Clases de complejidad aleatorizadas

IIC3810

Un ejemplo: multiplicación de matrices

Sean A, B y C tres matrices de $n \times n$ de números racionales

Un ejemplo: multiplicación de matrices

Sean A, B y C tres matrices de $n \times n$ de números racionales

Queremos verificar si $AB = C$

Un ejemplo: multiplicación de matrices

Sean A, B y C tres matrices de $n \times n$ de números racionales

Queremos verificar si $AB = C$

- ¿Cuántas multiplicaciones de números racionales necesitamos hacer para resolver este problema?

Un ejemplo: multiplicación de matrices

Sean A, B y C tres matrices de $n \times n$ de números racionales

Queremos verificar si $AB = C$

- ¿Cuántas multiplicaciones de números racionales necesitamos hacer para resolver este problema?
  - $O(n^3)$ con el algoritmo usual, $O(n^{2,807354})$ con el algoritmo de Strassen y $O(n^{2,372859})$ con el mejor algoritmo actual.

Un ejemplo: multiplicación de matrices

Sean A, B y C tres matrices de $n \times n$ de números racionales

Queremos verificar si $AB = C$

- ¿Cuántas multiplicaciones de números racionales necesitamos hacer para resolver este problema?
  - $O(n^3)$ con el algoritmo usual, $O(n^{2,807354})$ con el algoritmo de Strassen y $O(n^{2,372859})$ con el mejor algoritmo actual.

¿Podemos resolver este problema de manera más eficiente? ¿Con $O(n^2)$ multiplicaciones de números racionales?

Un ejemplo: multiplicación de matrices

Lema

Si $(d_1, \ldots, d_n)$ *y* $(e_1, \ldots, e_n)$ *son dos vectores distintos en* $\mathbb{Q}^n$*, entonces:*

$$\Pr_{(x_1,\ldots,x_n)\sim\{0,1\}^n}\left[\sum_{i=1}^{n} d_i \cdot x_i = \sum_{i=1}^{n} e_i \cdot x_i\right] \leq \frac{1}{2}$$

Un ejemplo: multiplicación de matrices

Lema

Si $(d_1, \ldots, d_n)$ *y* $(e_1, \ldots, e_n)$ *son dos vectores distintos en* $\mathbb{Q}^n$*, entonces:*

$$\Pr_{(x_1,\ldots,x_n)\sim\{0,1\}^n}\left[\sum_{i=1}^{n} d_i \cdot x_i = \sum_{i=1}^{n} e_i \cdot x_i\right] \leq \frac{1}{2}$$

Ejercicio

Demuestre el lema.

Un ejemplo: multiplicación de matrices

Ejercicios

1. Use el lema para construir un algoritmo que verifica si $A \cdot B = C$ realizando $O(n^2)$ multiplicaciones y con una probabilidad de error acotada por $\frac{1}{2}$.

2. Indique cómo modificar el algoritmo para que siga realizando $O(n^2)$ multiplicaciones pero su probabilidad de error está acotada por $(\frac{1}{2})^{100}$.

Algoritmos probabilísticos y Máquinas de Turing

¿Cómo podemos formalizar la idea de un algoritmo probabilístico utilizando la noción de MT?

¿Podemos definir clases de complejidad basados en los algoritmos probabilísticos?

Algoritmos probabilísticos y Máquinas de Turing

¿Cómo podemos formalizar la idea de un algoritmo probabilístico utilizando la noción de MT?

¿Podemos definir clases de complejidad basados en los algoritmos probabilísticos?

Vamos a responder a esta preguntas en las siguientes transparencias.

