Curso de Nivel Básico

Métodos algebraicos en combinatoria

Daniel A. Jaume

Departamento de Matemáticas
Facultad de Ciencias Físico Matemáticas y Naturales
Universidad Nacional de San Luis, Argentina

VII Encuentro Nacional de Álgebra

La Falda, Sierras de Córdoba, Argentina

4 al 8 de Agosto de 2014

www.famaf.unc.edu.ar/~ciem/elena7

MÉTODOS ALGEBRAICOS EN COMBINATORIA

DANIEL A. JAUME

Índice

1. Método (cota) del Álgebra Lineal

1.1. Villa (Im)Par. El método de la cota lineal consiste en la siguiente idea (muy simple): si uno desea acotar el tamaño de un conjunto, se asocia los elementos del conjunto con los elementos de un espacio vectorial V de dimensión *baja*, y se muestra que los vectores asociados son linealmente independientes, y por lo tanto el conjunto no puede tener más elementos que la dimensión del espacio V.

En honor a Babai y Frankl, pioneros en este campo, empezaremos con el problema de Villa Par.

Villa Par tiene 32 habitantes. Quienes tienen el vicio compulsivo de formar clubs (grandes o pequeños). Pero los clubs no se pueden formar de forma arbitraria. En gobierno municipal ha establecido las siguientes reglas que todo club debe satisfacer:

1. Cada club debe tener un número par de miembros.
2. Cada par de clubes debe tener en común un número par de miembros.
3. No pueden haber dos clubes formados por exactamente las mismas personas.

Los ciudadanos de Villa Par desean formar tantos clubes como puedan, respetando las reglas pues son bueno vecinos. Para que se den una idea del grado de obsesión que tienen, ellos registran inclusive el *club vacío*, que no posee miembros (¡ya que cero es par!). La pregunta que nos hacemos es:

Date: 25 de Julio de 2014.

¿Cuántos clubes se pueden formar en Villa Par?

Podemos hallar una cota inferior rápidamente, si hacemos un par de suposiciones adicionales, pues a mayor número de requisitos, menos elementos los cumplirán. Primera condició todo el mundo en Villa Par está casado. Segunda condición adicional: a fin de evitar la infidelidad (ilusos) los esposos deben pertenecer a los mismos clubes. (observe que con estas reglas adicionales, las reglas 1 y 2 son superfluas).

Con estas nuevas reglas se pueden formar $2^{16} = 65{,}536$ clubes ¿Por qué? Pues cada club se forma al tomar 16 decisiones binarias: la pareja 1 se asocia o no, la pareja 2 se asocia o no, ..., la pareja 16 se asocia o no. El conjunto de decisiones es igual al conjunto de clubes que se pueden formar en Villa Par (Casados y Esposados).

Entonces el número de clubes posibles en Villa Par es de más de 65.536. Lo cual es asombrosamente alto para una pequeã villa de 32 habitantes.

Después de un tiempo la situación se vuelve inmanejable y el municipio decide cambiar las reglas a fin de que no halla demasiados clubes. El intendente cree que no se necesita cambiar demasiado las reglas, de hecho, según él basta cambiar una sola palabra:

1. Cada club debe tener un número **impar** de miembros.
2. Cada par de clubes debe tener en común un número par de miembros.
3. No pueden haber dos clubes formados por exactamente las mismas personas.

Este cambio, motiva que el pueblo cambie su nombre a **Villa Impar**

Un breve análisis hace ver que última regla es redundante (¿Por qué?). Por lo que la ordenanza que regirá la formación de clubes en Villa Impar es:

(a) Cada club debe tener un número **impar** de miembros.
(b) Cada par de clubes debe tener en común un número par de miembros.

Con esta ordenanza es claro que se pueden armar al menos 32 clubes, por ejemplo:

- 32 clubes de 1 persona.
- 32 clubes de 31 personas.
- 31 clubes de 7 personas y uno de 31.

De hecho hay muchas formas de lograr 32 clubes que satisfagan la regla. Pero, curiosamente, es imposible formar 33 o clubes que satisfagan estas reglas.

Y más curiosamente, todas las soluciones conocidas (al menos para el autor) de este problema puramente combinatorio involucran álgebra lineal.

La idea es trabajar en el espacio ${\mathbb{F}_2}^{32}$ de dimensión 32. Supongamos que tengamos $C_1, \ldots, C_m$ clubs. A cada club le asociamos un vector de incidencia v_i con la siguiente regla: la entrada j-ésima del vector v_i es 1 si el ciudadano j es socio del club C_i y cero en todo otro caso (estamos asumiendo que hemos numerado los ciudadanos de Villa Impar del 1 al 32).

Es claro que el producto interno de dos vectores de incidencia da:

$$\langle v_i, v_j \rangle = |C_i \cap C_j|.$$

O si pensamos en la aritmética sobre el cuerpo $\mathbb{F}_2$

$$\langle v_i, v_j \rangle = \begin{cases} 1, & \text{si } i = j, \\ 0, & \text{si } i \neq j. \end{cases}$$

Ahora vamos a probar que estos vectores son linealmente independientes en ${\mathbb{F}_2}^{32}$. Consideremos:

$$\lambda_1 v_1 + \cdots + \lambda_m v_m = 0.$$

donde cada $\lambda_i \in \mathbb{F}_2$. Por supuesto, debemos probar que todos los escalares son nulos. Par ver el valor de λ_i vamos a multiplicar ambos lados por v_i:

$$\langle \lambda_1 v_1 + \cdots + \lambda_i v_i + \cdots + \lambda_m v_m, v_i \rangle = \langle 0, v_i \rangle.$$

Distribuyendo

$$\langle \lambda_1 v_1, v_i \rangle + \cdots \langle \lambda_i v_i, v_i \rangle + \cdots + \langle \lambda_m v_m, v_i \rangle = 0$$

de donde concluimos que $\lambda_i = 0$. Por lo tanto los vectores $v_1, \ldots, v_m$ linealmente independientes. Consecuentemente $m \leq 32$.

Ahora podemos establecer fácilmente el siguiente teorema:

Teorema 1.1 (Teorema de Villa Impar u Oddtown Theorem)**.** *En toda ciudad con n habitantes, no se pueden formar más de n clubes bajo las reglas:*

(a) *Cada club debe tener un número **impar** de miembros.*
(b) *Cada par de clubes debe tener en común un número par de miembros.*

Daremos otra demostración del Teorema de Villa Impar, usando la independencia lineal vía un argumento de rango. Recordemos brevemente algunas de las (des)igualdades de rango más importantes. Sean $\mathbf{A}, \mathbf{B}$ matrices sobre un cuerpo arbitrario $\mathbb{F}$, de tamaños adecuados para cada caso. Entonces:

1. $rk(\mathbf{A}) = rk(\mathbf{A}^T)$.
2. $rk(\mathbf{AB}) = rk(\mathbf{B}) - \dim(N(\mathbf{A}) \cap R(\mathbf{B}))$.
3. $rk(\mathbf{A}) - rk(\mathbf{B}) \leq rk(\mathbf{A} + \mathbf{B}) \leq rk(\mathbf{A}) + rk(\mathbf{B})$.
4. $rk(\mathbf{A} + rk(\mathbf{B}) - n \leq rk(\mathbf{AB}) \leq \text{mín}\{rk(\mathbf{A}, rk(\mathbf{B})\}$.

Tenemos por un lado n habitantes los cuales pueden ser identificados con $[n] := \{1, \ldots, n\}$, el segmento inicial de los primeros n enteros positivos. Por el otro tenemos un conjunto de clubes, el que puede ser identificado en con una familia de subconjuntos de $[n]$.

$$\mathcal{C} := \{C_1, \ldots, C_m\}$$

donde cada $C_i \in 2^{[n]}$.

Construimos, como es habitual en combinatoria, la matriz $\mathbf{M}$ de incidencia habitantes-clubes. Las filas de esta matriz están indizadas por los habitantes, las columnas por los clubes.

$$m_{i,C_j} = \begin{cases} 1, & \text{si } i \in C_j \\ 0, & \text{en todo otro caso.} \end{cases}$$

Por ejemplo tenemos 5 habitantes y los clubes son

$$\mathcal{C} := \{C_1 = \{1, 2, 3\}, C_2 = \{1, 2, 4\}, C_3 = \{5\}\}.$$

Tenemos que la matriz de incidencia es

$$\mathbf{M} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

De nuevo queremos ver que los vectores de incidencia de los clubes, i.e. (*id est*, latín, esto es) los vectores columnas de la matriz de incidencia M, son linealmente independientes sobre $\mathbb{F}_2$.

