

Un teorema fundamental

Tenemos los ingredientes necesarios para demostrar el último teorema de este capítulo.

Teorema (Schöning)

$$NP \cap co-AM \subseteq L_2^P$$

Demostración del teorema

Consideramos lenguajes sobre el alfabeto $\{0, 1\}$

- ▶ Es simple extender la demostración para un alfabeto arbitrario Σ

Demostración del teorema

Consideramos lenguajes sobre el alfabeto $\{0, 1\}$

- ▶ Es simple extender la demostración para un alfabeto arbitrario Σ

Sea $A \in \text{NP} \cap \text{co-AM}$

Demostración del teorema

Consideramos lenguajes sobre el alfabeto $\{0, 1\}$

- Es simple extender la demostración para un alfabeto arbitrario Σ

Sea $A \in \text{NP} \cap \text{co-AM}$

Tenemos que demostrar que $A \in L_2^P$, vale decir:

$$\Sigma_2^P(A) = \Sigma_2^P$$

Demostración del teorema

Sea $L \in \Sigma_2^P(A)$

- ▶ Tenemos que demostrar que $L \in \Sigma_2^P$

Demostración del teorema

Sea $L \in \Sigma_2^P(A)$

- Tenemos que demostrar que $L \in \Sigma_2^P$

Dado que $\bar{A} \in \text{AM}$, por el lema de amplificación para AM existe una MT probabilística no determinista M_1 tal que M_1 funciona en tiempo polinomial y para cada $w \in \{0, 1\}^n$:

$$\Pr_s(M_1(w, s) \text{ es incorrecto}) \leq \frac{1}{2^{2n+1}}$$

Demostración del teorema

Sea $L \in \Sigma_2^P(A)$

- Tenemos que demostrar que $L \in \Sigma_2^P$

Dado que $\bar{A} \in \text{AM}$, por el lema de amplificación para AM existe una MT probabilística no determinista M_1 tal que M_1 funciona en tiempo polinomial y para cada $w \in \{0, 1\}^n$:

$$\Pr_s(M_1(w, s) \text{ es incorrecto}) \leq \frac{1}{2^{2n+1}}$$

Podemos reescribir la probabilidad de error de la siguiente forma:

$$\Pr_s((w \in \bar{A} \wedge M_1(w, s) \text{ no acepta}) \vee$$

$$(w \notin \bar{A} \wedge M_1(w, s) \text{ acepta})) \leq \frac{1}{2^{2n+1}}$$

Demostración del teorema

Vamos a extender el resultado anterior para todos los strings de un cierto largo.

Notación

- ▶ Dado $X \subseteq \{0, 1\}^*$ y $n \in \mathbb{N}$, definimos $X_{=n} = \{x \in X \mid |x| = n\}$
- ▶ Definimos $L(M_1, s) = \{w \in \{0, 1\}^* \mid M_1(w, s) \text{ acepta}\}$

Demostración del teorema

Tenemos que:

$$\begin{aligned} \Pr_s(\bar{A}_{=n} \neq L(M_1, s)_{=n}) &= \Pr_s(\exists w \in \{0, 1\}^n : ((w \in \bar{A} \wedge w \notin L(M_1, s)) \vee \\ &\quad (w \notin \bar{A} \wedge w \in L(M_1, s)))) \\ &= \Pr_s(\exists w \in \{0, 1\}^n : ((w \in \bar{A} \wedge M_1(w, s) \text{ no acepta}) \vee \\ &\quad (w \notin \bar{A} \wedge M_1(w, s) \text{ acepta}))) \\ &\leq \sum_{w \in \{0, 1\}^n} \Pr_s((w \in \bar{A} \wedge M_1(w, s) \text{ no acepta}) \vee \\ &\quad (w \notin \bar{A} \wedge M_1(w, s) \text{ acepta})) \\ &\leq \sum_{w \in \{0, 1\}^n} \frac{1}{2^{2n+1}} = 2^n \frac{1}{2^{2n+1}} = \frac{1}{2^{n+1}} < \frac{1}{2^n} \end{aligned}$$

