

La existencia de FPRAS y las reducciones parsimoniosas

Sean $f, g : \Sigma^* \rightarrow \mathbb{N}$ dos funciones en $\#P$

Teorema

Si $f \leq_{par}^p g$ y existe un FPRAS para g , entonces existe un FPRAS para f

La existencia de FPRAS y las reducciones parsimoniosas

Sean $f, g : \Sigma^* \rightarrow \mathbb{N}$ dos funciones en $\#P$

Teorema

Si $f \leq_{par}^p g$ y existe un FPRAS para g , entonces existe un FPRAS para f

Demostración: Suponga que $h : \Sigma^* \rightarrow \Sigma^*$ es una función computable en tiempo polinomial tal que $f(w) = g(h(w))$ para todo $w \in \Sigma^*$

La existencia de FPRAS y las reducciones parsimoniosas

Además, suponga que $\mathcal{A}$ es un FPRAS para g , y defina un algoritmo aleatorizado $\mathcal{B} : \Sigma^* \times \mathbb{R}^+ \rightarrow \mathbb{N}$ de la siguiente forma:

Para cada $w \in \Sigma^*$ y $\varepsilon \in \mathbb{R}^+$: $\mathcal{B}(w, \varepsilon) = \mathcal{A}(h(w), \varepsilon)$

La existencia de FPRAS y las reducciones parsimoniosas

Además, suponga que $\mathcal{A}$ es un FPRAS para g , y defina un algoritmo aleatorizado $\mathcal{B} : \Sigma^* \times \mathbb{R}^+ \rightarrow \mathbb{N}$ de la siguiente forma:

Para cada $w \in \Sigma^*$ y $\varepsilon \in \mathbb{R}^+$: $\mathcal{B}(w, \varepsilon) = \mathcal{A}(h(w), \varepsilon)$

Para cada $w \in \Sigma^*$ y $\varepsilon \in \mathbb{R}^+$:

$$\begin{aligned} \Pr\left(|\mathcal{B}(w, \varepsilon) - f(w)| \leq \varepsilon \cdot f(w)\right) \\ &= \Pr\left(|\mathcal{A}(h(w), \varepsilon) - g(h(w))| \leq \varepsilon \cdot g(h(w))\right) \\ &\geq \frac{3}{4} \end{aligned}$$

La existencia de FPRAS y las reducciones parsimoniosas

Además, suponga que $\mathcal{A}$ es un FPRAS para g , y defina un algoritmo aleatorizado $\mathcal{B} : \Sigma^* \times \mathbb{R}^+ \rightarrow \mathbb{N}$ de la siguiente forma:

Para cada $w \in \Sigma^*$ y $\varepsilon \in \mathbb{R}^+$: $\mathcal{B}(w, \varepsilon) = \mathcal{A}(h(w), \varepsilon)$

Para cada $w \in \Sigma^*$ y $\varepsilon \in \mathbb{R}^+$:

$$\begin{aligned} \Pr\left(|\mathcal{B}(w, \varepsilon) - f(w)| \leq \varepsilon \cdot f(w)\right) \\ &= \Pr\left(|\mathcal{A}(h(w), \varepsilon) - g(h(w))| \leq \varepsilon \cdot g(h(w))\right) \\ &\geq \frac{3}{4} \end{aligned}$$

Por lo tanto $\mathcal{B}$ es un FPRAS para f



Utilizando las reducciones parsimoniosas

Suponiendo que $f \leq_{par}^p g$, el resultado anterior puede utilizarse de dos formas:

- ▶ Si tenemos un FPRAS para g , entonces podemos construir un FPRAS para f
- ▶ Si tenemos una demostración que no existe un FPRAS para f , entonces concluimos que no existe un FPRAS para g

Utilizando las reducciones parsimoniosas

Suponiendo que $f \leq_{par}^p g$, el resultado anterior puede utilizarse de dos formas:

- ▶ Si tenemos un FPRAS para g , entonces podemos construir un FPRAS para f
- ▶ Si tenemos una demostración que no existe un FPRAS para f , entonces concluimos que no existe un FPRAS para g

Vamos a encontrar otras funciones que no admiten FPRAS utilizando el resultado anterior.

Contando el número de cliques

Dado un grafo $G = (N, A)$, decimos que $S \subseteq N$ es un clique si para cada $a, b \in S$ se tiene que $(a, b) \in A$

Sea $\# \text{CLIQUE}$ una función que, dado un grafo G , retorna el número de cliques de G

Contando el número de cliques

Dado un grafo $G = (N, A)$, decimos que $S \subseteq N$ es un clique si para cada $a, b \in S$ se tiene que $(a, b) \in A$

Sea $\#CLIQUE$ una función que, dado un grafo G , retorna el número de cliques de G

Teorema

Si existe un FPRAS para $\#CLIQUE$, entonces $NP \subseteq BPP$

No existe un FPRAS para $\#$ CLIQUE: demostración

Dado un grafo $G = (N, A)$, defina $\overline{G} = (N, \overline{A})$ con $\overline{A} = (N \times N) \setminus A$