Una forma de probar esto es mostrando que el rango de la matriz de incidencia es al menos m, el número de columnas de la matriz.

Consideremos la matriz

$$\mathbf{A} = \mathbf{M}^T\mathbf{M},$$

la cual llamaremos matriz de intersección del sistema $\mathcal{C}$ de clubes. El nombre proviene siguiente hecho (haciendo las cuentas en $\mathbb{Q}$ o $\mathbb{R}$ o $\mathbb{C}$):

$$\mathbf{A}_{i,j} = |C_i \cap C_j|.$$

Pero, haciendo las cuentas en $\mathbb{F}_2$ tenemos que $\mathbf{A} = \mathbf{I}_m$, donde $\mathbf{I}_m$ representa la matriz identidad de orden m.

Ahora

$$m = rk(\mathbf{I}_m)) = rk(\mathbf{A}) = rk(\mathbf{M}^T\mathbf{M}) \leq rk(\mathbf{M}) \leq n.$$

1.2. Teorema de Graham-Pollak. Sea $G = (V,\ E)$ un grafo (finito), y sean $V_1, \ldots, V_r$ conjuntos de vértices de G. Denotemos por G_i al subgrafo de G inducido por los vertices en V_i. Si los grafos $G_i, \ldots, G_r$ son lado-disjuntos y entre todos contienen a todos los lados de G, diremos que los grafos $G_i, \ldots, G_r$ forman una **descomposición lado-disjunta** de G.

Un Clique bipartito es un grafo completo bipartito $K_{A,B} = (A \cup B, E)$ con $A \cap B = \emptyset$ y $E = A \times B$.

Sea $bd(K_n)$ el número más pequeño tal que el grafo completo K_n, puede ser descompuesto en $bd(K_n)$ cliques bipartitos lado-disjuntos. Esta cantidad esta bien definida, pues E forma una colección de $\frac{n(n-1)}{2}$ cliques bipartitos lado-disjuntos. Luego $bd(K - n) \leq \frac{n(n-1)}{2}$. Pero obviamente que podemos hacerlo mejor, por ejemplo K_5 puede ser descompuesto en 4 estrellas (grafos donde uno de los vertices está unido al resto, y no hay otras conexiones):

1. $K_{\{1\},\{2,3,4,5\}}$,
2. $K_{\{2\},\{3,4,5\}}$,
3. $K_{\{3\},\{4,5\}}$,
4. $K_{\{4\},\{5\}}$.

Por lo que claramente $f(5) \leq 4$. En general esta partición en cliques bipartitos funciona, y K_n puede ser descompuesto en $n-1$ cliques bipartitos lado-disjuntos: K_{A_i,B_i}, con $A_i = \{i\}$ y $B_i = \{i+1, \ldots, n\}$, para $i = 1, \ldots, n-1$. Esta es una forma de realizar la descomposición en $n-1$ cliques bipartitos lado-disjuntos, pero hay muchas otras.

Si bien ahora es claro que $f(n) \leq n-1$, el siguiente resultado clásico de Graham y Pollak (1971) nos dice que no podemos mejorar más.

Teorema 1.2. *Los lados de K_n no pueden ser descompuestos en menos de $n-1$ cliques bipartitos lado-disjuntos.*

Este es un resultado importante con multiples aplicaciones a la teoría de comunicaciones y computación, por lo que ha sido objeto de multiples demostraciones. Hasta hace muy poco, sólo se conocían demostraciones algebraicas. Recién en 2008 Vishwanathan y 2013 Chung dieron demostraciones puramente combinatorias.

Demostración. **(Trevberg 1982)** El polinomio

$$S(x_1, \ldots, x_n) := \sum_{1 \leq i < j \leq n} x_i x_j$$

nos da una representación algebraica del conjunto de lados de K_n. Y cada descomposición de K_n en cliques bipartitos lado-disjuntos nos da una forma de reescribir a $S(x)$.

Supongamos que los pares $(A_1, B_1), \ldots, (A_t, B_t)$ nos dan una descomposición de K_n es cliques bipartitos lado-disjuntos. Entonces

$$S(x_1, \ldots, x_n) = \sum_{k=1}^{t} \left(\sum_{i \in A_k} x_i \right) \left(\sum_{j \in B_k} x_j \right). \tag{1.1}$$

Ahora nos podemos olvidar del grafo, y simplemente tratar de hallar el mínimo t para el cual 1.1 vale, donde la única restricción es que $A_i \cap B_i = \emptyset$ para toda $i = 1, \ldots, t$, con $A_i, B_i \subset [n]$.

Ahora

$$\left(\sum_{i=1}^{n} x_i \right)^2 = \sum_{i=1}^{n} x_i^2 + 2 \sum_{1 \leq i < j \leq n} x_i x_j.$$

Por lo tanto

$$\sum_{i=1}^{n} x_i^2 = \left(\sum_{i=1}^{n} x_i \right)^2 - 2S(x_1, \ldots, x_n).$$

Supongamos que $t \leq n - 2$, recordando 1.1 tenemos que el sistema homogéneo de a lo más $n - 1$ ecuaciones:

$$\begin{cases} \sum_{i \in A_k} x_i &= 0, \text{ para } k = 1, \ldots, t. \\ \sum_{i=1}^{n} x_i &= 0 \end{cases}$$

tiene una solución no-trivial $\hat{x}_1, \ldots, \hat{x}_n$. Ahora, por un lado como $\sum_{i \in A_k} \hat{x}_i = 0$ y $\sum_{i=1}^{n} \hat{x}_i = 0$, tenemos que

$$\sum_{i=1}^{n} \hat{x}_i^2 = 0.$$

Pero como $\hat{x}_1, \ldots, \hat{x}_n$ es una solución no trivial:

$$\sum_{i=1}^{n} \hat{x}_i^2 > 0,$$

lo cual es ridículo. Luego $t \geq n - 1$. □

1.3. Autovalores y Teorema de Witsenhausen. Ahora abordaremos el problema general de descomponer un grafo finito G en un conjunto lado-disjunto de cliques bipartitos, de ahora en más **bicliques**. El **número de descomposición por bicliques** de un grafo G, denotado por $bd(G)$, es el mínimo número de bicliques lado-disjuntos en que se puede descomponer a G. Observe que este parámetro está bien definido para todo grafo finito. El teorema de Graham-Pollak nos dice que $bd(K_n) = n - 1$.

Sabemos que $bd(K_n) = 4$, y sean grafos B_1, B_2, B_3, B_4 una descomposición por bicliques lado-disjuntos del K_5. Por ejemplo

1. $B_1 = K_{\{1\},\{2,3,4,5\}}$,
2. $B_2 = K_{\{2\},\{3,4,5\}}$,
3. $B_3 = K_{\{3\},\{4,5\}}$,
4. $B_4 = K_{\{4\},\{5\}}$.

Denotemos por u_i y v_i a los vectores característicos de las particiones de B_i. Así:

1. $u_1 = (1, 0, 0, 0, 0)$ y $v_1 = (0, 1, 1, 1, 1)$,
2. $u_2 = (0, 2, 0, 0, 0)$ y $v_2 = (0, 0, 1, 1, 1)$,

3. $u_3 = (0,0,1,0,0)$ y $v_3 = (0,0,0,1,1)$,
4. $u_4 = (0,0,0,1,0)$ y $v_4 = (0,0,0,0,1)$.

