



PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
 ESCUELA DE INGENIERIA
 DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Tópicos Avanzados en Teoría de la Computación - IIC3810
Lista de Ejercicios 2

1. [**Responsable: Antonio López**] Demuestre el lema de Schwartz-Zippel. Vale decir, demuestre que dado un polinomio no nulo $p(x_1, \dots, x_n)$ de grado k y un subconjunto finito y no vacío A de $\mathbb{Q}$, si $a_1, \dots, a_n$ son elegidos de manera uniforme e independiente desde A , entonces:

$$\Pr(p(a_1, \dots, a_n) = 0) \leq \frac{k}{|A|}$$

2. [**Responsable: Raimundo Manterola**] En clases demostramos que para cada problema en $\text{RP} \cap \text{co-RP}$, existe un algoritmo que lo decide en tiempo polinomial esperado. En esta pregunta usted va a demostrar que la dirección opuesta también es cierta, lo que nos permite concluir que $\text{RP} \cap \text{co-RP}$ corresponde exactamente con la clase de problemas para los cuales existe un algoritmo que lo decide en tiempo polinomial esperado.

Sea L un lenguaje sobre un alfabeto Σ , y suponga que M es una MT probabilística tal que: (i) el alfabeto de entrada de M es Σ ; (ii) M funciona en tiempo polinomial; (iii) para cada $w \in \Sigma^*$, M retorna **sí**, **no** o **indefinido**; (iv) para cada $w \in \Sigma^*$ y $s \in \{0, 1\}^*$, si $M(w, s)$ retorna **sí**, entonces $w \in L$, y si $M(w, s)$ retorna **no**, entonces $w \notin L$; (v) existe un valor p fijo con $0 < p \leq 1$ tal que para cada $w \in \Sigma^*$, $\Pr_s(M(w, s) \text{ retorne } \textbf{sí o no}) = p$. Demuestre que $L \in \text{RP} \cap \text{co-RP}$.

3. [**Responsable: Andrés Quintana**] Demuestre que las clases RP y co-RP son cerradas bajo la noción de reducción $\leq_m^p$. ¿Son estas clases cerradas bajo la noción de reducción $\leq_T^p$? Justifique su respuesta.

Para resolver las siguientes preguntas, recuerde que dado un lenguaje $L \in \text{BPP}$ y un número natural $k \geq 1$, utilizando el lema de amplificación para BPP es posible construir un algoritmo aleatorizado A tal que A funciona en tiempo polinomial y para toda entrada w con $|w| = n$:

- si $w \in L$, entonces $\Pr(A \text{ acepte } w) \geq (1 - \frac{1}{n^{k+1}})$
- si $w \notin L$, entonces $\Pr(A \text{ acepte } w) \leq \frac{1}{n^{k+1}}$

De esta forma, dado $n \geq 5$, si generamos con distribución uniforme y de manera independiente n^k entradas

$w_1, w_2, \dots, w_{n^k}$ de largo n , entonces tenemos que:

$$\begin{aligned} \Pr\left(\bigwedge_{i=1}^{n^k} A \text{ entrega el resultado correcto con entrada } w_i\right) &= \\ \prod_{i=1}^{n^k} \Pr(A \text{ entrega el resultado correcto con entrada } w_i) &\geq \\ \prod_{i=1}^{n^k} \left(1 - \frac{1}{n^{k+1}}\right) &= \left(1 - \frac{1}{n^{k+1}}\right)^{n^k} = \left(\left(1 - \frac{1}{n^{k+1}}\right)^{n^{k+1}}\right)^{\frac{1}{n}} \geq \left(\frac{1}{4}\right)^{\frac{1}{n}} \geq \left(\frac{1}{4}\right)^{\frac{1}{5}} \geq \frac{3}{4} \end{aligned}$$

Vale decir, la probabilidad de que el algoritmo A entregue respuestas correctas con todas las entradas $w_1, w_2, \dots, w_{n^k}$ es mayor o igual a $\frac{3}{4}$.

4. **[Responsable: Ricardo Rodriguez]** Demuestre que BPP es cerrada bajo las nociones de reducción $\leq_m^p$ y $\leq_T^p$. Nótese que de esto se concluye que $\text{PTIME}^{\text{BPP}} = \text{BPP}$.
5. **[Responsable: David Ruz]** Demuestre que si $\text{SAT} \in \text{BPP}$, entonces $\text{SAT} \in \text{RP}$. Nótese que de esto se concluye que si $\text{NP} \subseteq \text{BPP}$, entonces $\text{RP} = \text{NP}$.