Auxiliar 11

Jerarquía polinomial, $\mathbf{P}_{/\mathbf{poly}}$ y clases probabilistas

Auxiliar: Sebastián Pérez S.

P1) Se define la clase $\mathbf{P}_{/\mathbf{poly}}$ como la clase de los lenguajes $L \subseteq \{0,1\}^*$ tales que existe un verificador polinomial V, un polinomio $p(\cdot)$ y una función $c : \mathbf{N} \to \{0,1\}^*$ con $|c(n)| \leq p(n)$ que cumplan

$$\omega \in L \iff V(\omega, c(|\omega|)) = 1.$$

A $\mathbf{P}_{/\mathbf{poly}}$ se le suele llamar la clase de los consejos polinomiales pues la máquina V decide la pertenencia de ω con la ayuda de la palabra $c(|\omega|)$ que solo depende del tamaño de ω. Se puede observar que $\mathbf{P} \subseteq \mathbf{P}_{/\mathbf{poly}}$.

a) Muestre que si $L \subseteq 1^*$, entonces $L \in \mathbf{P}_{/\mathbf{poly}}$.
b) Sea UHALT_{mT} el conjunto de palabras 1^n donde la expansión binaria de n es $\langle M, w\rangle_2$ tal que M es una mT que para en la entrada w. Pruebe que UHALT es indecidible.
c) Pruebe que $\mathbf{NP} \neq \mathbf{P}_{/\mathbf{poly}}$.
d) Pruebe que $\mathbf{P}_{/\mathbf{poly}} = \bigcup_{i \geq 0} \mathbf{SIZE}(n^i)$ donde $\mathbf{SIZE}(t(n))$ es la clase de los lenguajes en $\{0,1\}^*$ que son decididos por familias de circuitos de tamaño $\mathcal{O}(t(n))$.

P2) El objetivo de este problema es probar el Teorema de Karl-Lipton-Sipser (1980):

Teorema 1 (Karl-Lipton-Sipser) *Si* $\mathbf{NP} \subseteq \mathbf{P}_{/\mathbf{poly}}$, *entonces* $\mathbf{PH} = \Sigma_2$.

Para ello seguiremos el siguiente esquema:

a) Muestre que basta probar que $\Pi_2 \subseteq \Sigma_2$.
b) Suponiendo la hipótesis del teorema, muestre que para toda fórmula booleana de la forma $\Phi = \forall x \exists y \phi(x, y)$ con ϕ FNC, existe una fórmula booleana equivalente de la forma $\Phi' = \exists x' \forall y' \phi'(x', y')$ con ϕ' FNC y que dicho cálculo toma tiempo polinomial.
c) Concluya.

P3) Sea Σ un alfabeto no vacío y \$ un símbolo no perteneciente a Σ. Considere la función $\text{pad} : \Sigma^* \times \mathbf{N} \to \Sigma^*\$^*$ definida como $\text{pad}(w, \ell) = w\$^j$ donde $j = \text{máx}\{0, \ell - |w|\}$. Así $\text{pad}(s, \ell)$ es la función que agrega suficientes símbolos «\$» al final de la palabra w de manera que tenga largo al menos ℓ. Sea A un lenguaje sobre Σ y $f : \mathbf{N} \to \mathbf{N}$, definimos el lenguaje $\text{pad}(A, f)$ como

$$\text{pad}(A, f) \doteq \{\text{pad}(w, f(|w|)) : w \in A\}.$$

Pruebe que:

a) Si $A \in \mathbf{TIME}(n^6)$ entonces $\text{pad}(A, m^2) \in \mathbf{TIME}(n^3)$.
b) Pruebe que para todo lenguaje A y para todo natural $k \geq 1$, $A \in \mathbf{P}$ si y solo si $\text{pad}(A, m^k) \in \mathbf{P}$.
c) Pruebe que $\mathbf{P} \neq \mathbf{SPACE}(n)$.

P4) Sea $\mathbf{PP} = \mathbf{CCP}(\frac{1}{2}^+, \frac{1}{2})$, es decir, $L \in \mathbf{PP}$ si existe M verificador polinomial a tiempo $p(n)$ y un polinomio $q(n)$ tal que

$$x \in L \implies \mathbb{P}_{\rho \in \{0,1\}^{q(|x|)}}(M(x, \rho) = 1) > \frac{1}{2}$$
$$x \notin L \implies \mathbb{P}_{\rho \in \{0,1\}^{q(|x|)}}(M(x, \rho) = 1) \leq \frac{1}{2}.$$

a) Muestre que $\mathbf{BPP} \subseteq \mathbf{PP}$.
b) Muestre que $\mathbf{NP} \subseteq \mathbf{PP}$.
c) Pruebe que $\mathbf{PP} = \mathbf{coPP}$.