Tópicos em Complexidade Computacional

O Teorema de Ladner

Professor Murilo V. G. da Silva

Departamento de Informática

Universidade Federal do Paraná

17/06/2022

Problemas NP-intermediários

Existe algo em NP que não esteja P, mas que não seja NP-completo?

Teorema 6.1 [Ladner 1975]

Suponha que $\mathrm{P} \neq \mathrm{NP}$. Então existe $L \in \mathrm{NP} \setminus \mathrm{P}$ tal que L não é NP-completa.

Prova: Suponha que $\mathrm{P} \neq \mathrm{NP}$.

- A partir de uma função $H : \mathbb{N} \to \mathbb{N}$, definimos o problema:

$$\mathrm{SAT}_H = \{\llcorner\phi\lrcorner 1^{|\llcorner\phi\lrcorner|^{H(|\llcorner\phi\lrcorner|)}} \ : \ \phi \text{ é fórmula em CNF satisfazível}\}$$

- Vamos definir a seguinte função $H(n)$ específica:
  Caso 1: Se $\exists$ MT M_i, com $i < \log\log n$ tal que
  $\forall x$, $|x| \leq \log n$, a MT $M_i(x) = \mathrm{SAT}_H(x)$ usando no máximo $i|x|^i$ passos
  Então $H(n) = i$, para o menor i possível
  Caso 2: Se $\nexists$ tal MT M_i
  Então $H(n) = \log\log n$
- Note: $\mathrm{SAT}_H \in \mathrm{NP}$ (para a função definida acima)

Prova do Teorema de Ladner (cont.)

Afirmação (A.1)

$\mathrm{SAT}_H \in \mathrm{P} \Rightarrow H(n) = O(1)$

Prova de A.1:

- $\mathrm{SAT}_H \in \mathrm{P} \Rightarrow \exists M_i$ polinomial que resolve qualquer instância de SAT_H (i.e., não resolve apenas instâncias "pequenas" como na def. de $H(n)$)
- Seja c tal que a complexidade de M_i é no máximo $c \cdot n^c$
- Tome M_i tal que $i > c$ (podemos sempre tomar i grande o suficiente)
- Para $n > 2^{2^i}$, a definição de $H(n)$ sempre cai no Caso 1.
- Portanto $n > 2^{2^i}$, $H(n) \leq i \therefore H(n) = O(1)$

Corolário de A.1: $\forall n \; \exists C$ tal que $H(n) \leq C$.

Prova do Teorema de Ladner (cont.)

Afirmação A.2

$H(n) = O(1) \Rightarrow \mathrm{SAT}_H \in \mathrm{P}$

Prova da A.2:

- $H(n) = O(1) \Rightarrow$ a imagem de $H(n)$ é finita
- Portanto $\exists i$ tal que para infinitos valores de n, temos $H(n) = i$ (*)
- Consequência: M_i resolve SAT_H em tempo $i \cdot n^i$
  - Note: se M_i não resolvesse SAT_H, a maquina teria que falhar
  - Neste caso para $n > 2^x$, teríamos $H(n) \neq i$, contradizendo (*)
- Portanto $\mathrm{SAT}_H \in \mathrm{P}$

Corolário da A.2: Se $\mathrm{SAT}_H \in \mathrm{P}$, então $H(n) \to \infty$.

Prova do Teorema de Ladner (cont.)

Lembrando que:

- Estamos supondo que $\mathrm{P} \neq \mathrm{NP}$
- $\mathrm{SAT}_H \in \mathrm{NP}$

Afirmação (A.3)

$$\mathrm{SAT}_H \notin \mathrm{P}$$

Prova de A.3: Suponha que $\mathrm{SAT}_H \in \mathrm{P}$

- Pelo Corolário de A.1, $\exists C$, tal que $H(n) \leq C$
- Portanto SAT_H é "SAT com enchimento polinomial" (enchimento de tamanho no máximo n^C)
- Algoritmo Polinomial para $\mathrm{SAT}_H \Rightarrow$ Algoritmo Polinomial para SAT
- Logo $\mathrm{P} = \mathrm{NP}$. Contradição. $\therefore \mathrm{SAT}_H \notin \mathrm{P}$

Prova do Teorema de Ladner (cont.)

Afirmação (A.4)

SAT_H não é NP-completa.

Prova de A.3: Suponha que SAT_H é NP-Completa.

- Existe redução polinomial R de SAT para SAT_H
  Redução faz $R(\phi) = \phi' \underbrace{11...1}_{|\phi'|^{H(|\phi'|)}}$ em tempo polinomial $O(n^d)$
- De (A.3), temos que $\mathrm{SAT}_H \notin \mathrm{P}$
- Com isso, de (A.2), concluímos que $H(n) \to \infty$
- Portanto, para ϕ sufientemente grande, temos que $|\phi'| < |\phi|$
  (pois $|\phi' 11...1|$ é no máximo $O(n^d)$)
- Em particular, podemos tomar $|\phi'| < \sqrt[3]{|\phi|}$
- Isso implica em algoritmo polinomial para SAT.