Observe que la matriz de adyacencia de B_i como subgrafo de G se puede escribir en términos de los vectores característicos u_i y v_i:

$$\mathbf{D}(B_i) = u_i v_i^T + v_i u_i^T.$$

Por ejemplo:

$$\mathbf{D(B_3)} = u_3 v_3^T + v_3 u_3^T.$$

Pues

$$\begin{aligned} u_3 v_3^T + v_3 u_3^T &= \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} [0,0,0,1,1] + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} [0,0,1,0,0] \\ &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \\ &= \mathbf{D(B_3)}. \end{aligned}$$

Ahora estableceremos un resultado muy general, atribuido a Witsenhausen (en algún momento de los 80s):

Teorema 1.3. *Sea G un grafo finito y A su matriz de adyacencia. Definimos $n_+(A)$ y $n_-(A)$ como el número de autovalores positivos de A y el número de autovalores negativos de A, contando multiplicidades. Entonces*

$$bd(G) \geq \text{máx}\{n_+(A), n_-(A)\}.$$

Demostración. Sean $B_1, \ldots, B_t$ una descomposición por bicliques lado-disjuntos de un grafo finito G. Sean $D(B_i)$ la matriz de adyacencia del grafo B_i visto como subgrafo de G. Entonces es claro que

$$A(G) = \sum_{i=1}^{bd(G)} D(B_i).$$

Consideremos los siguientes subespacios de $\mathbb{R}^n$

$$\begin{aligned} W &= span\,\{w \in \mathbb{R}^n \,:\, w^T u_i = 0, \forall 1 \leq i \leq bd(G)\}, \\ P &= span\,\{\text{ Autovectores asociados a autovalores positivos de } A(G)\}. \end{aligned}$$

Es claro que

$$\dim(W) \geq n - bd(G).$$

Ahora, para todo $0 \neq p \in P$, tenemos que $p^T A(G)p > 0$. Por lo que $W \cap P = \{0\}$. Recordando que al ser $A(G)$ una matriz simétrica podemos conseguir una base (ortonormal) de $\mathbb{R}^n$ con autovectores de $A(G)$, tenemos que

$$\dim(W) \leq n - \dim(P) = n - n_+(A).$$

Entonces

$$n - bd(G) \leq \dim(W) \leq n - n_+(A)$$

de donde podemos concluir que $bd(G) \geq n_+(A)$. *Mutatis mutandis* (latín: cambiando lo que haya que cambiar) se prueba que $bd(G) \geq n_-(A)$. □

1.4. Ejercicios.

1. Intercambie **par** por **impar** en las reglas **(a)** y **(b)**. Bajo estas reglas espejo: todos los clubes deben tener un número par de miembros, y dos clubes deben compartir un número impar de miembros. Probar que no más de n clubes se pueden formar en un pueblo con n habitantes.
2. Sea $\mathbf{J}_n$ la matriz cuadra de orden n de todos 1s, por ejemplo
$$\mathbf{J}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$
Consideremos la matriz $\mathbf{J}_n - \mathbf{I}_n$, ceros en la diagonal y ceros en el resto de las posiciones, por ejemplo
$$\mathbf{J}_3 - \mathbf{I}_3 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$
Se pide:
   a) Calcular los autovalores de $\mathbf{J}_n - \mathbf{I}_n$.
   b) Calcular el determinante de $\mathbf{J}_n - \mathbf{I}_n$.
   c) Demostrar que el rango de $\mathbf{J}_n - \mathbf{I}_n$ sobre $\mathbb{F}_2$ es n si n es par y $n-1$ si n es impar.
3. Usando las reglas espejo dadas es el ejercicio 1, determinar el número máximo de clubes en un pueblo de n habitantes.
4. Sea $\mathbf{A}_{2n\times 2n}$ una matriz de ceros en la diagonal y ± 1 en el resto de las posiciones. Probar que $\mathbf{A}$ es no singular (sobre $\mathbb{R}$).
5. **Villa Impar Bipartita:** Suponga que hay m clubes rojos $R_1, \cdots, R_m$ y m clubes blancos $B_1, \cdots, B_m$ en un pueblo con n habitantes. Asuma que los clubes satisfacen las siguientes reglas:
   a) $|R_i \cap B_i|$ es impar para toda i.
   b) $|R_i \cap B_j|$ es par para toda $i \neq j$.
   Probar que $m \leq n$.
6. Hallar dos descomposiciones de K_6 y tres de K_7 en cliques bipartitos lado-disjuntos.
7. Deducir el Teorema de Graham-Pollak como corolario del Teorema de Witsenhausen.

2. Densidad Combinatoria y Ortogonalidad

2.1. Densidad Combinatoria. En la teoría computacional del aprendizaje la siguiente noción juega un rol importante:

Definición 2.1. Sea $A \subset \{0,1\}^n$, diremos que A es **(n,k)-denso** si existe un subconjunto de k coordenadas

$$S = \{i_1, \ldots, i_k\}$$

tales que la proyección de A sobre los índices en S contienen todas las posibles 2^k configuraciones (por supuesto, n y k son enteros no negativos con $0 \leq k \leq n$).

Por ejemplo, $A = \{(0,1)\}$ es (2,0)-denso, mientras que

$$B = \{(0,0,0), (0,0,1), (0,1,1), (1,1,0)\}$$

es (3,1)-denso y (3,2)-denso pero no es (3,3)-denso.

Una observación elemental, si A es (n,k)-denso y $A \subset B$, entonces B es (n,k)-denso.

El máximo k para el cual un subconjunto de $\{0,1\}^n$ es (n,k)-denso se llama **dimensión de Vapnik-Chervonenkis** del subconjunto (por brevedad: VC-dimensión). Así la VC-dimensión de B es 2.

El problema combinatorio es: dados n y k hallar un conjunto A (n,k)-denso, con la menor cantidad de vectores posibles.

Dados un vector $v = (v_1, \ldots, v_n)$, su proyección sobre un conjunto de coordenadas $S = \{i_1, \ldots, i_k\}$ es el vector

$$v|_S := (v_{i_1}, \ldots, v_{i_k})$$

. La proyección de un conjunto de vectores $A \subset \{0,1\}^n$ sobre S es el conjunto de vectores

$$A|_S := \{v|_S : v \in A\}.$$

Por lo tanto, A es (n,k)-denso si y sólo si $A|_S = \{0,1\}^k$ para al menos un subconjunto S de k coordenadas.

Es claro que todo subconjunto (n,k)-denso debe contener al menos 2^k vectores.

¿Qué tan grande puede ser un subconjunto de $\{0,1\}^n$ sin llegar a ser (n,k)-denso? Si A es el conjunto de todos los vectores de $\{0,1\}^n$ con menos de k unos, entonces:

- A **no** es(n,k)-denso.
- $H(n,k) := |A| = \sum_{i=0}^{k-1} \binom{n}{i}$

Por ejemplo, los $H(4,3) = \binom{4}{0} + \binom{4}{1} + \binom{4}{2} = 11$ vectores que siguen NO son (4,3)-densos

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array} \qquad \begin{array}{cccc} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{array} .$$

Pero basta que agreguemos uno más al conjunto, por ejemplo el

$$1 \quad 0 \quad 1 \quad 1 \; .$$

Para que el conjunto se vuelva (4,3)-denso, siendo las coordenadas adecuadas (en este caso) $S = \{1,3,4\}$.

Que todo subconjunto de $\{0,1\}^n$ con más de $H(n,k)$ elementos es (n,k)-denso es un hecho que ha sido redescubierto varias veces (en probabilidad, en teoría computacional del aprendizaje, etc), pues es de suma utilidad en muchos campos: lógica, teoría de conjuntos, probabilidad, etc.

Teorema 2.2. *Si $A \subset \{0,1\}^n$ y $|A| > H(n,k)$, entonces A es (n,k)-denso.*

Demostración. Por inducción sobre n y k. Si $k = 1$ entonces A tiene al menos dos vectores diferentes y por lo tanto es (n,1)-denso (hay al menos una coordenada en la que difieren). Ahora tomemos un subconjunto arbitrario $A \subset \{0,1\}^n$ de tamaño $|A| > H(n,k)$. Sea

$$B := A|_{\{1,\ldots,n-1\}}$$

la proyección de A sobre las primeras $n-1$ coordenadas. Sea C el conjunto de todos los vectores u de $\{0,1\}^{n-1}$ para los cuales **ambos** vectores $(u,0)$ y $(u,1)$ pertenecen a A. La siguiente observación es simple pero crucial:

$$|A| = |B| + |C|.$$

Ahora, si $|B| > H(n-1,k)$, entonces por hipótesis inductiva B es (n-1,k)-denso, y por lo tanto el conjunto A es (n,k)-denso (basta tomar las coordenadas que hacen que B sea (n-1,k)-denso).

