Classe NP

Esdras Lins Bispo Jr.
bispojr@ufg.br

Teoria da Computação
Bacharelado em Ciência da Computação

17 de agosto de 2017

Plano de Aula

Sumário

1. Revisão
   - Classe P
2. Classe NP

A Classe P

Definição 7.12

P é a classe de linguagens que são decidíveis em tempo polinomial sobre uma máquina de Turing determinística de uma única fita. Em outras palavras

$$\mathbf{P} = \bigcup_k \mathbf{TIME}\left(n^k\right).$$

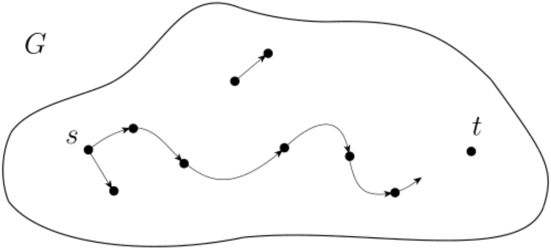
P é importante porque...

- **P** é invariante para todos os modelos de computação polinomialmente equivalentes à máquina de Turing determinística de uma única fita;
- **P** corresponde aproximadamente à classe de problemas que são realisticamente solúveis em um computador.

A Classe P

Problema do caminho em um grafo

$CAM = \{\langle G, s, t\rangle \mid G$ é um grafo direcionado que tem um caminho direcionado de s para $t\}$.



A Classe P

Teorema 7.14

$CAM \in \mathbf{P}$

Prova

$M =$ "Sobre a cadeia de entrada $\langle G, s, t \rangle$ em que G é um grafo direcionado com nós s e t:

1. Ponha uma marca sobre o nó s.
2. Repita o seguinte até que nenhum nó adicional seja marcado:
   1. Faça uma varredura em todas as arestas de G. Se uma aresta (a, b) for encontrada indo de um nó marcado a para um nó não marcado b, marque o nó b.
3. Se t estiver marcado, *aceite*. Caso contrário, *rejeite*.

UFG Regional Jataí

A Classe P

Problema dos números primos entre si

PRIM-ES $= \{\langle x, y \rangle \mid x$ e y são primos entre si $\}$.

Teorema 7.15

PRIM-ES $\in$ **P**

A Classe P

Prova (Parte 1): Algoritmo de Euclides (E)

$E =$ "Sobre a cadeia de entrada $\langle x, y \rangle$ em que x e y são números naturais em binário:

1. Repita até que $y = 0$:
    1. Atribua $x \leftarrow x \bmod y$.
    2. Intercambie x e y.
2. Dê como saída x".

Prova (Parte 2): Máquina de Turing que decide PRIM-ES

$R =$ "Sobre a cadeia de entrada $\langle x, y \rangle$ em que x e y são números naturais em binário:

1. Rode E sobre $\langle x, y \rangle$.
2. Se o resultado for 1, *aceite*. Caso contrário, *rejeite*".

Sumário

Classe NP

Questão

- Tentativas de evitar a força bruta em alguns problemas não têm sido bem sucedidas.

Classe NP

Questão

- Tentativas de evitar a força bruta em alguns problemas não têm sido bem sucedidas.
- Não se sabe se existem algoritmos de tempo polinomial que resolvem determinados problemas.

Classe NP

Questão

- Tentativas de evitar a força bruta em alguns problemas não têm sido bem sucedidas.
- Não se sabe se existem algoritmos de tempo polinomial que resolvem determinados problemas.

Possíveis soluções...

- Os algoritmos polinomiais para estes problemas utilizam técnicas desconhecidas; *ou*

UFG
Regional Jataí

Classe NP

Questão

- Tentativas de evitar a força bruta em alguns problemas não têm sido bem sucedidas.
- Não se sabe se existem algoritmos de tempo polinomial que resolvem determinados problemas.

Possíveis soluções...

- Os algoritmos polinomiais para estes problemas utilizam técnicas desconhecidas; *ou*
- Os algoritmos polinomiais para estes problemas simplesmente **não existem**.

