MA-53I Tópicos en Matemáticas Discretas I	**17 de Abril, 1999**

Pauta Control No. 1

Prof. Cátedra: M. Kiwi, M. Loebl, y M. Matamala

PROBLEMA 1: Se dice que $l\colon \mathbb{F}_2^n \to \mathbb{F}_2$ es *lineal* si $l(x+y) = l(x)+l(y)$ para todo $x,y \in \mathbb{F}_2^n$. El conjunto de funciones lineales de $\mathbb{F}_2^n$ en $\mathbb{F}_2$ se denota por $\mathcal{L}(\mathbb{F}_2^n,\mathbb{F}_2)$. Dados dos funciones f y g tales que $f,g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ se define la *distancia de f a g* por

$$D(f,g) \;=\; \mathbb{P}_{x\in_R\mathbb{F}_2^n}\left(f(x)\neq g(x)\right) \;=\; \frac{1}{|\mathbb{F}_2^n|}\sum_{x\in\mathbb{F}_2^n}\mathbb{I}_{\{\omega:f(\omega)\neq g(\omega)\}}(x)\,.$$

Pruebe que toda función de $\mathbb{F}_2^n$ en $\mathbb{F}_2$ está a una distancia de a lo más $1/2$ del espacio de funciones lineales de $\mathbb{F}_2^n$ en $\mathbb{F}_2$, i.e. pruebe el siguiente

Teorema 1 *Si $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, entonces existe $l \in \mathcal{L}(\mathbb{F}_2^n,\mathbb{F}_2)$ tal que $D(f,l)\leq 1/2$.*

Indicación: Pruebe que

1. $l \in \mathcal{L}(\mathbb{F}_2^n,\mathbb{F}_2)$ sí y sólo si $\exists\alpha\in\mathbb{F}_2^n$, tal que $l(x) = l_\alpha(x) \stackrel{\text{def}}{=} \sum_{i=1}^n \alpha_i\cdot x_i$ (aritmética en $\mathbb{F}_2$).
2. Para todo $b\in\mathbb{F}_2$ y $x\in\mathbb{F}_2^n$, si $x\neq 0$, entonces $\mathbb{P}_{\alpha\in_R\mathbb{F}_2^n}\left(l_\alpha(x)=b\right) = 1/2$.

SOLUCIÓN: Sea $\vec{e}_1,\ldots,\vec{e}_n$ la base canónica de $\mathbb{F}_2^n$, i.e., $\vec{e}_i$ es el vector n-dimensional cuya i-ésima coordenada es 1 y cuyas restantes coordenadas son 0. Si $l\in\mathcal{L}(\mathbb{F}_2^n,\mathbb{F}_2)$ entonces para todo $x\in\mathbb{F}_2^n$ se tiene, por linealidad, que

$$l(x) \;=\; l\Big(\sum_{i=1}^n x_i\vec{e}_i\Big) \;=\; \sum_{i=1}^n x_i\cdot l(\vec{e}_i)\,.$$

Luego, para toda función $l\in\mathcal{L}(\mathbb{F}_2^n,\mathbb{F}_2)$ existe $\alpha\in\mathbb{F}_2^n$ tal que $l(x) = l_\alpha(x)$ cualquiera sea $x\in\mathbb{F}_2^n$ (basta tomar $\alpha_i = l(\vec{e}_i)$ para todo $i\in\{1,\ldots,n\}$). El converso de la anterior afirmación es evidente.

Consideremos ahora $b\in\mathbb{F}_2$ y $x\in\mathbb{F}_2^n$ tal que $x\neq 0$. Como $x\neq 0$ entonces existe $j\in\{1,\ldots,n\}$ tal que $x_j\neq 0$, i.e., $x_j = 1$. Sin perdida de generalidad supongamos que $j=n$. Luego, condicionando, se obtiene que

$$\mathbb{P}_{\alpha\in_R\mathbb{F}_2^n}\left(l_\alpha(x)=b\right) \;=\; \sum_{a_1,\ldots,a_{n-1}\in\mathbb{F}_2}\frac{1}{|\mathbb{F}_2|^{n-1}}\,\mathbb{P}_{\alpha_n\in_R\mathbb{F}_2}\left(\alpha_n = b-\sum_{i=1}^{n-1}a_i\cdot x_i\right)\,.$$

Como cada término de la sumatoria es igual a $1/2$ se concluye que $\mathbb{P}_{\alpha\in_R\mathbb{F}_2^n}\left(l_\alpha(x)=b\right) = 1/2$.