Si $|B| \leq H(n-1,k)$ entonces, usando la identidad de Pascal,

$$\begin{aligned} |C| &= |A| - |B| > H(n,k) - H(n-1,k) \\ &= \sum_{i=0}^{k-1} \binom{n}{i} - \sum_{i=0}^{k-2} \binom{n-1}{i} \\ &= \sum_{i=0}^{k-2} \binom{n-1}{i} \\ &= H(n-1,k-1). \end{aligned}$$

Luego, por hipótesis inductiva el conjunto C es (n-1,k-1)-denso, y como $C \times \{0,1\} \subset A$, entonces el propio A es (n,k)-denso. □

En 1983, en forma independiente, Alon y Frankl, hicieron una observación a partir de la cual se puede deducir fácilmente el teorema que acabamos de ver: podemos restringir nuestra atención a subconjuntos de $\{0,1\}^n$ con una estructura muy particular, los conjuntos *cerrados hacia abajo o hereditarios.*

2.2. Conjuntos Hereditarios. Estamos interesados en trabajar con subconjuntos de $\{0,1\}^n$ que tengan la propiedad de ser cerrados al cambiar 1s por 0s en sus vectores. Por ejemplo si $(0,1,0,1,1) \in A$ entonces también están en A

$$\begin{matrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{matrix} .$$

Usando el orden habitual para vectores de $\{0,1\}^n$: $u \leq v$ si $u_i \leq v_i$ para todo $i \in \{1,\ldots,n\}$. Podemos dar la siguiente definición:

Definición 2.3. Un conjunto $A \subset \{0,1\}^n$ es **hereditario** o **cerrado hacia abajo** si $v \in A$ y $u \leq v$ implica que $u \in A$.

Dado un conjunto de coordenadas $S \subset \{1,\ldots,n\}$, definimos $t_S(A)$ como el número de vectores en la proyección $A|_S$.

Por ejemplo si A es el conjunto formado por los vectores

$$\begin{matrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{matrix}$$

y $S = \{1, 2, 4\}$, tenemos que $A|_S$ está formado por

$$\begin{matrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{matrix}$$

por lo que $t_S(A) = 3$.

Llamaremos i-ésimo vecino de v al vector $v_{i\to 0}$ que se obtiene de v cambiando la i-ésima coordenada (o bit) por 0 (cero). Por ejemplo, si $v = (0, 1, 0, 1, 1)$, tenemos que $v_{2\to 0} = (0, 0, 0, 1, 1)$ y $v_{3\to 0} = (0, 1, 0, 1, 1) = v$.

El siguiente teorema dice que para cualquier subconjunto A del n-cubo $\{0, 1\}^n$, existe un conjunto hereditario de la misma cardinalidad cuya sombra está a la izquierda (en algún sentido) de la sombra de A.

Teorema 2.4. *Para cada conjunto A del n-cubo $\{0, 1\}^n$ existe un conjunto $B \subset \{0, 1\}^n$ tal que:*

- $|B| = |A|$,
- *Para todo conjunto de coordenadas S tenemos que $t_S(B) \leq t_S(A)$.*

Por ejemplo tomemos el conjunto A

$$\begin{matrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{matrix} .$$

Este conjunto no es hereditario, pues el 3-vecino de $v = (1, 1, 1, 1, 1)$ es el vector $(1, 1, 0, 1, 1) \notin A$. Este vector v de A tiene una coordenada *mala*:$v \in A$ pero $v_{3\to 0} \notin A$. Por otro lado, el conjunto B formado por los vectores

$$\begin{matrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{matrix}$$

si es hereditario y satisface todas las condiciones del teorema.

¿Cómo podemos obtener un subconjunto B *bueno* para cualquier subconjunto A con vectores que posean coordenadas malas?

Sustituyendo los vectores con coordenadas malas por sus i-vecinos. Para lo cual definimos la siguiente transformación. Dado $i \in \{1, \ldots, n\}$ y un subconjunto $A \in \{\{0, 1\}^n$, definimos T_i como sigue: tome un vector $v \in A$ tal que $v_i = 1$, y vea si $v_{i\to 0}$ pertenece a A. Si es así, no haga nada. De lo contrario reemplace v en A por $v_{i\to 0}$.

Por ejemplo $T_5(A)$ solo cambia el primer vector de A:

$$\begin{matrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{matrix} .$$

Es claro que T es inyectiva: $|T_i(A)| = |A|$.

Un poco más sutil es ver que para todo subconjunto de coordenadas $S \in \{1, \ldots, n\}$ se tiene que $t_S(T_i(A)) \leq t_S(A)$ (Ejercicio).

Si A es hereditario $T_i(A) = A$ para todo $i \in \{1, \ldots, n\}$.

Demostración. $T_n(T_{n-1}(\cdots T_1(A)\cdots))$ es conjunto buscado. Notar que si A es hereditario, $T_n(T_{n-1}(\cdots T_1(A)\cdots)) = A$. □

Este teorema implica inmediatamente al teorema 2.2 (ejercicio).

El siguiente resultado de Kleitman (1966) sobre la intersección de conjuntos hereditarios tiene numerosas aplicaciones y generalizaciones.

Teorema 2.5. *Sean A, B dos subconjuntos hereditarios de $\{0,1\}^n$. Entonces*

$$|A \cap B| \geq \frac{|A||B|}{2^n}.$$

Demostración. Aplicaremos inducción sobre n. Los casos $n = 0$ y $n = 1$ son triviales. Dado $\omega \in \{0, 1\}$, definimos

$$A_\omega := \{(a_1, \ldots, a_{n-1}) \ : \ (a_1, \ldots, a_{n-1}, \omega) \in A\}$$

y

$$B_\omega := \{(b_1, \ldots, b_{n-1}) \ : \ (b_1, \ldots, b_{n-1}, \omega) \in B\}.$$

Llamaremos $\alpha_\omega := |A_\omega|$ y $\beta_\omega := |B_\omega|$.

Entonces

$$\begin{aligned} |A \cap B| &= |A_0 \cap B_0| + |A_1 \cap B_1| \\ &\geq \frac{\alpha_0\beta_0 + \alpha_1\beta_1}{2^{n-1}} \\ &= \frac{(\alpha_0 + \alpha_1)(\beta_0 + \beta_1)}{2^n} + \frac{(\alpha_0 - \alpha_1)(\beta_0 - \beta_1)}{2^n}. \end{aligned}$$

Ya que ambos conjuntos A y B son hereditarios (o cerrados hacia abajo), tenemos que $A_1 \subset A_0$ y $B_1 \subseteq B_0$, lo que implica que

$$(\alpha_0 - \alpha_1)(\beta_0 - \beta_1) \geq 0.$$

El teorema se sigue del hecho que $|A| = \alpha_0 + \alpha_1$ y $|B| = \beta_0 + \beta_1$. □

2.3. Ortogonalidad. La independencia lineal no es la única forma de obtener cotas superiores (usando algebra lineal). Si los miembros de una familia $\mathcal{F}$ puede ser asociada con los elementos de un espacio vectorial ${\mathbb{F}_q}^m$, entonces $|\mathcal{F}| \leq q^m$. Si somos afortunados, los vectores asociados puede que sean ortogonales a algún subespacio de dimensión d, y como $\dim(U) + \dim(U^\perp) = dim(V)$, podemos mejorar nuestra cota: $|\mathcal{F}| \leq q^{m-d}$.

Dadas dos familias $\mathcal{A}$ y $\mathcal{B}$ de subconjuntos de $[n]$, una pregunta habitual en combinatoria es que tan grande puede llegar a ser $|\mathcal{A}||\mathcal{B}|$. Si no sabemos nada de las familias, este número pude ser tan grande como 2^{2n}. Si sabemos algo, por ejemplo que las familias son monótonas crecientes (o monótonas decrecientes), i.e. cerradas hacia arriba o hacia abajo, el teorema de Kleitman nos da la siguiente cota no trivial:

$$|\mathcal{A}||\mathcal{B}| \leq 2^n |\mathcal{A} \cap \mathcal{B}|.$$

Si además sabemos que la paridad de las intersecciones se mantiene constante, podemos obtener una cota aún mejor.

Teorema 2.6 (Ahlswede-El Gamal-Pang 1984)**.** *Sean $\mathcal{A}$ y $\mathcal{B}$ dos familias de subconjuntos de $[n]$ con la propiedad que $|A \cap B|$ es par para todo $A \in \mathcal{A}$ y $B \in \mathcal{B}$. Entonces $|\mathcal{A}||\mathcal{B}| \leq 2^n$.*

Vamos a dar la demostración de Delsarte-Piret de 1985.

