AGRA 2015: COMBINATORIA ADITIVA, PRIMERA PARTE CONJUNTOS SUMA, EL FENÓMENO SUMA-PRODUCTO Y EL MÉTODO POLINOMIAL

J. WOLF

Índice

1. Introducción

En esta parte del curso se estudiarán los primeros resultados en combinatoria aditiva. Dicha área se inició en el contexto del estudio de la estructura de conjuntos de enteros en relación a las operaciones de suma y producto. En esta introducción a la materia, mostraremos que muchas de las cuestiones planteadas en los enteros se pueden considerar también en grupos abelianos y también en cuerpos finitos.

El desarrollo espectacular en los últimos años de esta área de investigación ha demostrado que no sólo se ocupa del estudio de problemas aislados, sino que ha jugado un papel

Date: Última actualización: el 20 noviembre 2015.

importante como punto de interacción de diversas áreas de las matemáticas. En esta primera parte usaremos especialmente técnicas combinatorias, geométricas y algebraicas, y ya más adelante en el curso se mostrará el uso de técnicas probabilísticas, analíticas y procedentes de la teoría de grafos. Finalmente destacar las conexiones íntimas de esta área con otros temas que se tratarán en esta escuela, como son los expansores o el análisis armónico mediante sus conexiones con el denominado problema de Kakeya.

2. La estructura de conjuntos suma

En combinatoria aditiva investigamos la estructura de conjuntos bajo la operación "+".[1] Dados conjuntos A y B en un grupo conmutativo, podemos definir el *conjunto suma* $A + B := \{a + b : a \in A, b \in B\}$. Es fácil ver que este conjunto suma tiene tamaño mayor o igual que máx$\{|A|, |B|\}$, y que dicho cardinal puede llegar a ser $|A||B|$ cuando todas la sumas son distintas.

En los enteros, grupo donde se inició el estudio de estas cuestiones en los años 60, observamos que el cardinal de $A + A$ es mínimo, por ejemplo, cuando A es una progresión aritmética (en este caso se puede calcular $|A+A| = 2|A|-1$). De manera similar, se observa que una progresión geométrica, por ejemplo, tiene un conjunto suma muy grande. [2]

En el lema siguiente mostramos que todo conjunto A cuyo conjunto suma tiene tamaño $2|A| - 1$ es una progresión aritmética.

Lema 2.1. *Sea $A \subseteq \mathbb{Z}$ un conjunto finito. Entonces $|A + A| \geq 2|A| - 1$, con igualdad si y solo si A es una una progresión aritmética.*

Demostración: Escribamos el conjunto A como una sucesión finita $a_1, \ldots, a_n$, escrita en orden creciente. Entonces

$$a_1 + a_1 < a_1 + a_2 < a_1 + a_3 < a_1 + a_4 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < a_n + a_n.$$

Por lo tanto, se deduce que hay como mínimo $2|A| - 1$ elementos distintos en el conjunto suma $A+A$. Observar que hubiera sido igualmente lícito el uso de la cadena de desigualdades

$$a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < a_2 + a_3 < \ldots < a_2 + a_n < a_3 + a_n < a_4 + a_n < \ldots < a_n + a_n.$$

[1] No podemos dar la historia completa de este campo de investigación, pero sugerimos al lector el libro [Nat10] para un tratamiento extenso de la teoría clásica.

[2] Es un primer indicio del hecho que las operaciones de adición y multiplicación no son compatibles. Veremos con más detalle este fenómeno en el Capítulo 3.

En el caso extremo, es decir cuando $|A+A| = 2|A|-1$, las dos cadenas presentadas deben ser idénticas. Concluímos pues que $a_2 + a_i = a_1 + a_{i+1}$ para $i = 2, \dots, n-1$, lo que obliga al conjunto A a ser una progresión aritmética. □

Ejercicio 2.2. *Sean $A, B \subset \mathbb{Z}$ conjuntos finitos verificando $|A+B| = |A| + |B| - 1$. Demostrar que A y B son progresiones aritméticas con la misma diferencia.*

Indicación: *El caso $|A| = |B|$ es más fácil.*

Como segundo ejemplo estudiaremos el mismo problema en un grupo cíclico módulo un primo p, que denotamos por $\mathbb{Z}_p$. Como ejercicio de calentamiento vamos a mostrar que cuando el tamaño de $A \subseteq \mathbb{Z}_p$ es mayor que la mitad del cardinal del grupo $\mathbb{Z}_p$, entonces el conjunto suma $A + A$ cubre todo el grupo.

