Ma50b Complejidad Computacional	**18 de Junio de 2009**

Pauta Control 3

Prof. Cátedra: M. Kiwi — *Prof. Auxiliar: T. González, I. Fantini*

PROBLEMA 1: Bastará establecer que NP $\subseteq$ BPP implica que SAT $\in$ RP. Para demostrar que SAT $\in$ RP la idea es usar una máquina tipo BPP para SAT (cuya existencia garantiza la hipótesis) y en la entrada $\langle\varphi\rangle$ intentar determininar una asignación de valores de verdad que satisfaga a φ. Si el procedimiento tiene éxito se acepta, y en caso contrario se rechaza. La estrategía para determinar la asignación que satisface φ es similar a la forma en que una máquina determinista a tiempo polinomial que decida SAT puede encontrar un certificado de pertenencia en SAT, si es que dicho certificado existe. No obstante, como solo tenemos acceso a una máquina probabilista para decidir pertenencia en SAT, luego que comete errores, hay cierta probabilidad de fracasar en determinar un certificado de pertenencia, aun si este existe. Se genera así una error en el caso que la instancia esté en SAT, pero no hay error si la instancia no lo está.

Formalmente, por hipótesis tenemos que existe M máquina de Turing probabilista a tiempo polinomial tal que

$$\begin{aligned} \omega \in \text{SAT} \quad &\Longrightarrow \quad \mathbb{P}_{\rho}\left(M(\omega,\rho) = acept\right) \geq \frac{2}{3}\,, \\ \omega \notin \text{SAT} \quad &\Longrightarrow \quad \mathbb{P}_{\rho}\left(M(\omega,\rho) = acept\right) \leq \frac{1}{3}\,. \end{aligned}$$

Sea M_ε la máquina de Turing probabilista que corresponde a amplificar M simulándola suficientes veces (y aceptando si la mayoría de las veces M acepta su entrada) de manera de reducir la posibilidad de error a $0 < \varepsilon < 1$. Se verifica vía Chernoff que se requieren $O(\log(1/\varepsilon))$ simulaciones de M para reducir su error a ε. Luego, si $\varepsilon = \Omega(1/polin(n))$ y M es a tiempo polinomial en n, entonces M_ε es a tiempo polinomial en n.

Sea M' la máquina de Turing probabilista que en la entrada $\langle\varphi\rangle$, con φ fórmula Booleana en las n variables $x_1,\ldots,x_n$, realiza lo siguiente:

(1) Para $j = 1,\ldots,n$
(2) $\quad a_j \leftarrow 0$
(3) $\quad$ Si $M_{1/3n}$ en la entrada $\langle\varphi|_{x_j=a_j;j=1,\ldots,i}\rangle$ rechaza, entonces $a_j \leftarrow 1$
(4) Aceptar si $\varphi(a_1,\ldots,a_n) = 1$, y rechazar en caso contrario.

Notar que M' es a tiempo polinomial dado que el loop en (1) se realiza a lo más n veces ($n \leq |\langle\varphi\rangle|$), (2) toma tiempo $O(1)$, (3) es a tiempo polinomial en n y (4) se puede realizar eficientemente. Además, dado que M' acepta $\langle\varphi\rangle$ solo si encuentra un certificado de pertenencia de $\langle\varphi\rangle$ en SAT, se tiene que en el caso $\langle\varphi\rangle \notin$ SAT dicho certificado no existe y por lo tanto la máquina M' nunca acepta. Luego,

$$\omega \notin \text{SAT} \quad \Longrightarrow \quad \mathbb{P}_{\rho}\left(M(\omega,\rho) = acept\right) = 0\,.$$

Supongamos ahora que $\langle\varphi\rangle \in$ SAT y que M' rechaza $\langle\varphi\rangle$. Como φ se puede satisfacer y $\varphi|_{x_j=a_j;j=1,\ldots,n} = \varphi(a_1,\ldots,a_n) \neq 1$, sigue que existe $i \in \{1,\ldots,n\}$ tal que $\varphi|_{x_j=a_j;j=1,\ldots,i-1}$ se satisface y $\varphi|_{x_j=a_j;j=1,\ldots,i}$ no se satisface. Necesariamente se debe tener que en el paso (3) la máquina $M_{1/3n}$ aceptó cuando debía rechazar, o rechazó cuando debía aceptar, i.e. la máquina $M_{1/3n}$ cometió un error, lo que sucede con probabilidad a lo más $1/3n$. Pero la probabilidad de que M se equivoque en alguna de las n simulaciones es a lo más $n(1/3n) \leq 1/3$. Luego,

$$\omega \in \mathrm{SAT} \quad \Longrightarrow \quad \mathbb{P}_\rho\left(M(\omega,\rho) = acept\right) \geq \frac{2}{3}\,.$$

Resumiendo, hemos concluido que SAT $\in$ RP.

