# La jerarquía baja para NP

IIC3810

# El poder de un lenguaje como oráculo

Sea $L$ un lenguaje.

Para tratar de entender qué tan difícil es decidir $L$ podemos pensar en qué logramos si lo usamos como oráculo.

# El poder de un lenguaje como oráculo

Sea $L$ un lenguaje.

Para tratar de entender qué tan difícil es decidir $L$ podemos pensar en qué logramos si lo usamos como oráculo.

**Ejemplo**

Veamos dos casos posibles para $L$

# El poder de un lenguaje como oráculo

Sea $L$ un lenguaje.

Para tratar de entender qué tan difícil es decidir $L$ podemos pensar en qué logramos si lo usamos como oráculo.

**Ejemplo**

Veamos dos casos posibles para $L$

- Si $L \in \mathrm{P}$, entonces $\mathrm{P}^L = \mathrm{P}$

# El poder de un lenguaje como oráculo

Sea $L$ un lenguaje.

Para tratar de entender qué tan difícil es decidir $L$ podemos pensar en qué logramos si lo usamos como oráculo.

**Ejemplo**

Veamos dos casos posibles para $L$

- Si $L \in \mathrm{P}$, entonces $\mathrm{P}^L = \mathrm{P}$
- Pero si $L \in \mathrm{NP} \cap \text{co-NP}$, entonces hay evidencia para creer que $\mathrm{P} \subsetneq \mathrm{P}^L$
  - Si no se tendría que $\mathrm{FACT} \in \mathrm{P}$

# El poder como oráculo de un lenguaje en $\mathrm{NP} \cap \text{co-NP}$

Suponga que $L \in \mathrm{NP} \cap \text{co-NP}$

# El poder como oráculo de un lenguaje en NP $\cap$ co-NP

Suponga que $L \in \text{NP} \cap \text{co-NP}$

¿Existe alguna clase $\mathcal{C}$ para la cual $\mathcal{C}^L = \mathcal{C}$?

# El poder como oráculo de un lenguaje en NP $\cap$ co-NP

Suponga que $L \in \text{NP} \cap \text{co-NP}$

¿Existe alguna clase $\mathcal{C}$ para la cual $\mathcal{C}^L = \mathcal{C}$?

**Teorema**

*Si $L \in NP \cap co\text{-}NP$, entonces $NP^L = NP$*

# El poder como oráculo de un lenguaje en NP $\cap$ co-NP

Suponga que $L \in \text{NP} \cap \text{co-NP}$

¿Existe alguna clase $\mathcal{C}$ para la cual $\mathcal{C}^L = \mathcal{C}$?

**Teorema**

*Si $L \in NP \cap co\text{-}NP$, entonces $NP^L = NP$*

**Ejercicio**

Demuestre el teorema.

# Una caracterización de NP $\cap$ co-NP basada en oráculos

El teorema anterior puede ser extendido para dar una caracterización de los problemas en NP $\cap$ co-NP

# Una caracterización de NP $\cap$ co-NP basada en oráculos

El teorema anterior puede ser extendido para dar una caracterización de los problemas en NP $\cap$ co-NP

**Teorema**

*Para cada lenguaje $L$ se tiene que $L \in NP \cap \text{co-}NP$ si y sólo si $NP^L = NP$*

# Una caracterización de NP $\cap$ co-NP basada en oráculos

El teorema anterior puede ser extendido para dar una caracterización de los problemas en NP $\cap$ co-NP

**Teorema**

*Para cada lenguaje $L$ se tiene que $L \in NP \cap co\text{-}NP$ si y sólo si $NP^L = NP$*

**Demostración:** Sólo nos falta demostrar la dirección ($\Leftarrow$)

# Una caracterización de NP $\cap$ co-NP basada en oráculos

El teorema anterior puede ser extendido para dar una caracterización de los problemas en NP $\cap$ co-NP

**Teorema**

*Para cada lenguaje $L$ se tiene que $L \in NP \cap co\text{-}NP$ si y sólo si $NP^L = NP$*

**Demostración:** Sólo nos falta demostrar la dirección ($\Leftarrow$)

Suponga que $\text{NP}^L = \text{NP}$

- Tenemos que demostrar que $L \in \text{NP} \cap \text{co-NP}$

# Una caracterización de $\mathrm{NP} \cap \text{co-NP}$ basada en oráculos

Sabemos que $L \in \mathrm{P}^L$ y $\overline{L} \in \mathrm{P}^L$

# Una caracterización de $\mathrm{NP} \cap \text{co-NP}$ basada en oráculos

Sabemos que $L \in \mathrm{P}^L$ y $\overline{L} \in \mathrm{P}^L$

Dado que $\mathrm{P}^L \subseteq \mathrm{NP}^L$, concluimos que $L \in \mathrm{NP}^L$ y $\overline{L} \in \mathrm{NP}^L$

# Una caracterización de NP $\cap$ co-NP basada en oráculos

Sabemos que $L \in \text{P}^L$ y $\overline{L} \in \text{P}^L$

Dado que $\text{P}^L \subseteq \text{NP}^L$, concluimos que $L \in \text{NP}^L$ y $\overline{L} \in \text{NP}^L$

Pero entonces $L \in \text{NP}$ y $\overline{L} \in \text{NP}$ dado que $\text{NP}^L = \text{NP}$

# Una caracterización de NP $\cap$ co-NP basada en oráculos

Sabemos que $L \in \mathrm{P}^L$ y $\overline{L} \in \mathrm{P}^L$

Dado que $\mathrm{P}^L \subseteq \mathrm{NP}^L$, concluimos que $L \in \mathrm{NP}^L$ y $\overline{L} \in \mathrm{NP}^L$

Pero entonces $L \in \mathrm{NP}$ y $\overline{L} \in \mathrm{NP}$ dado que $\mathrm{NP}^L = \mathrm{NP}$

Por lo tanto $L \in \mathrm{NP}$ y $L \in$ co-NP, vale decir, $L \in \mathrm{NP} \cap$ co-NP $\square$

# Un corolario fundamental: una propiedad de clausura para $\text{NP} \cap \text{co-NP}$

Recuerde que decimos que NP es cerrada bajo la noción de reducción $\leq_m^p$ ya que:

$$\text{si } L_1 \leq_m^p L_2 \text{ y } L_2 \in \text{NP, entonces } L_1 \in \text{NP}$$

También co-NP es cerrada bajo la noción de reducción $\leq_m^p$

# Un corolario fundamental: una propiedad de clausura para NP $\cap$ co-NP

Por el contrario se cree que NP y co-NP no son cerrados bajo la noción de reducción $\leq_T^p$ por el siguiente resultado:

**Proposición**

*Si NP (o co-NP) es cerrada bajo $\leq_T^p$, entonces NP $=$ co-NP*

# Un corolario fundamental: una propiedad de clausura para NP $\cap$ co-NP

Por el contrario se cree que NP y co-NP no son cerrados bajo la noción de reducción $\leq_T^p$ por el siguiente resultado:

**Proposición**

*Si NP (o co-NP) es cerrada bajo $\leq_T^p$, entonces NP $=$ co-NP*

**Ejercicio**

Demuestre la proposición.

# Un corolario fundamental: una propiedad de clausura para NP $\cap$ co-NP

¿Hereda NP $\cap$ co-NP las propiedades de clausura de NP y co-NP?

# Un corolario fundamental: una propiedad de clausura para NP $\cap$ co-NP

¿Hereda NP $\cap$ co-NP las propiedades de clausura de NP y co-NP?

De la caracterización de NP $\cap$ co-NP obtenemos el siguiente resultado:

**Corolario**

*NP $\cap$ co-NP es cerrado bajo $\leq_T^p$*

# Demostración del corolario

Suponga que $L_1 \leq_T^p L_2$ y $L_2 \in \mathrm{NP} \cap \text{co-NP}$

- Tenemos que demostrar que $L_1 \in \mathrm{NP} \cap \text{co-NP}$

# Demostración del corolario

Suponga que $L_1 \leq_T^p L_2$ y $L_2 \in \text{NP} \cap \text{co-NP}$

- Tenemos que demostrar que $L_1 \in \text{NP} \cap \text{co-NP}$

Dado que $L_1 \leq_T^p L_2$ tenemos que $\text{NP}^{L_1} \subseteq \text{NP}^{L_2}$

- ¿Por qué?

# Demostración del corolario

Suponga que $L_1 \leq_T^p L_2$ y $L_2 \in \text{NP} \cap \text{co-NP}$

- Tenemos que demostrar que $L_1 \in \text{NP} \cap \text{co-NP}$

Dado que $L_1 \leq_T^p L_2$ tenemos que $\text{NP}^{L_1} \subseteq \text{NP}^{L_2}$

- ¿Por qué?

Puesto que $L_2 \in \text{NP} \cap \text{co-NP}$, tenemos por la caracterización de $\text{NP} \cap \text{co-NP}$ que $\text{NP}^{L_2} = \text{NP}$

- Concluimos que $\text{NP}^{L_1} = \text{NP}$ ya que $\text{NP} \subseteq \text{NP}^{L_1} \subseteq \text{NP}^{L_2} = \text{NP}$

# Demostración del corolario

Suponga que $L_1 \leq_T^p L_2$ y $L_2 \in \text{NP} \cap \text{co-NP}$

- Tenemos que demostrar que $L_1 \in \text{NP} \cap \text{co-NP}$

Dado que $L_1 \leq_T^p L_2$ tenemos que $\text{NP}^{L_1} \subseteq \text{NP}^{L_2}$

- ¿Por qué?

Puesto que $L_2 \in \text{NP} \cap \text{co-NP}$, tenemos por la caracterización de $\text{NP} \cap \text{co-NP}$ que $\text{NP}^{L_2} = \text{NP}$

- Concluimos que $\text{NP}^{L_1} = \text{NP}$ ya que $\text{NP} \subseteq \text{NP}^{L_1} \subseteq \text{NP}^{L_2} = \text{NP}$

Dado que $\text{NP}^{L_1} = \text{NP}$, usando nuevamente la caracterización de $\text{NP} \cap \text{co-NP}$ obtenemos que $L_1 \in \text{NP} \cap \text{co-NP}$ $\square$

# La falla de completitud: Otra mirada al poder de un lenguaje

¿Puede un problema en NP $\cap$ co-NP ser NP-completo?