MT probabilística

Definición

Una MT probabilística es una tupla $M = (Q, \Sigma, \Gamma, q_0, \delta, F)$ *tal que:*

- Q *es un conjunto finito de estados*
- Σ *es un alfabeto finito tal que* $\vdash, \mathtt{B} \notin \Sigma$
- Γ *es un alfabeto finito tal que* $\Sigma \cup \{\vdash, \mathtt{B}\} \subseteq \Gamma$
- $q_0 \in Q$ *es el estado inicial*
- $F \subseteq Q$ *es un conjunto de estados finales*
- δ *es una función parcial:*

$$\delta \quad : \quad Q \times \Gamma \times \{0, 1\} \to Q \times \Gamma \times \{\leftarrow, \square, \rightarrow\}$$

MT probabilística: Funcionamiento

La entrada de una MT probabilística M consiste de un string $w \in \Sigma^*$ y un string $s \in \{0,1\}^\omega$

- w es el input que se quiere aceptar o rechazar
- s es un string infinito de símbolos 0 y 1, el cual es considerado como un string de bits aleatorios

En el estado inicial:

- M tiene en la primera cinta $\vdash w\mathtt{B}\cdots$ y en la segunda cinta $\vdash s$
- M está en el estado q_0
- Las cabezas lectoras de ambas cintas están en la posición 1

MT probabilística: Funcionamiento

En cada instante la máquina se encuentra en un estado q y sus cabezas lectoras están en posiciones p_1 y p_2

- Si el símbolo en la posición p_i $(i = 1, 2)$ es a_i y $\delta(q, a_1, a_2) = (q', b, X)$, entonces:
  - La máquina escribe el símbolo b en la posición p_1 de la primera cinta
  - Cambia de estado desde q a q'
  - Mueve la cabeza lectora de la primera cinta a la posición $p_1 - 1$ si X es $\leftarrow$, y a la posición $p_1 + 1$ si X es $\rightarrow$. Si X es $\square$, entonces esta cabeza lectora permanece en la posición p_1

MT probabilística: Funcionamiento

En cada instante la máquina se encuentra en un estado q y sus cabezas lectoras están en posiciones p_1 y p_2

- Si el símbolo en la posición p_i $(i = 1, 2)$ es a_i y $\delta(q, a_1, a_2) = (q', b, X)$, entonces:
  - La máquina escribe el símbolo b en la posición p_1 de la primera cinta
  - Cambia de estado desde q a q'
  - Mueve la cabeza lectora de la primera cinta a la posición $p_1 - 1$ si X es $\leftarrow$, y a la posición $p_1 + 1$ si X es $\rightarrow$. Si X es $\square$, entonces esta cabeza lectora permanece en la posición p_1
  - Mueve la cabeza lectora de la segunda cinta a la posición $p_2 + 1$

El tiempo de ejecución de una MT probabilística

La entrada de una MT probabilística M con alfabeto Σ consiste de dos strings $w \in \Sigma^*$ y $s \in \{0,1\}^\omega$

- Utilizamos la notación $M(w,s)$ para indicar las entradas de M
- Decimos que $M(w,s)$ acepta si M con entrada (w,s) se detiene en un estado final
  - El caso en que $M(w,s)$ rechaza se define de forma similar

El tiempo de ejecución de una MT probabilística

La entrada de una MT probabilística M con alfabeto Σ consiste de dos strings $w \in \Sigma^*$ y $s \in \{0,1\}^\omega$

- Utilizamos la notación $M(w,s)$ para indicar las entradas de M
- Decimos que $M(w,s)$ acepta si M con entrada (w,s) se detiene en un estado final
  - El caso en que $M(w,s)$ rechaza se define de forma similar

Primer supuesto

Consideramos una MT probabilística M que se detiene en todas sus entradas (w,s)

El tiempo de ejecución de una MT probabilística

Un paso de una MT probabilística M consiste en ejecutar una instrucción de la función de transición

El tiempo de ejecución de una MT probabilística

Un paso de una MT probabilística M consiste en ejecutar una instrucción de la función de transición

- Definimos $tiempo_M(w, s)$ como el número de pasos ejecutados por M con entrada (w, s)

El tiempo de ejecución de una MT probabilística

Un paso de una MT probabilística M consiste en ejecutar una instrucción de la función de transición

- Definimos $tiempo_M(w, s)$ como el número de pasos ejecutados por M con entrada (w, s)

