La relación de AM con la jerarquía baja

Teorema (Schöning)

$\mathrm{NP} \cap \text{co-AM} \subseteq \mathrm{Low}_2$.

La demostración de NP $\cap$ co-AM $\subseteq$ Low$_2$

Seguimos los siguientes pasos:

La demostración de NP $\cap$ co-AM $\subseteq$ Low$_2$

Seguimos los siguientes pasos:

1. Definición de la clase BP·NP que extiende a NP y BPP.

La demostración de $\mathsf{NP} \cap \text{co-}\mathsf{AM} \subseteq \mathsf{Low}_2$

Seguimos los siguientes pasos:

1. Definición de la clase BP·NP que extiende a NP y BPP.
2. Demostración de que $\mathsf{BP}{\cdot}\mathsf{NP} = \mathsf{AM}$.

La demostración de $\mathrm{NP} \cap \text{co-AM} \subseteq \mathrm{Low}_2$

Seguimos los siguientes pasos:

1. Definición de la clase BP·NP que extiende a NP y BPP.
2. Demostración de que $\mathrm{BP{\cdot}NP} = \mathrm{AM}$.
3. Enunciado de un lema de amplificación para BP·NP.

La demostración de $\mathrm{NP} \cap \text{co-AM} \subseteq \mathrm{Low}_2$

Seguimos los siguientes pasos:

1. Definición de la clase BP·NP que extiende a NP y BPP.
2. Demostración de que $\mathrm{BP{\cdot}NP} = \mathrm{AM}$.
3. Enunciado de un lema de amplificación para BP·NP.
4. Demostración de que $\mathrm{NP} \cap \text{co-BP{\cdot}NP} \subseteq \mathrm{Low}_2$.

Extendiendo la definición de BPP

Recuerde que un lenguaje L sobre un alfabeto Σ 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 $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \geq \frac{3}{4}$
- Si $w \notin L$, entonces $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \leq \frac{1}{4}$

Extendiendo la definición de BPP

Recuerde que un lenguaje L sobre un alfabeto Σ 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 $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \geq \frac{3}{4}$
- Si $w \notin L$, entonces $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \leq \frac{1}{4}$

Podemos extender la definición permitiendo a M ser no determinista

- $M(w, s)$ acepta si y sólo si existe una ejecución de M con entrada (w, s) que se detiene en un estado final

La clase de complejidad BP·NP

Definición

Sea L un lenguaje sobre un alfabeto Σ. Entonces L está en BP·NP si existe una MT probabilística no determinista *M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:*

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

AM $=$ BP·NP

Tenemos que BPP $\subseteq$ BP·NP y NP $\subseteq$ BP·NP

- ¿Por qué?

AM $=$ BP·NP

Tenemos que BPP $\subseteq$ BP·NP y NP $\subseteq$ BP·NP

- ¿Por qué?

Teorema

BP·NP $=$ AM.

La demostración de que $\mathrm{AM} = \mathrm{BP}{\cdot}\mathrm{NP}$

Considere la siguiente definición restringida de AM.

La demostración de que AM = BP·NP

Considere la siguiente definición restringida de AM. Para decidir si x pertenece a un lenguaje:

La demostración de que AM = BP·NP

Considere la siguiente definición restringida de AM. Para decidir si x pertenece a un lenguaje:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r usados.

La demostración de que AM = BP·NP

Considere la siguiente definición restringida de AM. Para decidir si x pertenece a un lenguaje:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r usados.
- **D** responde con un string m.

La demostración de que AM $=$ BP·NP

Considere la siguiente definición restringida de AM. Para decidir si x pertenece a un lenguaje:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r usados.
- **D** responde con un string m.
- **V** calcula el valor Booleano $F(x, r, m)$. Si $F(x, r, m) = 1$ entonces acepta, si no rechaza.

La demostración de que AM $=$ BP·NP

Considere la siguiente definición restringida de AM. Para decidir si x pertenece a un lenguaje:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r usados.
- **D** responde con un string m.
- **V** calcula el valor Booleano $F(x, r, m)$. Si $F(x, r, m) = 1$ entonces acepta, si no rechaza.
  - F es una función que se puede calcular en tiempo polinomial.

La demostración de que AM $=$ BP$\cdot$NP

Considere la siguiente definición restringida de AM. Para decidir si x pertenece a un lenguaje:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r usados.
- **D** responde con un string m.
- **V** calcula el valor Booleano $F(x, r, m)$. Si $F(x, r, m) = 1$ entonces acepta, si no rechaza.
  - F es una función que se puede calcular en tiempo polinomial.
  - **V** no utiliza bits aleatorios adicionales después de recibir la respuesta de **D**.

La demostración de que AM $=$ BP$\cdot$NP

Considere la siguiente definición restringida de AM. Para decidir si x pertenece a un lenguaje:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r usados.
- **D** responde con un string m.
- **V** calcula el valor Booleano $F(x, r, m)$. Si $F(x, r, m) = 1$ entonces acepta, si no rechaza.
  - F es una función que se puede calcular en tiempo polinomial.
  - **V** no utiliza bits aleatorios adicionales después de recibir la respuesta de **D**.

Llamamos $\text{AM}_{\text{non-adaptative}}$ a la clase definida por este protocolo.

La demostración de que AM $=$ BP·NP

Teorema

$BP{\cdot}NP = AM_{non\text{-}adaptative}$.

La demostración de que AM $=$ BP·NP

Teorema

$BP{\cdot}NP = AM_{non\text{-}adaptative}$.

Ejercicio

Demuestre el teorema.

La demostración de que AM = BP·NP

Teorema

$AM = AM_{non\text{-}adaptative}$.

La demostración de que AM = BP·NP

Teorema

$AM = AM_{\text{non-adaptative}}$.

De los dos teoremas anteriores obtenemos que AM = BP·NP.

La demostración de que AM $=$ BP·NP

Teorema

$AM = AM_{non\text{-}adaptative}$.

De los dos teoremas anteriores obtenemos que AM $=$ BP·NP.

- En la siguientes láminas vamos a demostrar que AM $\subseteq$ AM$_{\text{non-adaptative}}$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Suponga que $L \in$ AM.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Suponga que $L \in$ AM.

Entonces existe un protocolo que realiza los siguientes pasos para decidir si $x \in L$:

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Suponga que $L \in$ AM.

Entonces existe un protocolo que realiza los siguientes pasos para decidir si $x \in L$:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r_1 usados.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Suponga que $L \in$ AM.

Entonces existe un protocolo que realiza los siguientes pasos para decidir si $x \in L$:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r_1 usados.
- **D** responde con un string m.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Suponga que $L \in$ AM.

Entonces existe un protocolo que realiza los siguientes pasos para decidir si $x \in L$:

- **V** envía una pregunta a **D** que incluye los bits aleatorios r_1 usados.
- **D** responde con un string m.
- **V** genera otros bits aleatorios r_2 y calcula el valor Booleano $F(x, r_1, m, r_2)$. Si $F(x, r_1, m, r_2) = 1$ entonces acepta, si no rechaza.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Para **V** se cumple que:

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Para $\mathbf{V}$ se cumple que:

- Si $x \in L$, entonces existe demostrador $\mathbf{D}$ tal que

$$\mathbf{Pr}((\mathbf{V}, \mathbf{D}) \text{ acepta } x) \quad \geq \quad \frac{3}{4}$$

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$

Para **V** se cumple que:

- Si $x \in L$, entonces existe demostrador **D** tal que

$$\mathbf{Pr}((\mathbf{V}, \mathbf{D}) \text{ acepta } x) \quad \geq \quad \frac{3}{4}$$

- Si $x \notin L$, entonces para todo demostrador **D'** se tiene que:

$$\mathbf{Pr}((\mathbf{V}, \mathbf{D'}) \text{ acepta } x) \quad \leq \quad \frac{1}{4}$$

La demostración de que $\mathsf{AM} \subseteq \mathsf{AM}_{\text{non-adaptative}}$

Vamos a demostrar que $L \in \mathsf{AM}_{\text{non-adaptative}}$.

La demostración de que $\mathsf{AM} \subseteq \mathsf{AM}_{\text{non-adaptative}}$

Vamos a demostrar que $L \in \mathsf{AM}_{\text{non-adaptative}}$.

Fije un string x para el cual queremos decidir si $x \in L$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Vamos a demostrar que $L \in \text{AM}_{\text{non-adaptative}}$.

Fije un string x para el cual queremos decidir si $x \in L$.

Sea p un polinomio tal que el largo de los dos strings aleatorios utilizados por **V** es $p(|x|)$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Vamos a demostrar que $L \in \text{AM}_{\text{non-adaptative}}$.

