MA50B Complejidad Computacional **3 de Julio, 2002**

Pauta Examen

Profesor: M. Kiwi **Auxiliar: E. Moreno**

Problema 1:

(i).- Sea $L \in \text{NDTIEMPO}(T(n))$ y M la máquina de Turing no–determinista que decide L en tiempo $T(n)$. Sean además $c, C \in \mathbb{N}$ constantes tales que $T(n)$ puede calcularse a partir de 1^n en tiempo $cT(n) + C$.

Consideremos la máquina de Turing M' que en la entrada $\omega' = \omega \overbrace{\#\ldots\#}^{k}$ realiza los siguientes pasos

(1) Determina $m = |\omega|$.

(2) Simula durante $c|\omega'| + C$ pasos la máquina que calcula T en la entrada 1^m. Si en la mencionada cantidad de pasos no se obtiene $T(m)$, rechaza. Si se obtiene $T(m)$, entonces calcula y almacena $N = T(m) - m$ en una cinta auxiliar (lo que puede hacer en tiempo $O(T(m))$ pues T es tiempo constructible).

(3) Verifica que $k = N$ y rechaza en caso que la igualdad no se cumpla.

(4) Simula M en ω, acepta (respectivamente rechaza) si M acepta (respectivamente rechaza).

Claramente M' es una máquina de Turing no–determinista que decide $PAD_T L$. Como cada uno de los pasos (1)–(2) y (3)-(4) que realiza M' se pueden implementar en tiempo $O(|\omega'|)$ y $O(T(m)) = O(|\omega'|)$ respectivamente, sigue que M' es a tiempo $O(|\omega'|)$. Por lo tanto $PAD_T L \in \text{NDTIEMPO}(n)$.

(ii).- Sabemos que EXP $\subseteq$ NEXP.

Veamos que se tiene la inclusión contraria si NP = P. Si $L \in$ NEXP, entonces $L \in \text{NDTIEMPO}(T(n))$ donde $T(n) = 2^{n^c} + C$ para algún $c, C \in \mathbb{N}$ constantes. Por (i), sigue que $PAD_T L \in \text{NDTIEMPO}(n) \subseteq$ NP. Luego, por hipótesis, $PAD_T L \in$ P. Por lo tanto, existe una máquina de Turing determinista M a tiempo polinomial que decide $PAD_T L$. Sea entonces M' una máquina con la misma cantidad de cintas que M, que en la entrada ω escribe $T(|\omega|) - |\omega|$ veces # a continuación de ω, se coloca en la configuración inicial de M, simula M y acepta (respectivamente rechaza) si M acepta (respectivamete rechaza).

Claramente M' decide L. Además, M' requiere tiempo $O(T(|\omega|)$ en escribir los #, tiempo $O(T(|\omega|)$ en alcanzar el estado inicial de M y tiempo polinomial en $T(|\omega|)$ en simular M — en total tiempo $polin(T(n)) = 2^{O(n^d)}$ para algún $d \in \mathbb{N}$. Se concluye que $L \in$ EXP.

Problema 2:

Veamos primero que MIP $\subseteq$ PCP($polin(n), poli(n)$). Por definición, si $L \in$ MIP, entonces existen (V, P_1, P_2) sistema de demostración multi–probador tal que

— Si $\omega \in L$, entonces $\mathbb{P}_\rho\left((V \leftrightarrow P_1, P_2)(\omega, \rho) = acpt.\right) = 1$,

— Si $\omega \notin L$, entonces para todo P_1' y P_2', $\mathbb{P}_\rho\left((V \leftrightarrow P_1', P_2')(\omega, \rho) = acpt.\right) \leq 1/3$.

Recordar que una estrategia del i–ésimo probador, $i \in \{1, 2\}$, corresponde a una función $(\omega, h) \to P_i(\omega, h)$ donde h es una posible interacción entre el verificador y el probador que termina en una pregunta y $P_i(\omega, h)$ representa la respuesta del probador.

Dado ω, sea $\Pi_\omega = (\Pi_{\omega,1}, \Pi_{\omega,2})$ donde vemos a $\Pi_{\omega,i}$ como una tabla indexada por los posibles valores de la interacción h entre el verificador y el i–ésimo probador. En la posición h, la tabla $\Pi_{\omega,i}$ contiene $P_i(\omega, h)$.

Sea entonces V' un verificador con acceso a un oráculo Π_ω que en la entrada ω simula a V y obtiene de su oráculo las respuestas que P_1 y P_2 hubiesen dado. Claramente, si $\omega \in L$, entonces V' acepta con la misma probabilidad que V hubiese aceptado al interactuar con P_1 y P_2, i.e., con probabilidad 1. Si por el contrario, $\omega \notin L$, entonces por la forma en que V' interpreta su oráculo Π, este corresponde a dos estrategias P_1 y P_2. Como ningún par de estrategias de los probadores hace que V acepte con probabilidad mayor que $1/3$, se tiene que V' acepta con probabilidad a lo más $1/3$.

