

La complejidad de SAT

Tenemos que usar máquinas de Turing no deterministas para entender la complejidad exacta de SAT.

Dado: MT no determinista M con alfabeto A .

- Paso de M : ejecutar una instrucción de la relación de transición.
- $tiempo_M(w)$: número de pasos de M con entrada w en la ejecución más corta que acepta a w .

Sólo esta definido para palabras aceptadas por M .

Dado un número natural n :

$$t_M(n) = \max\{n\} \cup \{ tiempo_M(w) \mid w \in A^*, |w| = n \text{ y } M \text{ acepta } w \}.$$

¿Por que incluimos $\{n\}$ en la definición?

Clases de complejidad no deterministas

Un lenguaje L es aceptado en tiempo t por una MT M no determinista si:

- $L = L(M)$.
- t_M es $O(t)$.

Clases de Complejidad no deterministas

Dado: alfabeto A .

NTIME(t): Conjunto de todos los lenguajes que pueden ser aceptados en tiempo t por alguna MT no determinista.

Una clase fundamental:

$$\text{NP} = \bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k).$$

¿Por qué es tan importante esta clase? ¿Qué problemas están en esta clase? ¿Qué problemas son completos para esta clase?

Algunas propiedades de la clase NP

¿Dónde vive NP? $\text{PTIME} \subseteq \text{NP} \subseteq \text{EXPTIME}$.

- Se sabe que al menos una de estas inclusiones es estricta (¿por qué?), pero no se sabe cual.
- Tampoco se sabe si ambas inclusiones son estrictas.

¿Qué problemas están en NP?

Ejercicio: Muestre que **SAT** y **3-coloración de grafos** están en NP.

¿Qué problemas son completos para esta clase?

Teorema de Cook

Teorema (Cook): SAT es completo para la clase NP.

Demostración: Sea $L \in \text{NP}$. Tenemos que demostrar que L es reducible en tiempo polinomial a SAT.

Esto significa que existe una función $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ tal que:

- f es computable en tiempo polinomial.
- Para cada $w \in \{0, 1\}^*$ se tiene que $w \in L$ si y sólo si $f(w) \in \text{SAT}$.

Notación: $f(w) = \varphi_w$.

Teorema de Cook: Demostración

¿Qué sabemos de L ?

- Como $L \in \text{NP}$, existe una MT M no determinista tal que $L = L(M)$ y t_M es $O(n^k)$, donde $k > 0$ es una constante.

Vamos a representar el funcionamiento de M con entrada w usando la fórmula φ_w : **M acepta w si y sólo si φ_w es satisfacible.**

Suponemos:

- $M = (Q, \{0, 1\}, q_0, \delta, F)$, donde $F = \{q_m\}$ y no existe una transición en δ para q_m .
- $w = a_0 \cdots a_{n-1}$, donde cada $a_i \in \{0, 1\}$.

Teorema de Cook: Demostración

Usamos las siguientes variables proposicionales:

$$s_{t,p,a} \quad : \quad t \in [0, t_M(n)], p \in [-t_M(n), t_M(n)] \text{ y } a \in \{0, 1, \mathbf{B}\}.$$

$$c_{t,p} \quad : \quad t \in [0, t_M(n)] \text{ y } p \in [-t_M(n), t_M(n)].$$

$$e_{t,q} \quad : \quad t \in [0, t_M(n)] \text{ y } q \in Q.$$

φ_w : es definida como $\varphi_I \wedge \varphi_C \wedge \varphi_A \wedge \varphi_\delta$.

Teorema de Cook: Demostración

φ_I : Estado inicial.

$$c_{0,0} \wedge e_{0,q_0} \wedge \left(\bigwedge_{p=-t_M(n)}^{-1} s_{0,p,B} \right) \wedge \left(\bigwedge_{p=0}^{n-1} s_{0,p,a_i} \right) \wedge \left(\bigwedge_{p=n}^{t_M(n)} s_{0,p,B} \right).$$

Teorema de Cook: Demostración

φ_C : La máquina funciona correctamente.

φ_C se define como la conjunción de cuatro fórmulas. Primero, cada celda siempre contiene un único símbolo:

$$\bigwedge_{t=0}^{t_M(n)} \bigwedge_{p=-t_M(n)}^{t_M(n)} \left((s_{t,p,0} \vee s_{t,p,1} \vee s_{t,p,B}) \wedge (s_{t,p,0} \rightarrow (\neg s_{t,p,1} \wedge \neg s_{t,p,B})) \wedge \right. \\ \left. (s_{t,p,1} \rightarrow (\neg s_{t,p,0} \wedge \neg s_{t,p,B})) \wedge (s_{t,p,B} \rightarrow (\neg s_{t,p,0} \wedge \neg s_{t,p,1})) \right).$$

Teorema de Cook: Demostración

Segundo, la máquina siempre está en un único estado:

$$\bigwedge_{t=0}^{t_M(n)} \left(\bigvee_{q \in Q} (e_{t,q} \wedge \bigwedge_{q' \in (Q \setminus \{q\})} \neg e_{t,q'}) \right).$$

Tercero, la cabeza siempre está en una única posición:

$$\bigwedge_{t=0}^{t_M(n)} \left(\bigvee_{p=-t_M(n)}^{t_M(n)} (c_{t,p} \wedge \bigwedge_{p' \in ([-t_M(n), t_M(n)] \setminus \{p\})} \neg c_{t,p'}) \right).$$

Teorema de Cook: Demostración

Cuarto, el valor de una celda no cambia si no es apuntada por la cabeza lectora:

$$\bigwedge_{t=0}^{t_M(n)-1} \bigwedge_{p=-t_M(n)}^{t_M(n)} \left((\neg C_{t,p}) \rightarrow ((s_{t,p,0} \wedge s_{t+1,p,0}) \vee (s_{t,p,1} \wedge s_{t+1,p,1}) \vee (s_{t,p,B} \wedge s_{t+1,p,B})) \right).$$

Teorema de Cook: Demostración

φ_A : La máquina acepta w .

$$\bigvee_{t=0}^{t_M(n)} e_{t,q_m}.$$

Teorema de Cook: Demostración

φ_δ : relación δ define como funciona la máquina.

$$\bigwedge_{t=0}^{t_M(n)-1} \bigwedge_{p=-(t_M(n)-1)}^{t_M(n)-1} \left(\bigwedge_{(q,a) \in Q \times \{0,1,B\}} \left((e_{t,q} \wedge c_{t,p} \wedge s_{t,p,a}) \rightarrow \right. \right. \\ \left. \left. \left(\bigvee_{(q',a',k) : (q,a,q',a',k) \in \delta} (e_{t+1,q'} \wedge c_{t+1,p+k} \wedge s_{t+1,p,a'}) \right) \right) \right).$$

Representamos I como -1 y D como 1.