Ejercicio 2.3. *Sea p un número primo, y sean $A, B \subseteq \mathbb{Z}_p$ conjuntos tales que $|A|+|B| > p$. Demostrar que $A + B = \mathbb{Z}_p$.*

El siguiente es un teorema clásico que modela la versión modular del Lema 2.1.

Teorema 2.4 (Teorema de Cauchy-Davenport)**.** *Sean $A, B \subseteq \mathbb{Z}_p$. Entonces*

$$|A+B| \geq \min(p, |A| + |B| - 1).$$

Demostración: Sin pérdida de generalidad suponemos que $0 \in B$. Nótese que el teorema se cumple cuando $|A| + |B| > p$ (ver el Ejercicio 2.3), pero también trivialmente cuando $|A| = 1$ o $|B| = 1$. Supongamos entonces que los conjuntos A y B son tales que $|A| \geq 2, |B| \geq 2$, $|A| + |B| < p - 1$, pero $|A + B| < |A| + |B| - 1$. Elegimos conjuntos A y B con estas propiedades tales que el tamaño de B es mínimo.

Nuestro objetivo es construir conjuntos A', B' que satisfagan las mismas desigualdades, pero tal que $|B'| < |B|$. Primero observamos que, dado que $|B| \geq 2$, existe un elemento $b \in B, b \neq 0$. Si $a + b \in A$ para todo $a \in A$, entonces $a + jb \in A$ para todo $j = 0, 1, 2, \dots$. Pero en este caso $A \supseteq \{a + jb : j = 0, 1, 2 \dots\} = \mathbb{Z}_p$, lo que es imposible dado que $\mathbb{Z}_p \supseteq A \neq \mathbb{Z}_p$. En consecuencia existe $a^* \in A$ tal que $a^* + b \notin A$, y entonces $b \notin A - a^*$. Consideramos los conjuntos

$$A(a^*) = A \cup (B + a^*) \quad \text{and} \quad B(a^*) = B \cap (A - a^*)$$

(estos conjuntos $A(a^*)$ y $B(a^*)$ se conocen como la *e-transformada* de *Dyson* de los conjuntos A y B). Observamos que $b \notin B(a^*)$, y en consecuencia $|B(a^*)| < |B|$. Veamos ahora una propiedad muy útil para nuestra prueba:

Afirmación 2.5. *Se cumple la igualdad* $|A| + |B| = |A(a^*)| + |B(a^*)|$.

Demostración la Afirmación: La demostración es la siguiente:

$$|A(a^*)| - |A| = |A(a^*) \setminus A| = |a^* + (B \setminus B(a^*))| = |B \setminus B(a^*)| = |B| - |B(a^*)|.$$

□

Esto implica que

$$|A(a^*) + B(a^*)| \leq |A + B| < |A| + |B| - 1 = |A(a^*)| + |B(a^*)| - 1,$$

donde la segunda desigualdad se debe a la hipótesis, y la última igualdad se deduce de la Afirmación 2.5. Hemos llegado pues a la contradicción deseada. □

Para concluir esta sección preliminar estudiaremos ahora el caso de un espacio vectorial de dimensión finita n (pero arbitrariamente grande) sobre un cuerpo finito de característica p. Como veremos varias veces en este curso, el grupo $\mathbb{F}_p^n$ nos sirve a menudo como modelo que nos permitirá luego atacar problemas sobre la estructura de conjuntos de enteros (que pueden ser más complejos desde el punto de vista técnico).

