Clase Práctica 7

Ej 1:

1. Considerar el siguiente prolema:
   - LEX-SAT-BIT $= \{\langle \varphi, i \rangle : \varphi$ es una fórmula satisfacible y la menor asignación que la satisface (donde menor se define usando el orden lexicográfico) fija la variable i en $1\}$

   Probar LEX-SAT-BIT $\in \mathsf{P}^{\mathsf{NP}}$. Argumentar por qué el problema no debería estar en NP.

Idea:
Para esto voy a encontrar la menor asignación q' satisfaga φ y después ver q' el bit en i este en 1.

Creo M det. poly con acceso al oráculo SAT (q' pertenece a NP)

```
M: <φ, i>

  sol := ε
  for(k:=0; k < m; k++):        # m: Cant. de variables de φ.
    if( concat(sol,0) evaluada en φ es sat ):
      sol:= concat(sol, 0)
    else:
      sol := concat(sol, 1)
  ret (sol[i] == 1)
```

O(|φ|)

→ Preg. al oráculo, O(|φ|) para poner la query y evaluar φ con sol.

- No debería estar en NP porque debería resolver sat m veces para m fórmulas (cada asignación descubriendo la menor valuación válida en φ).

Ej 2:

2. Probar que $\mathsf{P}^{\mathsf{NP}} = \mathsf{P}^{\mathsf{coNP}} \subseteq \Sigma_2^p \cap \Pi_2^p$.

$P^{NP} = P^{coNP}$: Tienen el mismo poder, ya q' responden en O(1) la pertenencia o no en SAT (ya q' sé q' $P^{NP} = P^{SAT}$ y $P^{coNP} = P^{\overline{SAT}}$). Se ve facilmente igual.

$P^{NP} \subseteq \Sigma_2^p \cap \Pi_2^p$:

$P^{NP} \subseteq \Sigma_2^p$:

Sea $L \in P^{NP}$, por ende, hay una M máq. det. que corre en tiempo poly. y tiene acceso a un oráculo $\pi \in NP$ tal que $L(M^{\pi})$.

Luego, como $\pi \in NP$ tenga que existe una M_π máq. det. q' corre en tiempo poly. y sea p un polinomio, veo que:

$$x \in \pi \text{ sii } \exists u \in \{0,1\}^{p(|x|)} . M_\pi(x,u) = 1 .$$

Con esto, creo poder armar algo de la forma Σ_2^p.

$x \in L$ sii $\exists R, U^+, Q \forall U^-. M'(x, r_1, r_2, \dots, r_{t(|x|)}) \wedge \bigwedge^{t(|x|)} q_i$ es la query i q' hace la simulación

$M'(x, r_1, \dots, r_{t(|x|)}) \wedge \bigwedge_{i=1}^{t(|x|)} (r_i = 1 \Rightarrow M_\pi(q_i, u_i^+) = \hat{1}^{+}) \wedge (r_i = 0 \Rightarrow M_\pi(q_i, c_i^-) = 0)$

$Q_i = \{q_1, \dots, q_{t(|x|)}\}$ = Querys q' hace la simulación.
$R_i = \{r_1, \dots, r_{t(|x|)}\}$ = Respuestas a las querys
$U^-_i = \{u_1^-, \dots, u_{t(|x|)}^-\}$ = Certificados "malos" (son para decir q' para cualquier certificado no pertenece la palabra q_i a π).
$U^+_i = \{u_1^+, \dots, u_{t(|x|)}^+\}$ = Certificados para la pertenencia a π de cada query.
t : = Polinomio que acota el tiempo que tarda en correr M, no pueden haber más querys que el tiempo q' tarda en ejecutar la máquina.

M' : = Hace lo mismo que M, pero en vez de llamar al oráculo, llama a $M_\pi(q_i, c_i)$, lo cual es tiempo poly.

Se pueden dar vuelta los cuantificadores tranquilamente, por lo q' $L \in \Sigma_2^P \cap \Pi_2^P$. ✗

Ej. 3:

3. Probar que $E^E \neq E$.

Es evidente que se cumple que $E \subseteq E^E$, o sea, qvq $E^E \not\subseteq E$.