PROBLEMA 2: Sea L en BPL decidido por un máquina de Turing M a tiempo polinomial $p(n)$ y espacio $s(n) = O(\log n)$. Sin pérdida de generalidad podemos suponer que M posee una única cinta de trabajo. La idea de la demostración es definir una matríz estocástica en el grafo de descripciones instantáneas de M en la entrada ω, verificar que dicha matríz es de tamaño polinomial en $|\omega|$, y que calculando la t-ésima potencia de dicha matríz se puede determinar la probabilidad de pasar de una discripción instantánea a otra en exactamente t pasos. Eligiendo t suficientemente grande, pero polinomial en $|\omega|$, y mirando el coeficiente adecuado de la t-ésima potencia se obtiene la probabilidad de que la máquina M acepte ω. Con dicha valor es trivial decidir pertenencia en L.

Formalmente, recordemos primero que las descripciones instantáneas de M son de la forma (q,i,C) donde q representa el estado de M, i representa el índice de la celda de la cinta de entrada sobre el que está la cabeza lectora, y C corresponde a la secuencia de caracteres de las primeras $s(n)$ celdas de la cinta de trabajo de M (como es usual, mediante símbolos adicionales se indica la celda sobre la que se encuentra la cabeza lectora de la cinta de trabajo y el contenido de dicha celda).

Notar que si Σ y Q denotan el alfabeto de cinta y el conjunto de estados de M, entonces el número de descripciones instantáneas de M en entradas de largo n es a lo más

$$(n+2)s(n)|Q||\Sigma \cup \{\not b\}|^{s(n)} \quad = \quad O(polin(n))\,.$$

Sea P la matríz cuyas filas y columnas están indexadas por las descripciones instantáneas de M y tal que $P^{(\omega)}_{C,C'}$ es igual a la probabilidad de que M en la entrada ω pase de la descripción instantánea C a la C' en una transición. Claramente, $P^{(\omega)}_{C,C'}$ solo puede tomar valores en $\{0,1/2,1\}$ y una máquina de Turing puede facilmente calcular dicho valor. Además, como el número de configuraciones de M en ω es polinomial en $|\omega|$, se tiene que el tamaño de $P^{(\omega)}$ es polinomial en $|\omega|$. Sigue que una máquina de Turing puede determinar $P^{(\omega)}$ en tiempo polinomial en $|\omega|$.

Observar además, que $(P^{(\omega)})^t$ es la matríz cuyo coeficiente (C,C') corresponde a la probabilidad de que M en la entrada ω pase de la descripción instantánea C a la C' en exactamente t pasos. Como multiplicación de matrices es a tiempo polinomial, sigue que si t es polinomial en $|\omega|$, entonces $(P^{(\omega)})^t$ se puede calcular en tiempo polinomial en $|\omega|$.

Sin pérdida de generalidad podemos asumir que M tiene un único estado de aceptación, que se detiene con su cinta de trabajo en blanco y con todas sus cabezas lectoras sobre las primeras celdas de cada una de sus cintas. Sigue que M tiene una única descripción instantánea de aceptación, digamos C_{acept}. Si C_{inic} denota la descripción instantánea inicial de M, entonces se verifica que el coeficiente (C_{inic}, C_{acept}) de $(P^{(\omega)})^{p(|\omega|)}$ corresponde a la probabilidad $p_{acept}(\omega)$ que M acepte ω y que dicho valor se puede calcular en tiempo polinomial en $|\omega|$. Como $p_{acept}(\omega) \geq 2/3$ si y solo si M acepta ω (equivalentemente, $\omega \in L$), concluimos que se puede decidir pertenencia en L en tiempo polinomial, i.e. $L \in$ P.