Demostración. A cada subconjunto de $[n]$ le asociamos su vector de incidencia, estos pueden ser vistos como elementos de ${\mathbb{F}_2}^n$. Sean U y V los conjuntos de vectores de incidencias de correspondientes a las familias de subconjuntos $\mathcal{A}$ y $\mathcal{B}$. Observe dado $u \in U$ y $v \in V$, tenemos que

$$\langle u, v \rangle = 0.$$

Luego los espacios $span(U)$ y $span(V)$ son ortogonales, por lo que

$$\dim span(U) + span(V) \leq n.$$

Pues el producto escalar registra la cardinalidad de la intersección de los conjuntos representados por u y v respectivamente. Entonces

$$|\mathcal{A}||\mathcal{B}| = |U||V| \leq |span(U)||span(V)| \leq 2^{\dim(span(U))+\dim(span(V))} \leq 2^n. \tag{2.1}$$

□

2.4. Ejercicios.

1. Sean A y B son dos subconjuntos hereditarios de $\{0,1\}^n$. Cuáles de los siguientes son hereditarios:
   a) $A \cap B$,
   b) $A \cup B$,
   c) $A \triangle B$,
   d) $A \times B$.
2. Sea $A \subset \{0,1\}^n$, definamos $t_s(A) = \max t_S(A)$ sobre todos los $S \subset \{1, \ldots, n\}$ con $|S| = s$.
   a) Si $|A| \leq n$ entonces $t_{n-1}(A) = |A|$.
   b) Si $|A| \leq \lceil \frac{3}{2} n \rceil$ entonces $t_{n-1}(A) \geq |A| - 1$.
3. Probar el teorema de Ahlswede-El Gamal-Pang para intersección impar. Sean $\mathcal{A}$ y $\mathcal{B}$ dos familias de subconjuntos de $[n]$ con la propiedad que $|A \cap B|$ es impar para todo $A \in \mathcal{A}$ y $B \in \mathcal{B}$. Entonces $|\mathcal{A}||\mathcal{B}| \leq 2^n$. ¿Se puede mejorar la cota a 2^{n-1}?

3. Método Polinomial

3.1. Lema de DeMillo-Lipton-Schwartz-Zippel. El método polinomial está basado en diferentes extensiones del teorema factor para polinomios en una variable, al caso de polinomios en varias variables:

1. Todo polinomio (en una variable) de grado d tiene a lo más d raíces.
2. Para todo conjunto $S \subset \mathbb{F}$ existe un polinomio no-nulo f (con coeficientes en $\mathbb{F}$) de grado a lo más $|S|$ tal que $f(x) = 0$ para todo $x \in S$.

Estos resultados nos permiten obtener cotas para el tamaño de un conjunto S dado. Si hallamos un polinomio que se anula sobre S, entonces el grado del polinomio da una cota superior para la cardinalidad de S. Si todas las raíces de un polinomio pertenecen al conjunto S, entonces el grado del polinomio da una cota inferior para la cardinalidad de S.

Repasaremos primero algunos hechos sobre polinomios en cuerpos finitos de una y varias variables.

Dado un anillo conmutativo $\mathbb{R}$, un polinomio en una indeterminada es una expresión de la forma:

$$p(x) = a_0 + a_1 x + \cdots + a_t x^t$$

donde los coeficientes $a_0, a_1, \ldots, a_t \in \mathbb{R}$, y t es un entero no-negativo, el grado del polinomio.

$\mathbb{R}[x]$ denota el conjunto de todos los polinomios con coeficientes en el anillo conmutativo $\mathbb{R}$.

Todo polinomio $p(x)$ con coeficientes en el anillo conmutativo $\mathbb{R}$ define una función de $\mathbb{R}$ sobre $\mathbb{R}$, mapeando $r \in \mathbb{R}$ a $p(r)$ (mapeo evaluación): Así, si $p(x) = 3x + 4x^3$ en $\mathbb{Z}/8\mathbb{Z}$ tenemos que

$$p(2) = 3 \cdot 2 + 4 \cdot 2^3 = 6 + 4 \cdot 0 = 6.$$

En el anillo $\mathbb{Z}/8\mathbb{Z}$.

Pero los polinomios, no son funciones. Esto es debido a la definición de igualdad entre dos polinomios.

Dos polinomios

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

y

$$q(x) = b_0 + b_1 x + \cdots + b_m x^m$$

son iguales si y sólo si los coeficientes en cada potencia de ambos son iguales:

- $n = m$,
- $a_0 = b_0, a_1 = b_1, \ldots, a_n = b_n$.

Así en $\mathbb{Z}/2\mathbb{Z}$, los polinomios

$$p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

y

$$q(x) = 1 + x^3$$

son iguales si (y sólo si) $a_0 = a_3 = 1$ y $a_1 = a_2 = 0$.

Por otro lado dos funciones f y g de A en B, son iguales si para todo $a \in A$ se tiene que $f(a) = g(a)$.

Dos polinomios iguales también son iguales como funciones, pero puede ocurrir que dos polinomios sean iguales como funciones, pero no como polinomios. Por ejemplo en $\mathbb{Z}/2\mathbb{Z}$, los polinomios

$$p(x) = 1 + x$$

y

$$q(x) = 1 + x^3.$$

Son claramente diferentes como polinomios, pero vistos como funciones son idénticos:

$$p(0) = 1 = q(0), \ \mathbf{y} \ p(1) = 0 = q(1).$$

Este fenómeno no ocurre si el anillo sobre el que se definen los polinomios es un cuerpo infinito (para polinomios con coeficientes sobre un cuerpo infinito igualdad coeficiente a coeficiente es equivalente a igualdad como funciones).

De ahora en más trabajaremos con un cuerpo $\mathbb{F}$ fijo. El símbolo $\mathbb{F}[x_1, \ldots, x_n]$ denota el anillo de polinomios en n indeterminadas sobre el cuerpo $\mathbb{F}$ (decir "sobre el anillo/cuerpo" es equivalente a decir "a coeficientes en el anillo/cuerpo").

Un monomio de grado t (donde t es un entero no-negativo) es una expresión de la forma

$$x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$$

donde cada t_i es un entero no-negativo tal que

$$t_1 + t_2 + \cdots + t_n = t.$$

Observaciones:

- El único monomio de grado 0 (cero) es la constante 1.
- El polinomio **nulo** es el polinomio cuyos coeficientes son todos nulos.
- Hay $\binom{n+t-1}{t}$ monomios en n variables de grado t.
- Todo polinomio de $\mathbb{F}[x_1, \ldots, x_n]$ es una combinación lineal de monomios con coeficientes tomados de $\mathbb{F}$.
- Sea $p \in \mathbb{F}[x_1, \ldots, x_n]$, el grado de p, denotado $\deg(p)$, es el máximo grado de sus monomios con coeficientes no-nulos.
- Un polinomio se dice **homogéneo** si todos sus monomios con coeficientes no-nulos tienen el mismo grado.
- Una punto $a \in \mathbb{F}^n$ tal que $p(a) = 0$ es una **raíz** del polinomio $p \in \mathbb{F}[x_1, \ldots, x_n]$.
- Diremos que un polinomio $p \in \mathbb{F}[x_1, \ldots, x_n]$ **se anula sobre** un conjunto $E \subset \mathbb{F}^n$ si para todo elemento $e \in E$ tenemos que $p(e) = 0$.

Ocurre que con polinomios en varias variables sobre cuerpos infinitos podemos perder la relación entre el grado del polinomio y el número de raíces, por ejemplo

$$p(x, y) = x^2 + y^2 - 1$$

visto como polinomio de $\mathbb{R}[x, y]$ tiene infinitas raíces.

El siguiente ejemplo muestra que aún sobre cuerpos finitos la relación entre grado y número de raíces es no trivial para polinomios en varias indeterminadas. Consideremos el polinomio

$$x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$$

sobre $\mathbb{F}_2^5$, donde $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Este polinomio de grado 2 tiene 16 raíces:

0	0	0	0	0		0	1	0	1	0
0	0	0	0	1		0	1	0	0	1
0	0	0	1	0		0	0	1	0	1
0	0	1	0	0		0	0	1	1	1
0	1	0	0	0		0	1	1	1	0
1	0	0	0	0		1	1	1	0	0
1	0	1	0	0		1	1	0	0	1
1	0	0	1	0		1	0	0	1	1

mientras que el polinomio

$$x_1^2 - x_1$$

se anula sobre todo $\mathbb{F}_2^5$.