UFG
Regional Jataí

Classe NP

Questão

- Tentativas de evitar a força bruta em alguns problemas não têm sido bem sucedidas.
- Não se sabe se existem algoritmos de tempo polinomial que resolvem determinados problemas.

Possíveis soluções...

- Os algoritmos polinomiais para estes problemas utilizam técnicas desconhecidas; *ou*
- Os algoritmos polinomiais para estes problemas simplesmente **não existem**.

Curioso...

Existe um grupo de problemas deste tipo que, existindo um algoritmo polinomial que resolve um destes problemas, é possível resolver todos os problemas do grupo.

A Classe NP

Problema do caminho hamiltoniano em um grafo

$CAMHAM = \{\langle G, s, t\rangle \mid G$ é um grafo direcionado com um caminho hamiltoniano de s para $t\}$.

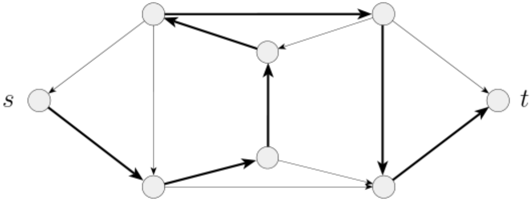


FIGURA **7.17**
Um caminho hamiltoniano passa por todo nó exatamente uma vez

Classe NP

Característica importante

O problema *CAMHAM* tem **verificabilidade polinomial**

Classe NP

Característica importante

O problema *CAMHAM* tem **verificabilidade polinomial**

Outro problema polinomialmente verificável...

$COMPOSTOS = \{x \mid x = pq, \text{ para inteiros } p, q > 1\}$

UFG
Regional Jataí

Classe NP

Característica importante

O problema *CAMHAM* tem **verificabilidade polinomial**

Outro problema polinomialmente verificável...

$COMPOSTOS = \{x \mid x = pq, \text{ para inteiros } p, q > 1\}$

Exemplo

$33 \in COMPOSTOS \therefore$

UFG
Regional Jataí

Classe NP

Característica importante

O problema *CAMHAM* tem **verificabilidade polinomial**

Outro problema polinomialmente verificável...

$COMPOSTOS = \{x \mid x = pq, \text{ para inteiros } p, q > 1\}$

Exemplo

$33 \in COMPOSTOS \therefore$

- $3 \times 11 = 33$
- $3, 11 \in \mathbb{Z}$

Classe NP

Característica importante

O problema *CAMHAM* tem **verificabilidade polinomial**

Outro problema polinomialmente verificável...

$COMPOSTOS = \{x \mid x = pq, \text{ para inteiros } p, q > 1\}$

Exemplo

$33 \in COMPOSTOS \therefore$

- $3 \times 11 = 33$
- $3, 11 \in \mathbb{Z}$

Porém...

Existem problemas que não podem ser verificados em tempo polinomial. Exemplo: $\overline{CAMHAM}$.

Classe NP

Definição 7.18

Um **verificador** para uma linguagem A é um algoritmo V, em que

$$A = \{\omega \mid V \text{ aceita } \langle \omega, c \rangle \text{ para alguma cadeia } c\}.$$

Classe NP

Definição 7.18

Um **verificador** para uma linguagem A é um algoritmo V, em que

$$A = \{\omega \mid V \text{ aceita } \langle \omega, c \rangle \text{ para alguma cadeia } c\}.$$

Detalhes

Medimos o tempo de um verificador somente em termos do comprimento de ω, portanto um **verificador de tempo polinomial** roda em tempo polinomial no comprimento de ω.

UFG
Regional Jataí

Classe NP

Definição 7.18

Um **verificador** para uma linguagem A é um algoritmo V, em que

$$A = \{\omega \mid V \text{ aceita } \langle \omega, c \rangle \text{ para alguma cadeia } c\}.$$

Detalhes

Medimos o tempo de um verificador somente em termos do comprimento de ω, portanto um **verificador de tempo polinomial** roda em tempo polinomial no comprimento de ω.