Segundo supuesto

Existe una función $f : \Sigma^* \to \mathbb{N}$ tal que para cada $w \in \Sigma^*$ y $s \in \{0,1\}^\omega$:

$$tiempo_M(w, s) \quad \leq \quad f(w)$$

El tiempo de ejecución de una MT probabilística

Un paso de una MT probabilística M consiste en ejecutar una instrucción de la función de transición

- Definimos $tiempo_M(w, s)$ como el número de pasos ejecutados por M con entrada (w, s)

Segundo supuesto

Existe una función $f : \Sigma^* \to \mathbb{N}$ tal que para cada $w \in \Sigma^*$ y $s \in \{0,1\}^\omega$:

$$tiempo_M(w, s) \quad \leq \quad f(w)$$

Vale decir, hay una cantidad máxima de bits aleatorios que deben ser utilizados con entrada w, la cual sólo depende de w

El tiempo de ejecución de una MT probabilística

Para estudiar el peor caso necesitamos la siguiente definición:

$$\mathit{tiempo}_M(w) \quad = \quad \text{máx}\{\mathit{tiempo}_M(w, s) \mid s \in \{0,1\}^\omega\}$$

El tiempo de ejecución de una MT probabilística

Para estudiar el peor caso necesitamos la siguiente definición:

$$tiempo_M(w) \quad = \quad \text{máx}\{tiempo_M(w, s) \mid s \in \{0,1\}^\omega\}$$

Con esto tenemos que el tiempo de funcionamiento de M en el peor caso es definido por la función t_M:

$$t_M(n) \quad = \quad \text{máx}\{tiempo_M(w) \mid w \in \Sigma^* \text{ y } |w| = n\}$$

La probabilidad de aceptar en una MT probabilística

Tercer supuesto

Si para una MT probabilística M con alfabeto Σ se tiene que $t_M(n) \leq g(n)$ para todo $n \in \mathbb{N}$, entonces suponemos que las entradas de M son de la forma (w, s) con $w \in \Sigma^*$, $s \in \{0,1\}^*$ y $|s| = g(n)$.

Dado el tiempo de ejecución de M no podemos usar más de $g(n)$ bits aleatorios para una entrada w de largo n.

La probabilidad de aceptar en una MT probabilística

Sea M una MT probabilística con alfabeto Σ y tal que $t_M(n) \leq g(n)$ para todo $n \in \mathbb{N}$.

La probabilidad de aceptar en una MT probabilística

Sea M una MT probabilística con alfabeto Σ y tal que $t_M(n) \leq g(n)$ para todo $n \in \mathbb{N}$.

Definición

Para cada $w \in \Sigma^*$ tal que $|w| = n$, la probabilidad de que M acepte w es definida de la siguiente forma:

$$\mathbf{Pr}_s(M \text{ acepte } w) = \frac{|\{s \in \{0,1\}^* \mid |s| = g(n) \text{ y } M(w,s) \text{ acepta}\}|}{2^{g(n)}}$$

Clases de complejidad probabilísticas

Vamos a definir una primera clase de complejidad considerando los algoritmos probabilísticos

- Esto nos va a permitir decir cuando un lenguaje es *aceptado* por una MT probabilística

Clases de complejidad probabilísticas

Vamos a definir una primera clase de complejidad considerando los algoritmos probabilísticos

- Esto nos va a permitir decir cuando un lenguaje es *aceptado* por una MT probabilística

Definición

Sea L un lenguaje sobre un alfabeto Σ. Entonces L está en RP 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* $\mathbf{Pr}(M \text{ acepte } w) \geq \frac{3}{4}$
- *Si $w \notin L$, entonces* $\mathbf{Pr}(M \text{ acepte } w) = 0$

Clases de complejidad probabilísticas

Vamos a definir una primera clase de complejidad considerando los algoritmos probabilísticos

- Esto nos va a permitir decir cuando un lenguaje es *aceptado* por una MT probabilística

Definición

Sea L un lenguaje sobre un alfabeto Σ. Entonces L está en RP 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* $\mathbf{Pr}(M \text{ acepte } w) \geq \frac{3}{4}$
- *Si $w \notin L$, entonces* $\mathbf{Pr}(M \text{ acepte } w) = 0$