Demostración del teorema

Sea $p(n) = t_{M_1}(n)$

- ▶ $p(n)$ es un polinomio, suponemos que $p(n)$ es $\Omega(n)$

Demostración del teorema

Sea $p(n) = t_{M_1}(n)$

- ▶ $p(n)$ es un polinomio, suponemos que $p(n)$ es $\Omega(n)$

Sea $B_n = \{s \in \{0, 1\}^{p(n)} \mid \overline{A}_{=n} = L(M_1, s)_{=n}\}$

Demostración del teorema

Sea $p(n) = t_{M_1}(n)$

- $p(n)$ es un polinomio, suponemos que $p(n)$ es $\Omega(n)$

Sea $B_n = \{s \in \{0, 1\}^{p(n)} \mid \overline{A}_{=n} = L(M_1, s)_{=n}\}$

Del resultado en la transparencia anterior concluimos que:

$$|B_n| > \left(1 - \frac{1}{2^n}\right) 2^{p(n)}$$

Demostración del teorema

$A \in NP$: existe una MT no determinista M_2 tal que M_2 funciona en tiempo polinomial y $A = L(M_2)$

Demostración del teorema

$A \in NP$: existe una MT no determinista M_2 tal que M_2 funciona en tiempo polinomial y $A = L(M_2)$

$L \in \Sigma_2^P(A)$: existe una MT determinista M_3^A y un polinomio $q(n)$ tales que M_3^A funciona en tiempo polinomial, M_3^A tiene un oráculo para A y para todo $w \in \{0, 1\}^*$:

$w \in L$ si y sólo si $\exists y \in \{0, 1\}^{q(|w|)} \forall z \in \{0, 1\}^{q(|w|)} : M_3^A$ acepta (w, y, z)

Demostración del teorema

Suponemos que $q(n)$ es $\Omega(n)$

Demostración del teorema

Suponemos que $q(n)$ es $\Omega(n)$

Además, suponemos que existe un polinomio $r(n)$ tal que cada llamada al oráculo A de M_3^A con entrada (w, y, z) utiliza strings en la cinta de consulta de largo $r(|w|)$

- ▶ ¿Por qué podemos suponer esto? ¿Deberíamos tener $r(|w|, |y|, |z|)$ en lugar de $r(|w|)$?
- ▶ La demostración también puede realizarse sin este supuesto

Demostración del teorema

Suponemos que $q(n)$ es $\Omega(n)$

Además, suponemos que existe un polinomio $r(n)$ tal que cada llamada al oráculo A de M_3^A con entrada (w, y, z) utiliza strings en la cinta de consulta de largo $r(|w|)$

- ▶ ¿Por qué podemos suponer esto? ¿Deberíamos tener $r(|w|, |y|, |z|)$ en lugar de $r(|w|)$?
- ▶ La demostración también puede realizarse sin este supuesto

Finalmente suponemos que $r(n)$ es $\Omega(n)$

Demostración del teorema

Vamos a utilizar M_1 , M_2 , M_3^A y los polinomios $p(n)$, $q(n)$, $r(n)$ para definir un lenguaje K tal que:

- ▶ Cada elemento de K es de la forma (w, y, z, s) con $w \in \{0, 1\}^*$, $y \in \{0, 1\}^{q(|w|)}$, $z \in \{0, 1\}^{q(|w|)}$ y $s \in \{0, 1\}^{p(r(|w|))}$
- ▶ $K \in \text{NP}$

Demostración del teorema

Defina una MT no determinista M_4 de la siguiente forma:

- ▶ La entrada de M_4 es un string (w, y, z, s) tal que $w \in \{0, 1\}^*$, $y \in \{0, 1\}^{q(|w|)}$, $z \in \{0, 1\}^{q(|w|)}$ y $s \in \{0, 1\}^{p(r(|w|))}$
- ▶ M_4 simula el funcionamiento de M_3^A con entrada (w, y, z)
 - ▶ Si M_3^A acepta, entonces M_4 rechaza, en otro caso M_4 acepta
- ▶ M_4 simula las llamadas al oráculo A realizadas por M_3^A . Para cada llamada con un string x en la cinta de consulta tal que $|x| = r(|w|)$, M_4 adivina la respuesta de A :
 - ▶ Si adivina una respuesta **sí**, entonces M_4 utiliza M_2 con entrada x para adivinar un testigo para esta respuesta
 - ▶ Si adivina una respuesta **no**, entonces M_4 utiliza M_1 con entrada (x, s) para adivinar un testigo para esta respuesta

