

Classe NP

Esdras Lins Bispo Jr.
bispojr@ufg.br

Teoria da Computação
Bacharelado em Ciência da Computação

26 de julho de 2016

Plano de Aula

1 Pensamento

2 Revisão

- Classe P
- Classe NP

3 Classe NP

- CLIQUE
- SOMA-SUBC
- P *versus* NP

Sumário

1 Pensamento

2 Revisão

- Classe P
- Classe NP

3 Classe NP

- CLIQUE
- SOMA-SUBC
- P *versus* NP

Pensamento



Pensamento



Frase

A força bruta, quando não é governada pela razão, desmorona sob o seu próprio peso.

Quem?

Quinto Horácio (65 a.C. - 8 a.C.)
Filósofo e poeta romano.

Sumário

1 Pensamento

2 Revisão

- Classe P
- Classe NP

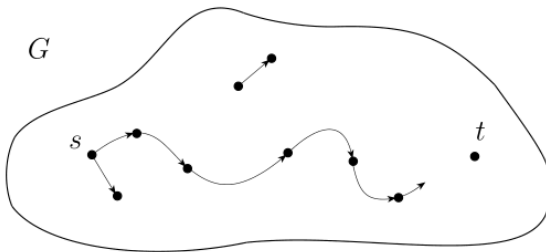
3 Classe NP

- CLIQUE
- SOMA-SUBC
- P *versus* NP

A Classe P

Problema do caminho em um grafo

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



A Classe P

Teorema 7.14

$$CAM \in P$$

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*.

A Classe P

Problema dos números primos entre si

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

Teorema 7.15

$\text{PRIM-ES} \in \mathbf{P}$

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*”.

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.

Sumário

1 Pensamento

2 Revisão

- Classe P
- Classe NP

3 Classe NP

- CLIQUE
- SOMA-SUBC
- P *versus* NP

A Classe NP

Problema do caminho hamiltoniano em um grafo

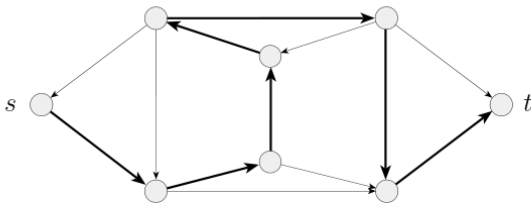
$$CAMHAM = \{\langle G, s, t \rangle \mid G \text{ é um grafo direcionado com um caminho hamiltoniano de } s \text{ para } t\}.$$


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

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

$33 \in \text{COMPOSTOS} \therefore$

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

$33 \in \text{COMPOSTOS} \therefore$

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

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

$33 \in \text{COMPOSTOS} \therefore$

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

Porém...

Existem problemas que não podem ser verificados em tempo polinomial. Exemplo: *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 .

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).

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

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.

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

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

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

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

Corolário

$\text{NP} \cong \bigcup_k \text{NTIME}(n^k)$

A Classe NP

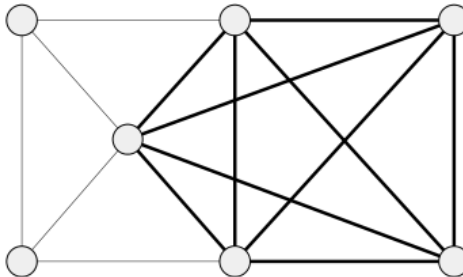
Problema do clique em um grafo

$CLIQUE = \{ \langle G, k \rangle \mid G \text{ é um grafo não-direcionado com um } k\text{-clique} \}$.

A Classe NP

Problema do clique em um grafo

$CLIQUE = \{ \langle G, k \rangle \mid G \text{ é um grafo não-direcionado com um } k\text{-clique} \}$.



A Classe NP

Teorema 7.24

CLIQUE \in NP

A Classe NP

Teorema 7.24

CLIQUE \in NP

Prova (usando o clique c como certificado para V)

V = “Sobre a cadeia de entrada $\langle\langle G, k \rangle, c \rangle$:

- 1 Teste se c é um conjunto de k nós em G ;
- 2 Teste se G contém todas as arestas conectando nós em c ;
- 3 Se ambos os testes retornam positivo, *aceite*. Caso contrário, *rejeite*.

A Classe NP

Teorema 7.24

CLIQUE \in NP

A Classe NP

Teorema 7.24

CLIQUE \in NP

Prova (construindo a MTN M)

M = “Sobre a cadeia de entrada $\langle G, k \rangle$, em que G é um grafo:

- 1 Não-deterministicamente selecione um subconjunto c de k nós de G ;
- 2 Teste se G contém todas as arestas conectando nós em c ;
- 3 Se sim, *aceite*. Caso contrário, *rejeite*.

A Classe NP

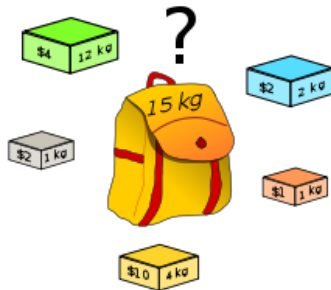
Problema da mochila

$\text{SOMA-SUBC} = \{\langle S, t \rangle \mid S = \{x_1, \dots, x_k\} \text{ e para algum } \{y_1, \dots, y_l\} \subseteq S, \text{ temos } \sum y_i = t\}.$

A Classe NP

Problema da mochila

$\text{SOMA-SUBC} = \{ \langle S, t \rangle \mid S = \{x_1, \dots, x_k\} \text{ e para algum } \{y_1, \dots, y_l\} \subseteq S, \text{ temos } \sum y_i = t \}.$



A Classe NP

Teorema 7.25

$\text{SOMA-SUBC} \in \text{NP}$

A Classe NP

Teorema 7.25

SOMA-SUBC \in NP

Prova (usando um verificador V)

V = “Sobre a entrada $\langle\langle S, t \rangle, c\rangle$:

- 1 Teste se c é uma coleção de números que somam t ;
- 2 Teste se S contém todos os números em c ;
- 3 Se ambos os testes retornam positivo, *aceite*. Caso contrário, *rejeite*.

A Classe NP

Teorema 7.25

$\text{SOMA-SUBC} \in \text{NP}$

A Classe NP

Teorema 7.25

SOMA-SUBC \in NP

Prova (construindo a MTN M)

M = “Sobre a entrada $\langle S, t \rangle$:

- 1 Não-deterministicamente selecione um subconjunto c de números em S ;
- 2 Teste se c é uma coleção de números que somam t ;
- 3 Se sim, *aceite*. Caso contrário, *rejeite*.

P *versus* NP

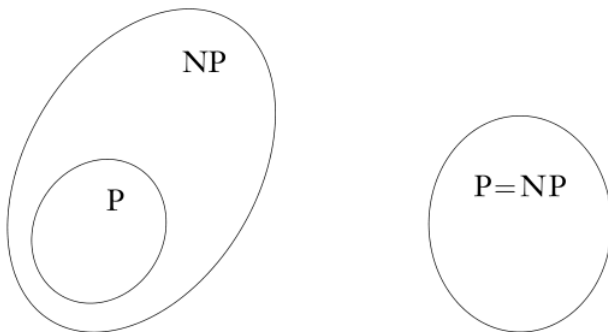


FIGURA 7.26
Uma dessas possibilidades é correta

Classe NP

Esdras Lins Bispo Jr.
bispojr@ufg.br

Teoria da Computação
Bacharelado em Ciência da Computação

26 de julho de 2016