Para demostrar el teorema enunciado, observar que

$$\mathbb{E}_{\alpha\in_R\mathbb{F}_2^n}\left(D(f,l_\alpha)\right) \;=\; \frac{1}{|\mathbb{F}_2^n|}\sum_{x\in\mathbb{F}_2^n}\mathbb{E}_{\alpha\in_R\mathbb{F}_2^n}\left(\mathbb{I}_{\{\omega:f(\omega)\neq g(\omega)\}}(x)\right) \;=\; \frac{1}{|\mathbb{F}_2^n|}\sum_{x\in\mathbb{F}_2^n}\mathbb{P}_{\alpha\in_R\mathbb{F}_2^n}\left(f(x)\neq l_\alpha(x)\right)\,.$$

Los términos de la sumatoria correspondientes a $x \neq 0$ son iguales a $1/2$ y el término correspondiente a $x = 0$ puede ser acotado trivialmente por 1. Luego,

$$\mathbb{E}_{\alpha \in_R \mathbb{F}_2^n}\left(D(f, l_\alpha)\right) \;\leq\; \frac{1}{|\mathbb{F}_2^n|}\left(1 + \sum_{x \in \mathbb{F}_2^n, x \neq 0} \frac{1}{2}\right) \;=\; \frac{1}{2} + \frac{1}{2|\mathbb{F}_2^n|}\,.$$

Luego, el Método del Primer Momento permite concluir que existe $\alpha \in \mathbb{F}_2^n$ tal que

$$D(f, l_\alpha) \;\leq\; \frac{1}{2} + \frac{1}{2|\mathbb{F}_2^n|}\,.$$

Pero como $|\mathbb{F}_2^n| \cdot D(f, l_\alpha)$ es un entero, sigue que la anterior desigualdad implica que $D(f, l_\alpha) \leq 1/2$ como queríamos concluir.

PROBLEMA 2: Elija uno de los dos siguientes resultados y pruebelo.

Teorema 2 *Sea $n = 2^k - 1$ y $d = 2t + 1$. Existe un espacio de probabilidad $(\Omega, \mathcal{F}, \mathbb{P})$ tal que $|\Omega| = 2(n+1)^t$ y variables aleatorias $X_1, \ldots, X_n$ d-independientes que toman valores 0 y 1 con probabilidad $1/2$. Además, tanto el espacio muestral como las variables aleatorias se pueden construir explícitamente dada una representación de $\mathbb{F}_{2^k}$ como un espacio vectorial k-dimensional sobre $\mathbb{F}_2$.*

Teorema 3 *Sea d un entero positivo par. Si las variables aleatorias $X_1, \ldots, X_n$ sobre el espacio muestral Ω son d-independientes y ninguna es constante con probabilidad 1, entonces*

$$|\Omega| \;\;\geq\;\; \sum_{j=0}^{d/2} \binom{n}{j}\,.$$

SOLUCIÓN: Ambos resultados fueron probados en cátedra. Consultar el cuaderno.

PROBLEMA 3: Diremos que un grafo $G = (V, E)$ es β-*arco–expansivo* si para cualquier subconjunto $S \subset V$ tal que $|S| \leq |V|/2$ se tiene que

$$E(S, V \setminus S) \;\stackrel{\text{def}}{=}\; |\{(u, v) \in E \,:\, u \in S, v \in V \setminus S\}| \;\geq\; \beta|S|\,.$$

Sea $G = (V, E)$ un grafo d-regular β-arco–expansivo. Pruebe que los arcos de G se pueden particionar en E_0 y E_1 tales que cada E_i es el conjunto de arcos de un grafo aproximadamente $\beta/2$-arco–expansivo en el mismo conjunto de vértices. Para ello, siga los siguientes pasos:

(i).- Pruebe que si $|E_i(S, V \setminus S)| \geq \beta(\frac{1}{2} - \epsilon)|S|$ para todo $S \subset V$ tal que $|S| \leq |V|/2$ y $G|_S$ es conexo, entonces también se cumple para todo $S \subset V$ tal que $|S| \leq |V|/2$.