Un ejercicio simple es demostrar que un conjunto $A \subseteq \mathbb{F}_p^n$ verifica $A+A = A$, y entonces $|A + A| = |A|$, si y solo si A es un subespacio (posiblemente afín) de $\mathbb{F}_p^n$. Un ejercicio un poco más avanzado muestra que incluso si relajamos la condición sobre el cardinal del conjunto suma, el conjunto A sigue pareciéndose a un subespacio en el sentido siguiente:

Ejercicio 2.6. *Sea p un número primo, y sea $A \subseteq \mathbb{F}_p^n$ un conjunto tal que $|A+A| \leq K|A|$ con $K < 3/2$. Demostrar que existe un subespacio (posiblemente afín) V de $\mathbb{F}_p^n$ que contiene A cumpliendo que $|A| \geq 2|V|/3$.*

En general, para cualquier grupo abeliano G y subconjunto finito A de G, denotamos por K la menor constante tal que $|A+A| \leq K|A|$. Esta constante la llamamos la *constante de doblamiento* de A. En la siguiente sección consideramos el régimen en el que la constante de doblamiento es grande pero permanece acotada (en comparación con el tamaño del conjunto A y el del grupo G, que tomamos tendiendo a infinito).

2.1. Crecimiento de conjuntos suma. El tema principal de esta capítulo es el análisis de conjuntos suma bajo la condición $|A+A| \leq K|A|$, donde K es una constante. Veremos que en este caso podemos concluir que A es un conjunto estructurado en un cierto sentido que describiremos con precisión más adelante. Concretamente, en la Sección 2.2 demostraremos que cuando $A \subseteq \mathbb{F}_p^n$ es un conjunto que cumple que $|A + A| \leq K|A|$, entonces

tiene que estar contenido de manera "eficiente" en un subespacio de $\mathbb{F}_p^n$ cuyo cardinal está acotado en función de K.

Naturalmente, cuando un conjunto está contenido en un subespacio, su crecimiento bajo la operación "+" está limitado: el conjunto suma iterado llenará todo el subespacio y no puede crecer más. Antes de demostrar el resultado principal sobre los conjuntos cuyo conjunto suma está acotado, demostramos que el crecimiento de un tal conjunto bajo la operación "+" es bastante lento. Este fenómeno fue cuantificado por Plünnecke [Plü69] en el teorema siguiente, conocido como la *desigualdad de Plünnecke*. Recientemente, Petridis [Pet12] logró demostrar este teorema de una manera muy elemental, Y nosotros seguiremos sus pasos.[3]

Teorema 2.7 (Desigualdad de Plünnecke)**.** *Sean $A, B \subseteq G$ conjuntos finitos tal que $|A + B| \leq K|A|$. Entonces para toda pareja de enteros $k, m \geq 1$*

$$|kB - mB| \leq K^{k+m}|A|.$$

Demostración: Sin pérdida de generalidad supongamos que $|A+B| = K|A|$. Elegimos un subconjunto no vacío $A' \subseteq A$ que minimice el cociente $|A' + B|/|A'|$, y escribimos $K' := |A' + B|/|A'|$. Observamos que $K' \leq K$, y que $|A' + B| = K'|A'|$ además de $|A'' + B| \geq K'|A''|$ para todo $A'' \subseteq A$.

Para continuar, supongamos que la siguiente afirmación es cierta (más tarde procederemos a demostrarla):

Afirmación 2.8. *Sean A', B, K' como descritos anteriormente. Entonces para todo conjunto C, $|A' + B + C| \leq K'|A' + C|$.*

Terminamos primero la demostración del teorema suponiendo que la afirmación es cierta. En primer lugar comprobamos que para todo $m \in \mathbb{N}$,

$$|A' + mB| \leq K'^m|A'|.$$

Efectivamente, para $m = 1$ la desigualdad se cumple por la hipótesis. Para $m > 1$, se supone que la desigualdad se cumple para $m - 1$ y se sustituye $C = (m - 1)B$ en la afirmación 2.8 para obtener $|A' + mB| \leq K'|A' + (m - 1)B|$. Por la hipótesis inductiva, el término a la derecha es menor que $K'^m|A'|$.

