Tópicos em Complexidade Computacional

Provas Interativas

Professor Murilo V. G. da Silva

Departamento de Informática

Universidade Federal do Paraná

07/07/2022

Sistema de prova interativa

Interação entre funções determinísticas:

Sejam $f, g : \{0,1\}^* \to \{0,1\}^*$ funções e $k \geq 0$ inteiro (pode depender do tamanho da entrada).

Uma *interação com k rodadas* (*k-interação*) entre f e g com entrada x, denotada $\langle f, g \rangle(x)$ é uma sequência de strings $a_1, a_2, ..., a_k$ tal que

- $a_1 = f(x)$
- $a_2 = g(x, a_1)$
- $a_3 = f(x, a_1, a_2)$

  $\vdots$
- $a_{2i+1} = f(x, a_1, ..., a2i) \quad 2i < k$
- $a_{2i+2} = g(x, a_1, ..., a_{2i+1}) \quad 2i + 1 < k$

(note que a_k pode ser a_{2i+1} ou a_{2i+2} dependendo da paridade de k

Definimos a saída da interação como: $\mathrm{OUT}_f\langle f, g \rangle(x) = f(x, a_1, ..., a_k)$

Sistema determinístico de prova iterativa:

A linguagem L admite um *sistema determinístico de prova iterativa de k rodadas* se existe MT polinomial V (i.e., uma função) que tem uma k-interação com qualquer função P tal que

Corretude: $x \in L \Rightarrow \exists P \ : \ \mathrm{OUT}_V\langle V, P \rangle(x) = 1$

Completude: $x \notin L \Rightarrow \forall P \ : \ \mathrm{OUT}_V\langle V, P \rangle(x) = 0$

Sistema de prova interativa

A classe dIP: Conjunto de toda linguagem que admite um sistema determinístico de prova interativa de k rodadas tal que $k = poly(|x|)$.

Lema 13.1: $d\mathrm{IP} = \mathrm{NP}$

Prova: Trivialmente, $L \in \mathrm{NP} \Rightarrow L$ admite um sistema de prova de uma rodada.

- Agora seja $L \in d\mathrm{IP}$.
  - Existe uma sistem de prova de $k = poly(n)$ rodadas para L.
  - Seja $(a_1, ..., a_k)$ as mensagens da k-interação. Note que:
  - $x \in L \Rightarrow \exists a_1, ..., a_k$ tal que $V(x, a_1, ..., a_k) = 1$
  - $x \notin L \Rightarrow \forall a_1, ..., a_k$ tal que $V(x, a_1, ..., a_k) = 0$
- Apresentaremos um verif. polinomial V_L e concluir que L está em NP: certif. $(a_1...a_k)$
- V_L testa se: $V(x) = a_1$, $V(x, a_1, a_2) = a_3$, ... , $V(x, a_1, ..., a_k) = 1$
- Note que se $x \in L$, $\exists c = a_1, ..., a_k$ tal que $V(x, c) = 1$
- Provando que $x \notin L$, $\forall c = a_1, ..., a_k$ tal que $V(x, c) = 0$ (usando contrapositiva):
  - $\exists(a_1, ..., a_k)$, mostramos que $\exists P$, **definindo** P, tal que $P(x, a_1)$, $P(x, a_1, a_2, a_3)$,...
  - Ou seja, um sistema de provas tal que $\mathrm{OUT}_V\langle V, P\rangle(x) = 1$
  - Isso implica que $x \in L$.

Sistema de prova interativa

Modelo para interação entre funções (com verificador probabilístico):

Sejam $f, g : \{0,1\}^* \to \{0,1\}^*$ funções e $k \geq 0$ inteiro (pode depender do tamanho da entrada).

Uma *interação com k rodadas* (*k-interação*) entre f e g com entrada x, denotada $\langle f, g \rangle(x)$ é uma sequência de strings $a_1, a_2, ..., a_k$ tal que

- $a_1 = f(x, r)$
- $a_2 = g(x, a_1)$
- $a_3 = f(x, r, a_1, a_2)$

  $\vdots$
- $a_{2i+1} = f(x, x, a_1, ..., a2i) \quad 2i < k$
- $a_{2i+2} = g(x, a_1, ..., a_{2i+1}) \quad 2i + 1 < k$

Definimos a saída da interação como: $\mathrm{OUT}_f\langle f, g \rangle(x) = f(x, r, a_1, ..., a_k)$

Observe que a **interação (e a saída)** é uma v.a. sobre $r \in_R \{0,1\}^m$

Sistema de prova iterativa (com verificador probabilístico):

A linguagem L admite um *sistema de prova iterativa de k rodadas* se existe MTP polinomial V que tem uma k-interação com qualquer função P tal que

Corretude: $x \in L \Rightarrow \exists P \ : \ \Pr[\mathrm{OUT}_V\langle V, P \rangle(x) = 1] \geq 2/3$

Completude: $x \notin L \Rightarrow \forall P \ : \ \Pr[\mathrm{OUT}_V\langle V, P \rangle(x) = 0] \leq 1/3$

Sistema de prova interativa

As classes $\mathrm{IP}[k]$: Linguagens que admitem um sistema de prova interativo de k rodadas.

A classe IP:

$$\mathrm{IP} = \bigcup_{c \geq 1} \mathrm{IP}[n^c]$$

Lema 13.2: As probabilidades da definição de sistema de prova iterativo podem ser alteradas (sem que as classes $\mathrm{IP}[k]$ e IP se alterem) da seguinte maneira

- De $2/3$ para $1 - 2^{-n^s}$
- De $1/3$ 2^{-n^s}

para qualquer constante $s > 0$.

Sistema de prova interativa para GNI

Dados dois grafos G_0 e G_1, queremos saber se eles **não são isomorfos**

- Obs: Sabemos que GI está em NP (o isomorfismo é o certificado)
- Mas não sabemos se GNI está em NP

Protocolo (de moeda privada) para GNI:

- V: Escolha bit aleatório i; Permute os vértices de G_i e obtenha H; Envie H para P
- P: identifica se $H \cong G_1$ ou $H \cong G_2$; Seja G_j tal grafo; Envie j para V
- V: Aceita se $i = j$ (cc. rejeita)

- Se $G_0 \ncong G_1$, V aceita com prob. 1
- Se $G_0 \cong G_1$, V aceita com prob. $1/2$

Protocolo Final: Rode duas vezes (em paralelo) o protocolo acima