Fije un string x para el cual queremos decidir si $x \in L$.

Sea p un polinomio tal que el largo de los dos strings aleatorios utilizados por **V** es $p(|x|)$.

- Sea $\ell = p(|x|)$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Considere la clase de función de hashing $\mathcal{H}(i,j)$.

- Recuerde que esta es una familia universal, que además satisface la propiedad de 2-independencia.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Considere la clase de función de hashing $\mathcal{H}(i, j)$.

- Recuerde que esta es una familia universal, que además satisface la propiedad de 2-independencia.

Defina un protocolo que con entrada x realiza los siguientes pasos:

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$

Considere la clase de función de hashing $\mathcal{H}(i, j)$.

- Recuerde que esta es una familia universal, que además satisface la propiedad de 2-independencia.

Defina un protocolo que con entrada x realiza los siguientes pasos:

- En la primera ronda **V'** elige al azar y con distribución uniforme $r_1 \in \{0, 1\}^\ell$, $z \in \{0, 1\}^\ell$ y $h \in \mathcal{H}(\ell, \ell)$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Considere la clase de función de hashing $\mathcal{H}(i, j)$.

- Recuerde que esta es una familia universal, que además satisface la propiedad de 2-independencia.

Defina un protocolo que con entrada x realiza los siguientes pasos:

- En la primera ronda **V'** elige al azar y con distribución uniforme $r_1 \in \{0,1\}^\ell$, $z \in \{0,1\}^\ell$ y $h \in \mathcal{H}(\ell, \ell)$.
- **V'** envía r_1, z, h a **D**.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Considere la clase de función de hashing $\mathcal{H}(i, j)$.

- Recuerde que esta es una familia universal, que además satisface la propiedad de 2-independencia.

Defina un protocolo que con entrada x realiza los siguientes pasos:

- En la primera ronda **V'** elige al azar y con distribución uniforme $r_1 \in \{0,1\}^\ell$, $z \in \{0,1\}^\ell$ y $h \in \mathcal{H}(\ell, \ell)$.
- **V'** envía r_1, z, h a **D**.
- **D** responde con un par de strings m, r_2 tal que $F(x, r_1, m, r_2) = 1$ y $h(r_2) = z$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Considere la clase de función de hashing $\mathcal{H}(i, j)$.

- Recuerde que esta es una familia universal, que además satisface la propiedad de 2-independencia.

Defina un protocolo que con entrada x realiza los siguientes pasos:

- En la primera ronda **V'** elige al azar y con distribución uniforme $r_1 \in \{0,1\}^\ell$, $z \in \{0,1\}^\ell$ y $h \in \mathcal{H}(\ell, \ell)$.
- **V'** envía r_1, z, h a **D**.
- **D** responde con un par de strings m, r_2 tal que $F(x, r_1, m, r_2) = 1$ y $h(r_2) = z$.
- **V'** calcula el valor Booleano $F(x, r_1, m, r_2)$. Si $F(x, r_1, m, r_2) = 1$ entonces acepta, si no rechaza.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

El procedimiento anterior es un protocolo AM$_{\text{non-adaptative}}$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

El procedimiento anterior es un protocolo AM$_{\text{non-adaptative}}$.

Tenemos que demostrar que para **V'** se cumple que:

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

El procedimiento anterior es un protocolo AM$_{\text{non-adaptative}}$.

Tenemos que demostrar que para **V'** se cumple que:

- Si $x \in L$, entonces existe demostrador **D** tal que

$$\mathbf{Pr}((\mathbf{V'}, \mathbf{D}) \text{ acepte } x) \quad \geq \quad \frac{3}{4}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

El procedimiento anterior es un protocolo AM$_{\text{non-adaptative}}$.

Tenemos que demostrar que para **V'** se cumple que:

- Si $x \in L$, entonces existe demostrador **D** tal que

$$\mathbf{Pr}((\mathbf{V'}, \mathbf{D}) \text{ acepte } x) \quad \geq \quad \frac{3}{4}$$

- Si $x \notin L$, entonces para todo demostrador **D'** se tiene que:

$$\mathbf{Pr}((\mathbf{V'}, \mathbf{D'}) \text{ acepte } x) \quad \leq \quad \frac{1}{4}$$

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$

Sea

$$W_{r_1} \quad = \quad \{r_2 \in \{0,1\}^{\ell} \mid \text{ existe string } m \text{ tal que } F(x, r_1, m, r_2) = 1\}.$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Sea

$$W_{r_1} \quad = \quad \{r_2 \in \{0,1\}^{\ell} \mid \text{ existe string } m \text{ tal que } F(x, r_1, m, r_2) = 1\}.$$

Sabemos que:

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Sea

$$W_{r_1} \quad = \quad \{r_2 \in \{0,1\}^{\ell} \mid \text{ existe string } m \text{ tal que } F(x, r_1, m, r_2) = 1\}.$$

Sabemos que:

- Si $x \in L$, entonces $\mathbf{Pr}_{r_1, r_2}(r_2 \in W_{r_1}) \geq \dfrac{3}{4}$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Sea

$$W_{r_1} \quad = \quad \{r_2 \in \{0,1\}^{\ell} \mid \text{ existe string } m \text{ tal que } F(x, r_1, m, r_2) = 1\}.$$

Sabemos que:

- Si $x \in L$, entonces $\mathbf{Pr}_{r_1, r_2}(r_2 \in W_{r_1}) \geq \frac{3}{4}$
- Si $x \notin L$, entonces $\mathbf{Pr}_{r_1, r_2}(r_2 \in W_{r_1}) \leq \frac{1}{4}$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$

Además, tenemos que:

$$\begin{aligned}
\mathbf{Pr}_{r_1,r_2}(r_2 \in W_{r_1}) &= \sum_{s_1 \in \{0,1\}^\ell} \mathbf{Pr}_{r_1,r_2}(r_2 \in W_{r_1} \mid r_1 = s_1) \cdot \mathbf{Pr}_{r_1,r_2}(r_1 = s_1) \\
&= \sum_{s_1 \in \{0,1\}^\ell} \mathbf{Pr}_{r_2}(r_2 \in W_{s_1}) \cdot \frac{1}{2^\ell} \\
&= \frac{1}{2^\ell} \sum_{s_1 \in \{0,1\}^\ell} \frac{|W_{s_1}|}{2^\ell} \\
&= \frac{1}{2^{2\ell}} \sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}|
\end{aligned}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \notin L$

Consideramos primero el caso $x \notin L$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \notin L$

Consideramos primero el caso $x \notin L$.

Por los resultados anteriores, tenemos que:

$$\frac{1}{2^{2\ell}} \sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}| \quad \leq \quad \frac{1}{4}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \notin L$

Consideramos primero el caso $x \notin L$.

Por los resultados anteriores, tenemos que:

$$\frac{1}{2^{2\ell}} \sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}| \quad \leq \quad \frac{1}{4}$$

Por lo tanto:

$$\sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}| \quad \leq \quad \frac{2^{2\ell}}{4}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \notin L$

En este caso necesitamos acotar superiormente la siguiente probabilidad:

$$\mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \right)$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \notin L$

En este caso necesitamos acotar superiormente la siguiente probabilidad:

$$\mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \right)$$

Tenemos que:

$$\mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \right) \; =$$

$$\sum_{s_1 \in \{0,1\}^\ell} \mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \;\middle|\; r_1 = s_1 \right) \cdot \mathbf{Pr}_{h,z,r_1}(r_1 = s_1) \; =$$

$$\frac{1}{2^\ell} \sum_{s_1 \in \{0,1\}^\ell} \mathbf{Pr}_{h,z}\left(\bigvee_{r_2 \in W_{s_1}} h(r_2) = z \right)$$

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \notin L$

Así, tenemos que:

$$
\begin{aligned}
\mathbf{Pr}_{h,z,r_1}\Bigg(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \Bigg) \ &= \\
& \frac{1}{2^\ell} \sum_{s_1 \in \{0,1\}^\ell} \mathbf{Pr}_{h,z}\Bigg(\bigvee_{r_2 \in W_{s_1}} h(r_2) = z \Bigg) \ \leq \\
& \frac{1}{2^\ell} \sum_{s_1 \in \{0,1\}^\ell} \sum_{r_2 \in W_{s_1}} \mathbf{Pr}_{h,z}(h(r_2) = z) \ = \\
& \frac{1}{2^\ell} \sum_{s_1 \in \{0,1\}^\ell} \sum_{r_2 \in W_{s_1}} \frac{1}{2^\ell} \ = \\
& \frac{1}{2^{2\ell}} \sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}| \ \leq \\
& \frac{1}{2^{2\ell}} \cdot \frac{2^{2\ell}}{4} \ = \ \frac{1}{4}
\end{aligned}
$$

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \notin L$

Dado que:

$$\mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \right) \quad \leq \quad \frac{1}{4}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \notin L$

Dado que:

$$\mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z\right) \quad \leq \quad \frac{1}{4}$$

Concluimos que para todo demostrador **D'** se tiene que:

$$\mathbf{Pr}((\mathbf{V'}, \mathbf{D'}) \text{ acepte } x) \quad \leq \quad \frac{1}{4}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Consideramos ahora el caso $x \in L$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Consideramos ahora el caso $x \in L$.

