
  - A MT procura na fita 1 o local apontado pelo conteúdo da fita 2.
  - 2 Interpreta o conteúdo da instrução.
  - Se a instrução usa o valor de um endereço, copiamos para a fita 3.
  - A MT então executa a instrução usando o rascunho.
  - A MT incrementa o conteúdo da fita 2 e recomeça o ciclo.



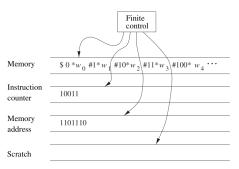
- Ciclo de instruções do computador:
  - A MT procura na fita 1 o local apontado pelo conteúdo da fita 2.
  - Interpreta o conteúdo da instrução.
  - Se a instrução usa o valor de um endereço, copiamos para a fita 3.
  - A MT então executa a instrução usando o rascunho.
  - A MT incrementa o conteúdo da fita 2 e recomeça o ciclo.



- Ciclo de instruções do computador:
  - A MT procura na fita 1 o local apontado pelo conteúdo da fita 2.
  - 2 Interpreta o conteúdo da instrução.
  - 3 Se a instrução usa o valor de um endereço, copiamos para a fita 3.
  - A MT então executa a instrução usando o rascunho.
  - A MT incrementa o conteúdo da fita 2 e recomeça o ciclo.



- Ciclo de instruções do computador:
  - A MT procura na fita 1 o local apontado pelo conteúdo da fita 2.
  - 2 Interpreta o conteúdo da instrução.
  - 3 Se a instrução usa o valor de um endereço, copiamos para a fita 3.
  - A MT então executa a instrução usando o rascunho.
  - A MT incrementa o conteúdo da fita 2 e recomeça o ciclo.



- Ciclo de instruções do computador:
  - A MT procura na fita 1 o local apontado pelo conteúdo da fita 2.
  - 2 Interpreta o conteúdo da instrução.
  - 3 Se a instrução usa o valor de um endereço, copiamos para a fita 3.
  - A MT então executa a instrução usando o rascunho.
  - A MT incrementa o conteúdo da fita 2 e recomeça o ciclo.

Embora a discussão anterior esteja longe de ser uma prova completa e formal, ela deve dar uma idéia de que podemos simular um computador típico em uma **MT**.

 Vamos ver melhor essa relação entre MTs e tudo o que pode ser computável . . . .

### Roteiro

- Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- 3 Referências

## Computação efetiva

Ao longo do curso temos capturado o conceito de "computação efetiva":

- Apresentamos modelos de computação cada vez mais poderosos:
  AFs, APs, MTs.
- Cada modelo é capaz de executar "algoritmos" mais gerais que o modelo anterior.

Mas, o que é um algoritmo?

## Computação efetiva

Ao longo do curso temos capturado o conceito de "computação efetiva":

- Apresentamos modelos de computação cada vez mais poderosos:
  AFs, APs, MTs.
- Cada modelo é capaz de executar "algoritmos" mais gerais que o modelo anterior.

#### Mas, o que é um algoritmo?

- Informalmente: uma sequência finita de instruções simples para realizar uma tarefa.
- Essa idéia de "procedimento" tem sido utilizada há muito tempo na Matemática<sup>3</sup>

<sup>&</sup>lt;sup>3</sup>Ex.: Algoritmo de Euclides para encontrar o máximo divisor comum (300 a.C.)

# Computação efetiva

Ao longo do curso temos capturado o conceito de "computação efetiva":

- Apresentamos modelos de computação cada vez mais poderosos:
  AFs, APs, MTs.
- Cada modelo é capaz de executar "algoritmos" mais gerais que o modelo anterior.

#### Mas, o que é um algoritmo?

- Informalmente: uma sequência finita de instruções simples para realizar uma tarefa.
- Essa idéia de "procedimento" tem sido utilizada há muito tempo na Matemática<sup>3</sup>

3

<sup>&</sup>lt;sup>3</sup>Ex.: Algoritmo de Euclides para encontrar o máximo divisor comum (300 a.C.).