Vale decir, para los lenguaje en RP tenemos algoritmos probabilísticos que pueden cometer errores sólo para los elementos que están en L

¿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 $\mathbf{Pr}(M \text{ acepte } w) \geq 1 - \frac{1}{4^\ell}$
- Si $w \notin L$, entonces $\mathbf{Pr}(M \text{ acepte } w) = 0$

¿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 $\mathbf{Pr}(M \text{ acepte } w) \geq 1 - \frac{1}{4^\ell}$
- Si $w \notin L$, entonces $\mathbf{Pr}(M \text{ acepte } w) = 0$

Ejercicio

Demuestre el lema de amplificación.

¿Dónde está la clase RP?

Teorema

$P \subseteq RP \subseteq NP$

¿Dónde está la clase RP?

Teorema

$P \subseteq RP \subseteq NP$

Ejercicio

Demuestre el teorema.

¿Dónde está la clase RP?

Teorema

$P \subseteq RP \subseteq NP$

Ejercicio

Demuestre el teorema.

Corolario

$P \subseteq co\text{-}RP \subseteq co\text{-}NP$

¿Qué sabemos sobre RP y co-RP?

Son problemas abiertos si P = RP o RP = co-RP

¿Qué sabemos sobre RP y co-RP?

Son problemas abiertos si P $=$ RP o RP $=$ co-RP

Pero se cree que P $=$ RP

- Puesto que si $L \in$ 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 RP $=$ co-RP $=$ P

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

¿Dónde está la clase BPP?

Teorema

$BPP = co\text{-}BPP$

¿Dónde está la clase BPP?

Teorema

$BPP = co\text{-}BPP$

Ejercicio

Demuestre el teorema.

¿Dónde está la clase BPP?

Teorema

BPP = co-BPP

Ejercicio

Demuestre el teorema.

Corolario

RP $\subseteq$ *BPP y co-RP* $\subseteq$ *BPP*

¿Dónde está la clase BPP?

Es un problema abierto si $\mathsf{P} = \mathsf{BPP}$

¿Dónde está la clase BPP?

Es un problema abierto si P = BPP

- De esto se concluiría que BPP = RP = co-RP = P

¿Dónde está la clase BPP?

Es un problema abierto si P = BPP

- De esto se concluiría que BPP = RP = co-RP = P

Vamos a demostrar que BPP está contenida en la jerarquía polinomial.

- En esta demostración vamos a considerar una versión equivalente pero más simple de la definición de BPP

Simplificando la definición de BPP

Sea M una MT probabilística con alfabeto de entrada Σ

Simplificando la definición de BPP

Sea M una MT probabilística con alfabeto de entrada Σ

Dado $w \in \Sigma^*$ y $s \in \{0,1\}^*$ tal que $t_M(|w|) \leq |s|$, decimos que $M(w,s)$ es incorrecto si:

$$w \in L \text{ y } M(w,s) \text{ rechaza}$$
$$\text{o}$$
$$w \notin L \text{ y } M(w,s) \text{ acepta}$$

Simplificando la definición de BPP

Sea M una MT probabilística con alfabeto de entrada Σ

Dado $w \in \Sigma^*$ y $s \in \{0,1\}^*$ tal que $t_M(|w|) \leq |s|$, decimos que $M(w,s)$ es incorrecto si:

$$w \in L \text{ y } M(w,s) \text{ rechaza}$$
$$\text{o}$$
$$w \notin L \text{ y } M(w,s) \text{ acepta}$$

Vamos a utilizar esta noción para dar una definición más simple de BPP

Una definición equivalente de BPP

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 $w \in \Sigma^*$:

$$\mathbf{Pr}_s(M(w,s) \text{ es incorrecto}) \leq \frac{1}{4}$$

Un lema de amplificación para BPP

Al igual que para el caso de RP, el valor $\frac{1}{4}$ en la definición de BPP pueden ser reemplazado por un valor arbitrariamente más pequeño.

