Ma50b Complejidad Computacional **11 de Julio de 2005**

Pauta Examen

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: J. Soto*

PROBLEMA 1:

(i).- Primero veamos que $\frac{1}{2}CLIQUE$ está en NP. Para ello basta tomar como testigo de $\langle G\rangle \in \frac{1}{2}CLIQUE$ un conjunto $S \subseteq V(G)$ y verificar que $|S| \geq |V(G)|/2$ y que $uv \in E(G)$ para todo $u,v \in S$.

Para establecer que $\frac{1}{2}CLIQUE$ es NP–duro veremos que $CLIQUE \leq_P \frac{1}{2}CLIQUE$. En efecto, sea G grafo, $n = |V(G)|$ y $k \in \mathbb{N}$. Si $k \leq n/2$, le agregamos a $V(G)$ un conjunto V' de $n-2k$ nodos y a $E(G)$ el conjunto de todos los arcos entre nodos en V' (i.e., $V' \times V'$) y todos los arcos entre nodos en $V(G)$ y V' (i.e., $V(G) \times V'$). Si $k > n/2$, le agregamos a $V(G)$ un conjunto V' de $2k-n$ nodos y ningún arco a $E(G)$. Cualquiera sea el caso, se obtiene un grafo no dirigido G' con $2|n-k|$ nodos que posee un clique de tamaño $|n-k|$ si y sólo si G tiene un clique de tamaño k, i.e.,

$$\langle G,k\rangle \in CLIQUE \Longleftrightarrow \langle G'\rangle \in \frac{1}{2}CLIQUE\,.$$

Es fácil ver $\langle G'\rangle$ se puede obtener en tiempo polinomial a partir de $\langle G\rangle$. Luego, hemos demostrado que $CLIQUE$ reduce en tiempo polinomial a $\frac{1}{2}CLIQUE$.

(ii).- Primero veamos que *SECUENCIAR* está en NP. Para ello basta tomar como testigo de $\langle T,D,P,k\rangle \in$ *SECUENCIAR* (con T, D, P y k como en el enunciado) una permutación π de $\{1,\ldots,r\}$, calcular $J = \left\{ j : \sum_{i=1}^{j} t_{\pi(i)} > d_{\pi(j)} \right\}$, y verificar que

$$\sum_{j\in J} p_{\pi(j)} \leq k\,.$$

Veamos ahora que $SUBSET\!-\!SUM \leq_P SECUENCIAR$. En efecto, sea $S = \{s_1,\ldots,s_m\} \subseteq \mathbb{N}$ un conjunto de sumandos y t un valor objetivo, definimos

- $k = \sum_{i=1}^{m} s_i - t$
- $d_i = t$ para todo $i \in \{1,\ldots,m\}$
- $t_i = p_i = s_i$ para todo $i \in \{1,\ldots,m\}$

Notar que si $\langle S,t\rangle \in SUBSET\!-\!SUM$, entonces existe $I \subseteq \{1,\ldots,m\}$ tal que $\sum_{i\in I} s_i = t$. Luego, si π es una permutación de $\{1,\ldots,m\}$ para la cual $\pi(\{1,\ldots,|I|\}) = I$, se tendrá que

$$J = \left\{ j : \sum_{i=1}^{j} t_{\pi(i)} > d_{\pi(j)} \right\} = \left\{ j : \sum_{i=1}^{j} s_{\pi(i)} > t \right\} = \{1,\ldots,m\} \setminus I\,.$$

Luego,

$$\sum_{j\in J} p_{\pi(j)} = \sum_{j\notin I} s_j = k\,.$$

En resumen, se tendrá que $\langle T, D, P, k\rangle \in SECUENCIAR$.

Por otro lado, si $\langle T, D, P, k\rangle \in SECUENCIAR$, entonces existe una permutación π de $\{1,\ldots,m\}$ tal que si $J = \left\{ j : \sum_{i=1}^{j} t_{\pi(i)} > d_{\pi(j)} \right\}$ se tiene que

$$\sum_{j\in J} s_{\pi(j)} = \sum_{j\in J} p_{\pi(j)} \leq k\,.$$

Luego,

$$\sum_{j\notin J} s_{\pi(j)} = \sum_{i=1}^{m} s_i - \sum_{j\in J} s_{\pi(j)} \geq \sum_{i=1}^{m} s_i - k = t.$$

Observar que $J = \{l,\ldots,m\}$ para algún l. Luego, como $l-1 \notin J$,

$$\sum_{j\notin J} s_{\pi(j)} = \sum_{i=1}^{l-1} s_{\pi(j)} \leq d_{\pi(l-1)} = t\,.$$

Sigue que $\sum_{i\in\pi(J)} s_i = \sum_{j\notin J} s_{\pi(j)} = t$, i.e., $\langle S, t\rangle \in SUBSET{-}SUM$. Hemos demostrado entonces que $SUBSET{-}SUM$ reduce en tiempo polinomial a $SECUENCIAR$.