Por los resultados anteriores, tenemos que:

$$\frac{1}{2^{2\ell}} \sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}| \quad \geq \quad \frac{3}{4}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Consideramos ahora el caso $x \in L$.

Por los resultados anteriores, tenemos que:

$$\frac{1}{2^{2\ell}} \sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}| \quad \geq \quad \frac{3}{4}$$

Por lo tanto:

$$\sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}| \quad \geq \quad \frac{3 \cdot 2^{2\ell}}{4}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

En este caso necesitamos acotar inferiormente la siguiente probabilidad:

$$\mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \right)$$

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \in L$

En este caso necesitamos acotar inferiormente la siguiente probabilidad:

$$\mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \right)$$

Dado $r_1 \in \{0,1\}^\ell$, $h \in \mathcal{H}(\ell,\ell)$ y $z \in \{0,1\}^\ell$, defina:

$$X_{r_1}(h,z) \quad = \quad |\{r_2 \mid r_2 \in W_{r_1} \text{ y } h(r_2) = z\}|$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

En este caso necesitamos acotar inferiormente la siguiente probabilidad:

$$\mathbf{Pr}_{h,z,r_1}\left(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \right)$$

Dado $r_1 \in \{0,1\}^\ell$, $h \in \mathcal{H}(\ell,\ell)$ y $z \in \{0,1\}^\ell$, defina:

$$X_{r_1}(h,z) \quad = \quad |\{r_2 \mid r_2 \in W_{r_1} \text{ y } h(r_2) = z\}|$$

Queremos dar una cota inferior para $\mathbf{Pr}_{h,z}(X_{r_1} > 0)$.

La desigualdad de Paley–Zygmund

Teorema (Paley–Zygmund)

Sea Z una variable aleatoria discreta tal que $Z \geq 0$ y $\theta \in [0, 1]$. Se tiene que:

$$\mathbf{Pr}(Z > \theta \cdot E[Z]) \quad \geq \quad (1 - \theta)^2 \cdot \frac{E[Z]^2}{E[Z^2]}$$

La desigualdad de Paley–Zygmund

Teorema (Paley–Zygmund)

Sea Z una variable aleatoria discreta tal que $Z \geq 0$ y $\theta \in [0, 1]$. Se tiene que:

$$\mathbf{Pr}(Z > \theta \cdot E[Z]) \quad \geq \quad (1 - \theta)^2 \cdot \frac{E[Z]^2}{E[Z^2]}$$

Corolario

Sea Z una variable aleatoria discreta tal que $Z \geq 0$. Se tiene que:

$$\mathbf{Pr}(Z > 0) \quad \geq \quad \frac{E[Z]^2}{E[Z^2]}$$

Demostración de la desigualdad de Paley–Zygmund

Tenemos que:

$$\begin{aligned}
E[Z] &= \sum_{z} z \cdot \mathbf{Pr}(Z = z) \\
&= \sum_{z \,:\, z \leq \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) + \sum_{z \,:\, z > \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) \\
&\leq \theta \cdot E[Z] + \sum_{z \,:\, z > \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z)
\end{aligned}$$

Demostración de la desigualdad de Paley–Zygmund

Tenemos que:

$$\begin{aligned} E[Z] &= \sum_{z} z \cdot \mathbf{Pr}(Z = z) \\ &= \sum_{z\,:\,z \leq \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) + \sum_{z\,:\,z > \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) \\ &\leq \theta \cdot E[Z] + \sum_{z\,:\,z > \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) \end{aligned}$$

Por lo tanto:

$$\sum_{z\,:\,z > \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) \quad \geq \quad (1 - \theta) \cdot E[Z]$$

Demostración de la desigualdad de Paley–Zygmund

Por la desigualdad de Cauchy-Schwarz:

$$\left(\sum_{z\,:\,z>\theta\cdot E[Z]} z\cdot\mathbf{Pr}(Z=z)\right)^2 =$$

$$\left(\sum_{z\,:\,z>\theta\cdot E[Z]} (z\cdot\sqrt{\mathbf{Pr}(Z=z)})\cdot\sqrt{\mathbf{Pr}(Z=z)}\right)^2 \le$$

$$\left(\sum_{z\,:\,z>\theta\cdot E[Z]} z^2\cdot\mathbf{Pr}(Z=z)\right)\cdot\left(\sum_{z\,:\,z>\theta\cdot E[Z]}\mathbf{Pr}(Z=z)\right) \le$$

$$E[Z^2]\cdot\mathbf{Pr}(Z>\theta\cdot E[Z])$$

Demostración de la desigualdad de Paley–Zygmund

Dado que $Z \geq 0$, sabemos que $E[Z] \geq 0$.

Demostración de la desigualdad de Paley–Zygmund

Dado que $Z \geq 0$, sabemos que $E[Z] \geq 0$.

Entonces dado que $\theta \in [0,1]$:

$$\left(\sum_{z\,:\,Z > \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) \right)^2 \quad \geq \quad (1-\theta)^2 \cdot E[Z]^2$$

Demostración de la desigualdad de Paley–Zygmund

Dado que $Z \geq 0$, sabemos que $E[Z] \geq 0$.

Entonces dado que $\theta \in [0,1]$:

$$\left(\sum_{z \,:\, Z > \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) \right)^2 \quad \geq \quad (1-\theta)^2 \cdot E[Z]^2$$

Poniendo todo junto concluimos que:

$$E[Z^2] \cdot \mathbf{Pr}(Z > \theta \cdot E[Z]) \quad \geq \quad (1-\theta)^2 \cdot E[Z]^2$$

Demostración de la desigualdad de Paley–Zygmund

Dado que $Z \geq 0$, sabemos que $E[Z] \geq 0$.

Entonces dado que $\theta \in [0, 1]$:

$$\left(\sum_{z\,:\,Z > \theta \cdot E[Z]} z \cdot \mathbf{Pr}(Z = z) \right)^2 \quad \geq \quad (1 - \theta)^2 \cdot E[Z]^2$$

Poniendo todo junto concluimos que:

$$E[Z^2] \cdot \mathbf{Pr}(Z > \theta \cdot E[Z]) \quad \geq \quad (1 - \theta)^2 \cdot E[Z]^2$$

Por lo tanto: $\mathbf{Pr}(Z > \theta \cdot E[Z]) \geq (1 - \theta)^2 \cdot \frac{E[Z]^2}{E[Z^2]}$ $\square$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Por la desigualdad de Paley–Zygmund concluimos que:

$$\mathbf{Pr}_{h,z}(X_{r_1} > 0) \quad \geq \quad \frac{E[X_{r_1}]^2}{E[X_{r_1}^2]}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Por la desigualdad de Paley–Zygmund concluimos que:

$$\mathbf{Pr}_{h,z}(X_{r_1} > 0) \quad \geq \quad \frac{E[X_{r_1}]^2}{E[X_{r_1}^2]}$$

Entonces tenemos que calcular $E[X_{r_1}]$ y $E[X_{r_1}^2]$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Dado $r_2 \in \{0,1\}^{\ell}$, $h \in \mathcal{H}(\ell,\ell)$ y $z \in \{0,1\}^{\ell}$, defina:

$$X_{r_1,r_2}(h,z) \quad = \quad \begin{cases} 1 & r_2 \in W_{r_1} \text{ y } h(r_2) = z \\ 0 & \text{en otro caso} \end{cases}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Dado $r_2 \in \{0,1\}^\ell$, $h \in \mathcal{H}(\ell,\ell)$ y $z \in \{0,1\}^\ell$, defina:

$$X_{r_1,r_2}(h,z) \quad = \quad \begin{cases} 1 & r_2 \in W_{r_1} \text{ y } h(r_2) = z \\ 0 & \text{en otro caso} \end{cases}$$

Tenemos que $X_{r_1} = \displaystyle\sum_{r_2 \in \{0,1\}^\ell} X_{r_1,r_2}$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Si $r_2 \in W_{r_1}$, para la variable aleatoria X_{r_1,r_2} tenemos que:

$$E[X_{r_1,r_2}] \;=\; 0 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 0) + 1 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1) \;=\; \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1) \;=\; \mathbf{Pr}_{h,z}(h(r_2) = z) \;=\; \frac{1}{2^{\ell}}$$

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \in L$

Si $r_2 \in W_{r_1}$, para la variable aleatoria X_{r_1,r_2} tenemos que:

$$E[X_{r_1,r_2}] \;=\; 0 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 0) + 1 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1) \;=\; \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1) \;=\; \mathbf{Pr}_{h,z}(h(r_2) = z) \;=\; \frac{1}{2^\ell}$$

Si $r_2 \notin W_{r_1}$, entonces $E[X_{r_1,r_2}] = 0$ ya que $\mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1) = 0$.

