Ma50b Complejidad Computacional **09 de Julio de 2008**

Examen

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: P. Camacho*

TIEMPO: 3.5 HRS.

PROBLEMA 1: (40 %)

(i).- (3.0 pts) Se define MaxCut como el lenguaje formado por las secuencias $\langle G,k\rangle$ donde $G=(V,E)$ es grafo, $k\in\mathbb{N}$, y existe $S\subseteq V$ tal que

$$\rho(S)=|\{uv\in E\,:\,|\{u,v\}\cap S|=1\}|\geq k\,.$$

Sea BISECCION el lenguaje formado por las secuencias $\langle G,k\rangle$ donde $G=(V,E)$ es grafo, $k\in\mathbb{N}$, y existe $S\subseteq V$, $|S|=|V\setminus S|$ tal que $\rho(S)\geq k$. Asuma que MaxCut es NP-completoy y pruebe que BISECCION es NP-completo.

(ii).- (3.0 pts) Se dice que un circuito es $\{\vee,\wedge\}$-monótono si sus puertas lógicas corresponden a disyunciones y conjunciones (en particular, no tiene puertas lógicas de negación). Sea $\text{CircVal}_{\{\vee,\wedge\}}$ el lenguaje conformado por palabras de la forma $\langle C,a\rangle$ donde C es un circuito $\{\vee,\wedge\}$-monótono en n-variables, $a\in\{0,1\}^n$ es una asignación de valores de verdad, y $C(a)=1$. Pruebe que $\text{CircVal}\leq_m^L \text{CircVal}_{\{\vee,\wedge\}}$ y concluya que $\text{CircVal}_{\{\vee,\wedge\}}$ es P-completo.

Indicación: Duplique puertas lógicas, elimine las negaciones y re-cablee.

PROBLEMA 2: (60 %)

(i).- (2.0 pts) Dado M máquina de Turing probabilista, sea $T_M(\omega)\in\mathbb{N}\cup\{+\infty\}$ el número esperado de transiciones que realiza M en la entrada ω (donde la esperanza esta tomada sobre los lanzamientos de monedas que realiza M en la entrada ω). Decimos que M es a tiempo esperado polinomial si existe $c>0$ tal que $\max\limits_{\omega:|\omega|=n} T_M(\omega)=O(n^c)$.

Se define la clase ZPP como el conjunto de lenguajes L para los cuales existe M máquina de Turing probabilista a tiempo esperado polinomial que decide L. Pruebe que $\text{ZPP}=\text{RP}\cap\text{coRP}$.

Indicación: Para probar una de las inclusiones use la desigualdad de Markov, y para la otra recuerde que el número esperado de lanzamientos necesarios para observar cara al lanzar repetidamente una moneda con probabilidad p de caer cara es $1/p$.

(ii).- (2.0 pts) Decimos que $b \in \mathbb{Z}_m^*$ es residuo cuadrático módulo $m \in \mathbb{N} \setminus \{0\}$ si existe un entero a tal que $b \equiv_m a^2$. Se define QNR como el conjunto de los $\langle b, m \rangle$ tales que b no es un residuo cuadrático módulo m. Sea el sistema de demostración interactivo que en la entrada $\langle b, m \rangle$, $b \in \mathbb{Z}_m^*$, $m \in \mathbb{N} \setminus \{0\}$ procede de la siguiente forma:

$$
\begin{aligned}
V: &\quad r \xleftarrow{Unif} \mathbb{Z}_m^*,\ c \xleftarrow{Unif} \{0,1\} \\
V: &\quad b' = r^2 \text{ mód } m \text{ si } c = 0, \text{ y } b' = br^2 \text{ mód } m \text{ si } c = 1 \\
V \rightarrow P: &\quad b' \\
P: &\quad c' = 0 \text{ si } b' \text{ es residuo cuadrático, y } c' = 1 \text{ en caso contrario} \\
V \leftarrow P: &\quad c' \in \{0,1\} \\
V: &\quad \text{acepta si y solo si } c = c'
\end{aligned}
$$

Para $b \in \mathbb{Z}_m^*$ y $m \in \mathbb{N} \setminus \{0\}$, determine las probabilidades de aceptación de $\langle b, m \rangle \in$ QNR y de $\langle b, m \rangle \notin$ QNR. Concluya que QNR $\in$ IP.

(iii).- (2.0 pts) Pruebe que MIP $\subseteq$ NEXP