Ma5201 Complejidad Computacional	**18 de Agosto de 2016**

Control 3

Prof. Cátedra: M. Kiwi — *Prof. Auxiliar: S. Pérez*

TIEMPO: 4.5 HRS

PROBLEMA 1:

(i).- (3.0 pts) En muchas circunstancias es de interés que un circuito Booleano siga operando de la manera adecuada aún si algunas de sus sub-componentes (puertas lógicas) fallan. Llamamos *corrupción* de una puerta lógica al intercambio de un AND por un OR, o de un NOT por una identidad (i.e., por 0 o 1). Se dice que un circuito es (k, j)-*reparable* si el efecto de hasta k corrupciones puede ser reparado reemplazando a lo más j puertas lógicas ($j \leq k$). Sea RepCirc el conjunto de instancias $\langle C, k, j\rangle$ donde C es un circuito Booleano (k, j)-reparable. Pruebe que RepCirc $\in \Sigma_3^{\mathrm{P}} \cup \Pi_3^{\mathrm{P}}$.

(ii).- (3.0 pts) Pruebe que si HamCycle $\in$ RP, entonces existe un algoritmo $\mathcal{A}$ a tiempo esperado polinomial que en la entrada $\langle G\rangle \in$ HamCycle retorna un cíclo Hamiltoniano de G.

PROBLEMA 2:

(i).- (3.0 pts) Sea φ una k-CNF con m claúsulas (sin variables repetidas en una misma claúsula). Pruebe que si $k > \lceil \log_2 m \rceil$, entonces φ se puede satisfacer.

(ii).- (3.0 pts) Sea $0 < \varepsilon < 1$. Se define PP_ε como la colección de lenguajes L para los que existe una máquina de Turing probabilista a tiempo polinomial $p(\cdot)$ tal que

$$\omega \in L \implies \mathbb{P}_{\rho \in \{0,1\}^{p(|\omega|)}}\big(M(\omega, \rho) = \text{acep}\big) > \varepsilon,$$
$$\omega \notin L \implies \mathbb{P}_{\rho \in \{0,1\}^{p(|\omega|)}}\big(M(\omega, \rho) = \text{acep}\big) < \varepsilon.$$

Pruebe que $\mathrm{PP}_\varepsilon = \mathrm{PP}$.

PROBLEMA 3: Implícito en la demostración vista de BPP $\subseteq \Sigma_2^{\mathrm{P}}$ esta que: Si $L \in$ BPP, $L \subseteq \{0,1\}^*$, es decidido por la máquina de Turing probabilista M en tiempo polinomial $p(\cdot)$ con error $1/2^m$, $m = p(n) + 1$, entonces

$$\omega \in L \cap \{0,1\}^n \implies \mathbb{P}_{\rho_1,\ldots,\rho_m}\big(\forall r, \exists i \in [m], M(\omega, r \oplus \rho_i) = \text{acep}\big) \geq \tfrac{1}{2},$$
$$\omega \notin L \cap \{0,1\}^n \implies \forall \rho_1, \ldots, \rho_m, \exists r, \forall i \in [m], M(\omega, r \oplus \rho_i) = \text{rech},$$

donde $\rho_1, \ldots, \rho_m$ y r están en $\{0,1\}^{p(n)}$.

(i).- (2.0 pts) Con la misma notación y utilizando el resultado anterior, verifique que

$$\begin{aligned}
\omega \in L \cap \{0,1\}^n &\implies \forall \rho_1, \ldots, \rho_m, \exists r, \forall i \in [m], M(\omega, r \oplus \rho_i) = \text{acep}, \\
\omega \notin L \cap \{0,1\}^n &\implies \mathbb{P}_{\rho_1, \ldots, \rho_m}\big(\forall r, \exists i \in [m], M(\omega, r \oplus \rho_i) = \text{rech}\big) \geq \tfrac{1}{2}.
\end{aligned}$$

(ii).- (4.0 pts) Use lo anterior para probar que BPP $\subseteq \mathcal{ZPP}^{\text{NP}}$.

Indicación: Defina un oráculo O cuyas instancias tienen la forma $(\omega, \sigma, \rho_1, \ldots, \rho_m)$, $\sigma \in \{\text{acep}, \text{rech}\}$, de forma que realizando 2 consultas a O con probabilidad al menos $1/2$ se pueda decidir si ω pertenece o no a L.