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \in L$

Si $r_2 \in W_{r_1}$, para la variable aleatoria X_{r_1,r_2} tenemos que:

$$E[X_{r_1,r_2}] \;=\; 0 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 0) + 1 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1) \;=\; \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1) \;=\; \mathbf{Pr}_{h,z}(h(r_2) = z) \;=\; \frac{1}{2^\ell}$$

Si $r_2 \notin W_{r_1}$, entonces $E[X_{r_1,r_2}] = 0$ ya que $\mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1) = 0$.

Por lo tanto:

$$E[X_{r_1}] \;=\; E\Bigg[\sum_{r_2 \in \{0,1\}^\ell} X_{r_1,r_2}\Bigg] \;=\; \sum_{r_2 \in \{0,1\}^\ell} E[X_{r_1,r_2}] \;=\; \sum_{r_2 \in W_{r_1}} \frac{1}{2^\ell} \;=\; \frac{|W_{r_1}|}{2^\ell}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Suponiendo que $r_2 \neq r_3$ para $r_2, r_3 \in W_{r_1}$, tenemos que:

$$\begin{aligned}
E[X_{r_1,r_2}X_{r_1,r_3}] &= 0 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2}X_{r_1,r_3} = 0) + 1 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2}X_{r_1,r_3} = 1) \\
&= \mathbf{Pr}_{h,z}(X_{r_1,r_2}X_{r_1,r_3} = 1) \\
&= \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1 \wedge X_{r_1,r_3} = 1) \\
&= \mathbf{Pr}_{h,z}(h(r_2) = z \wedge h(r_3) = z) \\
&= \frac{1}{2^{2\ell}}
\end{aligned}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Suponiendo que $r_2 \neq r_3$ para $r_2, r_3 \in W_{r_1}$, tenemos que:

$$\begin{aligned}
E[X_{r_1,r_2}X_{r_1,r_3}] &= 0 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2}X_{r_1,r_3} = 0) + 1 \cdot \mathbf{Pr}_{h,z}(X_{r_1,r_2}X_{r_1,r_3} = 1) \\
&= \mathbf{Pr}_{h,z}(X_{r_1,r_2}X_{r_1,r_3} = 1) \\
&= \mathbf{Pr}_{h,z}(X_{r_1,r_2} = 1 \wedge X_{r_1,r_3} = 1) \\
&= \mathbf{Pr}_{h,z}(h(r_2) = z \wedge h(r_3) = z) \\
&= \frac{1}{2^{2\ell}}
\end{aligned}$$

Suponiendo que $r_2 \neq r_3$ para $r_2, r_3 \in \{0,1\}^\ell$ tal que $r_2 \notin W_{r_1}$ o $r_3 \notin W_{r_1}$, tenemos que $E[X_{r_1,r_2}X_{r_1,r_3}] = 0$ ya que $\mathbf{Pr}_{h,z}(X_{r_1,r_2}X_{r_1,r_3} = 1) = 0$.

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \in L$

Entonces, considerando que $X_{r_1,r_2} = X_{r_1,r_2}^2$, obtenemos que:

$$
\begin{aligned}
E[X_{r_1}^2] &= E\left[\left(\sum_{r_2 \in \{0,1\}^\ell} X_{r_1,r_2}\right)^2\right] \\
&= E\left[\sum_{r_2,r_3 \in \{0,1\}^\ell \,:\, r_2 \neq r_3} X_{r_1,r_2} X_{r_1,r_3} + \sum_{r_2 \in \{0,1\}^\ell} X_{r_1,r_2}^2\right] \\
&= E\left[\sum_{r_2,r_3 \in \{0,1\}^\ell \,:\, r_2 \neq r_3} X_{r_1,r_2} X_{r_1,r_3} + \sum_{r_2 \in \{0,1\}^\ell} X_{r_1,r_2}\right] \\
&= \sum_{r_2,r_3 \in \{0,1\}^\ell \,:\, r_2 \neq r_3} E[X_{r_1,r_2} X_{r_1,r_3}] + \sum_{r_2 \in \{0,1\}^\ell} E[X_{r_1,r_2}] \\
&= \sum_{r_2,r_3 \in W_{r_1} \,:\, r_2 \neq r_3} E[X_{r_1,r_2} X_{r_1,r_3}] + \sum_{r_2 \in W_{r_1}} E[X_{r_1,r_2}] \\
&= \sum_{r_2,r_3 \in W_{r_1} \,:\, r_2 \neq r_3} \frac{1}{2^{2\ell}} + \sum_{r_2 \in W_{r_1}} \frac{1}{2^\ell} \\
&= \frac{|W_{r_1}| \cdot (|W_{r_1}| - 1)}{2^{2\ell}} + \frac{|W_{r_1}|}{2^\ell} \;\leq\; \frac{|W_{r_1}|^2}{2^{2\ell}} + \frac{|W_{r_1}|}{2^\ell}
\end{aligned}
$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Concluimos que:

$$\begin{aligned}
\mathbf{Pr}_{h,z}(X_{r_1} > 0) &\geq \frac{E[X_{r_1}]^2}{E[X_{r_1}^2]} \\
&\geq \frac{\left(\frac{|W_{r_1}|}{2^\ell}\right)^2}{\frac{|W_{r_1}|^2}{2^{2\ell}} + \frac{|W_{r_1}|}{2^\ell}} \\
&= \frac{\frac{|W_{r_1}|^2}{2^{2\ell}}}{\frac{|W_{r_1}|^2}{2^{2\ell}} + \frac{|W_{r_1}|}{2^\ell}} \\
&= \frac{|W_{r_1}|}{|W_{r_1}| + 2^\ell} \\
&\geq \frac{|W_{r_1}|}{2^\ell + 2^\ell} = \frac{|W_{r_1}|}{2^{\ell+1}}
\end{aligned}$$

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \in L$

Poniendo todo junto deducimos que:

$$
\begin{aligned}
&\mathbf{Pr}_{h,z,r_1}\Bigg(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \Bigg) \; = \\
&\quad \sum_{s_1 \in \{0,1\}^\ell} \mathbf{Pr}_{h,z,r_1}\Bigg(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \;\Bigg|\; r_1 = s_1 \Bigg) \cdot \mathbf{Pr}_{h,z,r_1}(r_1 = s_1) \; = \\
&\quad \frac{1}{2^\ell} \sum_{s_1 \in \{0,1\}^\ell} \mathbf{Pr}_{h,z}\Bigg(\bigvee_{r_2 \in W_{s_1}} h(r_2) = z \Bigg) \; = \\
&\quad \frac{1}{2^\ell} \sum_{s_1 \in \{0,1\}^\ell} \mathbf{Pr}_{h,z}(X_{s_1} > 0) \; \geq \\
&\quad \frac{1}{2^\ell} \sum_{s_1 \in \{0,1\}^\ell} \frac{|W_{s_1}|}{2^{\ell+1}} \; = \\
&\quad \frac{1}{2^{2\ell+1}} \sum_{s_1 \in \{0,1\}^\ell} |W_{s_1}| \; \geq \\
&\quad \frac{1}{2^{2\ell+1}} \cdot \frac{3 \cdot 2^{2\ell}}{4} \; = \; \frac{3}{8}
\end{aligned}
$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Dado que:

$$\mathbf{Pr}_{h,z,r_1}\Big(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z\Big) \quad \geq \quad \frac{3}{8}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Dado que:

$$\mathbf{Pr}_{h,z,r_1}\Bigg(\bigvee_{r_2 \in W_{r_1}} h(r_2) = z \Bigg) \quad \geq \quad \frac{3}{8}$$

Concluimos que existe un demostrador **D** tal que:

$$\mathbf{Pr}((\mathbf{V'}, \mathbf{D}) \text{ acepte } x) \quad \geq \quad \frac{3}{8}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Demostramos que:

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Demostramos que:

- Si $x \in L$, entonces existe demostrador **D** tal que

$$\mathbf{Pr}(\mathbf{V'}, \mathbf{D}) \text{ acepte } x) \quad \geq \quad \frac{3}{8}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Demostramos que:

- Si $x \in L$, entonces existe demostrador **D** tal que

$$\mathbf{Pr}(\mathbf{V'}, \mathbf{D}) \text{ acepte } x) \quad \geq \quad \frac{3}{8}$$

- Si $x \notin L$, entonces para todo demostrador **D'** se tiene que:

$$\mathbf{Pr}((\mathbf{V'}, \mathbf{D'}) \text{ acepte } x) \quad \leq \quad \frac{1}{4}$$

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Demostramos que:

- Si $x \in L$, entonces existe demostrador **D** tal que

$$\textbf{Pr}(\textbf{V'}, \textbf{D}) \text{ acepte } x) \quad \geq \quad \frac{3}{8}$$

- Si $x \notin L$, entonces para todo demostrador **D'** se tiene que:

$$\textbf{Pr}((\textbf{V'}, \textbf{D'}) \text{ acepte } x) \quad \leq \quad \frac{1}{4}$$

Para terminar la demostración necesitamos amplificar las probabilidades.

