MA5201 Caculabilidad y Complejidad Computacional.
Profesor: Marcos Kiwi.
Auxiliares: Benjamín Jauregui y Bernardo Subercaseaux
Fecha: 3 de junio de 2021.

Auxiliar extra C2

P1. La **jerarquía de la división $\mathbf{D}_i\mathbf{P}$** se define recursivamente como sigue

- $\mathbf{D}_1\mathbf{P} = \mathbf{NP}$
- $\mathbf{D}_i\mathbf{P} = \{B \backslash C \colon B \in \mathbf{NP} \text{ y } C \in \mathbf{D}_{i-1}\mathbf{P}\}$

Se denotará por **DP** a la clase $\mathbf{D}_2\mathbf{P}$.

a) Muestre que el lenguaje

$$Z = \{\langle G_1, k_1, G_2, k_2\rangle \colon G_1 \text{ tiene un } k_1\text{-clique y } G_2 \text{ no tiene un } k_2\text{-clique}\}$$

Es **DP**-completo.

b) Dado un grafo G, se denota por $\omega(G)$ el tamaño del clique más grande de G. Pruebe que

$$\textsc{ExactClique} = \{\langle G, k\rangle\} \colon \omega(G) = k$$

Es **DP**-completo.

P2. Se dice que un circuito es $\{\wedge, \vee\}$-monótono si sus puertas lógicas corresponden a disyunciones y conjunciones (i.e., no hay puertas lógicas de negación). Sea $\textsc{CirVal}_{\{\wedge,\vee\}}$ el lenguaje definido por

$$\textsc{CirVal}_{\{\wedge,\vee\}} = \{\langle C, a\rangle \colon C \text{ es un circuito } \{\wedge, \vee\}\text{-monótono y } C(a) = 1\}^1$$

Pruebe que $\textsc{CirVal} \leq_m^L \textsc{CirVal}_{\{\wedge,\vee\}}$ y concluya que $\textsc{CirVal}_{\{\wedge,\vee\}}$ es **P**-completo

P3.

Definición 1. Sea un lenguaje $L \subseteq \{0,1\}^*$. Se dice que $\mathcal{L} \in \mathbf{P}/\mathbf{poly}$ si existe una máquina de Turing determinista M a tiempo polinomial, un polinomio py una secuencia de *consejos* $(\alpha_n)_{n\in\mathbb{N}}$ tal que

- $\alpha_n \in \{0,1\}^*$ para todo n en $\mathbb{N}$
- $|\alpha_n| \leq p(n)$ para todo n en $\mathbb{N}$.

Y se cumple que

$$\forall \omega \in \{0,1\}^n, \omega \in L \iff M \text{ acepta } \langle \omega, \alpha_n\rangle$$

Definición 2. Decimos que un lenguaje $L \subseteq \{0,1\}^*$ es **decidido por una familia de circuitos de tamaño polinomial** si existe una familia de circuitos $(C_n)_{n\in\mathbb{N}}$ y un polinomio q tal que $|C_n| \leq q(n)$ para todo $n \in \mathbb{N}$ y

$$\forall n \in \mathbb{N}, \forall \omega \in \{0,1\}^n \colon \omega \in L \iff C_n(\omega) = 1$$

a) Pruebe que si $L \in \mathbf{P}$, entonces existe una familia de circuitos booleanos de tamaño polinomial que decide a L.

b) Pruebe quesi $L \in \mathbf{P}/\mathbf{poly}$ si y solo si existe una familia de circuitos booleanos de tamaño polinomial que decide a L. Concluya que $\mathbf{P} \subseteq \mathbf{P}/\mathbf{poly}$.

c) Lo establecido en (ii) sugiere que una estrategia para probar que $\mathbf{P} \neq \mathbf{NP}$es msotrar que existe un lenguaje en **NP** que no puede ser decidido por una familia de circuitos de tamaño polinomial. ¿Que lenguajes sería natural elegir para intentar la estrategia descrita? Argumente informalmente.

[1] Se asume que C es un circuito de n variables y $a \in \{0,1\}^n$