

¿Por qué utilizamos la probabilidad $\frac{3}{4}$?

El valor $\frac{3}{4}$ es arbitrario

- Podemos utilizar valores arbitrariamente más pequeños

¿Por qué utilizamos la probabilidad $\frac{3}{4}$?

El valor $\frac{3}{4}$ es arbitrario

- Podemos utilizar valores arbitrariamente más pequeños

Lema de amplificación

Sea L un lenguaje sobre un alfabeto Σ . Si $L \in \text{RP}$, entonces para cada $\ell \in \mathbb{N}$, 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 $\Pr(M \text{ acepte } w) \geq 1 - \frac{1}{4^\ell}$
- Si $w \notin L$, entonces $\Pr(M \text{ acepte } w) = 0$

¿Por qué utilizamos la probabilidad $\frac{3}{4}$?

El valor $\frac{3}{4}$ es arbitrario

- Podemos utilizar valores arbitrariamente más pequeños

Lema de amplificación

Sea L un lenguaje sobre un alfabeto Σ . Si $L \in \text{RP}$, entonces para cada $\ell \in \mathbb{N}$, 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 $\Pr(M \text{ acepte } w) \geq 1 - \frac{1}{4^\ell}$
- Si $w \notin L$, entonces $\Pr(M \text{ acepte } w) = 0$

Ejercicio

Demuestre el lema de amplificación

¿Dónde está la clase RP?

Teorema

$$PTIME \subseteq RP \subseteq NP$$

¿Dónde está la clase RP?

Teorema

$$P\text{TIME} \subseteq RP \subseteq NP$$

Ejercicio

Demuestre el teorema.

¿Dónde está la clase RP?

Teorema

$$PTIME \subseteq RP \subseteq NP$$

Ejercicio

Demuestre el teorema.

Corolario

$$PTIME \subseteq co-RP \subseteq co-NP$$

¿Qué sabemos sobre RP y co-RP?

Son problemas abiertos si $P\text{TIME} = RP$ o $RP = \text{co-RP}$

¿Qué sabemos sobre RP y co-RP?

Son problemas abiertos si $\text{PTIME} = \text{RP}$ o $\text{RP} = \text{co-RP}$

Pero se cree que $\text{PTIME} = \text{RP}$

- ▶ Puesto que si $L \in \text{RP}$, entonces hay un algoritmo para resolver L puede ser usado en la *práctica* como un algoritmo de tiempo polinomial
- ▶ De esto se concluiría que $\text{RP} = \text{co-RP} = \text{PTIME}$

¿Qué sabemos sobre RP y co-RP?

Son problemas abiertos si $\text{PTIME} = \text{RP}$ o $\text{RP} = \text{co-RP}$

Pero se cree que $\text{PTIME} = \text{RP}$

- ▶ Puesto que si $L \in \text{RP}$, entonces hay un algoritmo para resolver L puede ser usado en la *práctica* como un algoritmo de tiempo polinomial
- ▶ De esto se concluiría que $\text{RP} = \text{co-RP} = \text{PTIME}$

$\overline{\text{EQUIV-POL}}$ es un ejemplo de un problema que está en RP y para el cual no se sabe si está en PTIME.

¿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 polinomial *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 $w \in \bar{L}$, entonces $\Pr(M_2 \text{ acepte } w) \geq \frac{3}{4}$
 - ▶ Si $w \notin \bar{L}$, entonces $\Pr(M_2 \text{ acepte } w) = 0$

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 $s \in \{0, 1\}^*$ tal que $|s| = g(|w|)$
2. Verifique si $M_1(w, s)$ acepta. Si es así retorne **sí**, sino vaya al paso 3
3. Verifique si $M_2(w, s)$ acepta. 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 3 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 3 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.

Un ingrediente necesario

Al igual que para el caso de RP, los valores $\frac{3}{4}$ y $\frac{1}{4}$ en la definición de BPP pueden ser reemplazados por valores arbitrariamente más pequeños

Un ingrediente necesario

Al igual que para el caso de RP, los valores $\frac{3}{4}$ y $\frac{1}{4}$ en la definición de BPP pueden ser reemplazados por valores arbitrariamente más pequeños

Lema de amplificación para BPP

Sea L un lenguaje sobre un alfabeto Σ . Si $L \in \text{BPP}$, entonces para cada $\ell \in \mathbb{N}$, 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 $\Pr(M \text{ acepte } w) \geq 1 - \left(\frac{3}{4}\right)^\ell$
- ▶ Si $w \notin L$, entonces $\Pr(M \text{ acepte } w) \leq \left(\frac{3}{4}\right)^\ell$

Demostración del lema de amplificación para BPP

Como $L \in \text{BPP}$, existe una MT probabilística M_1 tal que $t_{M_1}(n)$ es $O(n^{k_1})$ 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 $\Pr(M_1 \text{ acepte } w) \leq \frac{1}{4}$

Demostración del lema de amplificación para BPP

Como $L \in \text{BPP}$, existe una MT probabilística M_1 tal que $t_{M_1}(n)$ es $O(n^{k_1})$ 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 $\Pr(M_1 \text{ acepte } w) \leq \frac{1}{4}$

Utilizamos la MT M_1 para construir la MT M mencionada en el enunciado del lema de amplificación.

