Práctica 8: Circuitos

Compilado: 6 de junio de 2025

1. Un lenguaje $\mathcal{L}$ es esparso si existe un polinomio p tal que $|\mathcal{L} \cap \{0,1^n\}| \leq p(n)$ para todo $n \in \mathbb{N}$. Probar que todo lenguaje esparso está en $\mathsf{P/poly}$.

2. Probar que existen lenguajes fuera de $\mathsf{P/poly}$.

3. Definimos la clase P_{advice} como la clase de lenguajes que se pueden resolver en tiempo polinomial asumiendo que se cuenta con un consejo a para cada tamaño n de tamaño polinomial en n. Es decir, $\Pi \in \mathsf{P}_{advice}$ si y solamente si existe una función $adv : \mathbb{N} \to \{0,1\}^\star$ y una máquina polinomial M tal que

$$x \in \Pi \iff M(x, adv(|x|)) = 1$$

   donde aparte existe un polinomio p con $|adv(n)| \leq p(n)$ (es decir, el consejo es chico).

   Probar que $\mathsf{P}_{advice} = \mathsf{P/poly}$.

4. Definimos $\mathsf{P}/f(n)$ como la clase de problemas que se resuelven con un consejo de tamaño $f(n)$ (y entonces $\mathsf{P/poly} = \bigcup_{k\in\mathbb{N}} \mathsf{P}/n^k$). Probar que $\mathsf{P} \neq \mathsf{P}/1 \cap \mathsf{R}$.

5. Probar que $\mathsf{NP} = \mathsf{P}$ si y solamente si $\mathsf{NP} \subseteq \mathsf{P}/\log(n)$.

6. Probar que si $\mathsf{NP} \not\subseteq \mathsf{P/poly}$ entonces $\mathsf{NP} \neq \mathsf{P}$.

7. Probar que si $\mathsf{EXP} \subseteq \mathsf{P/poly}$ entonces $\Sigma_2^p = \mathsf{EXP}$.
   Ayuda: Probar que si $\Pi \in \mathsf{EXP}$ y M es una máquina exponencial con Q estados que lo resuelve en $c2^{n^k}$ pasos entonces el lenguaje $\Pi_M = \{\langle x, i, t, p, q\rangle : i, t, p \leq c2^{|x|^k}, q \leq Q$, y en el timestep t el i-esimo bit de la memoria de M es 1, el puntero está en la posición p y la máquina está en el estado $q\}$ está en EXP. Usar el $\exists$ para adivinar el circuito que resuelve Π_M, y luego el $\forall$ para verificar que es el correcto.

8. Probar que si $\mathsf{PSPACE} \subseteq \mathsf{P/poly}$ entonces $\mathsf{PSPACE} = \Sigma_2^p \cap \Pi_2^p$.

9. Probar que los lenguajes

   - $\text{AND} = \{x_1 \dots x_n : \forall\, 1 \leq i \leq n,\ x_i = 1\}$
   - $\text{OR} = \{x_1 \dots x_n : \exists 1 \leq i \leq n,\ x_i = 1\}$

   están en NC^1. Usar esto para probar que que $\mathsf{AC}^d \subseteq \mathsf{NC}^{d+1}$ para todo $d \geq 0$.

10. Probar que $\mathsf{NC}^1 \subseteq \mathsf{L}$.

11. Decidir si las clases AC^k y NC^k están cerradas por unión, intersección y complemento.

12. Dadas dos matrices $A, B \in \{0,1\}^{n \times n}$ definimos el producto booleano como

$$(A \cdot B)_{ij} = \bigvee_{k=1}^{n} (A_{ik} \wedge B_{kj})$$

Considerar el lenguaje

- PBM $= \{\langle A, B, n, i, j\rangle : A, B \in n \times n, 0 \leq i, j < n, (A \cdot B)_{i,j} = 1\}$

Probar que:

a) PBM $\in \mathsf{AC}^0$.
b) El lenguaje
   - EBM $= \{\langle A, n, k, i, j\rangle : A \in \{0,1\}^{n \times n}, k \leq \log n, (A^{\cdot 2^k})_{ij} = 1\}$

   está en AC^1.
c) Concluir que $\mathsf{NL} \subseteq \mathsf{AC}^1$.

13. En este ejercicio se demuestra que el lenguaje

- MAJORITY $= \{x : x$ tiene mas 1s que 0s$\}$

está en NC^1.

a) Diseñar un circuito NC^0 que haga lo siguiente: dados 3 números de n bits x, y, z devuelve dos números u, v tales que $x + y + z = u + v$. **Ayuda**: Tomar $v_{i+1}u_i = x_i + y_i + z_i$.
b) Probar que el lenguaje $\mathcal{L} = \{\langle s_1, s_2, \ldots, s_k, r\rangle : s_i, r \subseteq \{0,1\}^*, s_1 + s_2 + \ldots + s_k = r\}$ está en NC^1.
c) Probar MAJORITY $\in \mathsf{NC}^1$.

14. Considerar HORN-SAT como la versión de SAT en la que cada cláusula tiene a lo sumo una variable no negada. Probar que HORN-SAT es P-completo. **Ayuda**: Para la pertenencia, recordar el algoritmo de resolución. Para la hardness, repasar la demostración del Teorema de Cook-Levin ¿Qué forma tiene la fórmula si la máquina es determinística?

15. Probar que $\mathsf{NC} \subsetneq \mathsf{PSPACE}$. **Ayuda**: probar que $\mathsf{NC}^k \subseteq \mathsf{SPACE}(\log^k n)$.

16. Sea REG el conjunto de lenguajes regulares. Probar que:

a) $\mathsf{REG} \not\subseteq \mathsf{AC}_0$.
b) $\mathsf{AC}_0 \not\subseteq \mathsf{REG}$.
c) $\mathsf{REG} \subseteq \mathsf{NC}_1$.