Práctica 8

Ej 1:

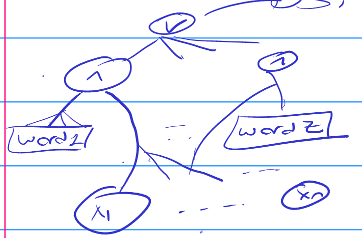
Consultar, una ayz me dijo q' era así, pero no estaba segura.

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

Idea: Para probar esto podría hacer una familia de circuitos los cuales tengan cierta estructura la cual me permita demostrar que para una entrada x con $|x| = n$, $C_n == 1$ sii $x \in \mathcal{L}$ con $\mathcal{L}$ esparso.

Voy a reescribir la def. de esparso para entenderlo mejor:
$\exists p$. p es un polinomio tq' $|\mathcal{L} \cap \{0,1\}^n| \leq p(n)$ para todo $n \in \mathbb{N}$.
↳ O sea, hay una cantidad polinomial de palabras de longitud n

Declaro entonces una flia de circuitos de la siguiente manera:



→ Si la entrada es alguna de estas da true, si no, false.
→ Veo bit a bit si es alguna de las palabras de $\mathcal{L}$ con longitud n.
→ Escribo todas las palabras (a lo sumo $p(n)$) q' pertenecen a $\mathcal{L}$ de tamaño n ↳ $a \leq p(n)$
→ Palabra con n bits

Estos circuitos tienen un tamaño polinomial, ya q' dependen de la cantidad de palabras de longitud n q' hayan en $\mathcal{L}$ (el cual ya sabemos q' es $p(n)$).
Son poly conjunciones (ver todas las palabras de longitud n de $\mathcal{L}$)
Luego poly diyunciones (veo q' la entrada coincida con alguna palabra de $\mathcal{L}$ con tamaño n)

Desp. ver el exacto poly (creo q' sería $n \cdot p(n)$).

Creería q' esto es suficiente prueba de q' existe una familia de circuitos $(C_n)_{n \in \mathbb{N}}$ donde se compute todo $\mathcal{L}$ (con $\mathcal{L}$ esparso)

★ Es más visual con advice (desp. rehacer)

Ej 2:

2. Probar que existen lenguajes fuera de P/poly.

Idea: Sale por diagonalización. La cantidad de lenguajes en P/poly es enumerable y sabemos q' la cant. de lenguajes es no numerable.

Más que nada debemos justificar q' la cant. de circuitos ó máq. poly con consejo es enumerable, esto se ve en q' se tiene una codificación para cada máq., por lo cual, cada uno es codificable finitamente y por ende enumerable

Como no se puede enumerar lo no numerable necesariamente existen lenguajes q' no estén en P/poly.