## A definição de algoritmo

Mas qual a definição formal de algoritmo?

- Precisamos deste conceito para podermos saber os limites da computação.
- Essa definição surgiu apenas no século XX.

### Roteiro

- Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- Referências

# Um pouco de história

Em 1900, David Hilbert preferiu a sua agora-famosa palestra no "Congresso Internacional de Matemáticos" em Paris, com <u>23 desafios</u> para o **século XX**.



#### • 10° problema:

escrever "um processo pelo qual possa ser determinado, com um número finito de operações" se um polinômio tem, ou não, raízes inteiras.

### Relembrando...

Um polinômio é uma soma de **termos**, em que cada termo é um produto de certas variáveis com uma constante, chamada de **coeficiente**.

• Exemplo de polinômio:

$$P = \underbrace{6x^3yz^2}_{termo} + 3xy^2 - x^3 - 10$$

- Uma raiz de P é uma valoração das variáveis que torne P=0.
- Para o exemplo acima temos as raízes:

$$x = 5$$
,  $y = 3$  e  $z = 0$ .

 Sabemos que alguns polinômios possuem raízes inteiras, outros não.

Vamos considerar apenas polinômios com coeficientes inteiros.

#### Relembrando...

Um polinômio é uma soma de **termos**, em que cada termo é um produto de certas variáveis com uma constante, chamada de **coeficiente**.

• Exemplo de polinômio:

$$P = \underbrace{6x^3yz^2}_{termo} + 3xy^2 - x^3 - 10$$

- Uma raiz de P é uma valoração das variáveis que torne P = 0.
- Para o exemplo acima temos as raízes:

$$x = 5$$
,  $y = 3$  e  $z = 0$ .

 Sabemos que alguns polinômios possuem raízes inteiras, outros não

Vamos considerar apenas polinômios com coeficientes inteiros.

#### Relembrando...

Um polinômio é uma soma de **termos**, em que cada termo é um produto de certas variáveis com uma constante, chamada de **coeficiente**.

• Exemplo de polinômio:

$$P = \underbrace{6x^3yz^2}_{termo} + 3xy^2 - x^3 - 10$$

- Uma raiz de P é uma valoração das variáveis que torne P = 0.
- Para o exemplo acima temos as raízes:

$$x = 5$$
,  $y = 3$  e  $z = 0$ .

 Sabemos que alguns polinômios possuem raízes inteiras, outros não.

Vamos considerar apenas polinômios com coeficientes inteiros.

#### Voltando ao 10° problema de Hilbert:

escrever "um processo pelo qual possa ser determinado, com um número finito de operações" se um polinômio tem, ou não, raízes inteiras.

- → Hilbert estava interessado em um algoritmo.
- Da maneira com que Hilbert definiu o problema, deu a entender que acreditava que tal algoritmo existia, alguém só precisava encontra-lo.

#### Voltando ao 10° problema de Hilbert:

escrever "um processo pelo qual possa ser determinado, com um número finito de operações" se um polinômio tem, ou não, raízes inteiras.

- → Hilbert estava interessado em um algoritmo.
- Da maneira com que Hilbert definiu o problema, deu a entender que acreditava que tal algoritmo existia, alguém só precisava encontra-lo.

Hoje sabemos que nenhum algoritmo existe para tal tarefa.

• Essa é uma tarefa computacionalmente insolúvel.

Mas para provar esse fato, era preciso uma definição formal do que era um **algoritmo**.

O 10° problema de Hilbert teve que esperar um tempo...

Hoje sabemos que nenhum algoritmo existe para tal tarefa.

• Essa é uma tarefa computacionalmente insolúvel.

Mas para <u>provar esse fato</u>, era preciso uma definição formal do que era um **algoritmo**.

O 10° problema de Hilbert teve que esperar um tempo...

O termo algoritmo teria sido cunhado por Ada Lovalace (1833) muito tempo antes em homenagem ao matemático Al-khwarizmi (820 d.C.).

Hoje sabemos que nenhum algoritmo existe para tal tarefa.

Essa é uma tarefa computacionalmente insolúvel.