El enunciado completo se deduce ahora a partir de la denominada *desigualdad de Ruzsa*: para todos los conjuntos U, V y W, tenemos que $|U||V - W| \leq |U + V||U + W|$. (La validez

[3]El argumento vale para todo grupo abeliano (y puede adaptarse a grupos no conmutativos, pero continuamos teniendo en mente al caso $G = \mathbb{F}_p^n$.

de esta desigualdad se prueba fácilmente al definir una aplicación $\phi : U \times (V - W) \to (U + V) \times (U + W)$, que asigna a $(u, x = v - w)$ el elemento $(u + v, u + w)$, donde para todo $x \in V - W$ fijamos una representación $v - w$, de manera inyectiva). Esta desigualdad demuestra que

$$|A'||kB - mB| \leq |A' + kB||A' + mB| \leq K'^k|A'| \cdot K'^m|A'| \leq K^{k+m}|A'|^2,$$

lo que implica $|kB - mB| \leq K^{k+m}|A'| \leq K^{k+m}|A|$. □

Demostración la Afirmación 2.8: Lo demostraremos por inducción sobre el cardinal del conjunto C. Cuando $|C| = 1$, la afirmación es trivial. Supongamos que el resultado es válido para C, y consideramos el conjunto $C' = C \cup \{x\}$. Observamos que

$$A' + B + C' = (A' + B + C) \cup [(A' + B + x) \setminus (D + B + x)],$$

donde D es el conjunto $D := \{a \in A' : a + B + x \subseteq A' + B + C\}$. Pero la propiedad que definía la constante K' implica que $|D + B| \geq K'|D|$, así que

$$|A' + B + C'| \leq |A' + B + C| + |A' + B| - |D + B| \leq K'(|A' + C| + |A'| - |D|). \tag{2.1}$$

Aplicamos el mismo argumento otra vez, escribiendo

$$A' + C' = (A' + C) \cup [(A' + x) \setminus (E + x)],$$

donde E es el conjunto $E := \{a \in A' : a + x \in A' + C\}$ y la unión es disjunta. Concluímos que, como $E \subseteq D$,

$$|A' + C'| = |A' + C| + |A'| - |E| \geq |A' + C| + |A'| - |D|,$$

lo que junto a (2.1) implica el enunciado de la afirmación. □

2.2. El teorema de Freiman-Ruzsa. Una vez demostrada la desigualdad de Plünnecke, nos podemos embarcar a obtener el resultado estructural prometido. El teorema 2.9 es un resultado espectacular de Ruzsa [Ruz99], que adaptó un teorema anterior de Freiman en el grupo de enteros [Fre73] al grupo $\mathbb{F}_p^n$. Es uno de los casos mas convincentes para el uso del grupo modelo.

Teorema 2.9 (Teorema de Freiman-Ruzsa)**.** *Sea $A \subseteq G = \mathbb{F}_p^n$ un conjunto tal que $|A + A| \leq K|A|$. Entonces A está contenido en un subespacio $H \leqslant \mathbb{F}_p^n$ de cardinal menor que $K^2 p^{K^4}|A|$.*

Demostración: La idea crucial (y ingeniosa) es elegir un subconjunto $X \subseteq 2A - A$ que sea máximo con la propiedad que las traslaciones $x + A$ para $x \in X$ sean disjuntas.

En primer lugar mostramos que un conjunto X que cumpla esta propiedad no puede ser demasiado grande. Efectivamente, tenemos $X + A \subseteq 3A - A$, y por la desigualdad de Plünnecke (el Teorema 2.7) sabemos que $|3A - A| \leq K^4|A|$. Ya que los conjuntos $x + A$ son disjuntos y de cardinal $|A|$ cada uno, obtenemos

$$K^4|A| \geq |3A - A| \geq |X + A| = \sum_{x \in X} |x + A| = |X||A|,$$

y en consecuencia $|X| \leq K^4$.

Enseguida comprobamos que

$$2A - A \subseteq X + (A - A).$$

Para ver esta afirmación, observamos que si $y \in 2A - A$, entonces $y + A \cap x + A \neq \emptyset$ para algún $x \in X$: si $y \in X$ el enunciado es trivial, y si $y \notin X$ se deduce de haber supuesto que con X elegimos un conjunto máximo. En ambos casos concluimos que $y \in X + (A - A)$.

Sumando A repetidamente a ambos lados de la inclusión antedicha, obtenemos

$$kA - A \subseteq (k - 1)X + (A - A) \tag{2.2}$$

para todo $k \geq 2$. Así pues, hemos conseguido codificar cada vez más sumandos de A dentro de pocas traslaciones de $A - A$ (el conjunto X es de tamaño constante).