PROBLEMA 2:

Supongamos que $L \in$ MIP. Se tiene entonces, por definición, que existe un verificador V a tiempo polinomial $p(\cdot)$ y un par de probadores honestos P_1 y P_2 tales que

- Si $\omega \in L$, entonces $\mathbb{P}_\rho\left((V \leftrightarrow P_1, P_2)(\omega) = acep\right) = 1$,
- Si $\omega \notin L$, entonces $\mathbb{P}_\rho\left((V \leftrightarrow \widetilde{P}_1, \widetilde{P}_2)(\omega) = acep\right) < 1/3$, para todo $\widetilde{P}_1, \widetilde{P}_2$,

donde las probabilidades están tomadas sobre los $\rho \in \{0,1\}^{p(|\omega|)}$.

Observar en particular que cada P_i, $i \in \{1,2\}$, le asocia a toda secuencia de la forma

$$h = \#q_1\#a_1\#q_2\#a_2\#\ldots\#q_i\#$$

una secuencia $P_i(h) \in \{0,1\}^*$.

Como V es a tiempo polinomial, las secuencias h factibles en la estrada ω están en $\{0,1,\#\}^{p(|\omega|)}$. Luego, hay una cantidad exponencial de ellas. Además, nuevamente por la polinomialidad del tiempo de ejecución de V, se tiene que $|P_i(h)| \leq p(|\omega|)$ cuando la entrada es ω.

Sea entonces la máquina de Turing M que en la entrada ω adivina para todo $h \in \{0,1,\#\}^{p(|\omega|)}$ e $i \in \{1,2\}$ el valor de $P_i(h) \in \{0,1\}^{p(|\omega|)}$. Como hay una cantidad exponencial en $|\omega|$ de tales h, y para un h fijo la adivinanza puede hacerse en tiempo polinomial, sigue que el paso descrito puede ser completado en tiempo exponencial por una máquina de Turing no determinista. A continuación la máquina M cicla sobre todas las secuencias $\rho \in \{0,1\}^{p(|\omega|)}$ y para cada una de ellas simula V (en la entrada ω y lanzamiento de monedas ρ), como si V estuviese interactuando con los probadores cuyas estrategias están dadas por P_1 y P_2. Esta simulación se puede hacer en tiempo polinomial para cada ρ fijo. La máquina M determina la fracción p de ρ's que hacen que la simulación anterior termine en aceptación. Esta fracción se puede calcular en tiempo

exponencial en $|\omega|$ (tiempo polinomial para cada una de los exponencialmente muchos valores posibles de ρ). Si $p > 1/3$ la máquina M acepta y en caso contrario rechaza.

Se tiene que M es una máquina determinista a tiempo exponencial que acepta si y sólo si $\omega \in L$, i.e., $L \in$ NEXP.

PROBLEMA 3:

(i).- Por simetría de la definición de nodos consistentes se concluye que G_ω es no dirigido.

Una máquina M puede construir G_ω a partir de ω ciclando sobre todos los pares de nodos $u = (\rho, \vec{a}) \in \Omega$ y $v = (\rho', \vec{a'}) \in \Omega$ y agregando uv como arco de G_ω en caso de cumplirse que:

1. $\rho \neq \rho'$,
2. Si para todo i y j tal que $q_i(\rho) = q_j(\rho')$, se tiene que $a_i = a_j$.

Notar en particular que la segunda propiedad puede verificarse simulando V en la entrada ω y secuencia de lanzamientos ρ (respectivamente ρ') y determinando $q_i(\rho)$ (respectivamente $q_i(\rho')$) para $i = 1, \ldots, q$, donde se asume en la determinación de $q_j(\rho)$ (respectivamente $q_j(\rho')$) que las respuestas obtenidas a consultas al oráculo previamente realizadas son $a_1, \ldots, a_{j-1}$ (respectivamente $a'_1, \ldots, a'_{j-1}$). Como V toma tiempo polinomial, esto último toma también tiempo polinomial en V. Como $|\Omega| = 2^{r(|\omega|)+q} = 2^{c'+q} n^c$, sigue fácilmente que el doble ciclo sobre Ω requerido para construir G_ω le toma a M un tiempo total polinomial en M.