Mas para <u>provar esse fato</u>, era preciso uma definição formal do que era um **algoritmo**.

O 10° problema de Hilbert teve que esperar um tempo...

O termo algoritmo teria sido cunhado por Ada Lovalace (1833) muito tempo antes em homenagem ao matemático Al-khwarizmi (820 d.C.).

### Roteiro

- Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- 3 Referências

A definição formal de algoritmo veio apenas em 1936 com os trabalhos de **Alonzo Church** e **Alan Turing**.



- Church propôs um sistema notacional chamado de cálculo- $\lambda$ .
- Turing, por sua vez, formalizou o conceito com suas máquinas.

MTs foram propostas com o nome de **a-machines**, "automatic machines", Church quem as renomeou mais tarde.

Estas duas definições foram demonstradas equivalentes.

• Tudo que um formalismo fazia, o outro também era capaz de fazer.

Essa conexão entre a noção informal e a definição precisa de algoritmo veio ser a chamada de **tese de Church-Turing**.

Noção intuitiva de algoritmos	é igual a	algoritmos de máquina de Turing
----------------------------------	-----------	------------------------------------

"Se uma função é efetivamente computável, então ela é computável por meio de uma máquina de Turing."

A tese de Church-Turing provê a definição de algoritmo necessária para resolver o 10° problema de Hilbert.

• Vamos reformular o problema em termos de linguagens:

$$D = \{p \mid p \text{ \'e um polinômio com raiz inteira}\}$$

• Queremos saber se *D* é **Turing-decidível**?

Ou seja, podemos escrever um **MT** que decide (sempre pára), e aceita  $w \in D \checkmark$  ou rejeita  $w \notin D \checkmark$ .

A tese de Church-Turing provê a definição de algoritmo necessária para resolver o 10° problema de Hilbert.

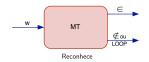
• Vamos reformular o problema em termos de linguagens:

$$D = \{p \mid p \text{ \'e um polinômio com raiz inteira}\}$$

Queremos saber se D é Turing-decidível?

Ou seja, podemos escrever um **MT** que decide (sempre pára), e aceita  $w \in D \checkmark$  ou rejeita  $w \notin D \checkmark$ .

Primeiro, podemos mostrar que a linguagem D é **Turing-reconhecível**:



- Podemos construir uma **MT** *M* que reconhece *D*:
  - "Sobre a cadeia de entrada p:
    - **Q** Calcule o valor de p com cada variável assumindo valores  $0, -1, 1, -2, 2, -3, 3, \dots$  Se em algum ponto o valor de p = 0, aceite a cadeia ✓"
- A máquina não para quando w ∉ D ← Não decide

Exemplo, 
$$p = 6x^3yz^2 + 3xy^2 - x^3 - 10 = 0$$
 quando  $x = ?$ ,  $y = ?$  e  $z = ?$ .

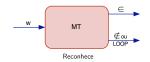
Primeiro, podemos mostrar que a linguagem D é **Turing-reconhecível**:



- Podemos construir uma **MT** *M* que reconhece *D*:
  - "Sobre a cadeia de entrada p:
    - **Q** Calcule o valor de p com cada variável assumindo valores  $0, -1, 1, -2, 2, -3, 3, \dots$  Se em algum ponto o valor de p = 0, aceite a cadeia ✓"
- A máquina não para quando w ∉ D ← Não decide

Exemplo, 
$$p = 6x^3yz^2 + 3xy^2 - x^3 - 10 = 0$$
 quando  $x = 5$ ,  $y = 3$  e  $z = 0$ .

Primeiro, podemos mostrar que a linguagem *D* é **Turing-reconhecível**:



- Podemos construir uma **MT** *M* que reconhece *D*:
  - "Sobre a cadeia de entrada p:
    - **Q** Calcule o valor de p com cada variável assumindo valores  $0, -1, 1, -2, 2, -3, 3, \dots$  Se em algum ponto o valor de p = 0, aceite a cadeia ✓"
- A máquina não para quando  $w \notin D \leftarrow N$ ão decide

Exemplo, 
$$p = 6x^3yz^2 + 3xy^2 - x^3 - 10 = 0$$
 quando  $x = 5$ ,  $y = 3$  e  $z = 0$ .

