Tópicos em Complexidade Computacional

BPP, RP e coRP

Professor Murilo V. G. da Silva

Departamento de Informática

Universidade Federal do Paraná

07/07/2022

Modelos para computação aleatorizada

Máquina de Turing Probabilística (MTP):

- MT com duas funções de transição δ_1 e δ_2
- A função é escolhida a cada passo de maneira probabilística: $\Pr[\delta_1] = \Pr[\delta_2] = \frac{1}{2}$
- Notação: $M(x)$ usado para a variável aleatória correspondendo à saída de M com x
- Dizemos que M executa em tempo $T(n)$ se ela sempre para em $T(|x|)$ passos **independente das escolhas aleatórias**

Note: Similaridade sintática e diferença semântica entre MTP's e MTN's.

- Em particular, $\Pr[M(x) = 1]$ é a fração dos ramos de aceitação da árvore de computações possíveis de M com x

As classes BPTIME e BPP: Seja $T : \mathbb{N} \to \mathbb{N}$ e L uma linguagem. Dizemos que a MTP M decide L em tempo $T(n)$ se

- M é de tempo $T(n)$ e $\Pr[M(x) = L(x)] \geq \frac{2}{3}$
- $\mathrm{BPTIME}(T(n))$ é a classe de linguagens decidíveis por MTPs em tempo $T(n)$
- $\mathrm{BPP} = \bigcup_c \mathrm{BPTIME}(n^c)$

Importante: Assim como a classe P, na classe BPP estamos lidando com um modelo para **pior caso** (i.e., robusto para qualquer entrada x).

Modelos para computação aleatorizada

BPP (definição alternativa): Uma linguagem L está em BPP se existe **MT** polinomial e polinômio p tal que

- $\forall x \in \{0,1\}$ $\Pr_{r \in_R \{0,1\}^{p(|x|)}}[M(x,r) = L(x)] \geq \frac{2}{3}$

Teorema 12.1: $\mathrm{BPP} \subseteq \mathrm{EXP}$.

Prova: Basta simular árvore de computações possíveis da MTP e contar o número de ramos de aceitação. (Alternativamente, rode a MT para todo r possível).

Acredita-se que $\mathrm{P} = \mathrm{BPP}$, mas isso ainda é um problema aberto.
Exemplos de problemas em BPP:

- Mediana (versão decisão)
- Primalidade
- Emparelhamento perfeito em grafos bipartidos
- Identidade de polinômios (em aberto se pertence a P).

As classes RP e coRP e ZPP

$\mathrm{RTIME}(T(n))$: Uma linguagem L está em $\mathrm{RTIME}(T(n))$ se $\exists$ MTP M de tempo $T(n)$ tal que

- $x \in L \Rightarrow [M(x) = L(x)] \geq \frac{2}{3}$
- $x \notin L \Rightarrow [M(x) \neq L(x)] = 0$

$$\mathrm{RP} = \bigcup_{c>0} RTIME(n^c)$$

Note que $\mathrm{RP} \subseteq \mathrm{BPP}$

Teorema 12.2: $\mathrm{RP} \subseteq \mathrm{NP}$.

Prova: Ramo de aceitação é um certificado para instâncias verdadeiras.

Definição: $\mathrm{coRP} = \{L \ : \ \overline{L} \in \mathrm{RP}\}$.

Note que $\mathrm{coRP} \subseteq \mathrm{BPP}$ e $\mathrm{coRP} \subseteq \mathrm{coNP}$.

Redução de Erro

Observe que se $L \in \mathrm{BPP}$, então existe uma MTP de tempo polinomial M tal que $\forall x$ $\Pr[M(x) = L(x)] \geq \frac{1}{2} + |x|^{-c}$.

Teorema 12.3: Seja L uma linguagem e suponha que existe uma MTP de tempo polinomial M tal que $\forall x$ $\Pr[M(x) = L(x)] \geq \frac{1}{2} + |x|^{-c}$, para alguma constante c. Então para toda constante $d > 0$ existe uma MTP M' de tempo polinomial tal que $\forall x$ $\Pr[M'(x) = L(x)] \geq 1 - 2^{-|x|^d}$.

Prova:Segue a descrição de M':

- M' faz k chamadas para M, onde $k = 8|x|^{2c+d}$
- Sejam $y_1, ..., y_k$ os bits de saída . M' reponde o bit que mais aparece

- Para $i = 1, 2, ..., k$, considere a v.a. X_i tal que
  - $X_i = 1$ se $y_i = L(x)$ $\quad$ $X_i = 0$ se $y_i \neq L(x)$
- Seja $p = \frac{1}{2} + |x|^{-c}$
- Como $X_1, ..., X_k$ são **v.a. indicadoras ind.**, para $i = 1, ..., k$ $E[X_i] = 1 = \Pr[X_i = 1] \geq p$
- Para δ suficientemente pequeno, pelo Limitante de Chernoff:
  - $\Pr[|\sum_{i=1}^{k} X_i - pk| \geq \delta pk] \leq e^{-(\frac{\delta}{4})pk}$
- Note: para $\delta = \frac{|x|^{-c}}{2}$ a máquina M' acerta (pois $\sum X_i \geq pk - \delta pk$)
- Portanto o limite superior para M' errar é $\leq 2^{-|x|^d}$

As classes RP e coRP e ZPP

$\mathrm{ZTIME}(T(n))$: $L \in \mathrm{ZTIME}T(n)$ se existe **MTP** de tempo **esperado** $T(n)$ tal que

- $x \in L \Leftrightarrow M(x) = L(x)$

$$\mathrm{ZPP} = \bigcup_{c>0} ZTIME(n^c)$$

Teorema: $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$