Ma5201 Complejidad Computacional **09 de Agosto de 2013**

Examen

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: P. Muñoz, D. Salas*

TIEMPO: 4.5 HRS

PROBLEMA 1:

(i).- (2.0 pts) Sea Dense el conjunto de instancias $\langle G,m,n\rangle$ donde $m,n \in \mathbb{N}$ y G es un grafo que posee algún subgrafo H tal que $|E(H)| \geq m$ y $n \geq |V(H)|$. Pruebe que Dense es NP-completo.

(ii).- (2.0 pts) Sea Bombas el conjunto de instancias $\langle G,K,\ell,L\rangle$ donde G es un grafo, $\ell : E(G) \to \mathbb{N}$ es una función que indica el largo de cada arco de G, y $K,L \in \mathbb{N}$ son tales que existe un subconjunto S de nodos de G, $|S| \leq K$, representando lugares donde instalar estaciones de bomberos, tal que para todo nodo v de G, representando lugares, exista un camino de largo a lo más L en G entre v y algún nodo perteneciente a S. Pruebe que Bombas es NP-completo.

Indicación: Bombas sigue siendo NP-completo, inclusive si se fija $L = 1$.

(iii).- Se dice que una claúsula C es de Horn si tiene a lo más un literal positivo, i.e. para algún $k \in \mathbb{N}$

$$C = \overline{x_1} \vee \overline{x_2} \vee \ldots \vee \overline{x_k} \vee y, \quad \text{o} \quad C = \overline{x_1} \vee \overline{x_2} \vee \ldots \vee \overline{x_k}.$$

Sea HornSAT la familia de instancias $\langle\varphi\rangle$ de SAT en que φ es una conjunción de claúsulas de Horn.

(iii.1).- (1.0 pts) Pruebe que HornSAT $\in$ P.

Indicación: Observe primero que si todos las claúsuals de una instancia $\langle\varphi\rangle$ de HornSAT tienen al menos dos literales, entonces φ se puede satisfacer.

(iii.2).- (1.0 pts) Pruebe que CircEval $\leq_L$ HornSAT.

PROBLEMA 2:

(i).- (1.5 pts) Pruebe que si NP $=$ coNP, entonces $\mathrm{P}^{\mathrm{NP}} = \mathrm{NP}$.

(ii).- (1.5 pts) Sea D^{P} la clase de lenguajes L tales que existe $X \in \mathrm{NP}$ e $Y \in \mathrm{coNP}$ para los cuales $L = X \cap Y$. Pruebe que si $\mathrm{P}^{\mathrm{NP}} = \mathrm{NP} \cup \mathrm{coNP}$, entonces $D^{\mathrm{P}} = \mathrm{NP} \cup \mathrm{coNP}$.

(iii).- Sea Iso el conjunto de instancias $\langle G_0, G_1 \rangle$ tales que G_0 y G_1 son grafos isomorfos. Considere el siguiente protocolo interactivo por medio del cual, en la entrada $\langle G_0, G_1 \rangle$, $V(G_0) = V(G_1) = [n]$, un probador P desea convencer a un verificador V que conoce una biyección $\pi \in S_n$ tal que $G_1 = \pi(G_0)$.

$$
\begin{array}{rl}
P: & \text{Elige } \sigma \in_R S_n \text{ y } b \in_R \{0,1\}. \text{ Calcula } H = \sigma(G_b). \\
P \to V: & H. \\
V: & b' \in_R \{0,1\}. \\
V \to P: & b'. \\
P: & \text{Calcula } \tau \text{ tal que } \tau = \sigma \text{ si } b = b',\ \tau = \sigma \circ \pi^{-1} \text{ si } b = 0 \text{ y } b' = 1, \text{ y } \tau = \sigma \circ \pi \text{ si } b = 1 \text{ y } b' = 0. \\
P \to V: & \tau. \\
V: & \textsc{Acepta} \text{ si y sólo si } H = \tau(G_{b'}).
\end{array}
$$

(iii.1).- (1.2 pts) Pruebe que

$$
\begin{aligned}
\langle G_0, G_1 \rangle \in \text{Iso} &\implies \mathbb{P}_{\sigma,b,b'}\left(\langle V \leftrightarrow P \rangle(\langle G_0, G_1 \rangle) = \textsc{Acepta}\right) = 1, \\
\langle G_0, G_1 \rangle \notin \text{Iso} &\implies \mathbb{P}_{\sigma,b,b'}\left(\langle V \leftrightarrow P \rangle(\langle G_0, G_1 \rangle) = \textsc{Acepta}\right) \leq \frac{1}{2}, \text{ para toda estrategia de } P,
\end{aligned}
$$

donde las probabilidades son sobre $b \in_R \{0,1\}$, $\sigma \in_R S_n$, y $b' \in_R \{0,1\}$.

(iii.2).- (1.8 pts) Sea (la variable aleatoria) $\textsc{Vista}_V[(V \leftrightarrow P)(\langle G_0, G_1 \rangle)] = (H, b', \tau)$ donde la aleatoriedad esta dada por las opciones probabilistas de V y P. Sea un verificador "deshonesto" V^* que no necesariamente realiza la elección de b' como el protocolo establece. Sea $B(G_0, G_1, H)$ la elección de b' que hace V^* después de recibir H. Considere el siguiente algoritmo Sim:

input: G_0 y G_1 tales que $V(G_0) = V(G_1) = [n]$.
1 Elegir $\sigma \in_R S_n$ y $b \in_R \{0,1\}$;
2 $H \leftarrow \sigma(G_b)$;
3 $b' \leftarrow B(G_0, G_1, H)$;
4 **if** $b' = b$ **then** return$((b', H, \sigma))$ **else** Volver al Paso 1;

Probar que si $\langle G_0, G_1 \rangle \in$ Iso, entonces en tiempo esperado polinomial Sim, en la entrada $\langle G_0, G_1 \rangle$, genera una salida (H, b', σ) distribuida exactamente igual que $\textsc{Vista}_{V^*}[(V^* \leftrightarrow P)(\langle G_0, G_1 \rangle)]$.[1]

[1]En palabras, se pide probar que si el verificador V^* se desvía del protocolo salvo por respetar el formato de los mensajes intercambiados, igual no obtiene información acerca de un isomorfismo entre G_0 y G_1, pues un intercambio distribuido de la misma forma que el que obtiene V^* puede ser generado sin conocer tal isomorfismo.