

# Tópicos em Complexidade Computacional

## A Hierarquia Polinomial

**Professor Murilo V. G. da Silva**

Departamento de Informática  
Universidade Federal do Paraná

07/07/2022

# Definição de problemas

Relembrando:

- $CI = \{\langle G, k \rangle : \text{existe um conjunto independente de tamanho } \geq k \text{ em } G\}$

Instâncias verdadeiras de CI:

- $\exists$  conjunto independente de tamanho  $k$  em  $G$
- Concretamente, um certificado para instâncias verdadeiras pode ser um vetor de  $n$  bits com  $k$  bits em 1 indexando vértices de um conjunto independente

O seguinte problema parece ser **mais fácil** ou **mais difícil** que o anterior?

$CI\text{-}EXATO = \{\langle G, k \rangle : \text{o maior conjunto independente de } G \text{ tem tamanho } k\}$

Instâncias verdadeiras de CI-E:

- $\exists$  conjunto de vértices independente de tamanho  $k$  em  $G$
- $\forall$  conjunto de vértices de tamanho  $> k$  em  $G$  não é independente  $G$
- Note: Não parece razoável que exista certificado de tamanho polinomial para instância verdadeira de CI-EXATO.

Mais um problema com “estrutura” parecida:

$MIN\text{-}EQ\text{-}DNF = \{\langle \phi, k \rangle : \exists \text{ fórmula DNF } \psi \text{ de tamanho } \leq k \text{ equivalente a } \phi\}$

Instâncias verdadeiras de MIN-EQ-DNF:

- $\exists$  fórmula DNF  $\psi$  tal que
- $\forall$  valoração  $v$ , temos  $\phi(v) = \psi(v)$

# A classe $\Sigma_2^P$

A classe  $\Sigma_2^P$ : Uma linguagem  $L$  está em  $\Sigma_2^P$  se  $\exists$  MT polinomial  $M_L$  e  $\exists$  polinômio  $q$  tal que

$$\bullet x \in L \iff \exists u_1 \in \{0, 1\}^{q(|x|)} \forall u_2 \in \{0, 1\}^{q(|x|)} M_L(x, u_1, u_2) = 1$$

**Exercício 10.1:** Mostre que  $\text{CI-EXATO} \in \Sigma_2^P$ .

**Exercício 10.2:** Mostre que

- $\bullet \text{NP} \subseteq \Sigma_2^P$
- $\bullet \text{co-NP} \subseteq \Sigma_2^P$

**Teorema 10.3 [Umans (2001)]** O problema é MIN-EQ-DNF  $\Sigma_2^P$ -completo.

Outros problemas em  $\Sigma_2^P$ :

- $\bullet$  Maior clique é exatamente  $k$
- $\bullet$  Menor coloração é exatamente  $k$
- $\bullet$   $\Sigma_2\text{SAT}$ : Dada uma fórmula  $\phi$  em CNF com  $n$  variáveis e dois vetores  $u_1, u_2$  destas variáveis  
Pergunta:  $\exists$  valoração  $v_1$  para variáveis de  $u_1$  e  $\forall$  valoração  $v_2$  das variáveis de  $u_2$ , temos que  $\phi(v_1, v_2) = 1$

# Definição de problemas (cont.)

Do primeiro slide:

$$\text{MIN-EQ-DNF} = \{ \langle \phi, k \rangle : \exists \text{ fórmula DNF } \psi \text{ de tamanho } \leq k \text{ equivalente à } \phi \}$$

Instâncias verdadeiras de MIN-EQ-DNF:

- $\exists$  fórmula DNF  $\psi$
- $\forall$  valoração  $v$ , temos  $\phi(v) = \psi(v)$

Agora considere:

$$\overline{\text{MIN-EQ-DNF}} = \{ \langle \phi, k \rangle : \forall \text{ fórmula DNF } \psi \text{ de tamanho } \leq k \\ \exists \text{ valoração } v \text{ tal que } \phi(v) \neq \psi(v) \}$$

Instâncias verdadeiras de  $\overline{\text{MIN-EQ-DNF}}$ :

- $\forall$  fórmula DNF  $\psi$  de tamanho  $\leq k$
- $\exists$  valoração  $v$  tal que  $\phi(v) \neq \psi(v)$

Para pensar: Que classe de problemas poderíamos incluir  $\overline{\text{MIN-EQ-DNF}}$ ?

# A Hierarquia Polinomial

A classe  $\Sigma_i^P$ : Uma linguagem  $L$  está em  $\Sigma_i^P$  se  $\exists$  MT polinomial  $M_L$  e  $\exists$  polinômio  $q$  tal que

$$\bullet x \in L \iff \exists u_1 \in \{0, 1\}^{q(|x|)} \forall u_2 \in \{0, 1\}^{q(|x|)} \dots Q_i u_i M_L(x, u_1, u_2, \dots, u_i) = 1$$

Note:  $\text{NP} = \Sigma_1^P$ .