### Mas será que existe alguma outra MT M' que decide D?

• Não. Provado em 1970 por Matijasevič

Portanto, D é Turing-reconhecível mas não é Turing-decidível.

• Não existe um algoritmo para o problema.

Para o caso em que p possuí apenas 1 variável é possível definir um "critério de parada", então a MT decide D'.

Mas será que existe alguma outra MT M' que decide D?

Não. Provado em 1970 por Matijasevič.

Portanto, D é Turing-reconhecível mas não é Turing-decidível.

• Não existe um algoritmo para o problema.

Para o caso em que  $\rho$  possuí apenas 1 variável é possível definir um "critério de parada", então a MT decide D'.

Mas será que existe alguma outra MT M' que decide D?

• Não. Provado em 1970 por Matijasevič.

Portanto, *D* é **Turing-reconhecível** mas não é **Turing-decidível**.

Não existe um algoritmo para o problema.

Para o caso em que p possuí apenas 1 variável é possível definir um "critério de parada", então a  $\mathbf{MT}$  decide D'.

Mas será que existe alguma outra MT M' que decide D?

• Não. Provado em 1970 por Matijasevič.

Portanto, *D* é **Turing-reconhecível** mas não é **Turing-decidível**.

• Não existe um algoritmo para o problema.

Para o caso em que p possuí apenas 1 variável é possível definir um "critério de parada", então a  $\mathbf{MT}$  decide D'.

**Tese de Church-Turing**: define que tudo que é computável, deve ser computável por **Máquinas de Turing**.

- Não pode ser provada, ela é uma hipótese (ou definição), na verdade.
- No entanto, é universalmente aceita.
  - Nenhuma modificação já proposta para MTs aumenta seu poder
  - Formalismos alternativos como  $\lambda$ -cálculo, sistemas de Post, funções  $\mu$ -recursivas, e outros são todos **Turing-equivalentes**.

Note, entretanto, que para mostrar que a tese é falsa: basta achar uma máquina que compute uma função que uma MT não possa computar.

**Tese de Church-Turing**: define que tudo que é computável, deve ser computável por **Máquinas de Turing**.

- Não pode ser provada, ela é uma hipótese (ou definição), na verdade.
- No entanto, é universalmente aceita.
  - Nenhuma modificação já proposta para MTs aumenta seu poder.
  - Formalismos alternativos como  $\lambda$ -cálculo, sistemas de Post, funções  $\mu$ -recursivas, e outros são todos **Turing-equivalentes**.

Note, entretanto, que para mostrar que a tese é falsa: basta achar uma máquina que compute uma função que uma MT não possa computar.

**Tese de Church-Turing**: define que tudo que é computável, deve ser computável por **Máquinas de Turing**.

- Não pode ser provada, ela é uma hipótese (ou definição), na verdade.
- No entanto, é universalmente aceita.
  - Nenhuma modificação já proposta para MTs aumenta seu poder.
  - Formalismos alternativos como  $\lambda$ -cálculo, sistemas de Post, funções  $\mu$ -recursivas, e outros são todos **Turing-equivalentes**.

Note, entretanto, que para mostrar que a tese é falsa: basta achar uma máquina que compute uma função que uma MT não possa computar.

#### Roteiro

- Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- 3 Referências

#### Vamos mudar de foco no curso para algoritmos e problemas:

- Ao aceitar a tese de Church-Turing, assumimos que a definição de algoritmo é equivalente a algoritmos de máquinas de Turing.
- As linguagens representarão os problemas reais, e
- As MTs serão utilizadas como modelo de computação para executar algoritmos.

Fizemos isso com o 10° problema de Hilbert.

Podemos descrever algoritmos para MTs em 3 níveis.