# La falla de completitud: Otra mirada al poder de un lenguaje

¿Puede un problema en NP $\cap$ co-NP ser NP-completo?

Se cree que la respuesta es no por el siguiente resultado:

**Proposición**

*Sea $L \in NP \cap co\text{-}NP$. Si $L$ es NP-completo, entonces $NP = co\text{-}NP$*

# La falla de completitud: Otra mirada al poder de un lenguaje

¿Puede un problema en NP $\cap$ co-NP ser NP-completo?

Se cree que la respuesta es no por el siguiente resultado:

**Proposición**

*Sea $L \in NP \cap$ co-NP. Si $L$ es NP-completo, entonces NP $=$ co-NP*

**Ejercicio**

Demuestre la proposición.

# La jerarquía polinomial relativizada

Vamos a definir una jerarquía que intenta formalizar las ideas mostradas en las láminas anteriores.

# La jerarquía polinomial relativizada

Vamos a definir una jerarquía que intenta formalizar las ideas mostradas en las láminas anteriores.

Para definir esta jerarquía primero tenemos que definir la relativización de la jerarquía polinomial a un lenguaje $L$.

# La jerarquía polinomial relativizada

**Notación**

*Dado un lenguaje L:*

$$\begin{aligned}\Sigma_0^P(L) &= P^L \\ \Sigma_{n+1}^P(L) &= NP^{\Sigma_n^P(L)}\end{aligned}$$

# La jerarquía polinomial relativizada

**Notación**

*Dado un lenguaje L:*

$$\begin{aligned}\Sigma_0^P(L) &= P^L \\ \Sigma_{n+1}^P(L) &= NP^{\Sigma_n^P(L)}\end{aligned}$$

**Ejemplo**

Tenemos que $\Sigma_1^P(L) = \mathrm{NP}^L$ y $\Sigma_2^P(L) = \mathrm{NP}^{(\mathrm{NP}^L)}$

- ¿Por qué?

# La jerarquía baja

**Definición (Low hierarchy)**

# La jerarquía baja

**Definición (Low hierarchy)**

Para cada $n \geq 0$, defina:

$$\mathrm{Low}_n \quad = \quad \{L \in \mathrm{NP} \mid \Sigma_n^P(L) = \Sigma_n^P\}$$

# La jerarquía baja

**Definición (Low hierarchy)**

Para cada $n \geq 0$, defina:

$$\text{Low}_n \quad = \quad \{L \in \text{NP} \mid \Sigma_n^P(L) = \Sigma_n^P\}$$

Además, la jerarquía baja se define como:

$$\text{LowH} \quad = \quad \bigcup_{n \in \mathbb{N}} \text{Low}_n$$

# La jerarquía baja

**Definición (Low hierarchy)**

Para cada $n \geq 0$, defina:

$$\text{Low}_n = \{L \in \text{NP} \mid \Sigma_n^P(L) = \Sigma_n^P\}$$

Además, la jerarquía baja se define como:

$$\text{LowH} = \bigcup_{n \in \mathbb{N}} \text{Low}_n$$

Note que en la definición anterior se incluye la condición $L \in \text{NP}$ para asegurar que la jerarquía esta dentro de NP.

# La jerarquía baja

**Definición (Low hierarchy)**

Para cada $n \geq 0$, defina:

$$\text{Low}_n \quad = \quad \{L \in \text{NP} \mid \Sigma_n^P(L) = \Sigma_n^P\}$$

Además, la jerarquía baja se define como:

$$\text{LowH} \quad = \quad \bigcup_{n \in \mathbb{N}} \text{Low}_n$$

Note que en la definición anterior se incluye la condición $L \in \text{NP}$ para asegurar que la jerarquía esta dentro de NP.

Un lenguaje $L$ se dice bajo para NP (low for NP) si $L \in \text{LowH}$.

# Algunas propiedades básicas de la jerarquía baja

**Proposición**

1. *Para todo* $n \geq 0$*:* $Low_n \subseteq NP$
2. *Para todo* $n \geq 0$*:* $Low_n \subseteq Low_{n+1}$
3. $Low_0 = P$
4. $Low_1 = NP \cap co\text{-}NP$

# Algunas propiedades básicas de la jerarquía baja

**Proposición**

1. *Para todo* $n \geq 0$*:* $Low_n \subseteq NP$
2. *Para todo* $n \geq 0$*:* $Low_n \subseteq Low_{n+1}$
3. $Low_0 = P$
4. $Low_1 = NP \cap co\text{-}NP$

**Ejercicio**

Demuestre la proposición.

# Una propiedad fundamental de la jerarquía baja

**Teorema (Schöning)**

Sea $L \in \mathrm{Low}_n$ para $n \geq 1$. Si $L$ es NP-completo, entonces $\mathrm{PH} = \Sigma_n^P$.

# Una propiedad fundamental de la jerarquía baja

**Teorema (Schöning)**

Sea $L \in \text{Low}_n$ para $n \geq 1$. Si $L$ es NP-completo, entonces $\text{PH} = \Sigma_n^P$.

**Ejercicio**

Demuestre el teorema.

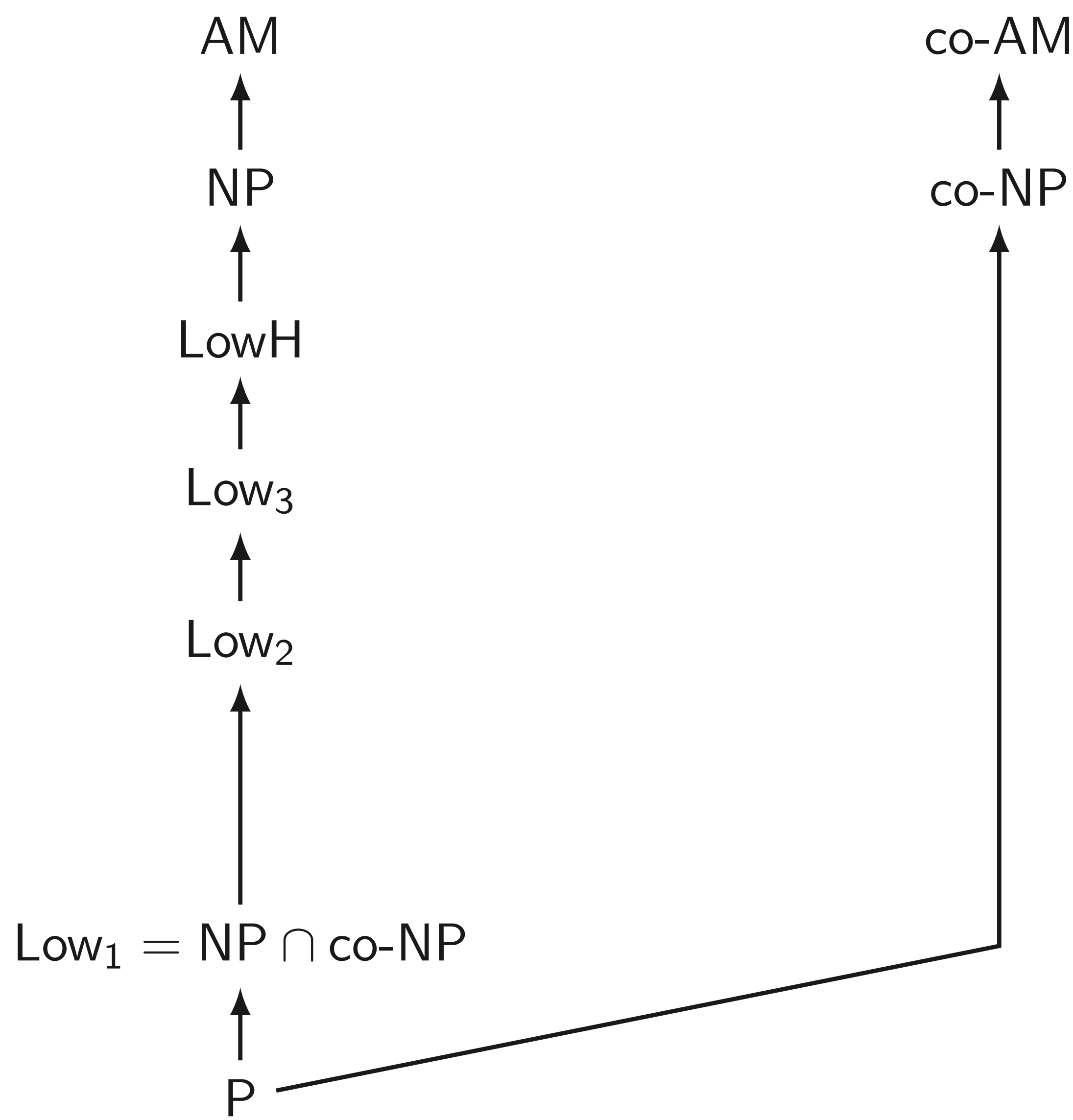
# Un mapa de la jerarquía baja

$$
\begin{array}{c}
\mathsf{AM} \\
\uparrow \\
\mathsf{NP} \\
\uparrow \\
\mathsf{LowH} \\
\uparrow \\
\mathsf{Low}_3 \\
\uparrow \\
\mathsf{Low}_2 \\
\uparrow \\
\mathsf{Low}_1 = \mathsf{NP} \cap \mathsf{co\text{-}NP} \\
\uparrow \\
\mathsf{P}
\end{array}
$$

# Un mapa de la jerarquía baja

$$
\begin{tikzcd}
\mathrm{AM} & & \text{co-AM} \\
\mathrm{NP} \arrow[u] & & \text{co-NP} \\
\mathrm{LowH} \arrow[u] & & \\
\mathrm{Low}_3 \arrow[u] & & \\
\mathrm{Low}_2 \arrow[u] & & \\
\mathrm{Low}_1 = \mathrm{NP} \cap \text{co-NP} \arrow[u] & & \\
\mathrm{P} \arrow[u] & &
\end{tikzcd}
$$