(ii).- Como G_ω tiene como conjunto de nodos a $\{0,1\}^{r(|\omega|)} \times \{0,1\}^q$ y no puede existir un arco entre dos nodos $(\rho, \vec{a})$ y $(\rho', \vec{a'})$ tales que $\rho = \rho'$ sigue necesariamente que un clique puede tener como tamaño máximo el número máximo de ρ's posibles, i.e., $2^{r(|\omega|)}$.

(iii).- Si $\omega \in L$, entonces existe Π tal que $V^\Pi(\omega, \rho) = acep$ cualquiera sea ρ. Sea entonces el conjunto de nodos de la forma $(\rho, \vec{a})$ tal que a_i es el bit que V hubiese leído del oráculo Π en su i–ésima consulta en la entrada ω y lanzamiento de monedas ρ. Es fácil ver que el conjunto de dichos nodos esta unívocamente determinado por el conjunto de ρ's, que todos son nodos de aceptación, y que cada par de ellos es consistente. En resumen, dichos nodos constituyen un clique en G_ω de tamaño $2^{r(|\omega|)}$.

(iv).- Sean $(\rho_1, \vec{a}_1), \ldots, (\rho_m, \vec{a}_m)$ los nodos de un clique en G_ω. En particular por definición de G_ω se tiene $\rho_i \neq \rho_j$ si $i \neq j$ y que cada par de estos nodos es consistente. Sea Π un oráculo cuyo l–ésimo bit es $(\vec{a}_i)_j$ si para algún ρ_i se tiene que el verificador V en la entrada ω y secuencia de lanzamientos de moneda ρ_i hubiese, en su j–ésimo acceso al oráculo, consultado el l–ésimo bit del mismo. Una observación crucial es que la consistencia entre cualquier par de nodos $(\rho_1, \vec{a}_1), \ldots, (\rho_m, \vec{a}_m)$ garantiza que si el l–ésimo bit de Π queda fijado por el anterior proceso, entonces este queda bien definido. Las posiciones del oráculo que no queden determinadas por el proceso antes descrito se fijan arbitrariamente (por ejemplo, se escogen todas iguales a 0). Sigue que $V^\Pi(\omega, \rho_i) = acep$ para $i = 1, \ldots, m$. Luego, si G_ω tiene un clique de tamaño m, entonces existe Π oráculo tal que

$$\mathbb{P}_\rho \left(V^\Pi(\omega, \rho) = acep \right) \geq \frac{m}{2^{r(|\omega|)}}.$$

La afirmación del enunciado se deduce inmediatamente.

(v).- Si $\omega \in L$, de (ii) y (iii) y la definición de PCP, se tiene que G_ω tiene un clique de tamaño $2^{r(|\omega|)}$. Si $\omega \notin L$, de (iv) y la definición de PCP, se tiene que G_ω no tiene cliques de tamaño $2^{r(|\omega|)}/3$.

Sea ahora una algoritmo $\mathcal{A}$ a tiempo polinomial que en la entrada $\langle G \rangle$, G grafo no dirigido, calcula una 3–aproximación $\mathcal{A}(\langle G \rangle) \in \mathbb{N}$ del tamaño del clique máximo de G, denotado $\mathrm{OPT}(\langle G \rangle)$. Formalmente, para todo grafo no dirigido G,

$$\mathrm{OPT}(\langle G \rangle) \leq 3\mathcal{A}(\langle G \rangle).$$

Sea entonces una máquina de Turing que en la entrada ω construye el grafo G_ω y simula $\mathcal{A}$ en $\langle G_\omega \rangle$. Si $\mathcal{A}(\langle G \rangle) < 2^{r(|\omega|)}/3$, entonces M rechaza y en caso contrario acepta.

Observar que si $\omega \in L$, entonces $\mathrm{OPT}(\langle G \rangle) = 2^{r(|\omega|)}$. Luego, $\mathcal{A}(\langle G \rangle) \geq 2^{r(|\omega|)}/3$, por lo que M acepta. En el caso que $\omega \notin L$, entonces $\mathcal{A}(\langle G \rangle) \leq \mathrm{OPT}(\langle G \rangle) < 2^{r(|\omega|)}/3$. Luego, M rechaza. En resumen, M decide L. Además, es fácil ver que M es a tiempo polinomial. Sigue que $\mathrm{NP} = \mathrm{P}$.