Denotemos por H el subgrupo de $\mathbb{F}_p^n$ generado por A y Y para el subgrupo generado por X. Deducimos de (2.2) que

$$H = \bigcup_{k \geq 1} (kA - A) \subseteq Y + (A - A).$$

Pero todo elemento de Y se puede escribir como suma de menos de $|X|$ elementos con coeficientes entre 1 y p, así que $|Y| \leq p^{|X|} \leq p^{K^4}$. La observación que

$$|H| \leq |Y||A - A| \leq K^2 p^{K^4} |A|$$

concluye la demostración. □

La dependencia del cardinal de H sobre la constante de doblamiento K se puede mejorar con más argumentos (en particular, utilizando las denominadas compresiones combinatorias, véase [GT09, EZ12, EZL14]). Sin embargo, el ejemplo siguiente muestra que la dependencia debe ser de naturaleza exponencial.

Ejemplo 2.10. *Consideremos el conjunto $A \subseteq \mathbb{F}_p^n$, que consiste en una unión de un subespacio H (muy grande) y $K-1$ vectores elegidos al azar (no contenidos en H). Entonces*

la constante de doblamiento de A es aproximadamente igual a K, pero todo subespacio H' conteniendo A debe ser de cardinal mayor que $p^{K-2}|A|$.

Sin embargo, el conjunto en este ejemplo se considera también muy estructurado: aparte de un número constante de elementos, el conjunto A está contenido en un subespacio de cardinal menor o igual que $|A|$ (a saber, el subespacio H mismo). Esta observación nos invita a dar la reformulación siguiente del teorema de Freiman-Ruzsa.

Teorema 2.11 (Teorema de Freiman-Ruzsa, reformulado)**.** *Sea $A \subseteq G = \mathbb{F}_p^n$ un conjunto tal que $|A + A| \leq K|A|$. Entonces existe un subespacio $H \leqslant \mathbb{F}_p^n$ de cardinal como máximo $C_1(K)|A|$ tal que para algún $x \in G$,*

$$|A \cap (x + H)| \geq \frac{|A|}{C_2(K)},$$

donde $C_1(K)$ y $C_2(K)$ son constantes que dependen únicamente de K.

Esta versión del teorema de Freiman-Ruzsa nos conduce a proponer la denominada *Conjetura Polinomial de Freiman-Ruzsa* (abreviada 'PFR' en inglés), que sigue siendo uno de los problemas abiertos fundamentales en combinatoria aditiva (para mas detalles véase la Sección 10 de [Gre05]).

Conjetura 2.12 (Conjetura polinomial de Freiman-Ruzsa)**.** *Las constantes $C_1(K)$ y $C_2(K)$ en el Teorema 2.11 dependen polinomialmente de K.*

El mejor resultado hasta la fecha se debe a Sanders [San12], quién consigue cotas casi óptimas para este problema.

El equivalente del teorema de Freiman-Ruzsa (el Teorema 2.11) en los enteros, demostrado por Freiman [Fre73], dice que un conjunto finito de enteros cuyo conjunto suma es pequeño está contenido de manera eficiente en una progresión aritmética multidimensional.

Teorema 2.13. *Sea $A \subseteq \mathbb{Z}$ un conjunto finito de enteros tal que $|A+A| \leq C|A|$ para alguna constante C. Entonces A está contenido en una traslación de una progresión aritmética multidimensional se la forma*

$$\{x \in \mathbb{Z} : x = \sum_{i=1}^{C_1} m_i x_i : m_i \in \mathbb{Z}, |m_i| \leq l_i\}$$

para algunos $x_1, \ldots, x_{C_1} \in \mathbb{Z}$, que es de dimensión C_1 y de cardinal menor o igual que $C_2|A|$, donde C_1 y C_2 constantes que dependen únicamente de C.

En ese contexto se puede formular una conjetura análoga a la Conjetura 2.12.

En la pasada década hemos visto también varias generalizaciones del Teorema 2.9 a otros grupos, incluso no conmutativos. Hasta ahora el resultado más general en esta dirección es [BGT12], y existen algunos artículos de revisión excelentes sobre este tema (ver [Gre14, San13, Hel13]).