Demostración del lema de amplificación para BPP

Considere el siguiente algoritmo que recibe como entrada $w \in \Sigma^*$:

1. Escoja al azar con distribución uniforme y de manera independiente strings $s_1, s_2, \dots, s_{2\ell+1}$ en $\{0, 1\}^*$ y tales que $|s_1| = |s_2| = \dots = |s_{2\ell+1}| = t_{M_1}(|w|)$
2. Construya el conjunto $A = \{i \in \{1, \dots, 2\ell + 1\} \mid M_1(w, s_i) \text{ acepta}\}$
3. Si $|A| \geq \ell + 1$, entonces retorne **sí**, sino retorne **no**

Demostración del lema de amplificación para BPP

Considere el siguiente algoritmo que recibe como entrada $w \in \Sigma^*$:

1. Escoja al azar con distribución uniforme y de manera independiente strings $s_1, s_2, \dots, s_{2\ell+1}$ en $\{0, 1\}^*$ y tales que $|s_1| = |s_2| = \dots = |s_{2\ell+1}| = t_{M_1}(|w|)$
2. Construya el conjunto $A = \{i \in \{1, \dots, 2\ell + 1\} \mid M_1(w, s_i) \text{ acepta}\}$
3. Si $|A| \geq \ell + 1$, entonces retorne **sí**, sino retorne **no**

Suponga que M es una MT probabilística que implementa este algoritmo

Demostración del lema de amplificación para BPP

Considere el siguiente algoritmo que recibe como entrada $w \in \Sigma^*$:

1. Escoja al azar con distribución uniforme y de manera independiente strings $s_1, s_2, \dots, s_{2\ell+1}$ en $\{0, 1\}^*$ y tales que $|s_1| = |s_2| = \dots = |s_{2\ell+1}| = t_{M_1}(|w|)$
2. Construya el conjunto $A = \{i \in \{1, \dots, 2\ell + 1\} \mid M_1(w, s_i) \text{ acepta}\}$
3. Si $|A| \geq \ell + 1$, entonces retorne **sí**, sino retorne **no**

Suponga que M es una MT probabilística que implementa este algoritmo

- Se tiene que $t_M(n)$ es $O(n^k)$ para una constante k ya que $t_{M_1}(n)$ es $O(n^{k_1})$ para una constante k_1

Demostración del lema de amplificación para BPP

Considere el siguiente algoritmo que recibe como entrada $w \in \Sigma^*$:

1. Escoja al azar con distribución uniforme y de manera independiente strings $s_1, s_2, \dots, s_{2\ell+1}$ en $\{0, 1\}^*$ y tales que $|s_1| = |s_2| = \dots = |s_{2\ell+1}| = t_{M_1}(|w|)$
2. Construya el conjunto $A = \{i \in \{1, \dots, 2\ell + 1\} \mid M_1(w, s_i) \text{ acepta}\}$
3. Si $|A| \geq \ell + 1$, entonces retorne **sí**, sino retorne **no**

Suponga que M es una MT probabilística que implementa este algoritmo

- Se tiene que $t_M(n)$ es $O(n^k)$ para una constante k ya que $t_{M_1}(n)$ es $O(n^{k_1})$ para una constante k_1

Vamos a demostrar que M satisface las condiciones del lema

Demostración del lema de amplificación para BPP

En primer lugar consideramos $w \in L$, y suponemos que

$$\Pr(M_1 \text{ acepte } w) = p$$

con $p \geq \frac{3}{4}$

Demostración del lema de amplificación para BPP

En primer lugar consideramos $w \in L$, y suponemos que

$$\Pr(M_1 \text{ acepte } w) = p$$

con $p \geq \frac{3}{4}$

Además suponemos que $p < 1$

- ▶ Si $p = 1$ entonces se tiene que $\Pr(M \text{ acepte } w) = 1 \geq 1 - (\frac{3}{4})^\ell$.
¿Por qué?