Veamos ahora que PCP($polin(n), polin(n)$) está contenida en NEXP. Por definición, si $L \in$ PCP($polin(n), polin(1)$), entonces existe un verificador V máquina probabilista con oráculo y a tiempo polinomial tal que

— Si $\omega \in L$, entonces existe Π_ω tal que $\mathbb{P}_\rho\left(V^{\Pi_\omega}(\omega, \rho) = acpt.\right) = 1$,

— Si $\omega \notin L$, entonces para todo Π se tiene que $\mathbb{P}_\rho\left(V^{\Pi}(\omega, \rho) = acpt.\right) \leq 1/3$.

Podemos suponer que el oráculo al que accede el verificador es de tamaño exponencial en $n = |\omega|$ — en efecto, las posibles consultas del verificador dependen de los posibles valores de ρ y del resultado de las consultas previas. Luego, como V es a tiempo polinomial, hay una cantidad exponencial de posibles consultas.

Para ver que $L \in$ NEXP basta considerar la máquina no–determinista M que en la entrada ω adivina Π, lo escribe en una de sus cintas, simula V con oráculo Π en cada uno de los posibles ρ y determina la fracción p de estos para los cuales V acepta. La máquina M acepta si $p = 1$ y rechaza en caso contrario. Es fácil ver que M decide L y es a tiempo exponencial.

PROBLEMA 3:

(i).- En efecto

$$h_\alpha = \langle h, (-1)^{l_\alpha} \rangle = \frac{1}{|\mathbb{F}_2|^n} \sum_{x \in \mathbb{F}_2^n} h(x)(-1)^{l_\alpha(x)} .$$

Luego, por definición de h,

$$h_\alpha = \frac{1}{|\mathbb{F}_2|^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus l_\alpha(x)} = \mathbb{P}_{x \in_R \mathbb{F}_2^n} \left(l_\alpha(x) = f(x) \right) - \mathbb{P}_{x \in_R \mathbb{F}_2^n} \left(l_\alpha(x) \neq f(x) \right) .$$

Como $\mathbb{P}\left(l_\alpha(x) = f(x) \right) = 1 - \mathbb{P}\left(l_\alpha(x) \neq f(x) \right)$, obtenemos la primera igualdad pedida.

Para establecer la segunda igualdad observar que

$$\begin{aligned} \mathbb{P}_{x,y \in_R \mathbb{F}_2^n} \left(f(x \oplus y) \neq f(x) \oplus f(y) \right) &= \frac{1}{|\mathbb{F}_2|^{2n}} \sum_{x,y \in \mathbb{F}_2^n} \frac{1}{2} \left(1 - (-1)^{f(x \oplus y) \oplus f(x) \oplus f(y)} \right) \\ &= \frac{1}{2} \left(1 - \frac{1}{|\mathbb{F}_2|^{2n}} \sum_{x,y,z \in \mathbb{F}_2^n : x \oplus y \oplus z = 0} h(x)h(y)h(z) \right) \\ &= \frac{1}{2} \left(1 - (h * h * h)(0) \right) . \end{aligned}$$

(ii).- Observar que,

$$\begin{aligned} \mathbb{P}\left(f(x \oplus y) \neq f(x) \oplus f(y) \right) &= \frac{1}{2} \left(1 - (h * h * h)(0) \right) \\ &= \frac{1}{2} \left(1 - \sum_\alpha (h * h * h)_\alpha (-1)^{l_\alpha(0)} \right) \\ &= \frac{1}{2} \left(1 - \sum_\alpha (h_\alpha)^3 \right) . \end{aligned}$$

Luego, si $h_{\alpha^*} = \max_\alpha h_\alpha$, como $(h_\alpha)^2 \geq 0$ y por Parseval,

$$\mathbb{P}\left(f(x \oplus y) \neq f(x) \oplus f(y) \right) \geq \frac{1}{2} \left(1 - h_{\alpha^*} \sum_\alpha (h_\alpha)^2 \right) = \frac{1}{2} \left(1 - h_{\alpha^*} \right) .$$

Por (i) sabemos que $h_{\alpha^*} = 1 - 2\mathbb{P}\left(f(x) \neq l_{\alpha^*}(x) \right)$, luego

$$\mathbb{P}\left(f(x \oplus y) \neq f(x) \oplus f(y) \right) \geq \mathbb{P}\left(f(x) \neq l_{\alpha^*}(x) \right) \geq \mathrm{Dist}_{\mathcal{L}_n}(f) .$$