No existe un FPRAS para $\# \text{CLIQUE}$: demostración

Dado un grafo $G = (N, A)$, defina $\overline{G} = (N, \overline{A})$ con $\overline{A} = (N \times N) \setminus A$

Tenemos que $\# \text{IS}(G) = \# \text{CLIQUE}(\overline{G})$

No existe un FPRAS para #CLIQUE: demostración

Dado un grafo $G = (N, A)$, defina $\overline{G} = (N, \overline{A})$ con $\overline{A} = (N \times N) \setminus A$

Tenemos que $\#IS(G) = \#CLIQUE(\overline{G})$

Concluimos que $\#IS \leq_{par}^p \#CLIQUE$

- ▶ Por lo tanto, si existe un FPRAS para #CLIQUE, entonces existe un FPRAS para #IS y $NP \subseteq BPP$ □

Otro ejemplo: las cláusulas de Horn

Recuerde que una cláusula se dice de Horn si contiene a lo más un literal positivo.

Ejemplo

$(p \vee \neg q \vee \neg r)$, p , $(\neg q \vee \neg r)$ y $\neg q$ son cláusulas de Horn, mientras que $(p \vee q)$ y $(p \vee \neg q \vee r \vee \neg s)$ no lo son.

Además, decimos que una fórmula proposicional φ es de Horn si φ es una conjunción de cláusulas de Horn.

La función #HORN-SAT

Sea #HORN-SAT una función que, dada una fórmula proposicional φ de Horn, retorna el número de valuaciones que satisfacen φ

La función $\#HORN-SAT$

Sea $\#HORN-SAT$ una función que, dada una fórmula proposicional φ de Horn, retorna el número de valuaciones que satisfacen φ

Teorema

$\#HORN-SAT$ es $\#P$ -completo.

La función $\#HORN-SAT$

Sea $\#HORN-SAT$ una función que, dada una fórmula proposicional φ de Horn, retorna el número de valuaciones que satisfacen φ

Teorema

$\#HORN-SAT$ es $\#P$ -completo.

Ejercicio

Demuestre que $L_{\#HORN-SAT} \in PTIME$

No existe un FPRAS para $\#HORN-SAT$

No existe un FPRAS para $\#HORN-SAT$

Teorema

Si existe un FPRAS para $\#HORN-SAT$, entonces $NP \subseteq BPP$

No existe un FPRAS para $\#HORN-SAT$

Teorema

Si existe un FPRAS para $\#HORN-SAT$, entonces $NP \subseteq BPP$

Demostración: Sea $G = (N, A)$ un grafo tal que $N \neq \emptyset$

No existe un FPRAS para #HORN-SAT

Teorema

Si existe un FPRAS para #HORN-SAT, entonces $NP \subseteq BPP$

Demostración: Sea $G = (N, A)$ un grafo tal que $N \neq \emptyset$

Por cada $v \in N$, considere una variable proposicional x_v , y defina φ_G como la siguiente fórmula proposicional:

$$\left(\bigwedge_{a \in N} (x_a \vee \neg x_a) \right) \wedge \left(\bigwedge_{(b,c) \in A} (\neg x_b \vee \neg x_c) \right)$$

No existe un FPRAS para $\# \text{HORN-SAT}$: demostración

Tenemos que φ_G es una fórmula proposicional de Horn
y $\# \text{IS}(G) = \# \text{HORN-SAT}(\varphi_G)$

- ▶ ¿Cómo se puede extraer un conjunto independiente de G desde una valuación que satisface φ_G ?

No existe un FPRAS para $\# \text{HORN-SAT}$: demostración

Tenemos que φ_G es una fórmula proposicional de Horn
y $\# \text{IS}(G) = \# \text{HORN-SAT}(\varphi_G)$

- ▶ ¿Cómo se puede extraer un conjunto independiente de G desde una valuación que satisface φ_G ?

Concluimos que $\# \text{IS} \leq_{par}^p \# \text{HORN-SAT}$

- ▶ ¿Cómo se maneja el caso en que $N = \emptyset$ en la reducción?

No existe un FPRAS para $\# \text{HORN-SAT}$: demostración

Tenemos que φ_G es una fórmula proposicional de Horn
y $\# \text{IS}(G) = \# \text{HORN-SAT}(\varphi_G)$

- ▶ ¿Cómo se puede extraer un conjunto independiente de G desde una valuación que satisface φ_G ?

Concluimos que $\# \text{IS} \leq_{par}^p \# \text{HORN-SAT}$

- ▶ ¿Cómo se maneja el caso en que $N = \emptyset$ en la reducción?

Por lo tanto, si existe un FPRAS para $\# \text{HORN-SAT}$, entonces existe un FPRAS para $\# \text{IS}$ y $\text{NP} \subseteq \text{BPP}$ □