Demostración del lema de amplificación para BPP

En primer lugar consideramos $w \in L$, y suponemos que

$$\Pr(M_1 \text{ acepte } w) = p$$

con $p \geq \frac{3}{4}$

Además suponemos que $p < 1$

- Si $p = 1$ entonces se tiene que $\Pr(M \text{ acepte } w) = 1 \geq 1 - (\frac{3}{4})^\ell$.
¿Por qué?

Tenemos entonces que:

$$\Pr(M \text{ rechace } w) = \sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^i (1-p)^{2\ell+1-i}$$

Demostración del lema de amplificación para BPP

Como $\frac{3}{4} \leq p < 1$, tenemos que $1 \leq \frac{p}{1-p}$

Entonces para $i \in \{0, \dots, \ell\}$ tenemos que:

$$\begin{aligned} p^i(1-p)^{2\ell+1-i} &\leq p^i(1-p)^{2\ell+1-i} \left(\frac{p}{1-p} \right)^{\ell-i} \\ &= p^\ell(1-p)^{\ell+1} \end{aligned}$$

Demostración del lema de amplificación para BPP

Por lo tanto:

$$\begin{aligned}\sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^i (1-p)^{2\ell+1-i} &\leq \sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^{\ell} (1-p)^{\ell+1} \\ &= p^{\ell} (1-p)^{\ell+1} \sum_{i=0}^{\ell} \binom{2\ell+1}{i} \\ &\leq p^{\ell} (1-p)^{\ell+1} 2^{2\ell+1}\end{aligned}$$

Demostración del lema de amplificación para BPP

Por lo tanto:

$$\begin{aligned}\sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^i (1-p)^{2\ell+1-i} &\leq \sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^{\ell} (1-p)^{\ell+1} \\ &= p^{\ell} (1-p)^{\ell+1} \sum_{i=0}^{\ell} \binom{2\ell+1}{i} \\ &\leq p^{\ell} (1-p)^{\ell+1} 2^{2\ell+1}\end{aligned}$$

El mayor valor de la función $f(x) = x(1-x)$ en el intervalo $[\frac{3}{4}, 1)$ se alcanza en $x = \frac{3}{4}$

Demostración del lema de amplificación para BPP

Por lo tanto:

$$\begin{aligned}\sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^i (1-p)^{2\ell+1-i} &\leq \sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^{\ell} (1-p)^{\ell+1} \\ &= p^{\ell} (1-p)^{\ell+1} \sum_{i=0}^{\ell} \binom{2\ell+1}{i} \\ &\leq p^{\ell} (1-p)^{\ell+1} 2^{2\ell+1}\end{aligned}$$

El mayor valor de la función $f(x) = x(1-x)$ en el intervalo $[\frac{3}{4}, 1)$ se alcanza en $x = \frac{3}{4}$

► Concluimos que $p(1-p) \leq \frac{3}{4} \cdot \frac{1}{4}$

Demostración del lema de amplificación para BPP

Concluimos que:

$$\begin{aligned} \sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^i (1-p)^{2\ell+1-i} &\leq p^{\ell} (1-p)^{\ell+1} 2^{2\ell+1} \\ &= (p(1-p))^{\ell} (1-p) 2^{2\ell+1} \\ &\leq \left(\frac{3}{4} \cdot \frac{1}{4}\right)^{\ell} \cdot \frac{1}{4} 2^{2\ell+1} \\ &= \frac{3^{\ell}}{4^{2\ell+1}} 2^{2\ell+1} \\ &= 2 \frac{3^{\ell}}{4^{2\ell+1}} 4^{\ell} \\ &= \frac{1}{2} \cdot \frac{3^{\ell}}{4^{\ell}} \\ &< \left(\frac{3}{4}\right)^{\ell} \end{aligned}$$

Demostración del lema de amplificación para BPP

Finalmente concluimos que:

$$\begin{aligned}\Pr(M \text{ rechace } w) &= \sum_{i=0}^{\ell} \binom{2\ell+1}{i} p^i (1-p)^{2\ell+1-i} \\ &< \left(\frac{3}{4}\right)^{\ell}\end{aligned}$$

De lo cual obtenemos que:

$$\Pr(M \text{ acepte } w) \geq 1 - \left(\frac{3}{4}\right)^{\ell}$$

Demostración del lema de amplificación para BPP

En segundo lugar consideramos $w \notin L$, y suponemos que

$$\Pr(M_1 \text{ acepte } w) = q$$

con $q \leq \frac{1}{4}$

Demostración del lema de amplificación para BPP

En segundo lugar consideramos $w \notin L$, y suponemos que

$$\Pr(M_1 \text{ acepte } w) = q$$

con $q \leq \frac{1}{4}$

Además suponemos que $0 < q$

- ▶ Si $q = 0$ entonces se tiene que $\Pr(M \text{ acepte } w) = 0 \leq (\frac{3}{4})^\ell$.
¿Por qué?