Un lema de amplificación para BPP

Al igual que para el caso de RP, el valor $\frac{1}{4}$ en la definición de BPP pueden ser reemplazado por un valor arbitrariamente más pequeño.

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 $w \in \Sigma^*$:

$$\mathbf{Pr}_s(M(w,s) \text{ es incorrecto}) \quad \leq \quad \left(\frac{3}{4}\right)^{\ell}$$

Un lema de amplificación para BPP

Al igual que para el caso de RP, el valor $\frac{1}{4}$ en la definición de BPP pueden ser reemplazado por un valor arbitrariamente más pequeño.

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 $w \in \Sigma^*$:

$$\mathbf{Pr}_s(M(w,s) \text{ es incorrecto}) \quad \leq \quad \left(\frac{3}{4}\right)^{\ell}$$

Ejercicio

Demuestre el lema de amplificación para BPP.

BPP está en la jerarquía polinomial

Teorema (Gács-Sipser-Lautemann)

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

BPP está en la jerarquía polinomial

Teorema (Gács-Sipser-Lautemann)

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

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

BPP está en la jerarquía polinomial

Teorema (Gács-Sipser-Lautemann)

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

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

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

Primer ingrediente: una caracterización de Σ_2^P

Proposition

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 $B \in P$ y para todo $u \in \Sigma^*$:

$u \in L$ *si y sólo si*

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

Primer ingrediente: una caracterización de Σ_2^P

Proposition

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 $B \in P$ 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

¿Cómo se concluye que esta caracterización es cierta?

Segundo ingrediente: una versión más fuerte del lema de amplificación

Proposition

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

$$\mathbf{Pr}_s(M(w,s) \text{ es incorrecto}) \leq \frac{1}{3t_M(|w|)}$$

Demostración de BPP $\subseteq \Sigma_2^P$

Sea L un lenguaje sobre un alfabeto Σ, y suponga que $L \in$ BPP

Demostración de BPP $\subseteq \Sigma_2^P$

Sea L un lenguaje sobre un alfabeto Σ, y suponga que $L \in$ BPP

Por lema de amplificación existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

$$\mathbf{Pr}_s(M(w,s) \text{ es incorrecto}) \quad \leq \quad \frac{1}{3t_M(|w|)}$$

Demostración de BPP $\subseteq \Sigma_2^P$

Sea L un lenguaje sobre un alfabeto Σ, y suponga que $L \in$ BPP

Por lema de amplificación existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

$$\mathbf{Pr}_s(M(w,s) \text{ es incorrecto}) \quad \leq \quad \frac{1}{3t_M(|w|)}$$

Además podemos suponer que $t_M(n) > 0$ para cada $n \in \mathbb{N}$

- ¿Por qué?

Demostración de BPP $\subseteq \Sigma_2^P$

Notación

Dados a y b en $\{0,1\}$, la operación $a \oplus b$ es definida como $(a+b) \bmod 2$

- Vale decir, $\oplus$ es el o exclusivo

Dados $x, y \in \{0,1\}^m$ con $x = a_1 a_2 \cdots a_m$ e $y = b_1 b_2 \cdots b_m$, la operación $x \oplus y$ da como resultado el siguiente string en $\{0,1\}^m$:

$$(a_1 \oplus b_1)(a_2 \oplus b_2) \cdots (a_m \oplus b_m)$$

Demostración de BPP $\subseteq \Sigma_2^P$

Defina el lenguaje A de la siguiente forma:

$$A = \{(w, y_1, \ldots, y_m, z) \mid w \in \Sigma^*, m = t_M(|w|), \\ y_i \in \{0,1\}^m \text{ para cada } i \in \{1, \ldots, m\}, z \in \{0,1\}^m \\ \text{y } M(w, y_j \oplus z) \text{ acepta para algún } j \in \{1, \ldots, m\} \}$$

Demostración de BPP $\subseteq \Sigma_2^P$

Defina el lenguaje A de la siguiente forma:

$$A = \{(w, y_1, \ldots, y_m, z) \mid w \in \Sigma^*, m = t_M(|w|), \\ y_i \in \{0,1\}^m \text{ para cada } i \in \{1, \ldots, m\}, z \in \{0,1\}^m \\ \text{y } M(w, y_j \oplus z) \text{ acepta para algún } j \in \{1, \ldots, m\} \}$$

