Complejidad Computacional
Tarea 3

Karla Adriana Esquivel Guzmán
Andrea Itzel González Vargas
Luis Pablo Mayo Vega
Carlos Gerardo Acosta Hernández

Entrega: 02/05/17
Facultad de Ciencias UNAM

Ejercicios

1.

Sea $L \in \{0,1\}^*$ tal que existe una PTM con tiempo polinomial de ejecución tal que $\forall\ \alpha \in \{0,1\}^*$

a) Si $\alpha \in L$ entonces $Pr[M(\alpha) = 1] \geq n^{-c}$

b) Si $\alpha \notin L$ entonces $Pr[M(\alpha) = 1] = 0$

Demuestra que para todo $d > 0$ existe una $M' \in PTM$ con tiempo polinomial de ejecución tal que $\forall\ \alpha \in \{0,1\}^*$:

a) Si $\alpha \in L$ entonces $Pr[M(\alpha) = 1] \geq 1 - 2^{-n^d}$;

b) Si $\alpha \notin L$ entonces $Pr[M(\alpha) = 1] = 0$

Demostración:
Teorema (Cota de Chernorff): Sean $X_1, \ldots, X_n$ un conjunto de variables booleanas aleatorias tales que cada X_i es un bit igual a 1 con probabilidad $\leq p$. Entonces:

$$Pr[|\Sigma_{i=1}^{k} X_i - pk| > \delta pk] < e^{-\frac{\delta^2}{4}pk}.$$

para una δ lo suficientemente pequeña.
M' simulará al M con la entrada α $k = n^{2c+d}$ veces. *M'* acepta si al menos una de las simulaciones acepta, rechaza si todas las simulaciones rechazan.
Sean $X_1, \ldots, X_k$ variables booleanas independientes con $E[X_i] = Pr[X_i = 1] \geq p\ con\ p = n^{-c}$.

Usando la configuración $\delta = n^{-c}/2$ garantizamos que si $\Sigma_{i=1}^{k} X_i \geq pk - \delta pk$ entonces obtendremos una respuesta correcta. Así acotamos la probabilidad de obtener una respuesta incorrecta a

$$e^{-\frac{1}{4|x|^{2c}}\frac{1}{2}^{|x|^{2c+d}}} \leq 2^{-n^d}$$

2. Demuestra que $ZPP = RP \cap coRP$

Dem.

$\boxed{\subseteq}$ **P.D.** $ZPP \subseteq RP \cap coRP$

Primero vemos que $ZPP \subseteq RP$:
Podemos hacer una simple transformación en ZPP que nos resulte en que todo lenguaje en ZPP esté en RP. Esta transformación consiste en lo siguiente. Sea $L \in ZPP$, cada vez que la PTM que define a L en ZPP falle en dar un resultado concreto (es decir no lance 0 o 1, más bien un error o un "no sé"), decimos que el resultado es 1, de manera que se cumple la restricción para que L esté en RP de que si $x \notin L$, entonces el resultado será siempre 0. A demás como la PTM falla con probabilidad menor a $1/2$, también se cumple la otra restricción de RP que dice que si $x \in L$, entonces el resultado será 1 con probabilidad mayor a $1/2$.

Vemos ahora que $ZPP \subseteq coRP$:
Análogamente al caso anterior, sea $L \in ZPP$, cada vez que la PTM que define a L en ZPP falla, diremos que el resultado es 0, de manera que se cumplan las restricciones para que L esté en $coRP$.

Como $ZPP \subseteq RP$ y $ZPP \subseteq coRP$, entonces $ZPP \subseteq RP \cap coRP$

$\boxed{\supseteq}$ **P.D.** $RP \cap coRP \subseteq ZPP$

3. Demuestra que $BPL \subseteq P$, donde BPL es la clase de lenguajes decidibles por PTM que utilizan espacio logarítmico.

Dem.
Sea L un lenguaje $\boldsymbol{BPL}$ y M una TM tal que para una entrada $x \in L$, $Pr[M(x) = L(x)] \leq \frac{2}{3}$. Supongamos que la cadena x es de longitud n, ahora bien, sea C el número de configuraciónes de $M(\cdot, x)$, entonces $S = C \times C$ es una matriz tal que $S_{c_1,c_2} = \frac{1}{2}$ si la configuración c_2 es obtenida en un sólo paso de M desde c_1 y $S_{c_1,c_2} = 0$ en cualquier otro caso. $\forall t$, la entrada $S^t_{c_1,c_2}$ nos dice la probabilidad de obtener la configuración c_2 a partir de c_1 en t pasos, donde S^t es la matriz resultante de la multiplicación de S con ella misma, t veces. Al calcular todas las potencias de S hasta el tiempo de ejecución de $M(\cdot, x)$, podemos calcular la probabilidad de de aceptación para $M(r, x)$ y decidir si $x \in L$. Notemos que cada probabilidad es un entero múltiplo de $\frac{1}{2^{p(n)}}$, de manera que puede ser representada con un número polinomial de dígitos. Por lo tanto $BPL \subseteq P$.