- Descrição formal: dando os estados e as transições de uma MT.
- ② Descrição da implementação: descrevemos como a máquina opera em termos de movimento de fita.
- Descrição alto nível: pseudocódigo em linguagem natural para descrever o algoritmo, omitindo detalhes de implementação.
  - Em geral, utilizaremos esse nível de descrição.

Vimos exemplos em todos os níveis.

Para apresentar algoritmos em alto nível para MTs, temos que a entrada deve ser sempre uma cadeia<sup>4</sup>.

 Se desejamos fornecer um objeto O para uma MT que não é uma cadeia, primeiro é preciso codificá-lo em uma cadeia (O).

 Se a entrada é um conjunto O<sub>1</sub>, O<sub>2</sub>,..., O<sub>k</sub>, codificamos todos em uma única cadeia (O<sub>1</sub>, O<sub>2</sub>,..., O<sub>k</sub>)

<sup>4</sup>O mesmo acontece em um computador real (dados são armazenados como sequências binárias).

Para apresentar algoritmos em alto nível para **MTs**, temos que a entrada deve ser sempre uma cadeia<sup>4</sup>.

- Se desejamos fornecer um objeto O para uma MT que não é uma cadeia, primeiro é preciso codificá-lo em uma cadeia (O).
  - Exemplos: polinômios, grafos, gramáticas, autômatos,
  - Vamos assumir que as MTs sempre conseguem codificar O em  $\langle O \rangle$
- Se a entrada é um conjunto  $O_1, O_2, \ldots, O_k$ , codificamos todos em uma única cadeia  $\langle O_1, O_2, \ldots, O_k \rangle$

<sup>&</sup>lt;sup>4</sup>O mesmo acontece em um computador real (dados são armazenados como sequências binárias).

Para apresentar algoritmos em alto nível para **MTs**, temos que a entrada deve ser sempre uma cadeia<sup>4</sup>.

- Se desejamos fornecer um objeto O para uma MT que não é uma cadeia, primeiro é preciso codificá-lo em uma cadeia (O).
  - Exemplos: polinômios, grafos, gramáticas, autômatos, ...
  - Vamos assumir que as **MTs** sempre conseguem codificar O em  $\langle O \rangle$
- Se a entrada é um conjunto  $O_1, O_2, \ldots, O_k$ , codificamos todos em uma única cadeia  $\langle O_1, O_2, \ldots, O_k \rangle$

<sup>&</sup>lt;sup>4</sup>O mesmo acontece em um computador real (dados são armazenados como sequências binárias).

Para apresentar algoritmos em alto nível para **MTs**, temos que a entrada deve ser sempre uma cadeia<sup>4</sup>.

- Se desejamos fornecer um objeto O para uma MT que não é uma cadeia, primeiro é preciso codificá-lo em uma cadeia (O).
  - Exemplos: polinômios, grafos, gramáticas, autômatos, ...
  - Vamos assumir que as **MTs** sempre conseguem codificar O em  $\langle O \rangle$ .
- Se a entrada é um conjunto  $O_1,O_2,\ldots,O_k$ , codificamos todos em uma única cadeia  $\langle O_1,O_2,\ldots,O_k \rangle$

<sup>&</sup>lt;sup>4</sup>O mesmo acontece em um computador real (dados são armazenados como sequências binárias).

Para apresentar algoritmos em alto nível para **MTs**, temos que a entrada deve ser sempre uma cadeia<sup>4</sup>.

- Se desejamos fornecer um objeto O para uma MT que não é uma cadeia, primeiro é preciso codificá-lo em uma cadeia (O).
  - Exemplos: polinômios, grafos, gramáticas, autômatos, ...
  - Vamos assumir que as **MTs** sempre conseguem codificar O em  $\langle O \rangle$ .
- Se a entrada é um conjunto  $O_1,O_2,\ldots,O_k$ , codificamos todos em uma única cadeia  $\langle O_1,O_2,\ldots,O_k \rangle$

<sup>&</sup>lt;sup>4</sup>O mesmo acontece em um computador real (dados são armazenados como sequências binárias).

$$A = \{\langle G \rangle | G \text{ \'e um grafo conexo } \}$$

- A linguagem A é Turing-decidível? Isto é, existe uma MT que decide A?
- Como seria a descrição de um alto nível dessa MT? Ou seja, qual seria o algoritmo?