Ejercicio

Demuestre que $A \in \mathrm{P}$

Demostración de BPP $\subseteq \Sigma_2^P$

Dada la caracterización de Σ_2^P en las transparencias anteriores, para demostrar que $L \in \Sigma_2^P$ basta demostrar la siguiente condición:

Para cada $w \in \Sigma^*$ tal que $t_M(|w|) = m$:

$w \in L$ si y sólo si

$$\exists y_1 \in \{0,1\}^m \cdots \exists y_m \in \{0,1\}^m \, \forall z \in \{0,1\}^m \, (w, y_1, \ldots, y_m, z) \in A$$

Demostración de BPP $\subseteq \Sigma_2^P$

Dada la caracterización de Σ_2^P en las transparencias anteriores, para demostrar que $L \in \Sigma_2^P$ basta demostrar la siguiente condición:

Para cada $w \in \Sigma^*$ tal que $t_M(|w|) = m$:

$w \in L$ si y sólo si

$$\exists y_1 \in \{0,1\}^m \cdots \exists y_m \in \{0,1\}^m \, \forall z \in \{0,1\}^m \, (w, y_1, \ldots, y_m, z) \in A$$

Para hacer esta demostración vamos a utilizar el método probabilístico.

- Para demostrar que un objeto con ciertas propiedades existe, en lugar de construirlo demostramos que la probabilidad de que exista es mayor que 0

La dirección ($\Rightarrow$) de la equivalencia

Suponga que $w \in L$ y $t_M(|w|) = m$

La dirección ($\Rightarrow$) de la equivalencia

Suponga que $w \in L$ y $t_M(|w|) = m$

Tenemos que:

$$\mathbf{Pr}_{y_1,\ldots,y_m}\left(\exists z \in \{0,1\}^m \bigwedge_{i=1}^{m} M(w, y_i \oplus z) \text{ rechaza}\right) \leq$$

$$\sum_{z\in\{0,1\}^m} \mathbf{Pr}_{y_1,\ldots,y_m}\left(\bigwedge_{i=1}^{m} M(w, y_i \oplus z) \text{ rechaza}\right) =$$

$$\sum_{z\in\{0,1\}^m} \prod_{i=1}^{m} \mathbf{Pr}_{y_i}\left(M(w, y_i \oplus z) \text{ rechaza}\right)$$

La dirección ($\Rightarrow$) de la equivalencia

Dado $a \in \{0,1\}^m$, la función $f : \{0,1\}^m \to \{0,1\}^m$ definida como $f(x) = x \oplus a$ es inyectiva

La dirección ($\Rightarrow$) de la equivalencia

Dado $a \in \{0,1\}^m$, la función $f : \{0,1\}^m \to \{0,1\}^m$ definida como $f(x) = x \oplus a$ es inyectiva

Por lo tanto dado que $w \in L$, concluimos que:

$$\mathbf{Pr}_{y_i}\Big(M(w, y_i \oplus z) \text{ rechaza}\Big) \quad \leq \quad \frac{1}{3m}$$

La dirección ($\Rightarrow$) de la equivalencia

Dado que $m > 0$ concluimos que:

$$\mathbf{Pr}_{y_1,\ldots,y_m}\left(\exists z \in \{0,1\}^m \bigwedge_{i=1}^{m} M(w, y_i \oplus z) \text{ rechaza}\right) \leq$$

$$\sum_{z\in\{0,1\}^m} \prod_{i=1}^{m} \mathbf{Pr}_{y_i}\left(M(w, y_i \oplus z) \text{ rechaza}\right) \leq$$

$$\sum_{z\in\{0,1\}^m} \prod_{i=1}^{m} \frac{1}{3m} =$$

$$\sum_{z\in\{0,1\}^m} \frac{1}{(3m)^m} =$$

$$\frac{2^m}{(3m)^m} < 1$$

La dirección ($\Rightarrow$) de la equivalencia

Por lo tanto existen $y_1 \in \{0,1\}^m$, ..., $y_m \in \{0,1\}^m$ tales que la siguiente condición es cierta:

