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

Examen

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

Tiempo: 4.5 hrs.

PROBLEMA 1:

(i).- Sea $L \subseteq \Sigma^*$ un lenguaje cualquiera, $\# \notin \Sigma$ y $T : \mathbb{N} \to \mathbb{N}$ una función tiempo constructible.[1] Se define

$$PAD_T L = \{\omega' \in (\Sigma \cup \{\#\})^* \, : \, \omega' = \omega \underbrace{\# \cdots\cdots \#}_{T(|\omega|)-|\omega|}, \omega \in L\} \, .$$

Pruebe que si $L \in$ NDTIEMPO$(T(n))$, entonces $PAD_T L \in$ NDTIEMPO(n).

(ii).- De (i) concluya que si NP $=$ P, entonces NEXP $=$ EXP.

PROBLEMA 2: Pruebe que MIP $\subseteq$ PCP$(polin(n), O(polin(n))) \subseteq$ NEXP.

PROBLEMA 3: Sea $\mathbb{F}_2$ el cuerpo finito de orden 2 cuyos elementos en lo sucesivo denotaremos por 0 y 1. Decimos que $l \in \mathbb{F}_2^n \to \mathbb{F}_2$ es lineal si cualquiera sean $x, y \in \mathbb{F}_2^n$ se tiene que $l(x \oplus y) = l(x) \oplus l(y)$. Al conjunto de funciones lineales de $\mathbb{F}_2^n \to \mathbb{F}_2$ lo denotaremos $\mathcal{L}_n$. Si para $\alpha, x \in \mathbb{F}_2^n$ se define $\alpha \cdot x = \oplus_{i=1}^n \alpha_i x_i$, es fácil ver que $\mathcal{L}_n = \{l_\alpha : \mathbb{F}_2^n \to \mathbb{F} \, : \, l_\alpha(x) = \alpha \cdot x\}$.

Sea $g, g', \psi, \chi : \mathbb{F}_2^n \to \{-1, +1\}$ y $\alpha \in \mathbb{F}_2^n$, definimos $\langle \psi, \chi \rangle = \dfrac{1}{|\mathbb{F}_2|^n} \displaystyle\sum_{x \in \mathbb{F}_2^n} \psi(x)\chi(x)$, y

— el α-ésimo coeficiente de Fourier de g por $g_\alpha = \langle g, (-1)^{l_\alpha} \rangle$,

— la convolución de g y g' por $g * g'(z) = \dfrac{1}{|\mathbb{F}_2|^n} \displaystyle\sum_{x, y \in \mathbb{F}_2^n : x \oplus y = z} g(x) g'(y)$.

En lo que sigue, sean $f : \mathbb{F}_2^n \to \mathbb{F}_2$ y $h \equiv (-1)^f$.

(i).- Pruebe que

— $h_\alpha = 1 - 2\mathbb{P}_{x \in_R \mathbb{F}_2^n} \left(f(x) \neq l_\alpha(x) \right)$,

— $(h * h * h)(0) = 1 - 2\mathbb{P}_{x, y \in_R \mathbb{F}_2^n} \left(f(x \oplus y) \neq f(x) \oplus f(y) \right)$.

[1] I.e., $T(n) \geq n \log(n)$ y dado 1^n se puede calcular en tiempo $O(T(n))$ la representación binaria de $T(n)$.

Indicación: Si $a, b \in \mathbb{F}_2$, entonces $(-1)^{a \oplus b} = 1$ si y sólo si $a = b$.

(ii).- Sabido es que

— $(g * g')_\alpha = g_\alpha g'_\alpha$,

— $g(x) = \sum_{\alpha \in \mathbb{F}_2^n} g_\alpha (-1)^{l_\alpha(x)}$,

— se cumple la igualdad de Parseval, i.e., que $g * g(0) = 1$.

Pruebe que,[2]

$$\mathbb{P}_{x,y \in_R \mathbb{F}_2^n} \left(f(x \oplus y) \neq f(x) \oplus f(y) \right) \geq \mathrm{Dist}_{\mathcal{L}_n}(f) \,.$$

[2] $\mathrm{Dist}_{\mathcal{L}_n}(f) \stackrel{\mathrm{def}}{=} \mathrm{mín}_{\alpha \in \mathbb{F}_2^n} \mathbb{P}_{x \in_R \mathbb{F}_2^n} \left(f(x) \neq l_\alpha(x) \right)$.