Los siguientes lemas recuperan la relación entre grado de un polinomio y número de raíces para polinomios en varias indeterminadas.

Lema 3.1. *Dado un conjunto $E \subset \mathbb{F}^n$ de tamaño*

$$|E| < \binom{n+d}{d}.$$

Existe un polinomio no-nulo $p \in \mathbb{F}[x_1, \ldots, x_n]$ de grado a lo más d que se anula sobre E.

Haremos algunas acotaciones antes de proceder a demostrar el lema. Como

$$\binom{n+d}{d} \longrightarrow \infty, \text{ cuando } d \to \infty$$

siempre podremos hallar un d (relativamente pequeño) tal que $|E| < \binom{n+d}{d}$. Por ejemplo, si tomamos los siguientes 5 puntos de $\mathbb{F}_2^5$,

$$\begin{array}{ccccc} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{array} .$$

El lema nos garantiza que existe un polinomio de grado 1 que se anula sobre estos puntos, pues

$$5 < 6 = \binom{6}{1} = \binom{5+1}{1}.$$

Por ejemplo $p(x_1, \ldots, x_5) = x_1 + x_3 + 1$.

Ahora daremos la demostración del lema 3.1.

Demostración. Denotemos por V_d al espacio vectorial de todos los polinomios de $\mathbb{F}[x_1, \ldots, x_n]$ de grado a lo más d. El conjunto de todos los monomios de grado a lo más d forma una base de V_d y como hay:

$$\sum_{k=0}^{d} \binom{n+k-1}{k} = \binom{n+d}{d}$$

monomios distintos de grado a lo más d tenemos que la dimensión de

$$\dim(V_d) = \binom{n+d}{d}.$$

Por otro lado, el espacio $\mathbb{F}_E$de todas las funciones $g : E \to \mathbb{F}$ tiene dimensión

$$|E| < \binom{n+d}{d}.$$

Por lo tanto tenemos que el mapeo (lineal) evaluación:

$$f \to (f(a))|_{a \in E}$$

de V_d en $\mathbb{F}^E$ no es inyectivo. Así al menos dos polinomios f_1 y f_2 de v_d deben ser mapeados al mismo elemento de $\mathbb{F}^E$. Así el polinomio $f = f_1 - f_2$ pertenece a V_d y es mapeado al elemento nulo de $\mathbb{F}^E$, i.e., f se anula sobre E. □

Ahora daremos la generalización al caso de polinomios en varias indeterminadas del hecho que un polinomio (en una variable) de grado d tiene a lo más d raíces.

Lema 3.2. *Todo polinomio $p \in \mathbb{F}[x_1, \ldots, x_n]$ de grado d, donde $\mathbb{F}$ es un cuerpo finito con q elementos, tiene a lo más dq^{n-1} raíces.*

Por ejemplo, el lema nos garantiza que el polinomio $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$ sobre $\mathbb{F}_2^5$ tienen a lo más 16 raíces, y que el polinomio $x_1^2 + 2$ sobre $\mathbb{F}_3^2$ tiene a lo más 6 raíces.

La demostración que daremos sigue a Dvir (2009) y Moshkovitz (2010).

Demostración. Sea $q = |\mathbb{F}|$, sin pérdida de generalidad podemos asumir que:

- $n \geq 2$,
- $1 \leq d \leq q$.

La demostración es por reducción al caso $n = 1$. Escribamos $f = g + h$ donde

- g es homogénea de grado d,
- h solo contiene monomios de grado estrictamente menor que d.

Cómo f no es el polinomio nulo, existe algún $w \in \mathbb{F}^n$, $w \neq 0$, tal que $g(w) = 0$ (recordar que g es homogéneo). Para cada $u \in \mathbb{F}^n$ definimos la recta que pasa por u en la dirección w:

$$L_u := \{u + tw \ : \ t \in \mathbb{F}\}.$$

Un par de observaciones:

- $L_u \cap L_v = \emptyset$ si $v \notin L_u$,
- $|L_u| = q$.

Por lo que podemos particionar a $\mathbb{F}^n$ en $q^n/q = q^{n-1}$ rectas.

Ahora mostraremos que sobre cada recta L_u puede haber a lo más d raíces de f. Para cada $u \in \mathbb{F}^n$, la función

$$p_u(t) := f(u + tw)$$

es un polinomio en la variable t de grado d, de hecho el coeficiente de t^d es $g(w) \neq 0$. Cómo $p_u(t)$ tiene a lo más d raíces, tenemos que el polinomio f puede tener a lo más d raíces en cada L_u. Como $\mathbb{F}^n$ fue particionado en q^{n-1} rectas, tenemos que f no puede tener más de dq^{n-q} raíces. □

DeMillo y Lipton (1978), Zippel (1979) y Schwartz (1980) de forma independiente probaron la siguiente generalización.

Lema 3.3 (DeMillo-Lipton-Schwartz-Zippel)**.** *Para todo conjunto $S \subset \mathbb{F}$ tal que $|S| > d$, se tiene que todo polinomio $f \in \mathbb{F}[x_1, \ldots, x_n]$ de grado d puede tener a lo más $d|S|^{n-1}$ raíces en S^n.*

Demostración. Suponga que f es un polinomio no nulo. La demostración es por inducción sobre n, el número de variables de f.

Para $n = 1$ el lema es trivialmente verdadero.

Ahora analicemos el caso $n \geq 2$. Para hacerlo reescribamos f en términos de las potencias de x_n:

$$f = f_0 + f_1 x_n + f_2 x_n^2 + \cdots + f_t x_n^t$$

donde $f_0, f_1, \ldots, f_t$ son polinomios en las $n - 1$ variables $x_1, x_2, \ldots, x_{n-1}$, el polinomio f_t no es el polinomio nulo, y $t \leq d$.

Ahora vamos a estimar (por arriba) el número de puntos $(a, b) \in S^{n-1} \times S$, tales que $f(a, b) = 0$. Analizaremos dos casos

> Caso 1. $f_t(a) = 0$. Como f_t no es el polinomio nulo, y tiene grado a lo más $d - t$, por hipótesis inductiva, este polinomio se anula a lo más en $(d - t)|S|^{n-2}$ puntos de S^{n-1}. Por lo tanto, en este caso, hay a lo más $(d - t)|S|^{n-1}$ puntos de $(a, b) \in \Sigma^{n-1} \times S$ para los cuales $f(a, b) = 0$ y $f_t(a) = 0$.
> Caso 2. $f_t(a) \neq 0$. Para todo punto $a \in S^{n-1}$ tal que $f_t(a) \neq 0$, el polinomio $f(a, x_n)$ es un polinomio en una variable de grado t, y no es el polinomio nulo. Por o tanto tiene a lo más t raíces. Como a lo suma hay $|S|^{n-1}$ de tales puntos a, el número de puntos $(a, b) \in S^{n-1} \times S$ para los cuales $f(a, b) = 0$ y $f_t(a) \neq 0$, es a lo más $t|s|^{n-1}$.

Por lo tanto, a lo más hay

$$(d-t)|S|^{n-1} + t|S|^{n-1} = d|S|^{n-1}$$

puntos de $(a,b) \in S^n$ para los cuales $f(a,b) = 0$. □

3.2. Solución del problema de Kakeya en cuerpos finitos. La conjetura de Kakeya es uno de los problemas no resueltos favoritos de Terence Tao en teoría geométrica de la medida. Esta conjetura desciende del problema de la aguja, planteado por Kakeya en 1971:

¿Cuál es la menor área en el plano requerida para rotar completamente (i.e. 360° de forma continua una aguja de longitud unitaria (y grosor cero)?

Por ejemplo, es claro que podemos hacer esto en un círculo de diámetro uno, y por lo tanto de área $\pi/4$. Pero al usar una deltoide solo usamos un área de $\pi/8$. En 1928, Besicovitch demostró que de hecho se puede rotar una aguja unitaria usando sólo una cantidad arbitrariamente pequeña de área (en realidad resolvió otro problema, pero su trabajo aplica). Este hecho contraintuitivo, motivó la definición de lo que conocemos como **conjunto de Kakeya-Besicovitch**: es un conjunto que contiene un segmento unitario en cada dirección.