Nomenclaturas...

Uma linguagem A é **polinomialmente verificável** se ela tem um verificador de tempo polinomial.

Classe NP

Certificado (Prova)

- A informação adicional, representada por c, utilizada por um verificador é chamada de **certificado** (ou prova) da pertinência a uma dada linguagem.

Classe NP

Certificado (Prova)

- A informação adicional, representada por c, utilizada por um verificador é chamada de **certificado** (ou prova) da pertinência a uma dada linguagem.
- Para verificadores polinomiais, o certificado tem comprimento polinomial (no comprimento de ω).

UFG
Regional Jataí

Classe NP

Certificado (Prova)

- A informação adicional, representada por c, utilizada por um verificador é chamada de **certificado** (ou prova) da pertinência a uma dada linguagem.
- Para verificadores polinomiais, o certificado tem comprimento polinomial (no comprimento de ω).

Exemplo

- Um certificado para uma cadeia $\langle G, s, t\rangle \in CAMHAM$ é um caminho hamiltoniano de s a t.

Classe NP

Certificado (Prova)

- A informação adicional, representada por c, utilizada por um verificador é chamada de **certificado** (ou prova) da pertinência a uma dada linguagem.
- Para verificadores polinomiais, o certificado tem comprimento polinomial (no comprimento de ω).

Exemplo

- Um certificado para uma cadeia $\langle G, s, t\rangle \in CAMHAM$ é um caminho hamiltoniano de s a t.
- Um certificado para um número composto $x \in COMPOSTOS$ é um dos seus divisores.

UFG Regional Jataí

Classe NP

Definição 7.19

NP é a classe das linguagens que têm verificadores de tempo polinomial.

Classe NP

Definição 7.19

NP é a classe das linguagens que têm verificadores de tempo polinomial.

Teorema 7.20

Uma linguagem está em **NP** sse ela é decidida por alguma máquina de Turing não-determinística de tempo polinomial.

UFG
Regional Jataí

Classe NP

Definição 7.19

NP é a classe das linguagens que têm verificadores de tempo polinomial.

Teorema 7.20

Uma linguagem está em **NP** sse ela é decidida por alguma máquina de Turing não-determinística de tempo polinomial.

Definição 7.21

NTIME(t(n)) $= \{L \mid L$ é uma linguagem decidida por uma MT não-determinística de tempo $O(t(n))\}$.

UFG
Regional Jataí

Classe NP

Definição 7.19

NP é a classe das linguagens que têm verificadores de tempo polinomial.

Teorema 7.20

Uma linguagem está em **NP** sse ela é decidida por alguma máquina de Turing não-determinística de tempo polinomial.

Definição 7.21

$\mathbf{NTIME(t(n))} = \{L \mid L$ é uma linguagem decidida por uma MT não-determinística de tempo $O(t(n))\}$.

Corolário

$\mathbf{NP} = \bigcup_k \mathbf{NTIME}(n^k)$

Classe NP

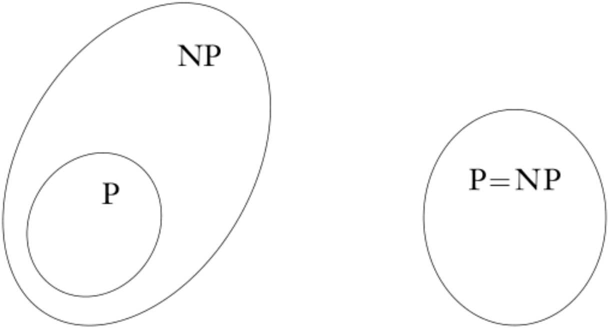


FIGURA 7.26
Uma dessas possibilidades é correta

Classe NP

Esdras Lins Bispo Jr.
bispojr@ufg.br

Teoria da Computação
Bacharelado em Ciência da Computação

17 de agosto de 2017