A classe  $\Pi_i^P$ : Uma linguagem  $L$  está em  $\Pi_i^P$  se  $\exists$  MT polinomial  $M_L$  e  $\exists$  polinômio  $q$  tal que

$$\bullet x \in L \iff \forall u_1 \in \{0, 1\}^{q(|x|)} \exists u_2 \in \{0, 1\}^{q(|x|)} \dots Q_i u_i M_L(x, u_1, u_2, \dots, u_i) = 1$$

Note:  $\text{coNP} = \Pi_1^P$ . De maneira mais geral,  $\Pi_i^P = \text{co}\Sigma_i^P$ .

A hierarquia polinomial:

$$\text{PH} = \bigcup_{i \geq 1} \Sigma_i^P$$

Obs: Não confundir o Teorema da Hierarquia de Tempo com a Hierarquia Polinomial!

**Lemma 10.4:**  $\Sigma_i^P \subseteq \Pi_{i+1}^P \subseteq \Sigma_{i+2}^P$

**Corolário 10.5:**  $\text{PH} = \bigcup_{i \geq 1} \Pi_i^P$

# A Hierarquia Polinomial

A hierarquia polinomial:

$$PH = \bigcup_{i \geq 1} \Sigma_i^P = \bigcup_{i \geq 1} \Pi_i^P$$

**Definição:**  $\Delta_i^P = \Sigma_i^P \cap \Pi_i^P$ , para  $i \geq 1$ .

**Definição:**  $\Delta_0^P = \Sigma_0^P = \Pi_0^P = P$ .

Generalizando a conjectura de que  $P \neq NP$  e  $NP \neq coNP$ :

- Conjectura de que  $\Sigma_i^P \neq \Sigma_{i+1}^P$
- Conjectura de que  $\Sigma_i^P \neq \Pi_i^P$
- Conjecturas acima referidas como conjecturas de que “a hierarquia não colapsa”

Razão do termo “não colapsa”:

**Teorema 10.6:**

- Para  $i \geq 0$ ,  $\Sigma_i^P = \Sigma_{i+1}^P \implies PH = \Sigma_i^P$
- Para  $i \geq 1$ ,  $\Sigma_i^P = \Pi_i^P \implies PH = \Sigma_i^P$

Faremos a prova do caso particular  $P = NP \implies PH = P$ .

# A Hierarquia Polinomial

## Prova de que $P = NP \Rightarrow PH = P$ :

Suponha que  $P = NP$ . Vamos concluir que  $PH \subseteq P$

- Obs: Como  $P \subseteq PH$ , concluiremos que  $P = PH$
- Estratégia: Mostrar por **indução** que  $\forall i \geq 1$  temos que  $\Sigma_i^P \subseteq P$  e  $\Pi_i^P \subseteq P$ .

Provando por indução:

**Base:**  $i = 1$

- Neste caso, queremos mostrar que  $\Sigma_1^P \subseteq P$  e  $\Pi_1^P \subseteq P$
- Como  $NP = \Sigma_1^P$  e como estamos assumindo  $P = NP$ , é direto que  $\Sigma_1^P \subseteq P$ .
- Como  $coNP = \Pi_1^P$  e como estamos assumindo  $P = NP$  (e consequentemente  $NP = coNP$ ), é direto também que  $\Pi_1^P \subseteq P$ .

**Indução:**

- Suponha que  $\Sigma_{i-1}^P \subseteq P$  e  $\Pi_{i-1}^P \subseteq P$
- Vamos concluir  $\Sigma_i^P \subseteq P$  e  $\Pi_i^P \subseteq P$ .

# A Hierarquia Polinomial

## Prova de que $P = NP \Rightarrow PH = P$ (cont.)

### Indução:

- Suponha que  $\Sigma_{i-1}^P \subseteq P$  e  $\Pi_{i-1}^P \subseteq P$  (\*)
- Vamos concluir  $\Sigma_i^P \subseteq P$  e  $\Pi_i^P \subseteq P$ .  
i.e., queremos  $\forall L \in \Sigma_i^P, L \in P$  e  $\forall L \in \Pi_i^P, L \in P$ .

Seja  $L \in \Sigma_i^P$  (e consequentemente  $\bar{L}$  uma linguagem arbitrária de  $\Pi_i^P$ )

- Então  $\exists$  MT polinomial  $M_L$  e polinômio  $q$  tal que
- $x \in L \Leftrightarrow \exists u_1 \in \{0, 1\}^{q(|x|)} \forall u_2 \in \{0, 1\}^{q(|x|)} \dots Q_i u_i M_L(x, u_1, u_2, \dots, u_i) = 1$

Seja  $L'$  a seguinte linguagem das strings  $\langle x, u_1 \rangle$  tal que

- $\langle x, u_1 \rangle \in L' \Leftrightarrow \forall u_2 \in \{0, 1\}^{q(|x|)} \dots Q_i u_i M_L(x, u_1, u_2, \dots, u_i) = 1$

Por definição,  $L' \in \Pi_{i-1}^P$ . Usando (\*), temos que  $L' \in P$ .