En 1981, Davies demostró que existen conjuntos de Kakeya-Besicovitch con medida de Lebesgue cero, pero los cuales seguían siendo objetos esencialmente bi-dimensionales: tienen dimensión de Hausdorff 2 y dimensión de Minkowski 2.Esto llevo a la siguiente conjetura en mayores dimensiones:

Conjetura 3.4 (de Kakeya:)**.** *Un conjunto de Kakeya-Besicovitch en $\mathbb{R}^n$ tiene dimensión de Minkowski y dimensión de Hausdorff igual a n.*

En 1999, Wolff propuso el análogo de la conjetura de Kakeya sobre cuerpos finitos a fin de evitar los problemas técnicos asociados con las dimensiones de Minkowski y Hausdorff. Dado un cuerpo finito $\mathbb{F}$, definimos un **conjunto de Kakeya** como cualquier subconjunto K de $\mathbb{F}^n$ que contenga una línea en cada dirección, i.e., para cada vector $w \in \mathbb{F}^n$ existe un vector $v \in \mathbb{F}^n$ tal que la línea $L_{v,w} := \{v + tw \,:\, t \in \mathbb{F}\} \subset K$.

Conjetura 3.5 (Conjetura de Kakeya en cuerpos finitos, Wolff 1999)**.** *Sea $E \subset \mathbb{F}^n$ un conjunto de Kakeya. Entonces $|K| \geq c_n|\mathbb{F}|^n$, donde c_n es una constante positiva que depende sólo de n.*

En 2009, Dvir sorprendió a toda la comunidad matemática que trabajaba en el las diferentes conjeturas de Kakeya (Tao incluido), al usar el método polinomial para probar la conjetura de Kakeya en cuerpos finitos.

Lema 3.6. *Sea $f \in \mathbb{F}[x_1, \ldots, x_n]$ un polinomio de grado a lo más $q-1$ sobre un cuerpo finito $\mathbb{F}$ con $q = |\mathbb{F}|$ elementos. Si f se anula sobre un conjunto de Kakeya K, entonces f es el polinomio nulo.*

El argumento de Dvir es el siguiente.

Demostración. Supongamos que f no es el polinomio nulo. Reescribamos f de la forma

$$f = \sum_{i=0}^{d} f_i$$

donde $0 \leq d \leq q-1$ es el grado de f y cada f_i es la componente homogénea de grado i de f, por lo que f_d es no nula. Como f es no-nulo y se anula sobre K, tenemos que $d \neq 0$.

Tomemos una dirección arbitraria w de $\mathbb{F}^n$, i.e. $0 \neq w \in \mathbb{F}^n$. Como K es un conjunto de Kakeya, existe $v \in \mathbb{F}^n$ tal que la recta $L_{v,w} = \{v + tw \ : \ t \in \mathbb{F}\} \subset K$. Por lo tanto

$$f(v + tw) = 0$$

para todo $t \in \mathbb{F}$. Ahora miremos un poco más en detalle a $f(v + tw)$. Es un polinomio en t de grado a lo más $q - 1$ sobre el cuerpo $\mathbb{F}$ (pues es del mismo grado que f). Pero se anula sobre todo $\mathbb{F}$, por lo que no le queda otra que ser el polinomio nulo. Ahora el coeficiente que acompaña a t^d es $f_d(w)$, por lo tanto $f_d(w) = 0$. Esto demuestra que f_d se anula sobre todos los puntos de $\mathbb{F}^n$. Pero como

$$dq^{n-1} \leq (q-1)q^{n-1} < q^n.$$

Tenemos que por el lema 3.2 que el polinomio f_d debe ser el polinomio nulo, lo que es una contradicción. □

Teorema 3.7 (Dvir 2009)**.** *Sea $K \subset \mathbb{F}^n$ un conjunto de Kakeya. Entonces*

$$|K| \geq \binom{|\mathbb{F}| + n - 1}{n} \geq \frac{|\mathbb{F}|^n}{n!}.$$

Demostración. Supongamos que

$$|K| < \binom{|\mathbb{F}| + n - 1}{n}.$$

Por el lema 3.1, existe un polinomio no-nulo $F \in \mathbb{F}[x_1, \ldots, x_n]$ de grado a lo más $|\mathbb{F}| - 1$ que se anula sobre K, lo cual contradice el lema 3.6. □

3.3. Nullstellensatz Combinatorio de Alon. Consideremos el siguiente "teorema" bien conocido de cursos básicos:

Teorema 3.8. *Sea $f \in \mathbb{F}[x]$ un polinomio de grado t. Si $S \subset \mathbb{F}$ tal que $|S| \geq t + 1$, entonces existe $s \in S$ tal que $f(s) \neq 0$.*

El Nullstellensatz Combinatorio de Alon (1999) generaliza este resultado para el caso de varias variables.

Teorema 3.9 (Nullstellensatz Combinatorio)**.** *Sea $f \in \mathbb{F}[x_1, \ldots, x_n]$ de grado d. Suponga que los coeficientes del monomio de f*

$$x_1^{t_1} \cdots x_n^{t_n}$$

es no nulo y que

$$t_1 + \cdots + t_n = d.$$

Si $S_1, \ldots, S_n$ son subconjuntos finitos de $\mathbb{F}$ tales que $|S_i| \geq t_i + 1$, entonces existe un punto $s \in S_1 \times \cdots \times S_n$ para el cual $f(s) \neq 0$.

El Nullstellensatz Combinatorio también es una generalización del lema de DeMillo-Lipton-Schartz-Zippel.

Este resultado sigue del un caso especial del Nullstellensatz de Hilbert:

Teorema 3.10 (Nullstellensatz)**.** *Sea $f \in \mathbb{F}[x_1, \ldots, x_n]$ y $S_1, \ldots, S_n$ son subconjuntos finitos del cuerpo $\mathbb{F}$. Si $f(s) = 0$ para todo $s \in S_1 \times \cdots \times S_n$, entonces existen polinomios $h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ tales que*

$$\deg(h_i) \leq \deg(f) - |S_i|$$

y

$$f([x_1,\ldots,x_n) = \sum_{i=1}^{n} h_i([x_1,\ldots,x_n) \prod_{s\in S_i}(x_i - s).$$

Daremos la demostración de Alon (1999) del Nullstellensatz, la cual requiere del siguiente lema.

Lema 3.11. *Sea $f \in \mathbb{F}[x_1,\ldots,x_n]$. Supongamos que el grado de f como polinomio en x_i es a lo más t_i, y que tenemos subconjuntos $S_i \subset \mathbb{F}$ tales que $|S_i| \geq t_i+1$. Si $f(s) = 0$ para todo $s \in S_1 \times \cdots \times S_n$, entonces f es el polinomio nulo.*

Demostración. Es por inducción sobre n, el número de variables. Para $n = 1$ el lema establece que un polinomio en una variable de grado a lo más t_1 puede tener a lo sumo t_1 raíces distintas. Asumiendo que el lema vale para $n-1$, probaremos que vale para $n \geq 2$.

Dando un polinomio $f = f(x_1,\ldots,x_n)$ y conjuntos S_i que satisfagan las hipótesis del lema, reescribamos f como un polinomio en x_n:

$$f = \sum_{i=0}^{t_n} f_i(x_i,\ldots,x_{n-1})x_n^i$$

donde cada f_i es un polinomio en las $n-1$ variables $x_1,\ldots,x_{n-1}$, donde el grado en x_j es a lo más t_j. Para cada

$$(s_1,\ldots,s_{n-1}) \in S_1 \times \cdots \times S_{n-1}.$$

Consideremos el polinomio en una variable x_n dado por

$$f(s_1,\ldots,s_{n-1},x_n).$$

Por hipótesis tenemos que para todo $s \in S_n$ se cumple que

$$f(s_1,\ldots,s_{n-1},s) = 0.$$

Por lo tanto, $f(s_1,\ldots,s_{n-1},x)$ es el polinomio nulo. Esto implica que $f_i(s_1,\ldots,s_{n-1}) = 0$ para todo $(s_1,\ldots,s_{n-1}) \in S_1 \times \cdots \times S_{n-1}$. Luego, por hipótesis inductiva, f_i es el polinomio nulo para cada i, lo que implica que f es el polinomio nulo. □

Ahora procederemos dar la demostración de Alon del Nullstellensatz.

