P, NP, NP-completude

Henrique Hepp

UFPR

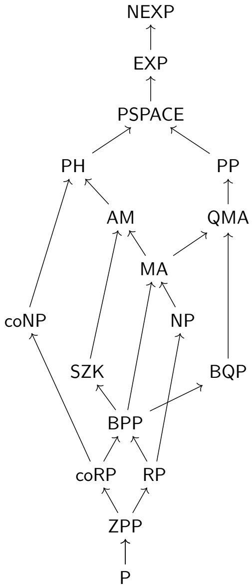
18 de março de 2019

Classe de Complexidade

Conjunto de problemas que podem ser resolvidos com uma máquina abstrata M usando a quantidade $f(n)$ de um recurso, sendo n o tamanho da entrada.

Definição: Problema de Decisão

Uma maquina *decide* uma linguagem $L \subseteq \{0,1\}^*$ se ela computa a função $f_L : \{0,1\}^* \rightarrow \{0,1\}$, onde $f_L(x) = 1 \Leftrightarrow x \in L$


NEXP
EXP
PSPACE
PH
PP
AM
QMA
MA
coNP
NP
SZK
BQP
BPP
coRP
RP
ZPP
P

Classes DTIME e NTIME

Seja $T : \mathbb{N} \rightarrow \mathbb{N}$ uma função, e c uma constante maior que 0.

Definição: Classe DTIME

A linguagem L está em $\mathrm{DTIME}(T(n))$ se existe uma maquina de Turing (MT) que *decide* L em tempo $c \cdot T(n)$.

Definição: Classe NTIME

A linguagem L está em $\mathrm{NTIME}(T(n))$ se existe uma maquina de Turing Não Determinística (MTN) que *decide* L em tempo $c \cdot T(n)$.

- exemplo $\mathrm{DTIME}(n^2)$

- Computação Eficiente = computar em tempo polinomial

Definição: Classe P

$$\mathsf{P} = \bigcup_{c \geqslant 1} \mathsf{DTIME}(n^c)$$

Classe P — Considerações

- P: algoritmos são polinomiais para toda entrada
  - complexidade para o caso médio (cap. 18)
  - soluções aproximadas (cap. 11 e 22)
- Precisão. Maquinas de Turing oferecem precisão limitada para números reais.
  - maquinas de Turing para números reais (cap. 16)
- Aleatoriedade. Maquinas de Turing são determinísticas.
  - BPP (cap. 7).
  - Acredita-se que P $=$ BPP (cap. 19 e 20)
- BQP: generalização de P por meio da computação quântica (cap. 10)
- Problemas de Decisão são limitados

Classe NP (soluções verificadas de modo eficiente)

Definição: Classe NP

$L \subseteq \{0,1\}^* \in \mathrm{NP}$ se existe:

- função polinomial p
- MT M em tempo polinomial (verificador de L)

tal que para todo $x \in \{0,1\}^*$:

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)} \text{ tal que } M(x,u) = 1$$

- Se $M(x,u) = 1$ então u é um *certificado* para x.
- $\mathrm{P} \subseteq \mathrm{NP}$, pois $p(|x|)$ pode ser 0.

Classe NP

Teorema: $\mathsf{NP} = \bigcup_{c \in \mathbb{N}} \mathsf{NTIME}(n^c)$

"verificar deterministicamente" $=$ "decidir não deterministicamente"

Teorema: NP $= \bigcup_{c \in \mathbb{N}}$ NTIME(n^c)

Definição: Classe NP

$L \subseteq \{0,1\}^* \in$ NP se existe:

- função polinomial p
- MT M em tempo polinomial (verificador de L)

tal que para todo $x \in \{0,1\}^*$:

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)} \text{ tal que } M(x,u) = 1$$

Definição: Classe NTIME

Para toda função $T : \mathbb{N} \to \mathbb{N}$ e $L \subseteq \{0,1\}^*$, L está em NTIME$(T(n))$ se existe uma constante $c > 0$ e uma MTN M tal que para todo $x \in \{0,1\}^*$ temos $x \in L \Leftrightarrow M(x) = 1$ em tempo $c \cdot T(n)$.

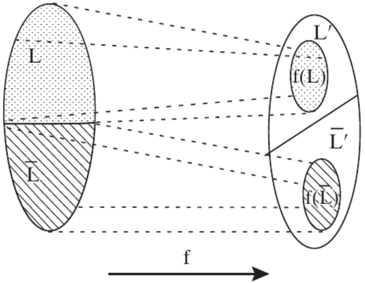
Definição: Redução

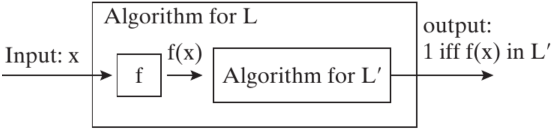
Uma linguagem $L \subseteq \{0,1\}*$ é *karp redutível em tempo polinomial para* $L' \subseteq \{0,1\}^*$, denotada por $L \leqslant_p L'$, se existe uma função computável em tempo polinomial $f : \{0,1\}^* \rightarrow \{0,1\}^*$ tal que para todo $x \in \{0,1\}^*$, $x \in L$ se e somente se $f(x) \in L'$.

Definição: NP-difícil e NP-completo

- L' é NP-*difícil* se $\forall L \in$ NP temos $L \leqslant_p L'$;
- L' é NP-*completo* se L' é NP-difícil e $L' \in$ NP.

Redução de Karp





- Se $L \leqslant_p L'$ e $L' \in \mathrm{P}$ então $L \in \mathrm{P}$

Redução de Karp

Teorema

1. (Transitividade) Se $L \leqslant_p L'$ e $L' \leqslant_p L''$, então $L' \leqslant_p L''$
2. Se L é NP-difícil e $L \in P$, então P = NP
3. Se L é NP-completo, então $L \in P$ se e somente se $P = NP$

Um problema NP-difícil

- TMSAT $= \{\langle \alpha, x, 1^n, 1^t \rangle : \exists u \in \{0,1\}^n$ tal que M_α tem como saída 1 para a entrada $\langle x, u \rangle$ em t passos$\}$, onde M_α denota uma MT determinística representada pela string α.

Teorema: TMSAT é NP-completo

$$\langle \llcorner M \lrcorner, x, 1^{p(|x|), 1^{q(m)}} \rangle \in \text{TMSAT} \Leftrightarrow$$

$$\exists_{u \in \{0,1\}^{p(|x|)}} \text{ tal que } M(x,u) = 1 \text{ em } q(m) \text{ passos } \Leftrightarrow$$

$$x \in L$$