Demostración del teorema

Sea (w, y, z, s) una posible entrada de M_4

- ▶ En particular $|s| = p(r(|w|))$

Lema

Si $s \in B_{r(|w|)}$, entonces M_4 acepta (w, y, z, s) si y sólo si M_3^A no acepta (w, y, z)

Demostración del teorema

Sea (w, y, z, s) una posible entrada de M_4

- ▶ En particular $|s| = p(r(|w|))$

Lema

Si $s \in B_{r(|w|)}$, entonces M_4 acepta (w, y, z, s) si y sólo si M_3^A no acepta (w, y, z)

Ejercicio

Demuestre el lema considerando que $s \in B_{r(|w|)}$ implica que $\bar{A}_{=r(|w|)} = L(M_1, s)_{=r(|w|)}$

Demostración del teorema

Sea $K = L(M_4)$

- ▶ Tenemos que $K \in \text{NP}$ puesto que M_4 es una MT no determinista que funciona en tiempo polinomial

Demostración del teorema

Sea $K = L(M_4)$

- ▶ Tenemos que $K \in \text{NP}$ puesto que M_4 es una MT no determinista que funciona en tiempo polinomial

La construcción de M_4 y K son los ingredientes fundamentales de la demostración

- ▶ Antes de mostrar cómo es utilizado K necesitamos enunciar una propiedad de los conjuntos B_n

Demostración del teorema

Dado que $p(n)$ es un polinomio no nulo, $B_n \subseteq \{0, 1\}^{p(n)}$ y $|B_n| > (1 - \frac{1}{2^n})2^{p(n)}$, concluimos que existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$:

- ▶ $\exists u_1 \in \{0, 1\}^{p(n)} \dots \exists u_{p(n)} \in \{0, 1\}^{p(n)} \forall v \in \{0, 1\}^{p(n)}$
 $\exists i \in \{1, \dots, p(n)\} : (u_i \oplus v \in B_n)$
- ▶ $\forall u_1 \in \{0, 1\}^{p(n)} \dots \forall u_{p(n)} \in \{0, 1\}^{p(n)} \exists v \in \{0, 1\}^{p(n)}$
 $\forall i \in \{1, \dots, p(n)\} : (u_i \oplus v \in B_n)$

Demostración del teorema

A partir de la propiedad anterior concluimos lo siguiente:

Lema

Para cada $w \in \{0, 1\}^$ tal que $r(|w|) \geq n_0$ se tiene que:*

$w \in L$ si y sólo si

$$\exists y \in \{0, 1\}^{q(|w|)}$$

$$\exists u_1 \in \{0, 1\}^{p(r(|w|))} \dots \exists u_{p(r(|w|))} \in \{0, 1\}^{p(r(|w|))}$$

$$\forall z \in \{0, 1\}^{q(|w|)}$$

$$\forall v \in \{0, 1\}^{p(r(|w|))} \neg \left(\bigwedge_{i=1}^{p(r(|w|))} (w, y, z, u_i \oplus v) \in K \right)$$

Demostración del teorema

Para terminar la demostración considere el lenguaje:

$$N = \left\{ (w, y, z, u_1, \dots, u_{p(r(|w|))}, v) \mid w \in \{0, 1\}^*, \right. \\ y \in \{0, 1\}^{q(|w|)}, z \in \{0, 1\}^{q(|w|)}, \\ u_1 \in \{0, 1\}^{p(r(|w|))}, \dots, u_{p(r(|w|))} \in \{0, 1\}^{p(r(|w|))}, \\ \left. v \in \{0, 1\}^{p(r(|w|))} \text{ y } \bigwedge_{i=1}^{p(r(|w|))} (w, y, z, u_i \oplus v) \in K \right\}$$

Demostración del teorema

Dado que $K \in \text{NP}$ concluimos que $N \in \text{NP}$

Por lo tanto existe una MT determinista M_5 y un polinomio $t(n)$ tales que M_5 funciona en tiempo polinomial y para todo $(w, y, z, u_1, \dots, u_{p(r(|w|))}, v)$:

$(w, y, z, u_1, \dots, u_{p(r(|w|))}, v) \in N$ si y solo si

$\exists z' \in \{0, 1\}^{t(|w|)} : M_5 \text{ acepta } (w, y, z, u_1, \dots, u_{p(r(|w|))}, v, z')$

Demostración del teorema

A partir de la propiedad anterior y el último lema obtenemos que para todo $w \in \{0, 1\}^*$ tal que $r(|w|) \geq n_0$:

$w \in L$ si y sólo si

$$\exists y \in \{0, 1\}^{q(|w|)}$$

$$\exists u_1 \in \{0, 1\}^{p(r(|w|))} \dots \exists u_{p(r(|w|))} \in \{0, 1\}^{p(r(|w|))}$$

$$\forall z \in \{0, 1\}^{q(|w|)}$$

$$\forall v \in \{0, 1\}^{p(r(|w|))}$$

$$\neg(\exists z' \in \{0, 1\}^{t(|w|)} : M_5 \text{ acepta } (w, y, z, u_1, \dots, u_{p(r(|w|))}, v, z'))$$

Demostración del teorema

Por lo tanto tenemos que para todo $w \in \{0, 1\}^*$ tal que $r(|w|) \geq n_0$:

$w \in L$ si y sólo si

$$\exists y \in \{0, 1\}^{q(|w|)}$$

$$\exists u_1 \in \{0, 1\}^{p(r(|w|))} \dots \exists u_{p(r(|w|))} \in \{0, 1\}^{p(r(|w|))}$$

$$\forall z \in \{0, 1\}^{q(|w|)}$$

$$\forall v \in \{0, 1\}^{p(r(|w|))}$$

$$\forall z' \in \{0, 1\}^{t(|w|)} : M_5 \text{ rechaza } (w, y, z, u_1, \dots, u_{p(r(|w|))}, v, z')$$

Demostración del teorema

Dado que $r(n)$ es $\Omega(n)$, sabemos que existe una cantidad fija de strings $w \in \{0, 1\}^*$ tales que $r(|w|) < n_0$

Demostración del teorema

Dado que $r(n)$ es $\Omega(n)$, sabemos que existe una cantidad fija de strings $w \in \{0, 1\}^*$ tales que $r(|w|) < n_0$

Concluimos que existe una MT determinista M_6 que funciona en tiempo polinomial y tal que para todo $w \in \{0, 1\}^*$:

$w \in L$ si y sólo si

$$\exists y \in \{0, 1\}^{q(|w|)}$$

$$\exists u_1 \in \{0, 1\}^{p(r(|w|))} \dots \exists u_{p(r(|w|))} \in \{0, 1\}^{p(r(|w|))}$$

$$\forall z \in \{0, 1\}^{q(|w|)}$$

$$\forall v \in \{0, 1\}^{p(r(|w|))}$$

$$\forall z' \in \{0, 1\}^{t(|w|)} : M_6 \text{ acepta } (w, y, z, u_1, \dots, u_{p(r(|w|))}, v, z')$$

Demostración del teorema

Dado que $r(n)$ es $\Omega(n)$, sabemos que existe una cantidad fija de strings $w \in \{0, 1\}^*$ tales que $r(|w|) < n_0$

Concluimos que existe una MT determinista M_6 que funciona en tiempo polinomial y tal que para todo $w \in \{0, 1\}^*$:

$w \in L$ si y sólo si

$$\exists y \in \{0, 1\}^{q(|w|)}$$

$$\exists u_1 \in \{0, 1\}^{p(r(|w|))} \dots \exists u_{p(r(|w|))} \in \{0, 1\}^{p(r(|w|))}$$

$$\forall z \in \{0, 1\}^{q(|w|)}$$

$$\forall v \in \{0, 1\}^{p(r(|w|))}$$

$$\forall z' \in \{0, 1\}^{t(|w|)} : M_6 \text{ acepta } (w, y, z, u_1, \dots, u_{p(r(|w|))}, v, z')$$

¡Tenemos entonces que $L \in \Sigma_2^P$, que era lo que debíamos demostrar!