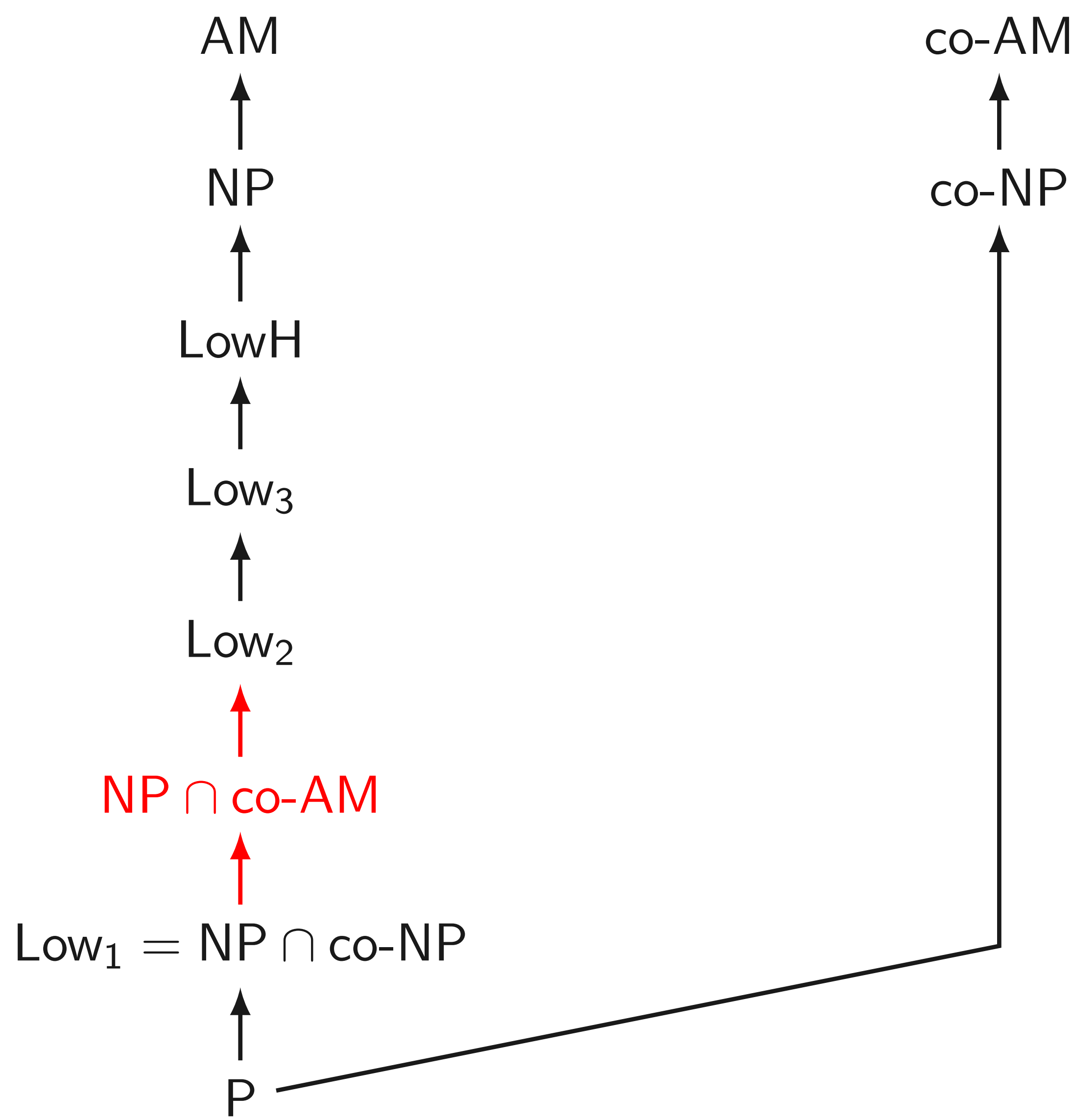
# Un mapa de la jerarquía baja



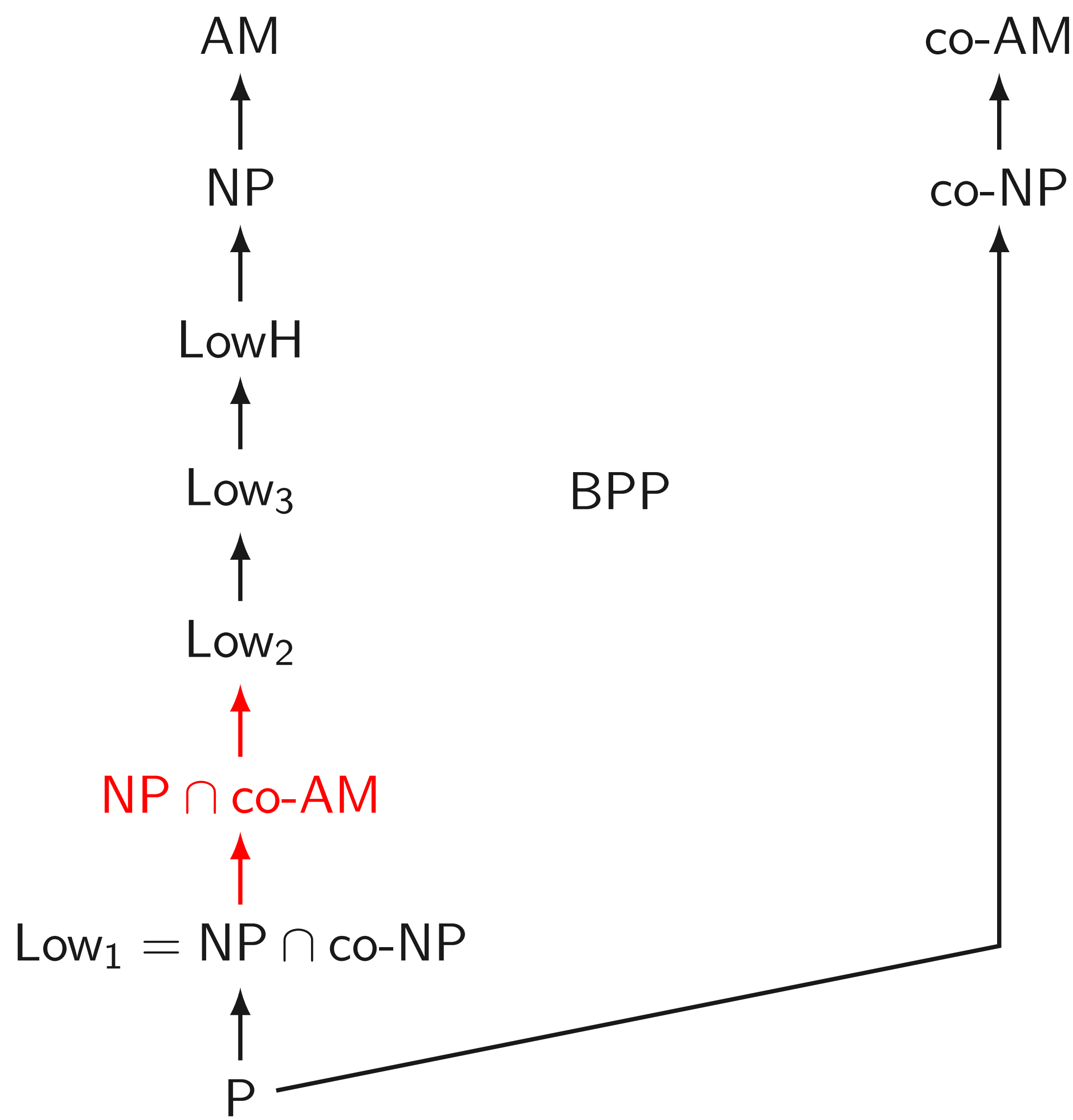
# Un mapa de la jerarquía baja

$$
\begin{tikzcd}
\mathsf{AM} & \mathsf{co\text{-}AM} \\
\mathsf{NP} \arrow[u] & \mathsf{co\text{-}NP} \arrow[u] \\
\mathsf{LowH} \arrow[u] & \\
\mathsf{Low}_3 \arrow[u] & \\
\mathsf{Low}_2 \arrow[u] & \\
\textcolor{red}{\mathsf{NP} \cap \mathsf{co\text{-}AM}} & \\
\mathsf{Low}_1 = \mathsf{NP} \cap \mathsf{co\text{-}NP} & \\
\mathsf{P} \arrow[u] \arrow[uuuuuur] &
\end{tikzcd}
$$