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \in L$

Esta amplificación es posible ya que $\frac{3}{8} - \frac{1}{4} = \frac{1}{8}$.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Esta amplificación es posible ya que $\frac{3}{8} - \frac{1}{4} = \frac{1}{8}$.

- Es posible si la diferencia entre las probabilidades para $x \in L$ y $x \notin L$ es una constante mayor que 0.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Esta amplificación es posible ya que $\frac{3}{8} - \frac{1}{4} = \frac{1}{8}$.

- Es posible si la diferencia entre las probabilidades para $x \in L$ y $x \notin L$ es una constante mayor que 0.

¿Pero cómo se hace la amplificación en este caso considerando que $\frac{3}{8} < \frac{1}{2}$?

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Esta amplificación es posible ya que $\frac{3}{8} - \frac{1}{4} = \frac{1}{8}$.

- Es posible si la diferencia entre las probabilidades para $x \in L$ y $x \notin L$ es una constante mayor que 0.

¿Pero cómo se hace la amplificación en este caso considerando que $\frac{3}{8} < \frac{1}{2}$?

- No podemos hacer esto utilizando la idea de repetir el protocolo t veces y calcular mayoría, esto va a hacer crecer el error.

La demostración de que $\text{AM} \subseteq \text{AM}_{\text{non-adaptative}}$: $x \in L$

Esta amplificación es posible ya que $\frac{3}{8} - \frac{1}{4} = \frac{1}{8}$.

- Es posible si la diferencia entre las probabilidades para $x \in L$ y $x \notin L$ es una constante mayor que 0.

¿Pero cómo se hace la amplificación en este caso considerando que $\frac{3}{8} < \frac{1}{2}$?

- No podemos hacer esto utilizando la idea de repetir el protocolo t veces y calcular mayoría, esto va a hacer crecer el error.

Lo que hacemos en la amplificación es repetir el experimento t veces obteniendo resultados Y_1, Y_2, ..., Y_t.

La demostración de que AM $\subseteq$ AM$_{\text{non-adaptative}}$: $x \in L$

Esta amplificación es posible ya que $\frac{3}{8} - \frac{1}{4} = \frac{1}{8}$.

- Es posible si la diferencia entre las probabilidades para $x \in L$ y $x \notin L$ es una constante mayor que 0.

¿Pero cómo se hace la amplificación en este caso considerando que $\frac{3}{8} < \frac{1}{2}$?

- No podemos hacer esto utilizando la idea de repetir el protocolo t veces y calcular mayoría, esto va a hacer crecer el error.

Lo que hacemos en la amplificación es repetir el experimento t veces obteniendo resultados Y_1, Y_2, ..., Y_t.

- Y verificamos si $\overline{Y} \geq \frac{1}{4} + \frac{1}{16}$, donde $\overline{Y} = \dfrac{1}{t} \displaystyle\sum_{i=1}^{t} Y_i$.

La demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$: $x \in L$

Esta amplificación es posible ya que $\frac{3}{8} - \frac{1}{4} = \frac{1}{8}$.

- Es posible si la diferencia entre las probabilidades para $x \in L$ y $x \notin L$ es una constante mayor que 0.

¿Pero cómo se hace la amplificación en este caso considerando que $\frac{3}{8} < \frac{1}{2}$?

- No podemos hacer esto utilizando la idea de repetir el protocolo t veces y calcular mayoría, esto va a hacer crecer el error.

Lo que hacemos en la amplificación es repetir el experimento t veces obteniendo resultados $Y_1, Y_2, \ldots, Y_t$.

- Y verificamos si $\overline{Y} \geq \frac{1}{4} + \frac{1}{16}$, donde $\overline{Y} = \dfrac{1}{t} \displaystyle\sum_{i=1}^{t} Y_i$.

Esto concluye la demostración de que $\mathrm{AM} \subseteq \mathrm{AM}_{\text{non-adaptative}}$. $\square$

Un lema de amplificación para BP·NP

Lema

Sea L un lenguaje sobre un alfabeto Σ y $p : \mathbb{N} \to \mathbb{N}$ un polinomio. Si $L \in$ BP·NP, entonces existe una MT probabilística no determinista M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$ con $|w| = n$:

$$\mathbf{Pr}_s(M(w, s) \text{ es incorrecto}) \quad \leq \quad \frac{1}{2^{p(n)}}$$

Un lema de amplificación para BP·NP

Lema

Sea L un lenguaje sobre un alfabeto Σ y $p : \mathbb{N} \to \mathbb{N}$ un polinomio. Si $L \in$ BP·NP, entonces existe una MT probabilística no determinista M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$ con $|w| = n$:

$$\mathbf{Pr}_s(M(w, s) \text{ es incorrecto}) \quad \leq \quad \frac{1}{2^{p(n)}}$$

Ejercicio

Demuestre la proposición.

Un teorema fundamental

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

Un teorema fundamental

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

Teorema (Schöning)

$\mathrm{NP} \cap \text{co-}\mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

Demostración de que $\mathsf{NP} \cap \mathsf{BP}{\cdot}\mathsf{NP} \subseteq \mathsf{Low}_2$

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

Demostración de que $\mathsf{NP} \cap \mathsf{BP}{\cdot}\mathsf{NP} \subseteq \mathsf{Low}_2$

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

- Es simple extender la demostración para un alfabeto arbitrario.

Demostración de que $\mathsf{NP} \cap \mathsf{BP}{\cdot}\mathsf{NP} \subseteq \mathsf{Low}_2$

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

- Es simple extender la demostración para un alfabeto arbitrario.

Sea $A \in \mathsf{NP} \cap \text{co-}\mathsf{BP}{\cdot}\mathsf{NP}$.

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

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

- Es simple extender la demostración para un alfabeto arbitrario.

Sea $A \in \mathrm{NP} \cap \text{co-BP}{\cdot}\mathrm{NP}$.

Tenemos que demostrar que $A \in \mathrm{Low}_2$, vale decir:

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

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

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

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

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

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

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

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

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

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

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

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

Podemos reescribir esta probabilidad de error de la siguiente forma:

$$\mathbf{Pr}_s((w \in \overline{A} \wedge M_1(w,s) \text{ no acepta}) \vee (w \not\in \overline{A} \wedge M_1(w,s) \text{ acepta})) \;\leq\; \frac{1}{2^{2n+1}}$$

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

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

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

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

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

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

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

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

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

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

- Sea $L_n(s) = \{w \in \{0,1\}^n \mid |s| = p(n) \text{ y } M_1(w,s) \text{ acepta}\}$.

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

Tenemos que:

$$
\begin{aligned}
&\mathbf{Pr}_{s\sim\{0,1\}^{p(n)}}(\overline{A}\cap\{0,1\}^n \neq L_n(s)) \;=\\
&\qquad \mathbf{Pr}_{s\sim\{0,1\}^{p(n)}}(\exists w\in\{0,1\}^n : ((w\in\overline{A}\wedge w\notin L_n(s))\vee\\
&\qquad\qquad\qquad\qquad\qquad (w\notin\overline{A}\wedge w\in L_n(s)))) \;=\\
&\qquad \mathbf{Pr}_{s\sim\{0,1\}^{p(n)}}(\exists w\in\{0,1\}^n : ((w\in\overline{A}\wedge M_1(w,s)\text{ no acepta})\vee\\
&\qquad\qquad\qquad\qquad\qquad (w\notin\overline{A}\wedge M_1(w,s)\text{ acepta}))) \;\leq\\
&\qquad \sum_{w\in\{0,1\}^n}\mathbf{Pr}_{s\sim\{0,1\}^{p(n)}}((w\in\overline{A}\wedge M_1(w,s)\text{ no acepta})\vee\\
&\qquad\qquad\qquad\qquad\qquad (w\notin\overline{A}\wedge M_1(w,s)\text{ acepta})) \;\leq\\
&\qquad \sum_{w\in\{0,1\}^n}\frac{1}{2^{2n+1}} \;=\; 2^n\frac{1}{2^{2n+1}} \;=\; \frac{1}{2^{n+1}} \;<\; \frac{1}{2^n}
\end{aligned}
$$

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

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

Del resultado en la lámina anterior concluimos que:

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

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

$A \in NP$: 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 de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

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 $r(|w|)$.

