

¿Qué sabemos sobre $RP \cap co-RP$?

Tenemos que $PTIME \subseteq RP \cap co-RP$

¿Podemos demostrar que $PTIME = RP \cap co-RP$?

¿Qué sabemos sobre $RP \cap co-RP$?

Tenemos que $PTIME \subseteq RP \cap co-RP$

¿Podemos demostrar que $PTIME = RP \cap co-RP$?

- ▶ Este es un problema abierto

¿Qué sabemos sobre $RP \cap co-RP$?

Tenemos que $PTIME \subseteq RP \cap co-RP$

¿Podemos demostrar que $PTIME = RP \cap co-RP$?

- ▶ Este es un problema abierto

Pero podemos demostrar que para cada problema en $RP \cap co-RP$ existe un algoritmo que lo decide en tiempo polynomial *esperado*.

Un algoritmo de tiempo polinomial esperado

Sea $L \in \text{RP} \cap \text{co-RP}$ con alfabeto Σ

Un algoritmo de tiempo polinomial esperado

Sea $L \in \text{RP} \cap \text{co-RP}$ con alfabeto Σ

Entonces existen MTs probabilísticas M_1 y M_2 tales que:

- ▶ $t_{M_1}(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:
 - ▶ Si $w \in L$, entonces $\Pr(M_1 \text{ acepte } w) \geq \frac{3}{4}$
 - ▶ Si $w \notin L$, entonces $\Pr(M_1 \text{ acepte } w) = 0$
- ▶ $t_{M_2}(n)$ es $O(n^\ell)$ y para cada $w \in \Sigma^*$:
 - ▶ Si $w \in L$, entonces $\Pr(M_2 \text{ acepte } w) = 1$
 - ▶ Si $w \notin L$, entonces $\Pr(M_2 \text{ rechace } w) \geq \frac{3}{4}$

Un algoritmo de tiempo polinomial esperado

Sea $g(n) = \max\{t_{M_1}(n), t_{M_2}(n)\}$

Un algoritmo de tiempo polinomial esperado

Sea $g(n) = \max\{t_{M_1}(n), t_{M_2}(n)\}$

Considere el siguiente algoritmo para decidir si $w \in L$:

1. Escoja al azar y con distribución uniforme un string $s_1 \in \{0, 1\}^*$ tal que $|s_1| = g(|w|)$
2. Verifique si $M_1(w, s_1)$ acepta. Si es así retorne **sí**, sino vaya al paso 3
3. Escoja al azar y con distribución uniforme un string $s_2 \in \{0, 1\}^*$ tal que $|s_2| = g(|w|)$
4. Verifique si $M_2(w, s_2)$ rechaza. Si es así retorne **no**, sino vaya al paso 1

Un algoritmo de tiempo polinomial esperado

El algoritmo anterior puede no detenerse.

- ▶ Si se detiene entrega el resultado correcto

Un algoritmo de tiempo polinomial esperado

El algoritmo anterior puede no detenerse.

- ▶ Si se detiene entrega el resultado correcto

¿Cuál es el tiempo *esperado* de funcionamiento del algoritmo?

Un algoritmo de tiempo polinomial esperado

El algoritmo anterior puede no detenerse.

- ▶ Si se detiene entrega el resultado correcto

¿Cuál es el tiempo *esperado* de funcionamiento del algoritmo?

- ▶ Calcular el número esperado de veces que se ejecuta la secuencia de pasos 1 al 4 se reduce a calcular la esperanza de una variable aleatoria con distribución geométrica de parámetro $\frac{3}{4}$

Un algoritmo de tiempo polinomial esperado

El algoritmo anterior puede no detenerse.

- ▶ Si se detiene entrega el resultado correcto

¿Cuál es el tiempo *esperado* de funcionamiento del algoritmo?

- ▶ Calcular el número esperado de veces que se ejecuta la secuencia de pasos 1 al 4 se reduce a calcular la esperanza de una variable aleatoria con distribución geométrica de parámetro $\frac{3}{4}$

Concluimos que el algoritmo funciona en tiempo polinomial esperado.

Una clase de complejidad probabilística más general

Una clase de complejidad probabilística más general

Definición

Sea L un lenguaje sobre un alfabeto Σ . Entonces L está en BPP si existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

- ▶ Si $w \in L$, entonces $\Pr(M \text{ acepte } w) \geq \frac{3}{4}$
- ▶ Si $w \notin L$, entonces $\Pr(M \text{ acepte } w) \leq \frac{1}{4}$

¿Dónde está la clase BPP?

Teorema

$$BPP = co-BPP$$

¿Dónde está la clase BPP?

Teorema

$$BPP = co-BPP$$

Ejercicio

Demuestre el teorema.

¿Dónde está la clase BPP?

Teorema

$$BPP = co-BPP$$

Ejercicio

Demuestre el teorema.

Corolario

$$RP \subseteq BPP \text{ y } co-RP \subseteq BPP$$

¿Dónde está la clase BPP?

Es un problema abierto si $\text{PTIME} = \text{BPP}$

¿Dónde está la clase BPP?

Es un problema abierto si $\text{PTIME} = \text{BPP}$

- ▶ De esto se concluiría que $\text{BPP} = \text{RP} = \text{co-RP} = \text{PTIME}$

¿Dónde está la clase BPP?

Es un problema abierto si $\text{PTIME} = \text{BPP}$

- ▶ De esto se concluiría que $\text{BPP} = \text{RP} = \text{co-RP} = \text{PTIME}$

Pero vamos a demostrar que BPP está contenida en la jerarquía polinomial.