

**Tarea 1***Profesor: M. Kiwi*

FECHA ENTREGA: 20 DE AGOSTO

PROBLEMA 6: (Chor, Goldreich - 1989) Sean  $a, b \in \mathbb{F}_{2^n}$  y  $h_{a,b}(x) = ax + b$  (aritmética en  $\mathbb{F}_{2^n}$ ). Pruebe que para todo  $x, x', y, y' \in \mathbb{F}_{2^n}$  tal que  $x \neq x'$ ,

$$\begin{aligned}\mathbb{P}_{a,b \in \mathbb{F}_{2^n}}(h_{a,b}(x) = y) &= \frac{1}{|\mathbb{F}_{2^n}|} \\ \mathbb{P}_{a,b \in \mathbb{F}_{2^n}}(h_{a,b}(x) = y, h_{a,b}(x') = y') &= \frac{1}{|\mathbb{F}_{2^n}|^2}.\end{aligned}$$

Observe que cada elemento de  $\mathbb{F}_{2^n}$  puede codificarse como una secuencia de  $n$  bits. Eligiendo  $2n$  bits independiente y uniformemente en  $\{0, 1\}$  se puede generar una codificación de  $a$  y  $b$ , y por lo tanto elegir al azar  $h_{a,b}(\cdot)$ . Con el objetivo de reducir el error, suponga que el algoritmo  $\mathcal{A}$  de tipo BPP se ejecuta  $k$  veces en la misma entrada  $\omega$ . Considere el algoritmo  $\mathcal{A}'$  que en vez de generar nuevos bits aleatorios en cada iteración, elige  $h_{a,b}(\cdot)$  al azar y usa la representación de  $h_{a,b}(i)$ ,  $i \in \{1, \dots, k\}$ , en vez de la secuencia de bits aleatorios de la  $i$ -ésima iteración de  $\mathcal{A}$ .

Pruebe que la probabilidad de error de  $\mathcal{A}'$  en la entrada  $\omega$  es a lo más  $4/k$ .

Indicación: Calcule el número esperado  $N$  de iteraciones en que  $\mathcal{A}'$  no se equivoca. Calcule la varianza de  $N$  y aplique la desigualdad de Chebyshev.

PROBLEMA 2: Problema 5 del Capítulo 7 del Arora-Barak (ver Definición 7.20).

PROBLEMA 3: Problema 7 del Capítulo 7 del Arora-Barak.

PROBLEMA 4: Problema 8 del Capítulo 7 del Arora-Barak.

PROBLEMA 5: Problema 12 del Capítulo 7 del Arora-Barak.