Demostración del Teorema 3.10, Nullstellensatz, Alon (1999). Definimos para cada i

$$d_i = |S_i| - 1$$

y consideremos los polinomios

$$g_i(x_i) := \prod_{s\in S_i}(x_i - s) = x_i^{d_i+1} - \sum_{j=0}^{d_i} a_{ij}x_i^j.$$

Observe que si $s \in S - i$, entonces $g_i(s) = 0$, lo que implica que

$$s^{d_i+1} = \sum_{j=0}^{d_i} a_{ij}x_i^j.$$

Esto sugiere utilizar la siguiente identidad para reducir el "x_i-grado"

$$x_i^{d_i+1} = \sum_{j=0}^{d_i} a_{ij}x_i^j. \tag{3.1}$$

Sea $\bar{f}$ el polinomio que se obtiene a partir de f, escribiendo a f como combinación lineal de monomios y reemplazando, las veces que haga falta, cada ocurrencias de potencial altas: $x_i^{t_i}$ con $t_i > d$ $(1 \leq i \leq n)$; por combinaciones lineales de potencias más pequeñas de x_i, usando la relación 3.1.

Miremos con atención al polinomio $\bar{f}$. El grado de $\bar{f}$ es a lo más d_i en x_i para cada $1 \leq i \leq n$. Tras meditarlo un rato, nos damos cuenta que $\bar{f}$ puede ser obtenido a partir de f restándole productos de la forma $h_i g_i$, donde

$$\deg(h_i) \leq \deg(f) - \deg(g_i) = \deg(f) - |S_i|$$

Por lo tanto

$$\bar{f}(x) = f(x) - \sum_{i=1}^{n} h_i(x) g_i(x). \tag{3.2}$$

Además como para $s \in S_1 \times \cdots \times S_n$ vale la relación 3.1, tenemos que

$$\bar{f}(s) = f(s) = 0.$$

Luego, por el lema 3.11, tenemos que $\bar{f}(s) = 0$ para todo $s \in \mathbb{F}^n$. Esto, junto con 3.2, implican que $f = \sum_{i=1}^{n} h_i g_i$. □

Ahora demostraremos el Nullstellensatz Combinatorio de Alon, 1999.

Demostración del Teorema 3.9. Sin pérdida de generalidad podemos asumir $|S_i| = t_i + 1$ para cada i. Supongamos que el resultado es falso, i.e., que para todo $t \in S_1 \times \cdots \times S_n$ tenemos que $f(t) = 0$. Definimos

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

Sean $h_1, \ldots, h_n$ los polinomios que nos da el Nullstellensatz (teorema 3.10), luego:

$$\deg(h_i) \leq \deg f - \deg(g_i) = \deg(f) - t_i - 1 \tag{3.3}$$

y además

$$f(x) = \sum_{i=1}^{n} h_i(x) g_i(x_i).$$

Lo que se puede reescribir de la siguiente forma:

$$f(x) = \sum_{i=1}^{n} x_i^{t_i+1} h_i(x) + (\text{términos de grado } < \deg(f)).$$

Por hipótesis, el coeficiente de $\prod_{i=1}^{n} x_i^{t_i}$ del lado izquierdo de la ecuación anterior es no cero, pero es imposible tener tal monomio del lado derecho, lo que nos da una contradicción. □

Para finalizar estas notas daremos una aplicación del Nullstellensatz Combinatorio a la teoría de números aditiva.

Dados dos conjuntos A y B de elementos de un cuerpo $\mathbb{F}$, definimos su **conjunto suma**

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

Por ejemplo es $\mathbb{Z}/5\mathbb{Z}$, si $A = \{2, 4\}$ y $B = \{2, 3\}$ tenemos que

$$A + B = \{0, 1, 2, 4\}.$$

Una pregunta relevante es si el tamaño de A y B nos dan un indicio de que del tamaño mínimo que puede tener $A + B$. El teorema de Cauchy-Davenport da una respuesta.

Teorema 3.12 (Cauchy-Davenport). *Si p es un primo, y A y B son dos subconjuntos no-vacíos de $\mathbb{Z}_p$, entonces*

$$|A+B| \geq \text{mín}\{p, |A|+|B|-1\}.$$

Usaremos el Nullstellensatz Combinatorio para realizar la prueba.

Demostración. Si $|A|+|B| > p$ es resultado es trivial, pues para todo $x \in \mathbb{Z}_p$ los conjuntos A y $x-B$ tienen intersección no vacía, lo que implica que $A+B=\mathbb{Z}_p$.

Asumamos entonces que $|A|+|B| \leq p$. La demostración procede por reducción al absurdo: supongamos que

$$|A+B| \leq |A|+|B|-2.$$

Sea $C \subset \mathbb{Z}_p$ tal que $A+B \subset C$ y $|C| = |A|+|B|-2$.

Definamos el polinomio

$$f(x,y) = \prod_{c \in C}(x+y-c).$$

Por definición,

$$f(a,b) = 0 \text{ para todo } (a,b) \in A \times B.$$

Ahora, llamando $t_1 = |A|-1$ y $t_2 = |B|-1$, notamos que el coeficiente de $x^{t_1}y^{t_2}$ en f es:

$$\binom{t_1+t_2}{t_1} = \binom{|A|+|B|-2}{|A|-1}$$

el cual es no cero en $\mathbb{Z}_p$, pues $|A|+|B|-2 < p$. Aplicando el Nullstellensatz Combinatorio obtenemos un punto $(a,b) \in A \times B$ para el cual $f(a,b) \neq 0$, contradicción. □

3.4. Ejercicios.

1. Sea p un primo impar. Consideremos un cuerpo $\mathbb{F}_p$. Entonces para todo $t \leq p-2$

$$\sum_{x \in \mathbb{F}_p} x^t = 0$$

en $\mathbb{F}_p$.

2. Demostrar el Lema de DeMillo-Lipton-Schwartz-Zippel usando el Nullstellensatz Combinatorio de Alon.
3. Probar el teorema de Olson usando el Nullstellensatz Combinatorio de Alon: Sean $(a_1,b_1),\ldots,(a_n,b_n)$ una sucesión de elementos en $\mathbb{Z}_p$ con $n \geq 2p-1$. Entonces existe un subconjunto no vacío $A \subset [n]$ tal que

$$\sum_{i \in A}(a_i,b_i) = (0,0).$$

4. Dos números distintos son escritos sobre los vértices de un 100-agono convexo. Probar que siempre podemos remover un número de cada vértice de forma en vértices adyacentes no queden números iguales.
5. Sea n un entero positivo. Consideremos el conjunto:

$$S = \{(x,y,z)\,|x,y,z \in [n], (x,y,z) \neq (0,0,0)\}.$$

Determinar el número más pequeño de planos tales que su unión contenga a S pero no al $(0,0,0)$.

6. Probar el teorema de Chevalley-Warning usando el Nullstellensatz Combinatorio: Sea p un primo, y $f_1, \ldots, f_m$ polinomios en $\mathbb{F}_p[x_1, \ldots, x_n]$. Si
$$\sum_{i=1}^{m} \deg(f_i) < n$$
entonces el número de ceros comunes de $f_1, \ldots, f_m$ es divisible por p.
7. Demostrar el teorema de Erdös-Ginzburg-Ziv (1961) a la Alon (i.e. usando el teorema de Chevalley-Warning, ver ejercicio 6): Cualquier sucesión de $2n-1$ enteros contiene una subsucesión de longitud n, tal que su suma es divisible por n.

Referencias

[1] Alon, Noga (1999): *Combinatorial Nullstellensatz*, Comb. Prob. Comput. 8, 7–29.
[2] Babai, L and Frankl, P (1992): *Linear Algebra Methods in Combinatorics*, Preliminary Version 2, University of Chicago.
[3] Brualdi, R (2010): *Introductory Combinatorics*, 5th Edition. Pretince Hall.
[4] Jukna, Stasys (2011): *Extremal Combinatorics*. 2nd Edition. Springer.
[5] Tait, M. (2013): *My favorite application using eigenvalues: Eigenvalues and the Graham-Pollak Theorem*. Personal Comunication

Departamento de Matemáticas, Facultad de Ciencias Físico Matemáticas y Naturales, Universidad Nacional de San Luis