Um grafo é conexo se todo vértice pode ser atingido a partir de qualquer outro vértice seguindo as arestas do grafo.

$$A = \{\langle G \rangle | G \text{ \'e um grafo conexo } \}$$

- A linguagem A é Turing-decidível? Isto é, existe uma MT que decide A?
- Como seria a descrição de um alto nível dessa MT? Ou seja, qual seria o algoritmo?

Um grafo é conexo se todo vértice pode ser atingido a partir de qualquer outro vértice seguindo as arestas do grafo.

$$A = \{\langle G \rangle | G \text{ \'e um grafo conexo } \}$$

- A linguagem A é Turing-decidível? Isto é, existe uma MT que decide A?
- Como seria a descrição de um alto nível dessa MT? Ou seja, qual seria o algoritmo?

Um grafo é conexo se todo vértice pode ser atingido a partir de qualquer outro vértice seguindo as arestas do grafo.

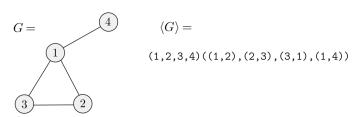
$$A = \{\langle G \rangle | G \text{ \'e um grafo conexo } \}$$

- A linguagem A é Turing-decidível? Isto é, existe uma MT que decide A?
- Como seria a descrição de um alto nível dessa MT? Ou seja, qual seria o algoritmo?

Um grafo é conexo se todo vértice pode ser atingido a partir de qualquer outro vértice seguindo as arestas do grafo.

Primeiro, como *codificar* G em  $\langle G \rangle$ ?

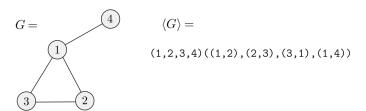
- Um grafo é um par ordenado G = (V, A), onde V é o conjunto de vértices e A o conjunto de arestas.
- Podemos codificar G como uma cadeia de símbolos:



Nos próximos exemplos, assumimos que a MT codifica  $O o \langle O \rangle$ 

Primeiro, como *codificar* G em  $\langle G \rangle$ ?

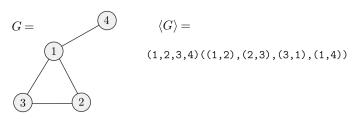
- Um grafo é um par ordenado G = (V, A), onde V é o conjunto de vértices e A o conjunto de arestas.
- Podemos codificar G como uma cadeia de símbolos:



Nos próximos exemplos, assumimos que a MT codifica  $O \rightarrow \langle O \rangle$ .

#### A seguinte **MT** decide *A*:

- "Sobre a cadeia de entrada (G):
  - Selecione o primeiro vértice de G e marque-o.
  - Repita o passo seguinte até que nenhum vértice novo seja marcado.
  - Para cada vértice em G, se ele estiver conectado a um vértice já marcado, marque-o.
  - Verifique todos os vértice de G. Se eles estão todos marcados, aceite a cadeia √; senão, rejeite a cadeia X"



Na próxima aula vamos falar de problemas não computáveis.

"Equivalente a tese de Church-Turing, se não há MT para resolver um problema, então o problema simplesmente não tem solução computacional!"

## Fim

Dúvidas?

### Roteiro

- Variantes de Máquinas de Turing (MT)
  - MTs multifita
  - MTs não-determinísticas
  - MTs e outros modelos
- A definição de Algoritmo
  - Os problemas de Hilbert
  - A tese de Church-Turing
  - Algoritmos e Máquinas de Turing
- Referências

#### Referências

#### Referências:

- "Introdução à Teoria da Computação" de M. Sipser, 2007.
- "Introdução à Teoria de Autômatos, Linguagens e Computação" de J. E. Hopcroft, R. Motwani, e J. D. Ullman, 2003.
- "Linguagens formais e autômatos" de Paulo F. B. Menezes, 2002.
- Materiais adaptados dos slides do Prof. Evandro E. S. Ruiz, da USP.