(ii).- Pruebe el siguiente

Teorema 4 [Cota de Chernoff] *Sean $X_1, \ldots, X_n$ variables aleatorias independientes tales que $\mathbb{P}(X_i = +1/2) = \mathbb{P}(X_i = -1/2) = 1/2$, y sea $S_n = X_1 + \ldots + X_n$. Si $a > 0$, entonces*

$$\mathbb{P}(S_n > a) \;\;<\;\; e^{-2a^2/n}\,.$$

Concluya que con probabilidad a lo más $e^{-2a^2/n}$ una binomial de parámetros $(n, 1/2)$ tome un valor mayor que $\frac{n}{2} + a$.

Indicación: Observe que $\mathbb{P}(S_n > a) = \mathbb{P}\left(e^{4a\cdot S_n/n} > e^{4a^2/n}\right)$ y que $(e^\lambda + e^{-\lambda})/2 \leq e^{\lambda^2/2}$.

(iii).- Cada arco de E se coloca en E_0 o E_1, con probabilidad $1/2$, siendo la elección para cada arco independiente. Par cada subconjunto conexo S tal que $|S| \leq |V|/2$, sea A_S el evento correspondiente a

$$E_0(S, V\setminus S) \; < \; \beta(\frac{1}{2} - \epsilon)|S|\,, \qquad \text{o} \qquad E_1(S, V\setminus S) \; < \; \beta(\frac{1}{2} - \epsilon)|S|\,.$$

Pruebe que $\mathbb{P}(A_S) \leq 2e^{-2\epsilon^2\beta|S|}$.

(iv).- Pruebe el siguiente

Teorema 5 **[Lema Local – Caso Asimétrico]** *Sea D un digrafo de dependencias para los eventos $A_1, \ldots, A_n$, sean $t_1, \ldots, t_n \geq 1$, y $0 \leq p < 1/8$. Se tiene que,*

$$\mathbb{P}(A_i) \; \leq \; p^{t_i}\,, \quad y \quad \sum_{j:(i,j)\in E(D)} (2p)^{t_j} \; \leq \; \frac{t_i}{2}\,, \qquad \forall\, i \in \{1, \ldots, n\} \qquad \Longrightarrow \qquad \mathbb{P}\left(\bigcap_{i=1}^{n} A_i^c\right) \; > \; 0\,.$$

Indicación: Use que si $0 \leq x_i \leq 1/4$ entonces $1 - x_i \geq e^{-6x_i/5}$ y que $2e^{-3/5} \geq 1$.

(v).- Asuma (sin demostrarlo) que dado $S \subset V$ hay en el digrafo de dependencias para los eventos $A_{S'}$ a lo más $(ed)^t|S|$ eventos $A_{S'}$ tales que $|S'| = t$, $G|_{S'}$ es conexo, y hay un arco en el digrafo de dependencias entre los nodos asociados a A_S y $A_{S'}$.

Concluya el siguiente

Teorema 6 *Para todo $\epsilon > 0$, $d \geq 3$, y β tal que $\sum_{t\geq 1}(4de^{1-2\epsilon^2\beta})^t \leq 1/2$, si $G = (V, E)$ es un grafo d-regular β-arco-expansivo, entonces hay una partición $E = E_0 \cup E_1$ tal que (V, E_0) y (V, E_1) son grafos $\beta(\frac{1}{2} - \epsilon)$-arco-expansivos.*

Indicación: Utilice el Lema Local (Caso Asimétrico) con $p = 2e^{-2\epsilon^2\beta}$ y $t_S = |S|$.