PROBLEMA 3: Sea $L \in \mathrm{NP}^{\mathrm{SAT}}$ decidido por una máquina de Turing no-determinista N a tiempo polinomial

$p(n)$ y con SAT como oráculo. Sigue que $\omega \in L$ si y solo si existe una secuencia de elecciones no-deterministas $c_1,\ldots,c_m \in \{0,1\}$, $m \leq p(|\omega|)$, y respuestas correctas a las consultas al oráculo $a_1,\ldots,a_k \in \{0,1\}$, $k \leq p(|\omega|)$, tales que; (1) realiza las elecciones no-deterministas $c_1,\ldots,c_m$, (2) para $i = 1,\ldots,k$, obtiene a_i como respuesta a la i-ésima consulta $\langle\varphi_i\rangle$ determinada por las elecciones no-deterministas $c_1,\ldots,c_m$, y (4) N alcanza un estado de aceptación. La condición (2) equivale a decir que si $a_i = 1$ entonces existe un u_i vector de variables Booleanas tal que $\varphi_i(u_i) = 1$, y si $a_i = 0$ entonces cualquiera sea v_i vector de variables Booleanas se tendrá que $\varphi_i(v_i) = 0$. Sigue que

$$\omega \in L \Longleftrightarrow \exists c_1,\ldots,c_m \in \{0,1\}, \exists a_1,\ldots,a_k \in \{0,1\}, \exists u_1,\ldots,u_k, \forall v_1,\ldots,v_k, \text{ tales que}$$
$$\bigwedge_{i=1}^{k} (a_i = 1 \Longrightarrow \varphi_i(u_i) = 1) \wedge \bigwedge_{i=1}^{k} (a_i = 0 \Longrightarrow \varphi_i(v_i) = 0)\,.$$

Es fácil verificar que una máquina de Turing alternante del tipo Σ_2P puede verificar en tiempo polinomial la afirmación a la derecha de la última equivalencia. Sigue que $L \in \Sigma_2^P$.

PROBLEMA 4:

(i).- Veamos primero que NP $\subseteq$ P$^{\#\mathrm{P}}$. Consideremos L en NP y N máquina de Turing no-determinista a tiempo polinomial. Sea M la máquina con oráculo f_N que en la entrada ω consulta al oráculo por el valor de $\sigma = f_N(\omega)$ y acepta si y solo si $\sigma \neq 0$. Claramente M acepta ω si y solo si N acepta ω. Luego, M decide L. Notar que como N es a tiempo polinomial, digamos $p(n)$, necesariamente se tiene que $f_N(\omega) \leq 2^{O(p(|\omega|)}$ y por lo tanto $|\langle\sigma\rangle| = O(p(|\omega|))$. Sigue que M es a tiempo polinomial, puesto que copiar la entrada a la cinta de pregunta demora tiempo lineal, y procesar la respuesta le toma tiempo polinomial.

Por último, dado que PP $\subseteq$ PESPACIO, una máquina a espacio polinomial puede decidir pertenencia en un oráculo $O \in$ PP, y por lo tanto simular en espacio polinomial una máquina de Turing a tiempo polinomial que tenga como oráculo a O. Sigue que P$^{\mathrm{PP}}$ $\subseteq$ PESPACIO.

(ii).- Veamos primero que P$^{\#\mathrm{P}}$ $\subseteq$ P$^{\mathrm{PP}}$. En efecto, sea L un lenguaje decidido por una máquina de Turing M a tiempo polinomial con acceso al oráculo $f_N \in$ #P donde N es una máquina de Turing no-determinista a tiempo polinomial $p(n)$. Por razones técnicas conviene asumir que cualquiera que sea la entrada, N nunca acepta en todas sus ramas de cálculo (es fácil modificar N para que se cumpla esta propiedad y la función en #P asociada a la máquina resultante sea idéntica a f_N).