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

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 $r(|w|)$?

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

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 $r(|w|)$?

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

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

Vamos a utilizar M_1, M_2, M_3^A y los polinomios $p(n)$, $q(n)$, $r(n)$ para definir una MT no determinista M_4 de tiempo polinomial.

Demostración de que $\mathrm{NP} \cap \mathrm{BP{\cdot}NP} \subseteq \mathrm{Low}_2$

Vamos a utilizar M_1, M_2, M_3^A y los polinomios $p(n)$, $q(n)$, $r(n)$ para definir una MT no determinista M_4 de tiempo polinomial.

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 $s \in \{0,1\}^{p(r(|w|))}$.

Demostración de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

M_4 con entrada (w, y, z, s) funciona de la siguiente forma:

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

M_4 con entrada (w, y, z, s) funciona de la siguiente forma:

- M_4 simula el funcionamiento de M_3^A con entrada (w, y, z).

Demostración de que $\text{NP} \cap \text{BP}\cdot\text{NP} \subseteq \text{Low}_2$

M_4 con entrada (w, y, z, s) funciona de la siguiente forma:

- 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.

Demostración de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

M_4 con entrada (w, y, z, s) funciona de la siguiente forma:

- 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:

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

M_4 con entrada (w, y, z, s) funciona de la siguiente forma:

- 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.

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

M_4 con entrada (w, y, z, s) funciona de la siguiente forma:

- 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 de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

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

- En particular $|s| = p(r(|w|))$.

Demostración de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

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 de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

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 $\overline{A} \cap \{0,1\}^{r(|w|)} = L_{r(|w|)}(s)$ si $s \in B_{r(|w|)}$.

¿Qué sabemos sobre B_n?

Lema

Sea $p : \mathbb{N} \to \mathbb{N}$ un polinomio no nulo. Entonces existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$ y $E \subseteq \{0,1\}^{p(n)}$ con $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$, las siguientes afirmaciones son ciertas:

¿Qué sabemos sobre B_n?

Lema

Sea $p : \mathbb{N} \to \mathbb{N}$ un polinomio no nulo. Entonces existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$ y $E \subseteq \{0,1\}^{p(n)}$ con $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$, las siguientes afirmaciones son ciertas:

1. $\exists u_1 \in \{0,1\}^{p(n)} \cdots \exists u_{p(n)} \in \{0,1\}^{p(n)} \forall v \in \{0,1\}^{p(n)}$
   $\exists i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$

¿Qué sabemos sobre B_n?

Lema

Sea $p : \mathbb{N} \to \mathbb{N}$ un polinomio no nulo. Entonces existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$ y $E \subseteq \{0,1\}^{p(n)}$ con $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$, las siguientes afirmaciones son ciertas:

1. $\exists u_1 \in \{0,1\}^{p(n)} \cdots \exists u_{p(n)} \in \{0,1\}^{p(n)} \forall v \in \{0,1\}^{p(n)}$
   $\exists i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$

2. $\forall u_1 \in \{0,1\}^{p(n)} \cdots \forall u_{p(n)} \in \{0,1\}^{p(n)} \exists v \in \{0,1\}^{p(n)}$
   $\forall i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$

¿Qué sabemos sobre B_n?

Lema

Sea $p : \mathbb{N} \to \mathbb{N}$ un polinomio no nulo. Entonces existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$ y $E \subseteq \{0,1\}^{p(n)}$ con $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$, las siguientes afirmaciones son ciertas:

1. $\exists u_1 \in \{0,1\}^{p(n)} \cdots \exists u_{p(n)} \in \{0,1\}^{p(n)} \, \forall v \in \{0,1\}^{p(n)}$
   $\exists i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$
2. $\forall u_1 \in \{0,1\}^{p(n)} \cdots \forall u_{p(n)} \in \{0,1\}^{p(n)} \, \exists v \in \{0,1\}^{p(n)}$
   $\forall i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$

Vamos a ver que este lema nos ayuda a terminar la demostración.

¿Qué sabemos sobre B_n?

Lema

Sea $p : \mathbb{N} \to \mathbb{N}$ un polinomio no nulo. Entonces existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$ y $E \subseteq \{0,1\}^{p(n)}$ con $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$, las siguientes afirmaciones son ciertas:

1. $\exists u_1 \in \{0,1\}^{p(n)} \cdots \exists u_{p(n)} \in \{0,1\}^{p(n)} \, \forall v \in \{0,1\}^{p(n)}$
   $\exists i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$
2. $\forall u_1 \in \{0,1\}^{p(n)} \cdots \forall u_{p(n)} \in \{0,1\}^{p(n)} \, \exists v \in \{0,1\}^{p(n)}$
   $\forall i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$

Vamos a ver que este lema nos ayuda a terminar la demostración.

- Y luego vamos a ver la demostración del lema.

¿Qué sabemos sobre B_n?

Dado que $p(n)$ es un polinomio no nulo, $B_n \subseteq \{0,1\}^{p(n)}$ y $|B_n| > (1 - \frac{1}{2^n})2^{p(n)}$,

¿Qué sabemos sobre B_n?

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 por el lema anterior que existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$:

¿Qué sabemos sobre B_n?

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 por el lema anterior que existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$:

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

¿Qué sabemos sobre B_n?

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 por el lema anterior que existe $n_0 \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n \geq n_0$:

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

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

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

Sabemos que para cada $w \in \{0,1\}^*$:

$$
\begin{aligned}
& w \in L \text{ si y sólo si} \\
& \qquad \exists y \in \{0,1\}^{q(|w|)} \\
& \qquad \forall z \in \{0,1\}^{q(|w|)}\ M_3^A \text{ acepta } (w, y, z)
\end{aligned}
$$

Demostración de que $\mathrm{NP} \cap \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{Low}_2$

Sabemos que para cada $w \in \{0,1\}^*$:

$$\begin{aligned} & w \in L \text{ si y sólo si} \\ & \qquad \exists y \in \{0,1\}^{q(|w|)} \\ & \qquad \forall z \in \{0,1\}^{q(|w|)}\ M_3^A \text{ acepta } (w, y, z) \end{aligned}$$

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

Demostración de que $\mathrm{NP} \cap \mathrm{BP}{\cdot}\mathrm{NP} \subseteq \mathrm{Low}_2$

Por lo tanto, a partir del lema concluimos que para cada $w \in \{0,1\}^*$ tal que $r(|w|) \geq n_0$:

Demostración de que NP $\cap$ BP$\cdot$NP $\subseteq$ Low$_2$

Por lo tanto, a partir del lema concluimos que para cada $w \in \{0,1\}^*$ tal que $r(|w|) \geq n_0$:

$w \in L$ si y sólo si

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

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

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

$$\forall v \in \{0,1\}^{p(r(|w|))} \left(\bigvee_{i=1}^{p(r(|w|))} M_4 \text{ no acepta } (w, y, z, u_i \oplus v) \right)$$

Demostración del teorema

Para terminar la demostración considere el lenguaje:

$$
\begin{aligned}
N \;=\; \Bigg\{ (w, y, z, u_1, \ldots, u_{p(r(|w|))}, v) \;\Bigg|\; & \\
& w \in \{0,1\}^*, \\
& y \in \{0,1\}^{q(|w|)}, \\
& z \in \{0,1\}^{q(|w|)}, \\
& u_1 \in \{0,1\}^{p(r(|w|))}, \\
& \ldots, \\
& u_{p(r(|w|))} \in \{0,1\}^{p(r(|w|))}, \\
& v \in \{0,1\}^{p(r(|w|))} \;\text{ y }\; \bigwedge_{i=1}^{p(r(|w|))} M_4 \text{ acepta } (w, y, z, u_i \oplus v) \Bigg\}
\end{aligned}
$$

Demostración del teorema

Dado que M_4 es una MT no determinista de tiempo polinomial, concluimos que $N \in \mathrm{NP}$.