SOLUCIÓN:

(i).- Sea $S \subset V$ un conjunto cualquiera tal que $|S| \leq |V|/2$ y $G|_S$ no es conexo. Sea $k > 1$ y $S_1, \ldots, S_k$ una partición de S tal que $G|_{S_1}, \ldots, G|_{S_k}$ son conexos. Luego, $E_i(S, V\setminus S) = \sum_{j=1}^{k} E_i(S_j, V\setminus S)$. Observar además, que para $i \neq j$ no hay arcos de G que vayan de un vértice en S_i a un vértice en S_j, i.e., $E_i(S_j, S_i) = \emptyset$ para todo $i \neq j$. Luego, $E_i(S_j, V\setminus S) = E_i(S_j, V\setminus S_j)$. Sigue que,

$$E_i(S, V\setminus S) \; = \; \sum_{j=1}^{k} E_i(S_j, V\setminus S_j)\,.$$

Como cada $G|_{S_j}$ es conexo y $|S_j| \leq |S| \leq |V|/2$, por hipótesis tenemos que

$$E_i(S, V\setminus S) \; \geq \; \sum_{j=1}^{k} \beta(\frac{1}{2} - \epsilon)\,|S_j| \; = \; \beta(\frac{1}{2} - \epsilon)\,|S|\,.$$

El caso en que $G|_S$ es conexo y $|S| \leq |V|/2$ esta cubierto por hipótesis.

(ii).- De la indicación y utilizando la desigualdad de Markov obtenemos que

$$\mathbb{P}\left(S_n > a\right) \;\leq\; \frac{1}{e^{4a^2/n}}\,\mathbb{E}\left(e^{4aS_n/n}\right).$$

Pero por independencia de las variables aleatorias $X_1,\ldots,X_n$ sigue que

$$\mathbb{E}\left(e^{4aS_n/n}\right) \;=\; \mathbb{E}\left(e^{4a\sum_{i=1}^n X_i/n}\right) \;=\; \prod_{i=1}^n \mathbb{E}\left(e^{4a^2X_i/n}\right) \;=\; \left(\frac{e^{-2a^2/n}+e^{2a^2/n}}{2}\right)^n.$$

Luego, de la desigualdad dada en la indicación se obtiene que $\mathbb{E}\left(e^{4aS_n/n}\right) \leq e^{2a^2/n}$. Sigue que

$$\mathbb{P}\left(S_n > a\right) \;\leq\; \frac{e^{2a^2/n}}{e^{4a^2/n}} \;=\; e^{-2a^2/n}.$$

Además, si X es una binomial de parámetros $(n,1/2)$, entonces $X-\frac{n}{2}$ sigue la misma distribución que S_n por lo que

$$\mathbb{P}\left(X > \frac{n}{2}+a\right) \;=\; \mathbb{P}\left(S_n > a\right) \;=\; e^{-2a^2/n}.$$

(iii).- De la desigualdad de Boole sigue que

$$\mathbb{P}\left(A_S\right) \;\leq\; \mathbb{P}\left(E_0(S,V\setminus S) \;<\; \beta(\frac{1}{2}-\epsilon)|S|\right) + \mathbb{P}\left(E_1(S,V\setminus S) \;<\; \beta(\frac{1}{2}-\epsilon)|S|\right).$$

El resultado deseado lo obtendremos probando que cada término a la derecha de la desigualdad se puede acotar por $e^{-2\epsilon^2\beta|S|}$. En efecto, sean $e_1,\ldots,e_N$ los arcos de G que van de un vértice en S a un vértice en $V\setminus S$. Como G es β-arco expansivo, $N \geq \beta|S|$. Sean además $X_1,\ldots,X_N$ variables aleatorias tales que

$$X_j \;=\; \begin{cases} 1 & \text{si } e_j \in E_i, \\ 0 & \text{si } e_j \notin E_i. \end{cases}$$