Demostración del lema de amplificación para BPP

En segundo lugar consideramos $w \notin L$, y suponemos que

$$\Pr(M_1 \text{ acepte } w) = q$$

con $q \leq \frac{1}{4}$

Además suponemos que $0 < q$

- Si $q = 0$ entonces se tiene que $\Pr(M \text{ acepte } w) = 0 \leq (\frac{3}{4})^\ell$.
¿Por qué?

Tenemos entonces que:

$$\Pr(M \text{ acepte } w) = \sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^i q^{2\ell+1-i}$$

Demostración del lema de amplificación para BPP

Como $0 < q \leq \frac{1}{4}$, tenemos que $1 \leq \frac{1-q}{q}$

Entonces para $i \in \{0, \dots, \ell\}$ tenemos que:

$$\begin{aligned}(1-q)^i q^{2\ell+1-i} &\leq (1-q)^i q^{2\ell+1-i} \left(\frac{1-q}{q}\right)^{\ell-i} \\ &= (1-q)^\ell q^{\ell+1}\end{aligned}$$

Demostración del lema de amplificación para BPP

Por lo tanto:

$$\begin{aligned}\sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^i q^{2\ell+1-i} &\leq \sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^{\ell} q^{\ell+1} \\ &= (1-q)^{\ell} q^{\ell+1} \sum_{i=0}^{\ell} \binom{2\ell+1}{i} \\ &\leq (1-q)^{\ell} q^{\ell+1} 2^{2\ell+1}\end{aligned}$$

Demostración del lema de amplificación para BPP

Por lo tanto:

$$\begin{aligned}\sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^i q^{2\ell+1-i} &\leq \sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^{\ell} q^{\ell+1} \\ &= (1-q)^{\ell} q^{\ell+1} \sum_{i=0}^{\ell} \binom{2\ell+1}{i} \\ &\leq (1-q)^{\ell} q^{\ell+1} 2^{2\ell+1}\end{aligned}$$

El mayor valor de la función $f(x) = x(1-x)$ en el intervalo $(0, \frac{1}{4}]$ se alcanza en $x = \frac{1}{4}$

Demostración del lema de amplificación para BPP

Por lo tanto:

$$\begin{aligned}\sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^i q^{2\ell+1-i} &\leq \sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^{\ell} q^{\ell+1} \\ &= (1-q)^{\ell} q^{\ell+1} \sum_{i=0}^{\ell} \binom{2\ell+1}{i} \\ &\leq (1-q)^{\ell} q^{\ell+1} 2^{2\ell+1}\end{aligned}$$

El mayor valor de la función $f(x) = x(1-x)$ en el intervalo $(0, \frac{1}{4}]$ se alcanza en $x = \frac{1}{4}$

► Concluimos que $(1-q)q \leq \frac{3}{4} \cdot \frac{1}{4}$

Demostración del lema de amplificación para BPP

Concluimos que:

$$\begin{aligned}\sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^i q^{2\ell+1-i} &\leq (1-q)^{\ell} q^{\ell+1} 2^{2\ell+1} \\ &= ((1-q)q)^{\ell} q 2^{2\ell+1} \\ &\leq \left(\frac{3}{4} \cdot \frac{1}{4}\right)^{\ell} \cdot \frac{1}{4} 2^{2\ell+1}\end{aligned}$$

Demostración del lema de amplificación para BPP

Concluimos que:

$$\begin{aligned}\sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^i q^{2\ell+1-i} &\leq (1-q)^\ell q^{\ell+1} 2^{2\ell+1} \\ &= ((1-q)q)^\ell q 2^{2\ell+1} \\ &\leq \left(\frac{3}{4} \cdot \frac{1}{4}\right)^\ell \cdot \frac{1}{4} 2^{2\ell+1}\end{aligned}$$

Como en el caso anterior concluimos que:

$$\sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^i q^{2\ell+1-i} < \left(\frac{3}{4}\right)^\ell$$

Demostración del lema de amplificación para BPP

Finalmente concluimos que:

$$\begin{aligned}\Pr(M \text{ acepta } w) &= \sum_{i=0}^{\ell} \binom{2\ell+1}{i} (1-q)^i q^{2\ell+1-i} \\ &\leq \left(\frac{3}{4}\right)^{\ell}\end{aligned}$$