$$\forall z \in \{0,1\}^m \bigvee_{i=1}^{m} M(w, y_i \oplus z) \text{ acepta}$$

La dirección ($\Rightarrow$) de la equivalencia

Por lo tanto existen $y_1 \in \{0,1\}^m$, ..., $y_m \in \{0,1\}^m$ tales que la siguiente condición es cierta:

$$\forall z \in \{0,1\}^m \bigvee_{i=1}^{m} M(w, y_i \oplus z) \text{ acepta}$$

Concluimos que:

$$\exists y_1 \in \{0,1\}^m \cdots \exists y_m \in \{0,1\}^m \, \forall z \in \{0,1\}^m \, (w, y_1, \ldots, y_m, z) \in A$$

La dirección ($\Leftarrow$) de la equivalencia

Suponga que $w \notin L$ y $t_M(|w|) = m$

- Para demostrar la dirección ($\Leftarrow$) consideramos el contrapositivo

La dirección ($\Leftarrow$) de la equivalencia

Suponga que $w \notin L$ y $t_M(|w|) = m$

- Para demostrar la dirección ($\Leftarrow$) consideramos el contrapositivo

Además, suponga que $y_1 \in \{0,1\}^m$, ..., $y_m \in \{0,1\}^m$

La dirección ($\Leftarrow$) de la equivalencia

Suponga que $w \notin L$ y $t_M(|w|) = m$

- Para demostrar la dirección ($\Leftarrow$) consideramos el contrapositivo

Además, suponga que $y_1 \in \{0,1\}^m$, ..., $y_m \in \{0,1\}^m$

Dado que $w \notin L$ y $m > 0$ tenemos que:

$$\begin{aligned}
\mathbf{Pr}_z\left(\bigvee_{i=1}^{m} M(w, y_i \oplus z) \text{ acepta}\right) &\leq \sum_{i=1}^{m} \mathbf{Pr}_z\Big(M(w, y_i \oplus z) \text{ acepta}\Big) \\
&\leq \sum_{i=1}^{m} \frac{1}{3m} \\
&= \frac{m}{3m} \\
&= \frac{1}{3}
\end{aligned}$$

La dirección ($\Leftarrow$) de la equivalencia

Se concluye que:

$$\begin{aligned}
\mathbf{Pr}_z\left(\bigwedge_{i=1}^{m} M(w, y_i \oplus z) \text{ rechaza}\right) &= 1 - \mathbf{Pr}_z\left(\bigvee_{i=1}^{m} M(w, y_i \oplus z) \text{ acepta}\right) \\
&\geq 1 - \frac{1}{3} \\
&= \frac{2}{3}
\end{aligned}$$

La dirección ($\Leftarrow$) de la equivalencia

Se concluye que:

$$\begin{aligned}
\mathbf{Pr}_z\left(\bigwedge_{i=1}^{m} M(w, y_i \oplus z) \text{ rechaza}\right) &= 1 - \mathbf{Pr}_z\left(\bigvee_{i=1}^{m} M(w, y_i \oplus z) \text{ acepta}\right) \\
&\geq 1 - \frac{1}{3} \\
&= \frac{2}{3}
\end{aligned}$$

Por lo tanto tenemos que existe $z \in \{0,1\}^m$ tal que $M(w, y_i \oplus z)$ rechaza para cada $i \in \{1, \ldots, m\}$

La dirección ($\Leftarrow$) de la equivalencia

Dado que $y_1, \ldots, y_m$ son elementos arbitrarios en el conjunto $\{0,1\}^m$, tenemos finalmente que:

$$\forall y_1 \in \{0,1\}^m \cdots \forall y_m \in \{0,1\}^m \, \exists z \in \{0,1\}^m \, (w, y_1, \ldots, y_m, z) \notin A$$

□

Las clases de complejidad probabilísticas en una figura