Observar que $E_i(S,V\setminus S) = \sum_{j=1}^N X_j \geq \sum_{j=1}^{\beta|S|} X_j$. Luego,

$$\mathbb{P}\left(E_i(S,V\setminus S) \leq \beta(\frac{1}{2}-\epsilon)|S|\right) \;\leq\; \mathbb{P}\left(\sum_{j=1}^{\beta|S|} X_j \leq \beta(\frac{1}{2}-\epsilon)|S|\right) \;=\; \mathbb{P}\left(\sum_{j=1}^{\beta|S|} X_j \geq \frac{\beta|S|}{2}+\beta\epsilon|S|\right),$$

donde la última desigualdad se tiene porque $\sum_{j=1}^{\beta|S|} X_j$ se distribuye como una binomial de parámetros $(\beta|S|,1/2)$ luego su distribución es simétrica en torno a $\beta|S|/2$. Finalmente, aplicamos (ii) y obtenemos que

$$\mathbb{P}\left(E_i(S,V\setminus S) \leq \beta(\frac{1}{2}-\epsilon)|S|\right) \;\leq\; e^{-2(\epsilon\beta|S|)^2/(\beta|S|)} \;=\; e^{-2\epsilon^2\beta|S|}.$$

(iv).- Tomemos $x_i = (2p)^{t_i}$ para todo $i \in \{1,\ldots,n\}$. Observar que como $0 \leq p \leq 1/8$ y $t_i \geq 1$ tenemos que $0 \leq x_i \leq (2/8)^{t_i} \leq 1/4$. Verifiquemos que se cumplen las condiciones del Lema Local de Lovász. En efecto,

$$x_i \prod_{j:(i,j)\in E(D)} (1-x_j) \;\geq\; x_i\, e^{-\frac{6}{5}\sum_{j:(i,j)\in E(D)} x_j} \;\geq\; x_i\, e^{-3t_i/5} \;=\; p^{t_i}(2e^{-3/5})^{t_i} \;\geq\; p^{t_i} \;\geq\; \mathbb{P}\left(A_i\right),$$

donde la primera desigualdad es consecuencia de la primera parte de la indicación, la segunda desigualdad es por hipótesis, la tercera desigualdad es consecuencia de la segunda parte de la indicación, y la última desigualdad es nuevamente por hipótesis. Sigue que el Caso Asimétrico del Lema Local es consecuencia del caso general del Lema Local.

(v).- Sea $p = 2e^{-2\epsilon^2\beta}$, $t_S = |S|$, y A_S como en (iii). Sea además D el digrafo de dependencias para los eventos A_S. Observar que

$$p \;=\; 2e^{-2\epsilon^2\beta} \;\leq\; \frac{1}{4}(4de^{1-2\epsilon^2\beta}) \;\leq\; \frac{1}{4}\sum_{t\geq 1}(4de^{1-2\epsilon^2\beta})^t \;\leq\; \frac{1}{8}\,,$$

donde la última desigualdad se tiene por hipótesis.

Por (iii) y puesto que $t_S = |S| \geq 1$ se tiene que

$$\mathbb{P}\left(A_S\right) \;\leq\; 2e^{-2\epsilon^2\beta|S|} \;\leq\; p^{t_S}\,.$$

Por otro lado, para todo S subconjunto conexo de vértices de G tal que $|S| \leq |V|/2$,

$$\sum_{S':(S,S')\in E(D)} (2p)^{t_{S'}} \;\leq\; \sum_{t\geq 1}\left\{\sum_{S':(S,S')\in E(D),|S'|=t} (2p)^t\right\} \;\leq\; \sum_{t\geq 1}|S|(2edp)^t \;\leq\; \frac{t_S}{2}\,,$$

donde la segunda desigualdad se obtiene del hecho, señalado en el enunciado, que la sumatoria entre llaves es sobre a lo más $|S|(ed)^t$ términos, y la última desigualdad es por hipótesis. Como se cumplen las hipótesis del Caso Asimétrico del Lema Local entonces sabemos que $\cap_S A_S^c \neq \emptyset$ siendo la intersección sobre todos los $S \subset V$ tal que $G|_S$ es conexo. Por definición de A_S y por (i) lo anterior equivale a decir que para todo S subconjunto de vértices de G tal que $|S| \leq |V|/2$ se tiene que

$$E_0(S, V\setminus S) \;\geq\; \beta(\frac{1}{2}-\epsilon)|S|\,, \qquad \text{o} \qquad E_1(S, V\setminus S) \;\geq\; \beta(\frac{1}{2}-\epsilon)|S|\,.$$

En otras palabras (V, E_0) y (V, E_1) son grafos $\beta(\frac{1}{2}-\epsilon)$–arco–expansivos.