

La Jerarquía Polinomial

IIC3810

La noción de oráculo

¿Qué tienen en común los problemas CROM y EQUIV?

- ▶ Si encontramos un algoritmo polinomial para un problema NP-completo, entonces estos problemas pueden ser resueltos en tiempo polinomial
- ▶ Un problema NP-completo puede ser visto como un *oráculo* para estos problemas

Vamos a introducir la noción de MT con oráculo.

- ▶ Vamos a mostrar que sirve para caracterizar a los problemas anteriores, y a muchos otros problemas ...

MT con oráculo

Definición

MT determinista con oráculo para $A \subseteq \Sigma^$:*

$$M^A = (Q, \Sigma, \Gamma, q_0, \delta, F)$$

- ▶ Q es un conjunto finito de estados tal que $q_?, q_{YES}, q_{NO} \in Q$
- ▶ Σ es un alfabeto finito tal que $\vdash, \sqcup \notin \Sigma$
- ▶ Γ es un alfabeto finito tal que $\Sigma \cup \{\vdash, \sqcup\} \subseteq \Gamma$
- ▶ $q_0 \in Q$ es el estado inicial
- ▶ $F \subseteq Q$ es un conjunto de estados finales
- ▶ δ es una función parcial:

$$\delta : Q \times \Gamma \times \Gamma \rightarrow Q \times \Gamma \times \{\leftarrow, \square, \rightarrow\} \times \Gamma \times \{\leftarrow, \square, \rightarrow\}$$

*La segunda cinta es la **cinta de consulta***

MT con oráculo: Funcionamiento

La definición anterior puede extenderse fácilmente al caso de no determinismo.

Una MT M con oráculo para A funciona como una MT tradicional excepto cuando entra al estado $q_?$:

- ▶ Cinta de consulta: $\vdash wBB \dots$, para $w \in \Sigma^*$

La cabeza lectora de la cinta de consulta está en la posición 1

- ▶ M invoca al oráculo para A , y su siguiente estado es q_{YES} o q_{NO} dependiendo de su respuesta
 - ▶ $w \in A$ si y sólo si el estado es q_{YES}

MT con oráculo: Tiempo de ejecución

El tiempo de ejecución de una MT con oráculo se define como para el caso de las MTs tradicionales.

- Una invocación al oráculo se considera como un paso

Ejemplo

CROM es aceptado por una MT determinista $M^{\text{CROM}^\leq}$ que funciona en tiempo $O(n)$

- También podemos usar SAT como oráculo. ¿En que tiempo funcionaría la MT?

Clases de complejidad y la noción de oráculo

Una primera clase definida en términos de MTs con oráculos:

Definición

$PTIME^A$: Lenguajes L para los cuales existe una MT determinista M^A tal que $L = L(M^A)$ y M^A funciona en tiempo $O(n^k)$.

Tenemos que:

- ▶ $CROM$ está en $PTIME^{SAT}$
 - ▶ También está contenido en $PTIME^A$, para cualquier problema A que es NP-completo
- ▶ NP y co-NP están contenidos en $PTIME^{SAT}$

Clases de complejidad y la noción de oráculo

Una definición mas general:

Definición

$$PTIME^{NP} = \bigcup_{A \in NP} PTIME^A$$

En realidad esta definición no es más general:

Proposición

$$PTIME^{NP} = PTIME^{SAT}$$

Ejercicio

Demuestre la proposición.

Equivalencia de expresiones aritméticas: Complejidad

¿Cuál es la complejidad de EQUIV?

- ▶ ¿Está en PTIME^{NP} ?

Nuevamente la noción de oráculo nos puede ayudar a entender la complejidad de un problema.

Una segunda clase definida en términos de oráculos

Definición

- ▶ NP^A : Lenguajes L para los cuales existe una MT **no** determinista M^A tal que $L = L(M^A)$ y M^A funciona en tiempo $O(n^k)$
- ▶ NP^{NP} : $\bigcup_{A \in NP} NP^A$

Podemos describir mejor la complejidad de EQUIV.

Ejercicio

Demuestre que $EQUIV \in co-NP^{NP}$.

- ▶ Esto es equivalente a demostrar que $\overline{EQUIV} \in NP^{NP}$