3. Geometría de incidencia y el fénomeno suma-producto

3.1. El teorema de Szemerédi-Trotter. Para empezar trataremos de responder a una pregunta aparentemente inocente en el marco de la geometría euclidiana: dado un conjunto P de puntos y un conjunto L de rectas en el plano, ¿cuántas incidencias puede haber entre puntos de P y rectas de L? Dicho de otro modo, buscamos una cota superior para la cantidad

$$I(P,L) := |\{(p,\ell) \in P \times L : p \in \ell\}|.$$

Trivialmente $I(P,L) \leq |P||L|$, pero esta desigualdad está muy lejos de ser óptima. El ejercicio siguiente mejora la cota.

Ejercicio 3.1. *Usar la desigualdad de Cauchy-Schwarz para demostrar que todo conjunto finito P de puntos y L de rectas en el plano cumplen*

$$I(P,L) \leq \text{mín}(|P|^{1/2}|L| + |P|, |L|^{1/2}|P| + |L|).$$

De hecho esta cota se puede mejorar. Para demostrarlo, vamos a utilizar argumentos procedentes de la teoría de grafos. Recuérdese que un *grafo* $G = (V,E)$ es un conjunto V de *vértices* (muchas veces representados por puntos en el plano) junto con un conjunto $E \subseteq V \times V$ de *aristas* (representadas por líneas conectando dos vértices). El *número de cruce*, también llamado número de cruzamiento, de un grafo G es el menor número de cruces de aristas en un diagrama plano del grafo G. Si el número de cruce de G es 0, se dice que el grafo es *plano* (es decir, puede representarse sin cortes de aristas). En un grafo plano conexo [4] se cumple la *fórmula de Euler*, es decir

$$|F| - |E| + |V| = 2,$$

donde F es el conjunto de "caras" del diagrama plano del grafo G (es decir, cada una de las regiones 2-dimensionales en la que el dibujo del grafo divide el plano).

[4]Un grafo G se dice *conexo* si, para cualquier par de vértices u y v en G, existe al menos una trayectoria (una sucesión de vértices adyacentes, conectados por aristas) de u a v.

Lema 3.2. *Sea G un grafo con n vértices y e aristas. Entonces el número de cruce de G es mayor o igual a $e-(3n-6)$.*

DEMOSTRACIÓN: Suponemos que H es un grafo plano, y sus conjuntos de vértices, aristas y caras se denotan por V, E, F, respectivamente. Podemos suponer también que H es conexo, porque si no lo fuera podríamos añadir aristas hasta que lo sea, y ello no afecta a la demostración. Por la fórmula de Euler sabemos que

$$|F| - |E| + |V| = 2.$$

Entonces si t es el número de pares (f, e) tal que $f \in F$, $e \in E$ y la cara f está limitada por la arista e, entonces $t \leq 2|E|$ and $t \geq 3|F|$, so $|E| \leq 3|V| - 6$. Concluímos que si $e > 3n-6$, entonces el grafo G no puede ser plano, y en consecuencia todo diagrama del grafo G debe contener como mínimo un cruce. Quitamos una de las aristas de este cruce para obtener un grafo G' con n vértices y $e-1$ aristas. Podemos repetir este proceso $e-(3n-6)$ veces, así que G tenía como mínimo $e-(3n-6)$ cruces. □

Lema 3.3. *Sea G un grafo con n vértices y $e \geq 4n$ aristas. Entonces el número de cruce de G es mayor o igual a $e^3/(64n^2)$.*

DEMOSTRACIÓN: Supongamos que G tiene un diagrama con s cruces. Vamos a elegir un subgrafo H de G al azar, y contar el número de aristas y cruces inducidos en H.

Para obtener H, elegimos cada vértice de G independientemente con probabilidad p (un parámetro que fijaremos al final). Sea H el subgrafo de G inducido en este conjunto de vértices. Está claro que el número esperado de vértices de H es pn, mientras el número esperado de aristas de H es p^2e (ambos vértices conectados por la arista deben haber sido elegidos). De manera similar, el número esperado de cruces en H es p^4s, lo que implica, por el Lema 3.2, que

$$p^4 s \geq p^2 e - (3pn - 6) \geq p^2 e - 3n.$$

En consecuencia $s \geq e/p^2 - 3n/p^3$, y cuando escribimos $p := 4n/e < 1$ (par la hipótesis sobre G), obtenemos $s \geq e/(4n/e)^2 - 3n/(4n/e)^3 = e^3/(64n^2)$, que es precisamente la desigualdad deseada. □

La demostración precedente se debe a Ajtai, Chvátal, Newborn y Szemerédi, y independientemente Leighton. Ahora ya tenemos todos los ingredientes para demostrar una cota superior óptima para $I(P, L)$, conocida bajo el nombre *Teorema de Szemerédi-Trotter* [STJ83], cuya demostración elegante se debe a Szekely.