- Logo  $\exists$  MT polinomial  $M'$  tal que  $\langle x, u_1 \rangle \in L' \Leftrightarrow M'(x, u)$

**Ideia chave:**  $M'(x, u)$  é equivalente à  $\forall u_2 \in \{0, 1\}^{q(|x|)} \dots Q_i u_i M_L(x, u_1, u_2, \dots, u_i) = 1$

**Portanto:**  $x \in L \Leftrightarrow \exists u_1 \in \{0, 1\}^{q(|x|)} M'(x, u) \therefore L \in NP$

Como  $P = NP$ , então  $L \in P$ . (Além disso,  $\bar{L} \in \text{coP}$ . Logo  $\bar{L} \in P$ ).

# Colapso, completude de problemas, etc

Terminologia: Diremos que a *hierarquia polinomial colapsa* se  $\exists i$  tal que  $PH = \Sigma_i^P$

Normalmente acredita-se que a hierarquia polinomial não colapsa.

$\Sigma_i$ SAT: Para  $i = 1, 2, \dots$  definimos  $\Sigma_i$ SAT como o problema de determinar se

$$\exists u_1 \forall u_2 \dots Q_i u_i \phi(u_1, u_2, \dots, u_i) = 1 \text{ tal que}$$

- $\phi$  é uma fórmula booleana em CNF
- $u_1, u_2, \dots, u_i$  são vetores booleanos

O problema  $\Pi_i$ SAT é definido de maneira análoga.

**Exercício 10.7:**  $\Sigma_i$ SAT é  $\Sigma_i^P$ -completo  
 $\Pi_i$ SAT é  $\Pi_i^P$ -completo

Observe:  $\Sigma_i$ SAT  $\leq_p$  TQBF e  $\Pi_i$ SAT  $\leq_p$  TQBF

**Teorema 10.8:**  $PH \subseteq PSPACE$

**Prova:** Seja  $L \in PH$ .

- Como  $PH = \Sigma_1^P \cup \Sigma_2^P \cup \Sigma_3^P \cup \dots$ , então  $\exists i$  tal que  $L \in \Sigma_i^P$
- Portanto  $L \leq_p \Sigma_i^P$ SAT  $\therefore L \leq_p$  TQBF  $\therefore L \in PSPACE$

# Colapso, completude de problemas, etc

Vimos que existem problemas completos para cada nível de PH.

- Mas existe problema PH-completo? Provavelmente não:

**Teorema 10.9:** Se existe problema PH-completo, então a hierarquia polinomial colapsa.

**Prova:** Suponha que  $L$  seja PH-completo (em particular, note que  $L \in \text{PH}$ ).

- Então  $\exists i$  tal que  $L \in \Sigma_i^P$ . Seja  $M_L$  a MT da definição de  $\Sigma_i^P$  para  $L$
- Seja  $L' \in \text{PH}$ . Como  $L$  é PH-completo, então existe redução  $R$  de  $L'$  para  $L$
- Então  $L'$  pode ser expresso como problema de  $\Sigma_i^P$ :  
A máquina  $M_{L'}$  é  $M(R(x))$
- Portanto  $\forall L' \in \text{PH}, L' \in \Sigma_i^P. \therefore \text{PH} \subseteq \Sigma_i^P$ .

**Corolário 10.10:** Se  $\text{PH} = \text{PSPACE}$ , então a hierarquia polinomial colapsa.

**Prova:** Se  $\text{PH} = \text{PSPACE}$ , então TQBF é completo para PH. Consequentemente PH colapsa.

# A hierarquia polinomial e Oráculos

Relembrando:

- Dado um problema  $L$  que seja completo para uma classe  $C$
- Escrevemos  $M^C$  para nos referirmos à MTO  $M^L$ 
  - Exemplo: Escrevemos  $M^{NP}$  para nos referirmos à uma MT com oráculo para SAT

Assim,

- $P^{NP}$ : problemas que admitem MTs polinomiais com oráculo para SAT  
Simplificando: MTs polinomiais com oráculo para problemas de NP
- $NP^{NP}$ : problemas que admitem MTNs polin. com oráculo para problemas de NP
- $NP^{NP^{NP}}$ : problemas que admitem MTNs polin. com oráculo para problemas de  $NP^{NP}$   
(obs: ainda não provamos que  $NP^{NP}$  tem problema completo, mas isso é verdade)

**Teorema 10.11:** Para  $i = 1, 2, \dots$ , temos que  $\Sigma_i^P = NP^{\Sigma_{i-1}^P}$