Sea $\pi \in E$-completo y $L \in E^\pi$, tengo a M máq. det. q' corre en tiempo exp. y $\Pi(M)$.

Sea Z máq. det. q' corre en tiempo exp. con el oráculo π tal q' $L(Z^\pi)$

Lo veo por el contrarrecíproco, suponiendo q' $L \in E^\pi$ y $L \in E$ para cualquier L.

Luego, M' máq. det. que corre en E de manera q' por cada llamado al oráculo q' hacía la máq. det. que decidía L con el oráculo π, M' llama a M con la query correspondiente.

Como π es E-completo, se necesita sí o sí una máq. det. q' corra en tiempo E para decidir si $x \in \pi$ (mínimamente una máq. así).

El tema es que Z^π podría tener una query de tamaño exp. respecto a la entrada, por lo cual, esto llevaría a q' M(query) corre en tiempo exponencial respecto a |query|, o sea, $2^{2^{|x|}}$ x es la entrada original de Z^π.

Como sé que $Z^\pi = o(4^n)$, obtengo q' $L \notin E$. Contradicción! (La máq. corre en 2E, no en E)

Otra forma: (más formal) (y q' sé q' está bien)

Veo que por jerarquía temporal no son iguales, ya que $E^E = 2E$ (que es lo q' voy a tener q' probar)

$\subseteq$) Trivial

$\supseteq$) Sea $\pi \in 2E$-completo, qvq $\pi \in E^E$.

$x \in \pi$ sii $M(x) = 1$ (Corre en $2^{2^{|x|^K}}$ para un K ctte)

Defino $\Pi_{pad} = \{x 0 1^{2^{|x|^K}} : x \in \pi\}$

Lema: $\Pi_{pad} \in E$

$\pi_{pad}: \langle y \rangle$

Parseo $y = x01^{2^{|x|^k}}$

return $M(x)$

Defino $A^{\pi_{pad}}(x)$:

$y = x01^{2^{|x|^k}}$

return $\pi_{pad}(y)$

$A^{\pi_{pad}}$ va a resolver π, probando q' $\pi \in E^E$

Tarda exponencial

$A^{\pi_{pad}}$ corre en exp. con el oráculo π_{pad}.

γ

Ej 4:

4. Probar que $\mathsf{NP}^{\mathsf{NP} \cap \mathsf{coNP}} = \mathsf{NP}$.

$\supseteq$) Trivial.

$\subseteq$)

Sea $L \in NP^{NP \cap coNP}$, N máq. no-det. con acceso a un oráculo $\pi \in NP \cap coNP$.

Si: $\pi \in NP \cap coNP$, significa q' tengo una M máq. det. poly. q' con un certificado puede decidir si pertenece ~~a no~~ una palabra x a π.

Lo ya q' el complemento de π está en $NP \cap coNP$ también.

Luego, cada llamado al oráculo podría ser reemplazado por una verificación no-det. de la query con un certificado inventado y esta corre poly. ya q' si $q \in \pi$ ó si $q \notin \pi$ es verificable en tiempo poly.

Por último, es posible computar L con una máq. no-det. q' corre en tiempo poly, o sea $L \in NP$

Ej 5:

5. Dada una clase $\mathcal{C}$, se define $\mathtt{low}(\mathcal{C}) = \{\Pi \subseteq \Sigma^\star : \mathcal{C}^\Pi = \mathcal{C}\}$. Probar que $\mathtt{low}(\mathsf{NP}) = \mathsf{NP} \cap \mathsf{coNP}$.

Por el ej 4 sé q' $NP \cap coNP \subseteq low(NP)$.

QvQ: $low(NP) \subseteq NP \cap coNP$

O sea, $\{\pi \subseteq \Sigma^* : NP^\pi = NP\} \subseteq NP \cap coNP$

A ver, si: $\pi \notin NP \subseteq coNP$ veo qué sucede:

Si $\pi \notin NP$, entonces ahora por ejemplo el mismo π es decidible pero $\pi \notin NP$ y $\pi \in NP^\pi$, o sea que gano poder con el oráculo π, parece, $NP^\pi \neq NP \cap coNP$.

Por último, $low(NP) \subseteq NP \cap coNP$, o sea:

$$low(NP) = NP \cap coNP.$$

γ