Demostración del teorema

Dado que M_4 es una MT no determinista de tiempo polinomial, concluimos que $N \in \mathrm{NP}$.

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 $(w, y, z, u_1, \ldots, u_{p(r(|w|))}, v)$:

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

Demostración del teorema

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

Demostración del teorema

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

$w \in L$ si y sólo si

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

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

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

$$\forall v \in \{0,1\}^{p(r(|w|))} \neg \left(\bigwedge_{i=1}^{p(r(|w|))} M_4 \text{ acepta } (w, y, z, u_i \oplus v) \right)$$

Demostración del teorema

Considerando la definición de M_5 concluimos que para cada $w \in \{0,1\}^*$ tal que $r(|w|) \geq n_0$:

Demostración del teorema

Considerando la definición de M_5 concluimos que para cada $w \in \{0,1\}^*$ tal que $r(|w|) \geq n_0$:

$w \in L$ si y sólo si

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

El lema pendiente

Para terminar la demostración nos falta demostrar este lema:

Lema

Sea $p : \mathbb{N} \to \mathbb{N}$ *un polinomio no nulo. Entonces existe* $n_0 \in \mathbb{N}$ *tal que para todo* $n \in \mathbb{N}$ *con* $n \geq n_0$ *y* $E \subseteq \{0,1\}^{p(n)}$ *con* $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$*, las siguientes afirmaciones son ciertas:*

1. $\exists u_1 \in \{0,1\}^{p(n)} \cdots \exists u_{p(n)} \in \{0,1\}^{p(n)} \, \forall v \in \{0,1\}^{p(n)}$
   $\exists i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$
2. $\forall u_1 \in \{0,1\}^{p(n)} \cdots \forall u_{p(n)} \in \{0,1\}^{p(n)} \, \exists v \in \{0,1\}^{p(n)}$
   $\forall i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$

La demostración del lema

Como $p(n)$ es un polinomio, existe $n_1 \in \mathbb{N}$ tal que:

$$(\forall n \in \mathbb{N} : n \geq n_1) : (p(n) < 2^n)$$

La demostración del lema

Como $p(n)$ es un polinomio, existe $n_1 \in \mathbb{N}$ tal que:

$$(\forall n \in \mathbb{N} : n \geq n_1) : (p(n) < 2^n)$$

Como $p(n)$ es un polinomio no nulo, existe $n_2 \in \mathbb{N}$ tal que:

$$(\forall n \in \mathbb{N} : n \geq n_2) : (1 \leq p(n))$$

La demostración del lema

Como $p(n)$ es un polinomio, existe $n_1 \in \mathbb{N}$ tal que:

$$(\forall n \in \mathbb{N} : n \geq n_1) : (p(n) < 2^n)$$

Como $p(n)$ es un polinomio no nulo, existe $n_2 \in \mathbb{N}$ tal que:

$$(\forall n \in \mathbb{N} : n \geq n_2) : (1 \leq p(n))$$

A partir de estos números definimos $n_0 = \text{máx}\{1, n_1, n_2\}$

La demostración del lema

En la demostración del lema consideramos:

La demostración del lema

En la demostración del lema consideramos:

- $n \geq n_0$

La demostración del lema

En la demostración del lema consideramos:

- $n \geq n_0$
- $E \subseteq \{0, 1\}^{p(n)}$ tal que $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$

Demostración de la parte 1 del lema

Para obtener una contradicción suponemos que la condición es falsa.

Demostración de la parte 1 del lema

Para obtener una contradicción suponemos que la condición es falsa.

Entonces se tiene que:

$$\forall u_1 \in \{0,1\}^{p(n)} \cdots \forall u_{p(n)} \in \{0,1\}^{p(n)}$$
$$\exists v \in \{0,1\}^{p(n)}\, \forall i \in \{1,\ldots,p(n)\} : (u_i \oplus v \notin E)$$

Demostración de la parte 1 del lema

Sea v_j el j-ésimo elemento de $\{0, 1\}^{p(n)}$ en orden lexicográfico.

Demostración de la parte 1 del lema

Sea v_j el j-ésimo elemento de $\{0,1\}^{p(n)}$ en orden lexicográfico.

Definimos:

$$U \quad = \quad \{(u_1, \ldots, u_{p(n)}) \mid \forall i \in \{1, \ldots, p(n)\} : u_i \in \{0,1\}^{p(n)}\}$$

Demostración de la parte 1 del lema

Sea v_j el j-ésimo elemento de $\{0,1\}^{p(n)}$ en orden lexicográfico.

Definimos:

$$U \quad = \quad \{(u_1,\ldots,u_{p(n)}) \mid \forall i \in \{1,\ldots,p(n)\} : u_i \in \{0,1\}^{p(n)}\}$$

Podemos reescribir la condición inicial como:

$$\forall (u_1,\ldots,u_{p(n)}) \in U \ \exists j \in \{1,\ldots,2^{p(n)}\} \ \forall i \in \{1,\ldots,p(n)\} : (u_i \oplus v_j \notin E)$$

Demostración de la parte 1 del lema

Para cada $j \in \{1, \ldots, 2^{p(n)}\}$ definimos:

$$U_j \quad = \quad \{(u_1, \ldots, u_{p(n)}) \in U \mid \forall i \in \{1, \ldots, p(n)\} : u_i \oplus v_j \notin E\}$$

Demostración de la parte 1 del lema

Para cada $j \in \{1, \ldots, 2^{p(n)}\}$ definimos:

$$U_j \quad = \quad \{(u_1, \ldots, u_{p(n)}) \in U \mid \forall i \in \{1, \ldots, p(n)\} : u_i \oplus v_j \notin E\}$$

Tenemos entonces que:

$$U \quad = \quad \bigcup_{j=1}^{2^{p(n)}} U_j$$

Demostración de la parte 1 del lema

Para cada $j \in \{1, \ldots, 2^{p(n)}\}$ definimos:

$$U_j \quad = \quad \{(u_1, \ldots, u_{p(n)}) \in U \mid \forall i \in \{1, \ldots, p(n)\} : u_i \oplus v_j \not\in E\}$$

Tenemos entonces que:

$$U \quad = \quad \bigcup_{j=1}^{2^{p(n)}} U_j$$

Entonces existe $\ell \in \{1, \ldots, 2^{p(n)}\}$ tal que:

$$|U_\ell| \;\geq\; \frac{|U|}{2^{p(n)}} \;=\; \frac{2^{p(n)^2}}{2^{p(n)}} \;=\; 2^{p(n)^2 - p(n)}$$

Demostración de la parte 1 del lema

Considere la función $f : U \to U$ definida como:

$$f(u_1, \ldots, u_{p(n)}) \quad = \quad (u_i \oplus v_\ell, \ldots, u_{p(n)} \oplus v_\ell)$$

Tenemos que f es una biyección.

Demostración de la parte 1 del lema

Considere la función $f : U \to U$ definida como:

$$f(u_1, \ldots, u_{p(n)}) \quad = \quad (u_i \oplus v_\ell, \ldots, u_{p(n)} \oplus v_\ell)$$

Tenemos que f es una biyección.

Además, para cada $(u_1, \ldots, u_{p(n)}) \in U_\ell$ se tiene que $f(u_1, \ldots, u_{p(n)}) \in \overline{E}^{p(n)}$

Demostración de la parte 1 del lema

Considere la función $f : U \to U$ definida como:

$$f(u_1, \ldots, u_{p(n)}) \quad = \quad (u_i \oplus v_\ell, \ldots, u_{p(n)} \oplus v_\ell)$$

Tenemos que f es una biyección.