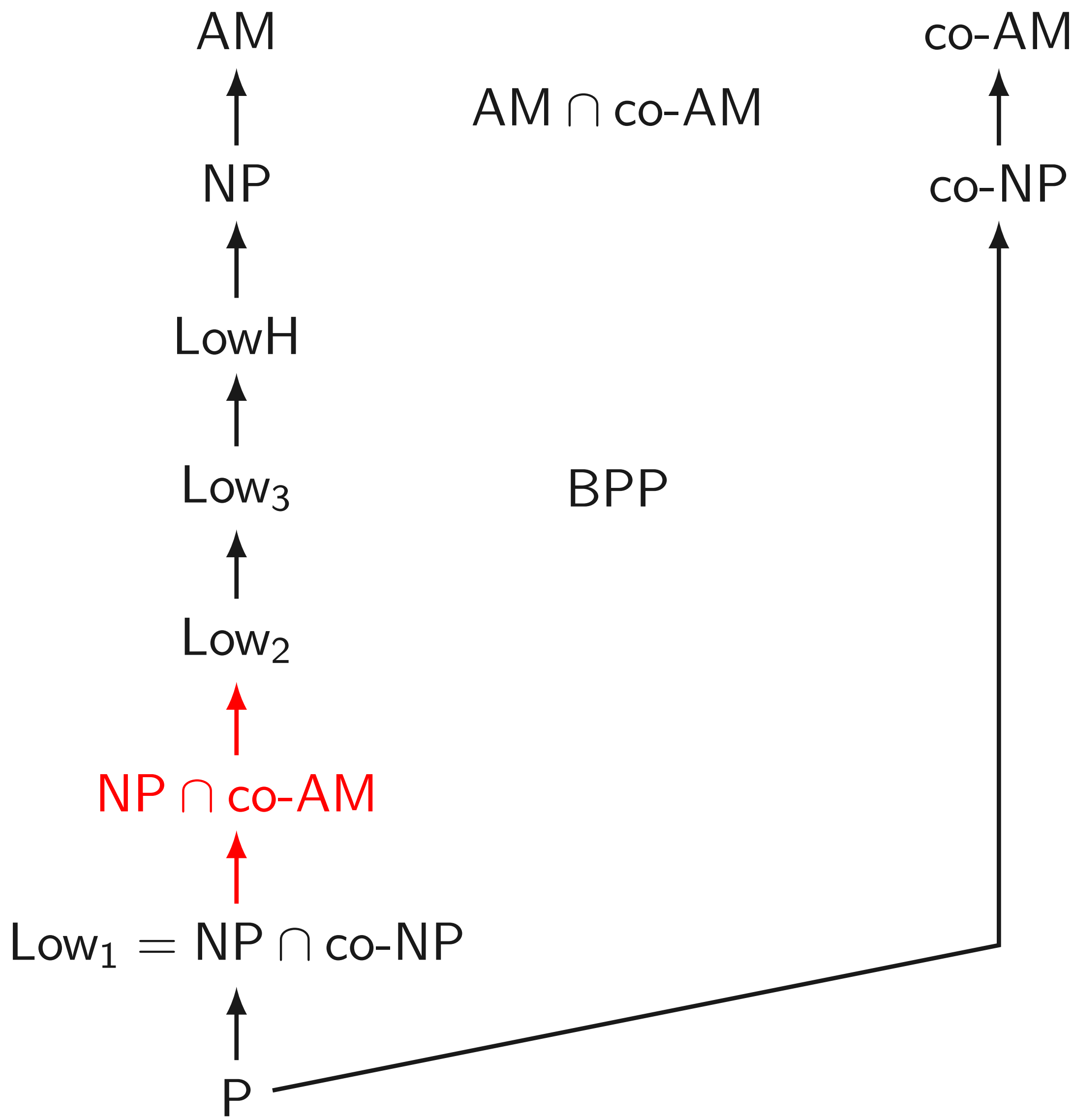
# Un mapa de la jerarquía baja



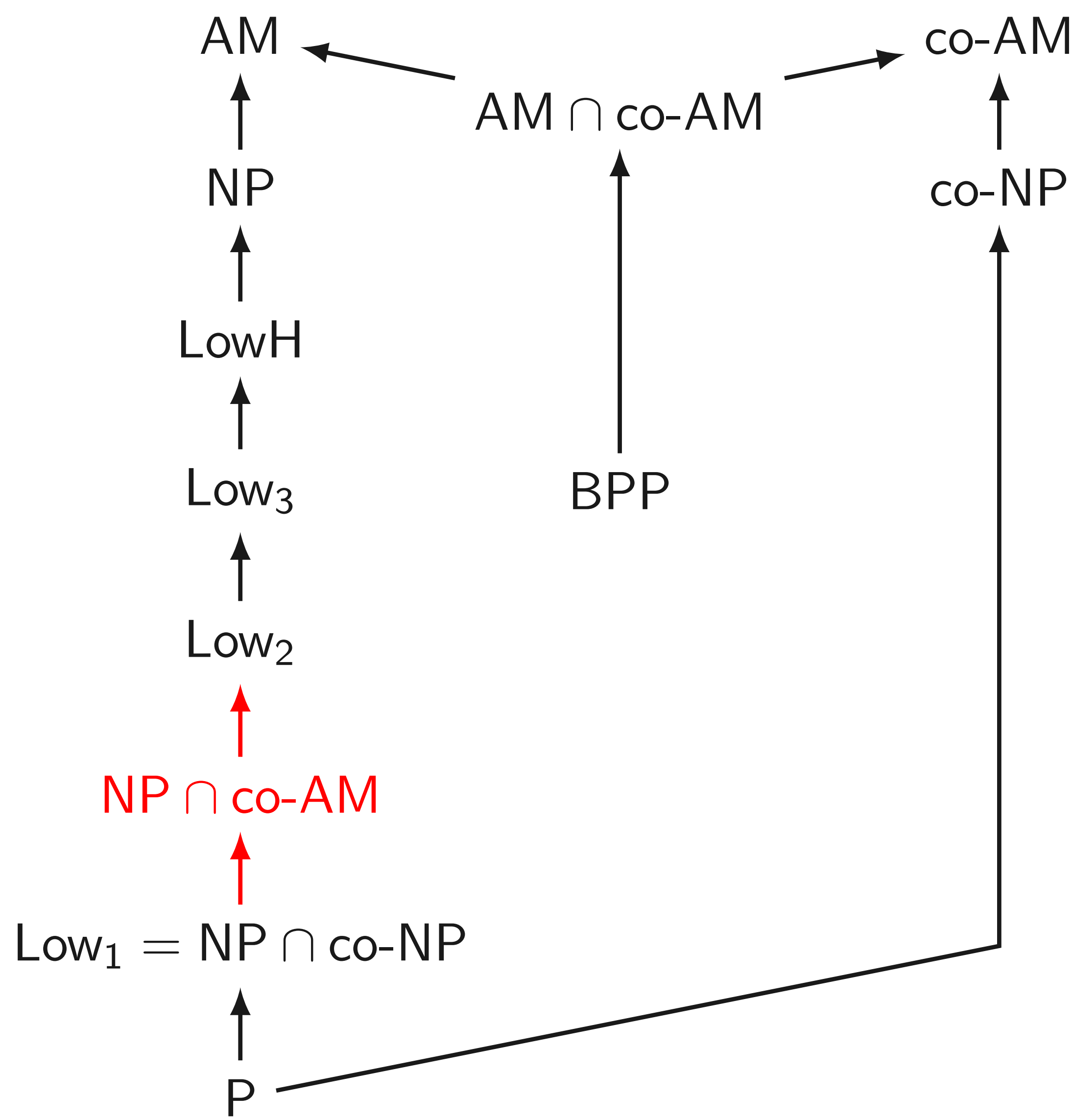
# Un mapa de la jerarquía baja



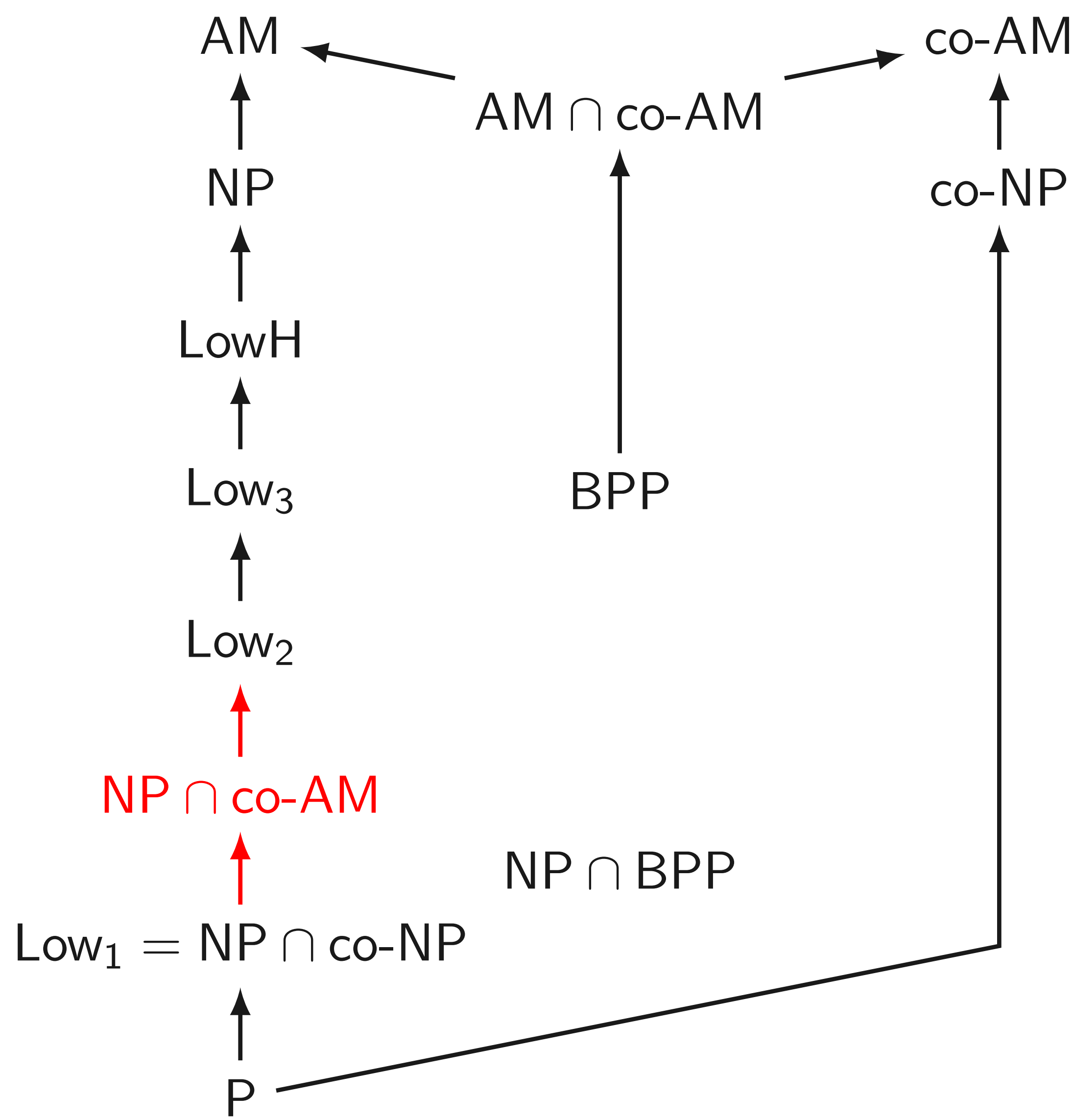
# Un mapa de la jerarquía baja



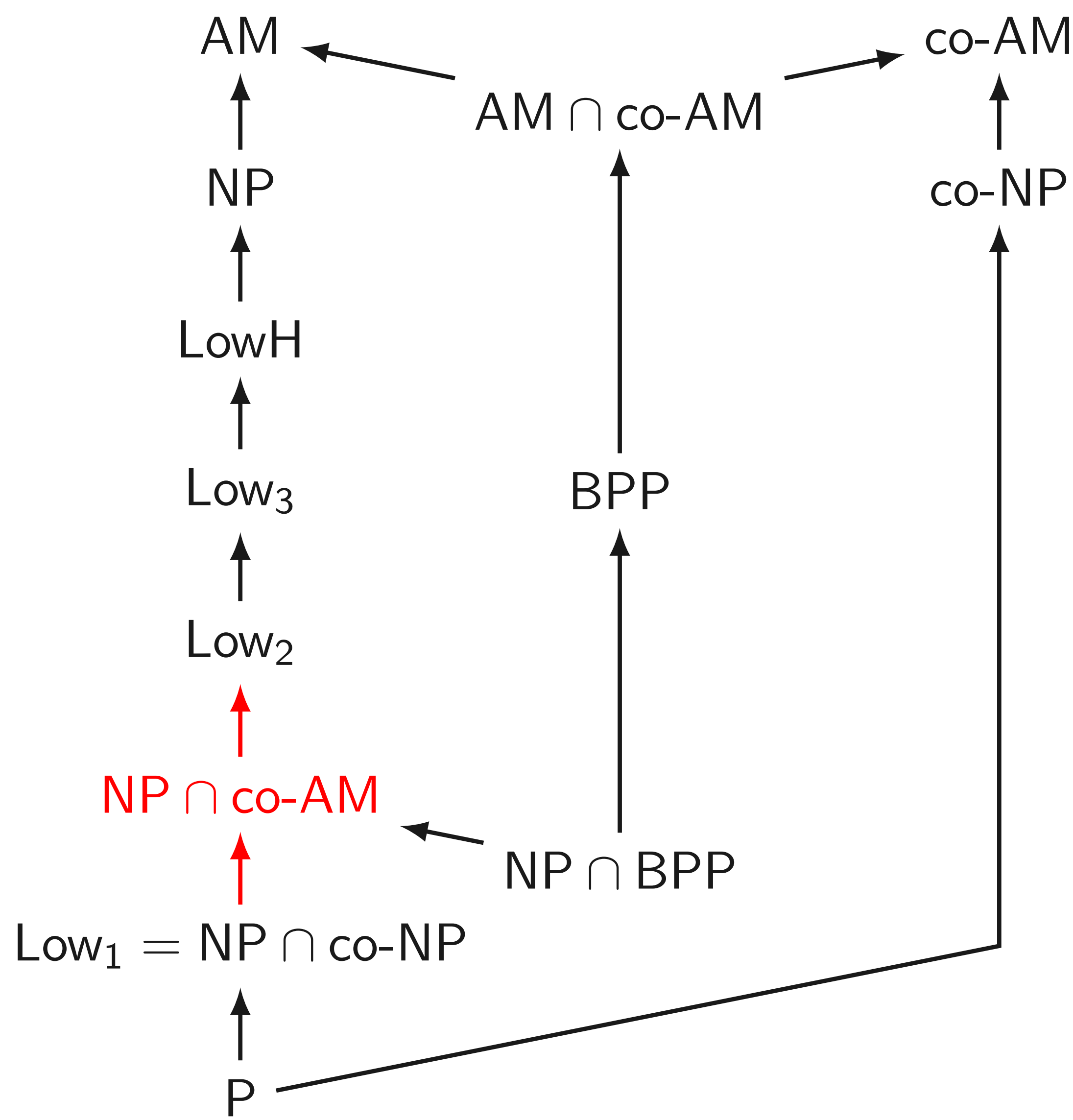
# Un mapa de la jerarquía baja



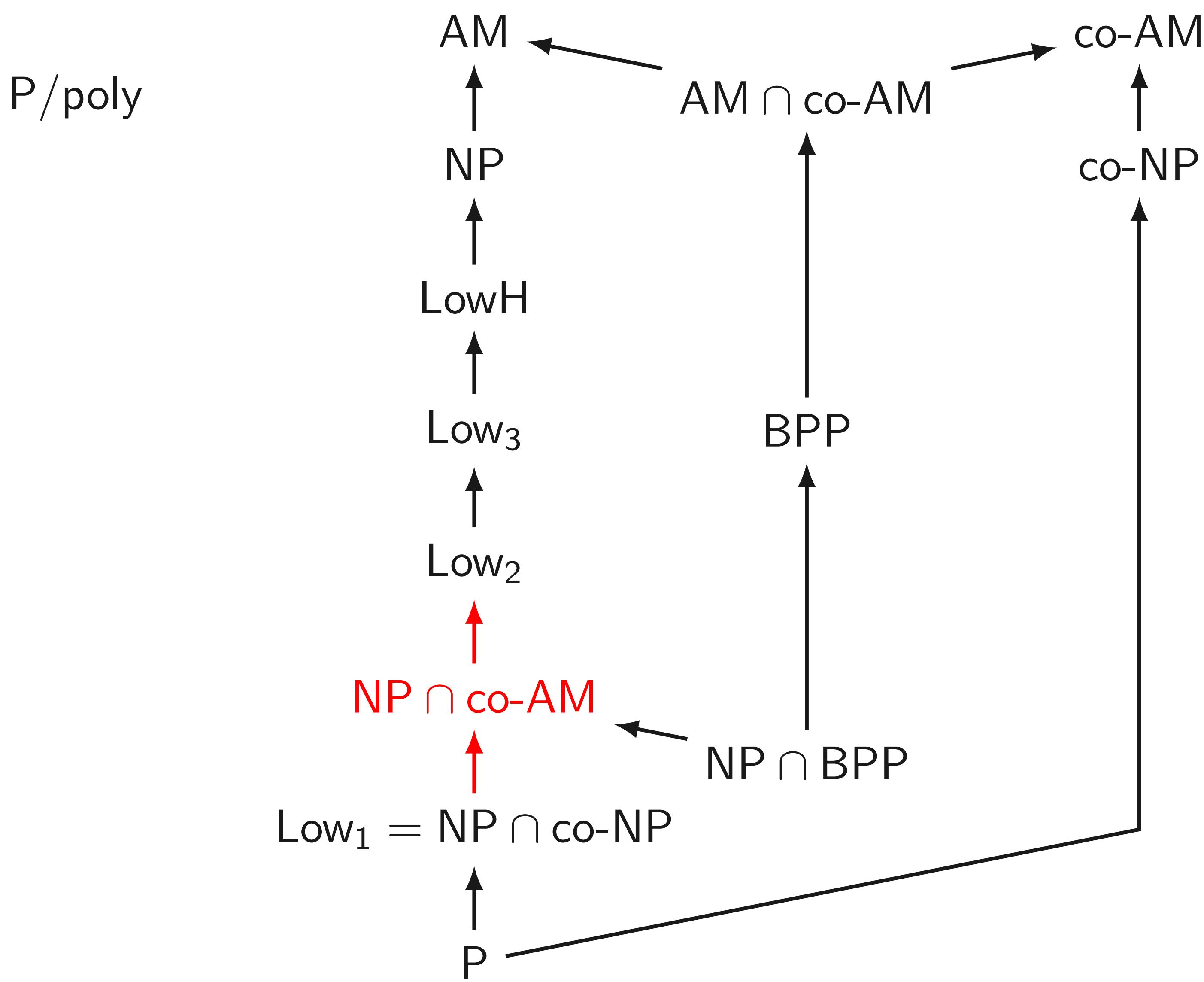
# Un mapa de la jerarquía baja



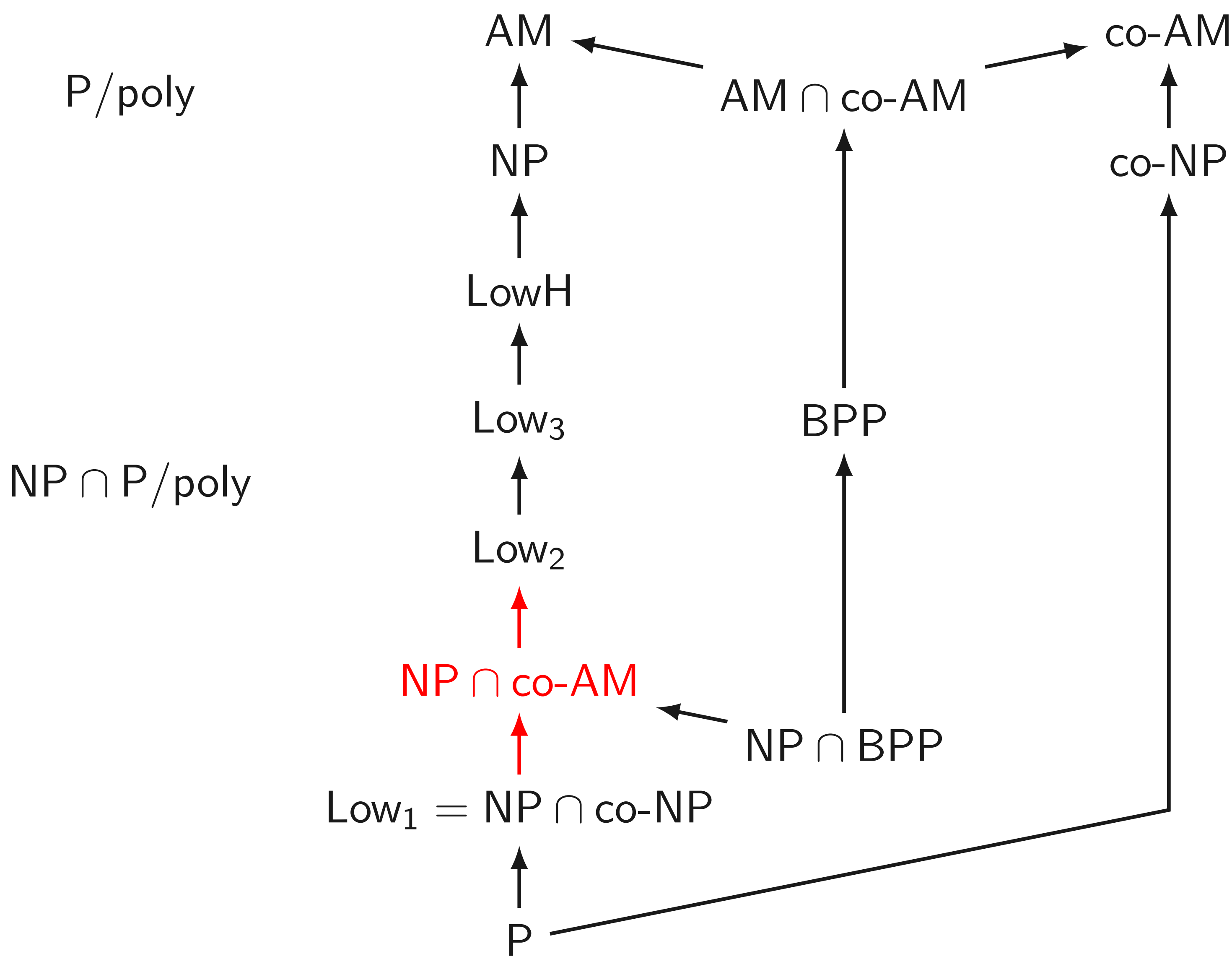
# Un mapa de la jerarquía baja



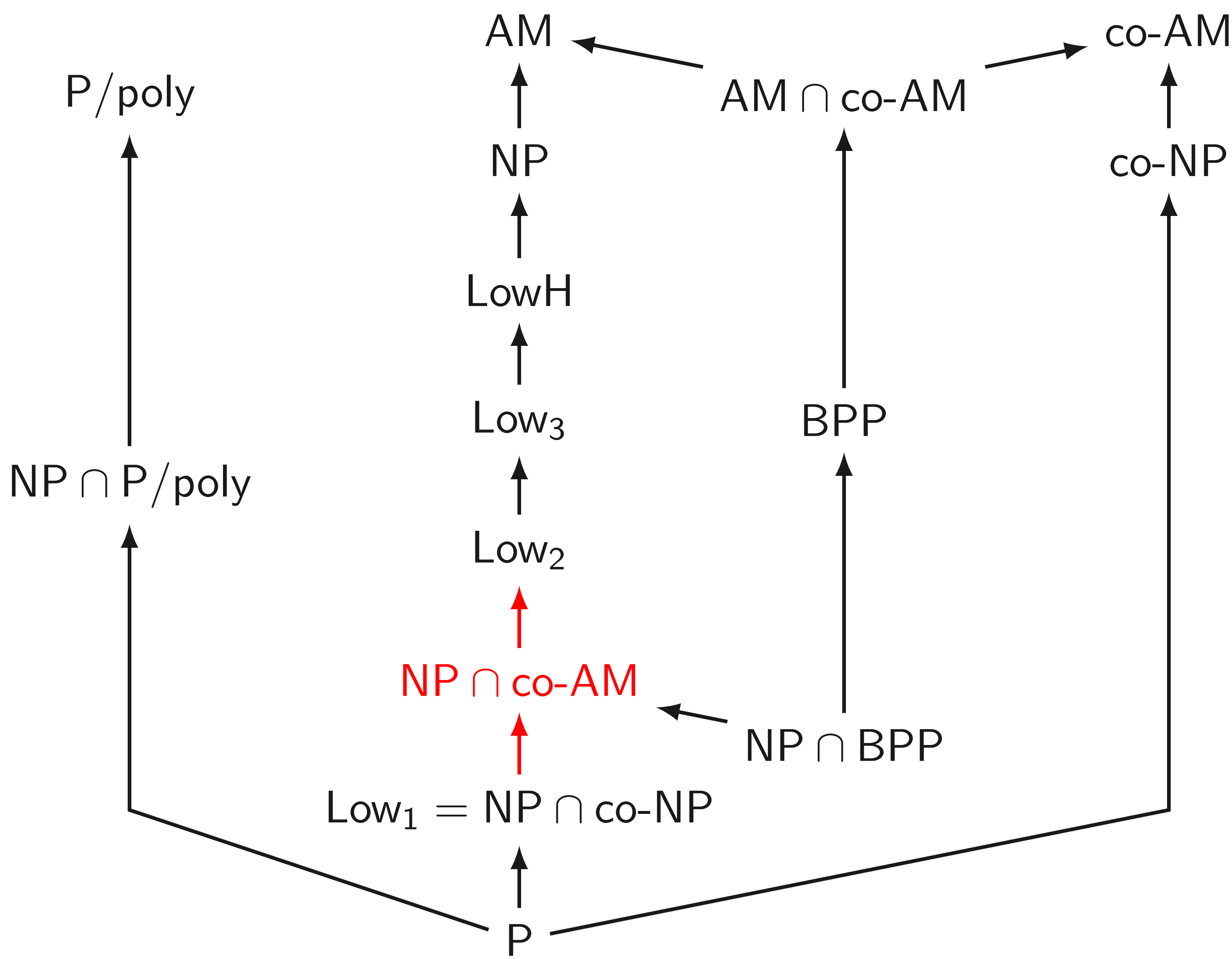
# Un mapa de la jerarquía baja



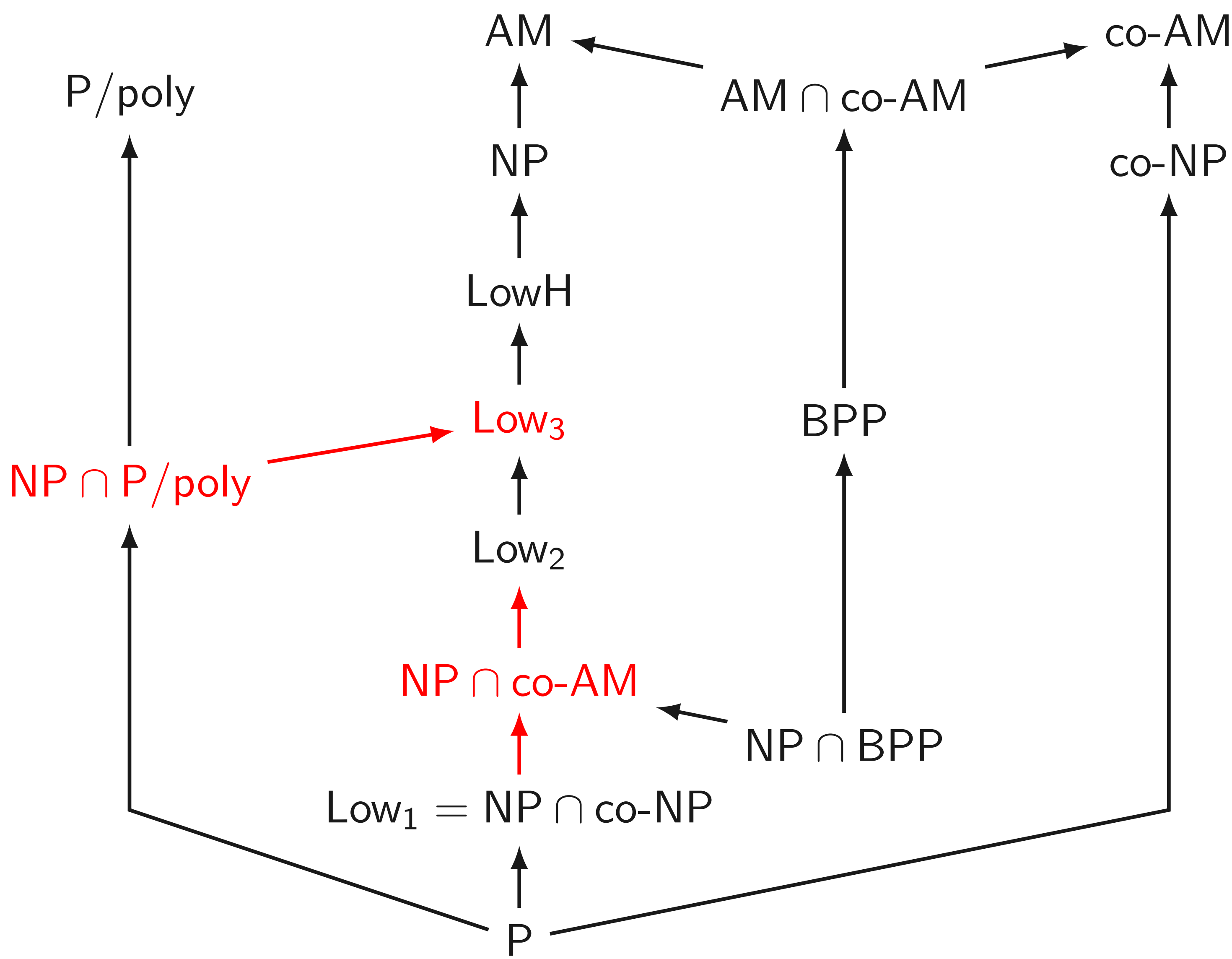
# Un mapa de la jerarquía baja



# Un mapa de la jerarquía baja



# Un mapa de la jerarquía baja



# La clase P/poly

Sea $L$ un lenguaje sobre el alfabeto $\{0, 1\}$.

# La clase P/poly

Sea $L$ un lenguaje sobre el alfabeto $\{0, 1\}$.

$L$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos si:

# La clase P/poly

Sea $L$ un lenguaje sobre el alfabeto $\{0, 1\}$.

$L$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos si:

- El número de entradas de $C_n$ es $n$, para cada $n \geq 0$.

# La clase P/poly

Sea $L$ un lenguaje sobre el alfabeto $\{0, 1\}$.

$L$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos si:

- El número de entradas de $C_n$ es $n$, para cada $n \geq 0$.
- Para cada $w \in \{0, 1\}^n$, se tiene que $w \in L$ si y sólo si $C_n(w) = 1$.

# La clase P/poly

Sea $L$ un lenguaje sobre el alfabeto $\{0, 1\}$.

$L$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos si:

- El número de entradas de $C_n$ es $n$, para cada $n \geq 0$.
- Para cada $w \in \{0, 1\}^n$, se tiene que $w \in L$ si y sólo si $C_n(w) = 1$.