Teorema 3.4 (Teorema de Szemerédi-Trotter)**.** *Sea P un conjunto finito de puntos en $\mathbb{R}^2$, y L un conjunto finito de rectas. Entonces el número de incidencias entre P y L satisface*

$$I(P,L) \leq 4|L|^{2/3}|P|^{2/3} + 4|P| + |L|.$$

DEMOSTRACIÓN: Denotamos $|P| = n$ y $|L| = m$. Definimos un grafo G con conjunto de vértices P tal que $(p,p') \in P \times P$ es una arista si y solo si los puntos p y p' definen una recta $\ell \in L$. Para todo $\ell \in L$, sea $s(\ell) := |\{p \in P : p \in \ell\}|$. Ahora

$$|E(G)| \geq \sum_{\ell \in L}(s(\ell) - 1) = I(P,L) - m,$$

y entonces si $I(P,L) - m \geq 4n$, el número de cruce de G está acotado superiormente por m^2, y, por el Lema 3.3, también acotado inferiormente por $(I(P,L) - m)^3/(64n^2)$. Deducimos que

$$I(P,L) - m \leq (64n^2m^2)^{1/3} = 4n^{2/3}m^{2/3},$$

y así $I(P,L) \leq 4n^{2/3}m^{2/3} + m$. Para obtener el resultado del teorema, nos queda por observar que en el caso contrario al que acabamos de estudiar, el número de incidencias cumple que $I(P,L) < 4n + m$. □

Ejercicio 3.5. *Se denota por $[N]$ el conjunto de naturales $\{0, 1, 2, \ldots, N\}$. Considerando los elementos del retículo $[N] \times [2N^2]$, y el conjunto de todas las rectas con pendientes entre 1 y N que pasen por uno de los puntos del retículo, demostrar que la cota superior en el enunciado del Teorema 3.4 es óptima (a excepción de la constante).*

Ejercicio 3.6. *Generalizar el Teorema 3.4 en el sentido siguiente. Sea P un conjunto de n puntos en $\mathbb{R}^2$, y sea L una familia de curvas simples de tamaño m tal que cada par de curvas se intersecan en un máximo de t puntos, y tal que cada par de puntos pertenece a un máximo de s curvas. Entonces el número de incidencias entre P y L satisface*

$$I(P,L) \ll |L|^{2/3}|P|^{2/3}t^{1/3}s^{1/3} + s|P| + |L|.$$

Véase Pach y Sharir [PS98], y [WYZ13] para generalizaciones a curvas con d grados de libertad.

Ejercicio 3.7. *Sea P un conjunto finito de elementos en $\mathbb{R}^2$, y sea $k \geq 2$ un entero. Demostrar que el número de rectas conteniendo como mínimo K puntos de P está acotado superiormente por $O(|P|^2/k^3 + |P|/k)$.*

Como ejercicio suplementario, deducimos del Teorema 3.4 el siguiente resultado de Beck.

Ejercicio 3.8. *Demostrar que existen constantes C_1 y C_2 tal que, cuando P es un conjunto finito de puntos en el plano, y L_P es el conjunto de rectas generadas por P, una de las siguientes afirmaciones vale:*

- *Existe una recta $\ell \in L_P$ conteniendo como mínimo $C_1|P|$ puntos de P;*
- $|L_P| \geq C_2|P|^2$.

