

BPP está en la jerarquía polinomial

Teorema (Gács-Sipser-Lautemann)

$$BPP \subseteq \Sigma_2^P \cap \Pi_2^P$$

Como sabemos que $BPP = \text{co-BPP}$, nos basta demostrar que $BPP \subseteq \Sigma_2^P$

- ▶ Antes de realizar esta demostración vamos a ver dos ingredientes necesarios para ella

Una generalización de la noción de lenguaje

Sea Σ un alfabeto.

Un lenguaje L puede tener como elementos pares de strings sobre Σ

- ▶ Tenemos entonces que $L \subseteq \Sigma^* \times \Sigma^*$

L es un lenguaje como los que habíamos definido antes puesto que un par de strings también es un string

- ▶ Podemos representar (x, y) como un string $x\#y$ donde $\#$ es un símbolo nuevo

En las siguientes transparencias vamos a considerar lenguajes que consisten de pares o tuplas de strings.

Una caracterización de NP

Proposición

Sea L un lenguaje sobre un alfabeto Σ . Entonces L está en NP si y sólo si existe un lenguaje $A \subseteq \Sigma^ \times \Sigma^*$ y un polinomio $p(n)$ tales que $A \in PTIME$ y para todo $u \in \Sigma^*$:*

$$u \in L \text{ si y sólo si } (\exists v \in \Sigma^*, |v| = p(|u|)) : (u, v) \in A$$

Ejercicio

Demuestre la proposición.

Primer ingrediente: una caracterización de Σ_2^P

Proposición

Sea L un lenguaje sobre un alfabeto Σ . Entonces L está en Σ_2^P si y sólo si existe un lenguaje $B \subseteq \Sigma^* \times \Sigma^* \times \Sigma^*$ y un polinomio $q(n)$ tales que $B \in PTIME$ y para todo $u \in \Sigma^*$:

$u \in L$ si y sólo si

$$(\exists v_1 \in \Sigma^*, |v_1| = q(|u|))(\forall v_2 \in \Sigma^*, |v_2| = q(|u|)) : (u, v_1, v_2) \in B$$

Ejercicio

Demuestre la dirección $\Leftarrow$ de la proposición.

- Esta es la dirección que vamos a utilizar para demostrar que $BPP \subseteq \Sigma_2^P$