Sea O el lenguaje de los $\langle N', q, \sigma\rangle$ tales que N' es una máquina de Turing no-determinista, q es un polinomio, y más de la mitad de las ramas de cálculo de N' en σ que terminan en $q(|\sigma|)$ pasos son de aceptación. Afirmamos que $O \in$ PP. En efecto, sea P la máquina de Turing probabilista que en la entrada $\langle N', q, \sigma\rangle$ simula N en σ durante $q(|\sigma|)$ pasos pero usando lanzamientos de moneda en vez de no-determinismo, acepta si N' acepta y rechaza en caso contrario. Claramente P es a tiempo polinomial en $q(|\sigma|)$, luego también en $q(|\langle N', q, \sigma\rangle|)$. Como $\mathbb{P}_\rho\left(P(\langle N', q, \sigma\rangle, \rho) = acept\right) = f_N(\sigma)/2^{p(|\sigma|)}$ sigue que

$$\langle N', q, \sigma\rangle \in O \quad\Longrightarrow\quad \mathbb{P}_\rho\big(P(\langle N', q, \sigma\rangle, \rho) = acept\big) > \frac{1}{2}\,.$$
$$\langle N', q, \sigma\rangle \notin O \quad\Longrightarrow\quad \mathbb{P}_\rho\big(P(\langle N', q, \sigma\rangle, \rho) = acept\big) \leq \frac{1}{2}\,.$$

Se deja como ejercicio probar que la clase PP no cambia si para las instancias negativas la probabilidad de error es menor o igual a $1/2$ en vez de estrictamente menor que $1/2$.

Para simular M^{f_N} en una entrada ω mediante una máquina de Turing M' con oráculo O, basta mostrar como M' puede, dado σ, calcular en tiempo polinomial en $|\sigma|$ el valor de $f_N(\sigma)$ vía consultas a su oráculo O. Para establecer esto último, considera el procedimiento descrito a continuaución. Cuando M le consulta a su oráculo por el valor de f_N en σ, la máquina M' construye una máquina probalista N_i, $1 \leq i \leq p(|\sigma|)$, y luego consulta a su oráculo por la pertenencia de $\langle N_i, p+1, \sigma\rangle$ en O obteniendo como respuesta $b_i = 1$ si $\langle N_i, p+1, \sigma\rangle$ está en O y $b_i = 0$ en caso contrario. Sea B_i el entero cuya expresión en binario es $b_1 b_2 \ldots b_i$ (definimos $B_0 = 0$). Sea R_N una máquina probabilita que simular N pero usando lanzamientos de moneda en vez de no-determinismo. La máquina N_i primero lanza una moneda y si sale cara simula R_N en la entrada σ, y si la moneda sale sello, entonces acepta si un entero t_i elegido al azar en $\{0, \ldots, 2^{p(|\omega|)} - 1\}$ es estrictamente menor que $2^{p(|\omega|)-i}(2^i - 2B_{i-1} - 1)$. Notar que por construcción, N_i es a tiempo $p(n)+1$.

Como $f_N(\omega)$ toma valores entre 0 y $2^{p(|\omega|)} - 1$ (esto último por nuestro supuesto que N no acepta en todas su ramas de cáculo), dicho valor lo podemos representar en binario como una secuencia de $p(|\omega|)$ bits (el más significativo primero). Afirmamos que el i-ésimo bit de $f_N(\omega)$ es igual a b_i, es decir es 1 si y solo si $\langle N_i, p, \sigma\rangle \in O$. En efecto, por inducción en $i \geq 1$. Si $i = 1$, entonces $b_1 = 1$ si y solo si N_1 acepta σ con probabilidad al menos $1/2$. Pero,

$$\begin{aligned}
\mathbb{P}_\rho\left(N_1(\sigma,\rho) = acept\right) &= \frac{1}{2} \cdot \frac{2^{p(|\sigma|)-1}}{2^{p(|\sigma|)}} + \frac{1}{2} \cdot \mathbb{P}_\rho\left(R_N(\sigma,\rho) = acept\right) \\
&= \frac{1}{4} + \frac{f_N(\omega)}{2^{p(|\sigma|)+1}}\,.
\end{aligned}$$

Luego, $b_1 = 1$ si y solo si $f_N(\sigma) \geq 2^{p(|\sigma|)-1}$, i.e. b_1 es el bit más significativo de $f_N(\sigma)$ como se quería demostrar. Supongamos entonces que $b_1, \ldots, b_i$ son los i bits más significativos de $f_N(\sigma)$. Notar que $b_{i+1} = 1$ si y solo si N_{i+1} acepta σ con probabilidad al menos $1/2$. Pero,

$$\begin{aligned}
\mathbb{P}_\rho\left(N_{i+1}(\sigma,\rho) = acept\right) &= \frac{1}{2} \cdot \frac{2^{p(|\sigma|)-i-1}(2^{i+1} - 2B_i - 1)}{2^{p(|\sigma|)}} + \frac{1}{2} \cdot \mathbb{P}_\rho\left(R_N(\sigma,\rho) = acept\right) \\
&= \frac{1}{2}\left(1 - \frac{2B_i + 1}{2^{i+1}}\right) + \frac{f_N(\omega)}{2^{p(|\sigma|)+1}}\,.
\end{aligned}$$