$L \in$ P/poly si existe una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos y un polinomio $p(n)$ tal que:

# La clase P/poly

Sea $L$ un lenguaje sobre el alfabeto $\{0,1\}$.

$L$ es aceptado por una familia $\{C_n\}_{n\in\mathbb{N}}$ de circuitos Booleanos si:

- El número de entradas de $C_n$ es $n$, para cada $n \geq 0$.
- Para cada $w \in \{0,1\}^n$, se tiene que $w \in L$ si y sólo si $C_n(w) = 1$.

$L \in$ P/poly si existe una familia $\{C_n\}_{n\in\mathbb{N}}$ de circuitos Booleanos y un polinomio $p(n)$ tal que:

- $L$ es aceptado por $\{C_n\}_{n\in\mathbb{N}}$.

# La clase P/poly

Sea $L$ un lenguaje sobre el alfabeto $\{0,1\}$.

$L$ es aceptado por una familia $\{C_n\}_{n\in\mathbb{N}}$ de circuitos Booleanos si:

- El número de entradas de $C_n$ es $n$, para cada $n \geq 0$.
- Para cada $w \in \{0,1\}^n$, se tiene que $w \in L$ si y sólo si $C_n(w) = 1$.

$L \in \mathrm{P/poly}$ si existe una familia $\{C_n\}_{n\in\mathbb{N}}$ de circuitos Booleanos y un polinomio $p(n)$ tal que:

- $L$ es aceptado por $\{C_n\}_{n\in\mathbb{N}}$.
- La palabra sobre el alfabeto $\{0,1\}$ que representa a $C_n$ como un grafo etiquetado es de largo a lo más $p(n)$, para cada $n \geq 0$.

# $NP \cap P/poly \subseteq Low_3$

**Teorema**

*$NP \cap P/poly \subseteq Low_3$.*

# $\mathsf{NP} \cap \mathsf{P/poly} \subseteq \mathsf{Low}_3$

**Teorema**

*$NP \cap P/poly \subseteq Low_3$.*

**Demostración:** Sea $A \in \mathsf{NP} \cap \mathsf{P/poly}$.

# $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

**Teorema**

*$NP \cap P/poly \subseteq Low_3$.*

**Demostración:** Sea $A \in \mathrm{NP} \cap \mathrm{P/poly}$.

- Tenemos que demostrar que $\Sigma_3^P(A) = \Sigma_3^P$.

# $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

**Teorema**

*$NP \cap P/poly \subseteq Low_3$.*

**Demostración:** Sea $A \in \mathrm{NP} \cap \mathrm{P/poly}$.

- Tenemos que demostrar que $\Sigma_3^P(A) = \Sigma_3^P$.

Necesitamos una caracterización de $\Sigma_3^P(A)$ para hacer esta demostración.

# Una caracterización de NP relativizado

Dado un lenguaje $L$ sobre el alfabeto $\{0, 1\}$.

# Una caracterización de NP relativizado

Dado un lenguaje $L$ sobre el alfabeto $\{0, 1\}$.

**Lema**

*$L \in NP^A$ si y sólo si existe una $MT$ determinista $M^A$ de tiempo polinomial y un polinomio $p(n)$ tales que $M^A$ tiene un oráculo para $A$ y para todo $u \in \{0, 1\}^*$:*

$$u \in L \quad \text{si y sólo si} \quad \exists v \in \{0,1\}^{p(|u|)} : M^A \text{ acepta } (u, v)$$

# Una caracterización de NP relativizado

Dado un lenguaje $L$ sobre el alfabeto $\{0,1\}$.

**Lema**

*$L \in NP^A$ si y sólo si existe una $MT$ determinista $M^A$ de tiempo polinomial y un polinomio $p(n)$ tales que $M^A$ tiene un oráculo para $A$ y para todo $u \in \{0,1\}^*$:*

$$u \in L \quad \text{si y sólo si} \quad \exists v \in \{0,1\}^{p(|u|)} : M^A \text{ acepta } (u,v)$$

**Ejercicio**

Demuestre el lema.

# Una caracterización de $\Sigma_3^P$ relativizado

**Lema**

*$L \in \Sigma_3^P(A)$ si y sólo si existe una MT determinista $M^A$ de tiempo polinomial y un polinomio $p(n)$ tales que $M^A$ tiene un oráculo para $A$ y para todo $u \in \{0,1\}^*$:*

*$u \in L$ si y sólo si*

$$\exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} :$$

$$M^A \text{ acepta } (u, v_1, v_2, v_3)$$

# Una caracterización de $\Sigma_3^P$ relativizado

**Lema**

*$L \in \Sigma_3^P(A)$ si y sólo si existe una MT determinista $M^A$ de tiempo polinomial y un polinomio $p(n)$ tales que $M^A$ tiene un oráculo para $A$ y para todo $u \in \{0,1\}^*$:*

*$u \in L$ si y sólo si*

$$\exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} :$$

$$M^A \text{ acepta } (u, v_1, v_2, v_3)$$

**Ejercicio**

Demuestre el lema.

# La demostración de que $\mathrm{NP} \cap \mathrm{P}/\mathrm{poly} \subseteq \mathrm{Low}_3$

Sólo tenemos que demostrar que $\Sigma_3^P(A) \subseteq \Sigma_3^P$.

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Sólo tenemos que demostrar que $\Sigma_3^P(A) \subseteq \Sigma_3^P$.

- Puesto que $\Sigma_3^P \subseteq \Sigma_3^P(A)$.

# La demostración de que $\mathsf{NP} \cap \mathsf{P}/\mathsf{poly} \subseteq \mathsf{Low}_3$

Sólo tenemos que demostrar que $\Sigma_3^P(A) \subseteq \Sigma_3^P$.

- Puesto que $\Sigma_3^P \subseteq \Sigma_3^P(A)$.

Sea $L \in \Sigma_3^P(A)$.

# La demostración de que $\mathrm{NP} \cap \mathrm{P}/\mathrm{poly} \subseteq \mathrm{Low}_3$

Sólo tenemos que demostrar que $\Sigma_3^P(A) \subseteq \Sigma_3^P$.

- Puesto que $\Sigma_3^P \subseteq \Sigma_3^P(A)$.

Sea $L \in \Sigma_3^P(A)$.

Por el lema anterior, sabemos que existe una MT determinista $M^A$ de tiempo polinomial y un polinomio $p(n)$ tales que $M^A$ tiene un oráculo para $A$ y para todo $u \in \{0,1\}^*$:

$$u \in L \ \text{ si y sólo si } \ \exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} : M^A \text{ acepta } (u, v_1, v_2, v_3)$$

# La demostración de que NP $\cap$ P/poly $\subseteq$ Low$_3$

Como $A \in \mathrm{P/poly}$, sabemos que $A$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos.

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Como $A \in \mathrm{P/poly}$, sabemos que $A$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos.

- Suponemos que el tamaño de $C_n$ es a lo más $q(n)$ para un polinomio fijo $q$.

# La demostración de que NP $\cap$ P/poly $\subseteq$ Low$_3$

Como $A \in$ P/poly, sabemos que $A$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos.

- Suponemos que el tamaño de $C_n$ es a lo más $q(n)$ para un polinomio fijo $q$.

Para $M^A$, podemos suponer que existe un polinomio $r(n)$ tal que todas las llamadas al oráculo $A$ son de tamaño $r(|u|)$.

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Como $A \in \mathrm{P/poly}$, sabemos que $A$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos.

- Suponemos que el tamaño de $C_n$ es a lo más $q(n)$ para un polinomio fijo $q$.

Para $M^A$, podemos suponer que existe un polinomio $r(n)$ tal que todas las llamadas al oráculo $A$ son de tamaño $r(|u|)$.

- $u$ es el string para el cual queremos saber si $u \in L$.

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Como $A \in \mathrm{P/poly}$, sabemos que $A$ es aceptado por una familia $\{C_n\}_{n \in \mathbb{N}}$ de circuitos Booleanos.

- Suponemos que el tamaño de $C_n$ es a lo más $q(n)$ para un polinomio fijo $q$.

Para $M^A$, podemos suponer que existe un polinomio $r(n)$ tal que todas las llamadas al oráculo $A$ son de tamaño $r(|u|)$.

- $u$ es el string para el cual queremos saber si $u \in L$.
- ¿Por qué podemos suponer esto?

# La demostración de que $\mathsf{NP} \cap \mathsf{P}/\mathsf{poly} \subseteq \mathsf{Low}_3$

Podemos reemplazar $A$ por la familia de circuitos $\{C_n\}_{n\in\mathbb{N}}$ que acepta $A$.

# La demostración de que NP $\cap$ P/poly $\subseteq$ $\text{Low}_3$

Podemos reemplazar $A$ por la familia de circuitos $\{C_n\}_{n \in \mathbb{N}}$ que acepta $A$.

Existe una MT determinista $M_1$ de tiempo polinomial tal que para todo $u \in \{0,1\}^*$:

$u \in L$ si y sólo si

$$\exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} :$$

$$M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})$$

# La demostración de que $\mathrm{NP} \cap \mathrm{P}/\mathrm{poly} \subseteq \mathrm{Low}_3$

Podemos reemplazar $A$ por la familia de circuitos $\{C_n\}_{n\in\mathbb{N}}$ que acepta $A$.

Existe una MT determinista $M_1$ de tiempo polinomial tal que para todo $u \in \{0,1\}^*$:

$u \in L$ si y sólo si

$$\exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} :$$
$$M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})$$

¿Pero cómo construimos $C_{r(|u|)}$?

# La demostración de que $\mathrm{NP} \cap \mathrm{P}/\mathrm{poly} \subseteq \mathrm{Low}_3$

Podemos reemplazar $A$ por la familia de circuitos $\{C_n\}_{n \in \mathbb{N}}$ que acepta $A$.

Existe una MT determinista $M_1$ de tiempo polinomial tal que para todo $u \in \{0,1\}^*$:

$u \in L$ si y sólo si

$$\exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} :$$

$$M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})$$

¿Pero cómo construimos $C_{r(|u|)}$?

- No tenemos un algoritmo que construya estos circuitos.