Además, para cada $(u_1, \ldots, u_{p(n)}) \in U_\ell$ se tiene que $f(u_1, \ldots, u_{p(n)}) \in \overline{E}^{p(n)}$

- Concluimos que $|U_\ell| \leq |\overline{E}^{p(n)}| = |\overline{E}|^{p(n)}$

Demostración de la parte 1 del lema

Tenemos entonces que $2^{p(n)^2-p(n)} \leq |U_\ell| \leq |\overline{E}|^{p(n)}$, de lo cual concluimos:

$$2^{p(n)-1} \quad \leq \quad |\overline{E}|$$

Demostración de la parte 1 del lema

Tenemos entonces que $2^{p(n)^2 - p(n)} \leq |U_\ell| \leq |\overline{E}|^{p(n)}$, de lo cual concluimos:

$$2^{p(n)-1} \quad \leq \quad |\overline{E}|$$

Dado que $E \cup \overline{E} = \{0,1\}^{p(n)}$, sabemos que $|E| = 2^{p(n)} - |\overline{E}|$

- Tenemos entonces que $|E| \leq 2^{p(n)} - 2^{p(n)-1} = (1 - \frac{1}{2}) \cdot 2^{p(n)}$

Demostración de la parte 1 del lema

Tenemos entonces que $2^{p(n)^2 - p(n)} \leq |U_\ell| \leq |\overline{E}|^{p(n)}$, de lo cual concluimos:

$$2^{p(n)-1} \quad \leq \quad |\overline{E}|$$

Dado que $E \cup \overline{E} = \{0,1\}^{p(n)}$, sabemos que $|E| = 2^{p(n)} - |\overline{E}|$

- Tenemos entonces que $|E| \leq 2^{p(n)} - 2^{p(n)-1} = (1 - \frac{1}{2}) \cdot 2^{p(n)}$

Pero esto contradice que $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$

- Puesto que $|E| \leq (1 - \frac{1}{2}) \cdot 2^{p(n)} \leq (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$ ya que $n \geq n_0 \geq 1$

Demostración de la parte 2 del lema

Para obtener una contradicción suponemos que la condición es falsa.

Demostración de la parte 2 del lema

Para obtener una contradicción suponemos que la condición es falsa.

Entonces se tiene que:

$$\exists u_1 \in \{0,1\}^{p(n)} \cdots \exists u_{p(n)} \in \{0,1\}^{p(n)}$$
$$\forall v \in \{0,1\}^{p(n)} \, \exists i \in \{1,\ldots,p(n)\} : (u_i \oplus v \notin E)$$

Demostración de la parte 2 del lema

Sea $u_1, \ldots, u_{p(n)}$ una secuencia de strings en $\{0,1\}^{p(n)}$ que satisfacen la condición anterior.

Demostración de la parte 2 del lema

Sea u_1, ..., $u_{p(n)}$ una secuencia de strings en $\{0,1\}^{p(n)}$ que satisfacen la condición anterior.

Definimos $V = \{0,1\}^{p(n)}$, y reescribimos la condición anterior como:

$$\forall v \in V\, \exists i \in \{1, \ldots, p(n)\} : (u_i \oplus v \notin E)$$

Demostración de la parte 2 del lema

Para cada $j \in \{1, \ldots, p(n)\}$ definimos:

$$V_j \quad = \quad \{v \in V \mid u_j \oplus v \notin E\}$$

Demostración de la parte 2 del lema

Para cada $j \in \{1, \ldots, p(n)\}$ definimos:

$$V_j \quad = \quad \{v \in V \mid u_j \oplus v \notin E\}$$

Tenemos entonces que:

$$V \quad = \quad \bigcup_{j=1}^{p(n)} V_j$$

Demostración de la parte 2 del lema

Para cada $j \in \{1, \ldots, p(n)\}$ definimos:

$$V_j = \{v \in V \mid u_j \oplus v \notin E\}$$

Tenemos entonces que:

$$V = \bigcup_{j=1}^{p(n)} V_j$$

Entonces existe $\ell \in \{1, \ldots, p(n)\}$ tal que:

$$|V_\ell| \geq \frac{|V|}{p(n)} = \frac{2^{p(n)}}{p(n)}$$

Demostración de la parte 2 del lema

Considere la función $g : V \to V$ definida como:

$$g(v) \quad = \quad u_\ell \oplus v$$

Tenemos que g es una biyección.

Demostración de la parte 2 del lema

Considere la función $g : V \to V$ definida como:

$$g(v) \quad = \quad u_\ell \oplus v$$

Tenemos que g es una biyección.

Además, para cada $v \in V_\ell$ se tiene que $g(v) \in \overline{E}$

Demostración de la parte 2 del lema

Considere la función $g : V \to V$ definida como:

$$g(v) \quad = \quad u_\ell \oplus v$$

Tenemos que g es una biyección.

Además, para cada $v \in V_\ell$ se tiene que $g(v) \in \overline{E}$

- Concluimos que $|V_\ell| \leq |\overline{E}|$

Demostración de la parte 2 del lema

Tenemos entonces que $\frac{2^{p(n)}}{p(n)} \leq |V_\ell| \leq |\overline{E}|$

Demostración de la parte 2 del lema

Tenemos entonces que $\frac{2^{p(n)}}{p(n)} \leq |V_\ell| \leq |\overline{E}|$

Dado que $|E| = 2^{p(n)} - |\overline{E}|$, tenemos que:

$$|E| \ \leq \ 2^{p(n)} - \frac{2^{p(n)}}{p(n)} \ = \ (1 - \frac{1}{p(n)}) \cdot 2^{p(n)}$$

Demostración de la parte 2 del lema

Dado que $n \geq n_0$ tenemos que:

$$
\begin{aligned}
1 \leq p(n) < 2^n \quad & \Rightarrow \quad \frac{1}{2^n} < \frac{1}{p(n)} \\
& \Rightarrow \quad -\frac{1}{p(n)} < -\frac{1}{2^n} \\
& \Rightarrow \quad \left(1 - \frac{1}{p(n)}\right) < \left(1 - \frac{1}{2^n}\right) \\
& \Rightarrow \quad \left(1 - \frac{1}{p(n)}\right) \cdot 2^{p(n)} < \left(1 - \frac{1}{2^n}\right) \cdot 2^{p(n)}
\end{aligned}
$$

Demostración de la parte 2 del lema

Dado que $n \geq n_0$ tenemos que:

$$
\begin{aligned}
1 \leq p(n) < 2^n \quad & \Rightarrow \quad \frac{1}{2^n} < \frac{1}{p(n)} \\
& \Rightarrow \quad -\frac{1}{p(n)} < -\frac{1}{2^n} \\
& \Rightarrow \quad \left(1 - \frac{1}{p(n)}\right) < \left(1 - \frac{1}{2^n}\right) \\
& \Rightarrow \quad \left(1 - \frac{1}{p(n)}\right) \cdot 2^{p(n)} < \left(1 - \frac{1}{2^n}\right) \cdot 2^{p(n)}
\end{aligned}
$$

Obtenemos una contradicción dado que $|E| \leq (1 - \frac{1}{p(n)}) \cdot 2^{p(n)}$ y por hipótesis $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$. $\square$

La consecuencia final: isomorfismo de grafos

Ya demostramos que GRAPH-ISO $\in$ co-AM.

La consecuencia final: isomorfismo de grafos

Ya demostramos que GRAPH-ISO $\in$ co-AM.

- De hecho, demostramos que $\overline{\text{GRAPH-ISO}} \in$ AM.

La consecuencia final: isomorfismo de grafos

Ya demostramos que GRAPH-ISO $\in$ co-AM.

- De hecho, demostramos que $\overline{\text{GRAPH-ISO}} \in$ AM.

Concluimos entonces que GRAPH-ISO $\in$ Low$_2$ desde el resultado NP $\cap$ co-AM $\subseteq$ Low$_2$.

La consecuencia final: isomorfismo de grafos

Ya demostramos que GRAPH-ISO $\in$ co-AM.

- De hecho, demostramos que $\overline{\text{GRAPH-ISO}} \in$ AM.

Concluimos entonces que GRAPH-ISO $\in$ Low_2 desde el resultado NP $\cap$ co-AM $\subseteq$ Low_2.

Teorema (Schöning)

GRAPH-ISO $\in$ Low_2.

La consecuencia final: isomorfismo de grafos

El resultado anterior es una de las razones para creer que GRAPH-ISO no es un problema NP-completo:

La consecuencia final: isomorfismo de grafos

El resultado anterior es una de las razones para creer que GRAPH-ISO no es un problema NP-completo:

Corolario

Si GRAPH-ISO es NP-completo, entonces $PH = \Sigma_2^P$.

La consecuencia final: isomorfismo de grafos

El resultado anterior es una de las razones para creer que GRAPH-ISO no es un problema NP-completo:

Corolario

Si GRAPH-ISO es NP-completo, entonces $PH = \Sigma_2^P$.

Obtenemos como consecuencia el siguiente corolario:

Corolario

Si L es un problema GI-completo y L es NP-completo, entonces $PH = \Sigma_2^P$.

La consecuencia final: isomorfismo de grafos

El resultado anterior es una de las razones para creer que GRAPH-ISO no es un problema NP-completo:

Corolario

Si GRAPH-ISO es NP-completo, entonces $PH = \Sigma_2^P$.

Obtenemos como consecuencia el siguiente corolario:

Corolario

Si L es un problema GI-completo y L es NP-completo, entonces $PH = \Sigma_2^P$.

Ejercicio

Demuestre el último corolario.