Luego, $b_{i+1} = 1$ si y solo si

$$\frac{f_N(\omega)}{2^{p(|\sigma|)}} - \frac{B_i}{2^i} \quad \geq \quad \frac{1}{2^{i+1}}\,,$$

i.e. b_{i+1} es el $(i+1)$-ésimo bit más significativo de $f_N(\sigma)$. Esto concluye la demostración de la afirmación y establece que vía $p(|\sigma|)$ consultas al oráculo O la máquina M' puede determinar el valor de $f_N(\sigma)$

Como todas las consultas que hace a su oráculo f_N la máquina M' en la entrada ω tienen largo acotado por $p(|\omega|)$, sigue que M'^O en la entrada ω será a tiempo polinomial. Además, por el procedimiento descrito más arriba, M' con oráculo O puede determinar bit a bit el valor de $f_N(\sigma)$ para cualquier consulta σ que M le haga a su oráculo. El número de consultas requeridas por M' por cada consulta σ de M a su oráculo es polinomial en $|\sigma|$, luego polinomial en $|\omega|$. Sigue que M' es a tiempo polinomial. Por construcción tenemos que M'^O y M^{f_N} deciden el mismo lenguaje. En resumen, $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{P}^{\mathrm{PP}}$.

Falta demostrar que $\mathrm{P}^{\mathrm{PP}} \subseteq \mathrm{P}^{\#\mathrm{P}}$. Sea L en P^{PP} decidido por una máquina de Turing M a tiempo polinomial con acceso al oráculo $O \in \mathrm{PP}$. Sea R la máquina de Turing probabilista a tiempo polinomial $p(n)$ tal que

$$\begin{aligned}
\sigma \in O \quad &\Longrightarrow \quad \mathbb{P}_\rho\left(R(\sigma,\rho) = acept\right) > \frac{1}{2}\,, \\
\sigma \notin O \quad &\Longrightarrow \quad \mathbb{P}_\rho\left(R(\sigma,\rho) = acept\right) < \frac{1}{2}\,.
\end{aligned}$$

Sin pérdida de generalidad podemos modificar R de forma que en cada una de sus transiciones lance una moneda (potencialmente ignorando el resultado). Además, siempre podemos asumir que R acepta/rechaza su entrada σ al cabo de exactamente $p(|\sigma|)$ transiciones. En efecto, basta considerar una nueva máquina probabilista que simula R en la entrada σ manteniendo un contador para la cantidad de transiciones simuladas y postponer la decisión de aceptar/rechazar hasta que el contador alcance el valor $p(|\sigma|)$. Notar que la nueva máquina será a tiempo polinomial y acepta/rechaza con exactamente la misma probabilidad que la máquina original.

Sea N la máquina no-determinista que simula R pero que en vez de realizar los lanzamientos de moneda de R hace transiciones no-deteministas, una por cada posible resultado del lanzamiento de la moneda. Notar que el árbol de cálculo de N en la entrada σ tiene exactamente $2^{p(|\sigma|)}$ ramas, y que

$$\mathbb{P}_{\rho}\left(R(\sigma,\rho) = acept\right) \quad = \quad \frac{f_N(\sigma)}{2^{p(|\sigma|)}}.$$

Luego, si M' es la máquina de Turing que en la entrada σ simula M en σ y cada vez que esta última consulta a su oráculo por la pertenencia de σ en O, entonces M' consulta a su oráculo f_N por el valor de $f_N(\sigma)$. Si $f_N(\sigma) > 2^{p(|\sigma|)-1}$ (respectvimente, $f_N(\sigma) < 2^{p(|\sigma|)-1}$), entonces M' prosigue como si $\sigma \in O$ (respectivamente $\sigma \notin O$). La máquina M' acepta/rechaza si M acepta/rechaza. Es fácil ver que M' tiene la misma complejidad de tiempo que M, luego es a tiempo polinomial.