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Podemos intentar usar un cuantificador existencial para introducir la familia de circuitos $\{C_n\}_{n \in \mathbb{N}}$:

$$
\begin{aligned}
& u \in L \ \text{ si y sólo si} \\
& \qquad \exists C_{r(|u|)} \in \{0,1\}^{q(r(|u|))} \\
& \qquad\qquad \exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} : \\
& \qquad\qquad\qquad M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})
\end{aligned}
$$

# La demostración de que NP $\cap$ P/poly $\subseteq$ Low$_3$

Podemos intentar usar un cuantificador existencial para introducir la familia de circuitos $\{C_n\}_{n \in \mathbb{N}}$:

$$u \in L \text{ si y sólo si}$$
$$\exists C_{r(|u|)} \in \{0,1\}^{q(r(|u|))}$$
$$\exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} :$$
$$M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})$$

¿Qué problema tiene esta fórmula?

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Podemos intentar usar un cuantificador existencial para introducir la familia de circuitos $\{C_n\}_{n \in \mathbb{N}}$:

$$
\begin{aligned}
&u \in L \ \text{ si y sólo si} \\
&\qquad \exists C_{r(|u|)} \in \{0,1\}^{q(r(|u|))} \\
&\qquad\qquad \exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} : \\
&\qquad\qquad\qquad M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})
\end{aligned}
$$

¿Qué problema tiene esta fórmula?

- No estamos seguros si el circuito $C_{r(|u|)}$ es el correcto.

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Para solucionar el problema usamos el hecho de que $A \in \mathrm{NP}$.

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Para solucionar el problema usamos el hecho de que $A \in \mathrm{NP}$.

Sabemos que existe una MT determinista $M_2$ de tiempo polinomial y un polinomio $s(n)$ tales que para todo $u \in \{0,1\}^*$:

$$u \in A \text{ si y sólo si } \exists v \in \{0,1\}^{s(|u|)} : M_2 \text{ acepta } (u, v)$$

# La demostración de que $\mathsf{NP} \cap \mathsf{P/poly} \subseteq \mathsf{Low}_3$

Entonces podemos verificar que el circuito $C_{r(|u|)}$ es el correcto de la siguiente forma:

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Entonces podemos verificar que el circuito $C_{r(|u|)}$ es el correcto de la siguiente forma:

$u \in L$ si y sólo si

$$\exists C_{r(|u|)} \in \{0,1\}^{q(r(|u|))}$$

$$\forall x_1 \in \{0,1\}^{r(|u|)} [C_{r(|u|)}(x_1) = 1 \to \exists y_1 \in \{0,1\}^{s(|u|)} : M_2 \text{ acepta } (x_1, y_1)] \wedge$$

$$\forall x_2 \in \{0,1\}^{r(|u|)} [C_{r(|u|)}(x_2) = 0 \to \forall y_2 \in \{0,1\}^{s(|u|)} : M_2 \text{ no acepta } (x_2, y_2)] \wedge$$

$$\exists v_1 \in \{0,1\}^{p(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} :$$

$$M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})$$

# La demostración de que NP $\cap$ P/poly $\subseteq$ Low$_3$

Reordenando la expresión obtenemos:

$$
\begin{aligned}
& u \in L \;\; \text{si y sólo si} \\
& \qquad \exists C_{r(|u|)} \in \{0,1\}^{q(r(|u|))} \\
& \qquad \exists v_1 \in \{0,1\}^{p(|u|)} \\
& \qquad \forall x_1 \in \{0,1\}^{r(|u|)} \\
& \qquad \forall x_2 \in \{0,1\}^{r(|u|)} \\
& \qquad \forall y_2 \in \{0,1\}^{s(|u|)} \\
& \qquad \forall v_2 \in \{0,1\}^{p(|u|)} \\
& \qquad \exists y_1 \in \{0,1\}^{s(|u|)} \\
& \qquad \exists v_3 \in \{0,1\}^{p(|u|)} \\
& \qquad\qquad [C_{r(|u|)}(x_1) = 1 \to M_2 \text{ acepta } (x_1, y_1)] \wedge \\
& \qquad\qquad\qquad [C_{r(|u|)}(x_2) = 0 \to M_2 \text{ no acepta } (x_2, y_2)] \wedge \\
& \qquad\qquad\qquad\qquad M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})
\end{aligned}
$$

# La demostración de que $\mathrm{NP} \cap \mathrm{P}/\mathrm{poly} \subseteq \mathrm{Low}_3$

Sea $M_3$ una MT determinista de tiempo polinomial que con entrada $(u, C_{r(|u|)}, v_1, x_1, x_2, y_2, v_2, y_1, v_3)$ verifica la siguiente condición

$$[C_{r(|u|)}(x_1) = 1 \rightarrow M_2 \text{ acepta } (x_1, y_1)] \wedge \\ [C_{r(|u|)}(x_2) = 0 \rightarrow M_2 \text{ no acepta } (x_2, y_2)] \wedge \\ M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})$$

# La demostración de que $\mathrm{NP} \cap \mathrm{P}/\mathrm{poly} \subseteq \mathrm{Low}_3$

Sea $M_3$ una MT determinista de tiempo polinomial que con entrada $(u, C_{r(|u|)}, v_1, x_1, x_2, y_2, v_2, y_1, v_3)$ verifica la siguiente condición

$$[C_{r(|u|)}(x_1) = 1 \to M_2 \text{ acepta } (x_1, y_1)] \wedge \\ [C_{r(|u|)}(x_2) = 0 \to M_2 \text{ no acepta } (x_2, y_2)] \wedge \\ M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})$$

¿Cómo se construye esta MT?

# La demostración de que $\text{NP} \cap \text{P}/\text{poly} \subseteq \text{Low}_3$

Sea $M_3$ una MT determinista de tiempo polinomial que con entrada $(u, C_{r(|u|)}, v_1, x_1, x_2, y_2, v_2, y_1, v_3)$ verifica la siguiente condición

$$[C_{r(|u|)}(x_1) = 1 \to M_2 \text{ acepta } (x_1, y_1)] \wedge \\ [C_{r(|u|)}(x_2) = 0 \to M_2 \text{ no acepta } (x_2, y_2)] \wedge \\ M_1 \text{ acepta } (u, v_1, v_2, v_3, C_{r(|u|)})$$

¿Cómo se construye esta MT?

- ¿Cómo se verifica que $C_{r(|u|)}(x_1) = 1$?

# La demostración de que $\mathrm{NP} \cap \mathrm{P}/\mathrm{poly} \subseteq \mathrm{Low}_3$

Tenemos que para todo $u \in \{0,1\}^*$:

$$
\begin{array}{l}
u \in L \ \text{ si y sólo si} \\
\qquad \exists C_{r(|u|)} \in \{0,1\}^{q(r(|u|))} \exists v_1 \in \{0,1\}^{p(|u|)} \\
\qquad\qquad \forall x_1 \in \{0,1\}^{r(|u|)} \forall x_2 \in \{0,1\}^{r(|u|)} \forall y_2 \in \{0,1\}^{s(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \\
\qquad\qquad\qquad \exists y_1 \in \{0,1\}^{s(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} \\
\qquad\qquad\qquad\qquad M_3 \text{ acepta } (u, C_{r(|u|)}, v_1, x_1, x_2, y_2, v_2, y_1, v_3)
\end{array}
$$

# La demostración de que $\mathrm{NP} \cap \mathrm{P}/\mathrm{poly} \subseteq \mathrm{Low}_3$

Tenemos que para todo $u \in \{0,1\}^*$:

$$
\begin{array}{l}
u \in L \text{ si y sólo si} \\
\qquad \exists C_{r(|u|)} \in \{0,1\}^{q(r(|u|))} \exists v_1 \in \{0,1\}^{p(|u|)} \\
\qquad\qquad \forall x_1 \in \{0,1\}^{r(|u|)} \forall x_2 \in \{0,1\}^{r(|u|)} \forall y_2 \in \{0,1\}^{s(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \\
\qquad\qquad\qquad \exists y_1 \in \{0,1\}^{s(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} \\
\qquad\qquad\qquad\qquad M_3 \text{ acepta } (u, C_{r(|u|)}, v_1, x_1, x_2, y_2, v_2, y_1, v_3)
\end{array}
$$

Concluimos que $L \in \Sigma_3^P$.

# La demostración de que $\mathrm{NP} \cap \mathrm{P/poly} \subseteq \mathrm{Low}_3$

Tenemos que para todo $u \in \{0,1\}^*$:

$$
\begin{aligned}
& u \in L \ \text{ si y sólo si} \\
& \qquad \exists C_{r(|u|)} \in \{0,1\}^{q(r(|u|))} \exists v_1 \in \{0,1\}^{p(|u|)} \\
& \qquad\qquad \forall x_1 \in \{0,1\}^{r(|u|)} \forall x_2 \in \{0,1\}^{r(|u|)} \forall y_2 \in \{0,1\}^{s(|u|)} \forall v_2 \in \{0,1\}^{p(|u|)} \\
& \qquad\qquad\qquad \exists y_1 \in \{0,1\}^{s(|u|)} \exists v_3 \in \{0,1\}^{p(|u|)} \\
& \qquad\qquad\qquad\qquad M_3 \text{ acepta } (u, C_{r(|u|)}, v_1, x_1, x_2, y_2, v_2, y_1, v_3)
\end{aligned}
$$

Concluimos que $L \in \Sigma_3^P$.

- ¿Es un problema que tengamos distintos polinomios en la condición anterior? $\square$

# Un corolario fundamental

**Corolario**

*Si* $NP \subseteq P/poly$*, entonces* $PH = \Sigma_3^P$.

# Un corolario fundamental

**Corolario**

*Si* $NP \subseteq P/poly$*, entonces* $PH = \Sigma_3^P$.

**Ejercicio**

Demuestre el corolario.

# Un corolario fundamental

**Corolario**

*Si NP $\subseteq$ P/poly, entonces* $PH = \Sigma_3^P$.

**Ejercicio**

Demuestre el corolario.

- Note que este resultado es una versión más débil del teorema de Karp-Lipton, el cual nos dice que si NP $\subseteq$ P/poly, entonces PH $= \Sigma_2^P$.