3.2. El fenómeno suma-producto en los números reales. En esta sección estudiamos una aplicación importante del Teorema de Szemerédi-Trotter en la combinatoria aritmética, que mostramos en primer lugar en el contexto de los números reales. Dado un conjunto finito $A \subseteq \mathbb{R}$, definimos como ya hemos hecho anteriormente el conjunto suma $A + A := \{a + a' : a, a' \in A\}$. De manera similar, podemos definir el *conjunto producto* $A \cdot A := \{aa' : a, a' \in A\}$, cuyo cardinal también varia entre $|A|$ y $|A|^2$. Nótese, sin embargo, que los casos de mínimo cardinal son muy distintos para el conjunto suma y el conjunto producto: el tamaño del primer conjunto se minimiza cuando A es una progresión aritmética, pero en este caso el conjunto producto es muy grande. A la inversa, cuando A es una progresión geométrica, el conjunto producto está minimizado, pero el conjunto suma alcanza el cardinal máximo. La siguiente pregunta es por lo tanto natural: ¿Es posible que el conjunto suma y el conjunto producto sean pequeños simultáneamente?

Efectivamente, la estructura aditiva y la estructura multiplicativa no parecen coexistir fácilmente. Con este propósito Erdős y Szemerédi [ES83] conjeturaron lo siguiente.

Conjetura 3.9 (Conjetura de Erdős-Szemerédi)**.** *Sea $A \subseteq \mathbb{R}$ un conjunto finito. Entonces para todo $\epsilon > 0$,*

$$\max(|A + A|, |A \cdot A|) \gg |A|^{2-\epsilon}.$$

Dicho de otra manera, por lo menos uno de los dos conjuntos–suma o producto–debe alcanzar su cardinal máximo. En [ES83] Erdős y Szemerédi demostraron un exponente de $1+\epsilon$, y este exponente ha sido mejorado varias veces desde entonces. Aún así, la Conjetura 3.9 se mantiene como uno de los grandes problemas abiertos en combinatoria aritmética.

Comenzamos presentando un argumento simple pero muy elegante debido a Elekes [Ele97].

Teorema 3.10. *Sea $A \subseteq \mathbb{R}$ un conjunto finito. Entonces*

$$|A + A|^2|A \cdot A|^2 \gg |A|^5,$$

y en particular,

$$\max(|A + A|, |A \cdot A|) \gg |A|^{5/4}.$$

DEMOSTRACIÓN: Consideramos el conjunto de puntos $P = (A + A) \times (A \cdot A)$, junto con el conjunto de rectas $L = \{y = a(x - b) : a, b \in A\}$. Inmediatamente observamos que $|P| = |A + A||A \cdot A|$ y que $|L| = |A|^2$. Cada recta de la forma $y = a(x - b)$ contiene como mínimo $|A|$ puntos de P, es decir, los de la forma $(b + a', aa')$ para $a' \in A$. Por lo tanto,

$$I(P, L) \geq |L||A| = |A|^3.$$

Pero por el Teorema de Szemerédi-Trotter (el Teorema 3.4) también tenemos la desigualdad

$$I(P, L) \ll |P|^{2/3}|L|^{2/3} + |P| + |L| = |A + A|^{2/3}|A \cdot A|^{2/3}|A|^{4/3} + |A + A||A \cdot A| + |A|^2.$$

Combinando las cotas se obtiene la desigualdad deseada. □

Ejercicio 3.11. *Modificando el argumento de Elekes, demostrar que para todos conjuntos finitos $A, B, C \subseteq \mathbb{R}$ tales que $|A| = |B| = |C|$,*

$$|AB||A + C| \gg \sqrt{|A|^3|B||C|}.$$

Ejercicio 3.12. *Considerando el conjunto de puntos $P = A(A+1) \times A(A+1)$ y el conjunto de rectas $L = \{y = ax/b + a : a \in A, b \in A + 1\}$, demostrar que*

$$|A(A + 1)| \gg |A|^{5/4}.$$

(El exponente ha sido mejorado a 24/19 por Jones and Roche-Newton [JRN12]*.)*

Algunos años más tarde la estimación suma-producto de Elekes fue mejorada por Solymosi [Sol05], logrando

$$|A + A|^8|A \cdot A|^3 \gg \frac{|A|^{14}}{\log^3 |A|},$$

y en particular

$$\max(|A + A|, |A \cdot A|) \gg \frac{|A|^{14/11}}{\log^{3/11} |A|}.$$

Ejercicio 3.13. *Deducir de este resultado de Solymosi que cuando el cardinal del conjunto suma es mínimo (es decir, $|A + A| \ll |A|$), el cardinal del conjunto producto debe alcanzar casi el máximo (es decir, $|A \cdot A| \gg |A|^{2-o(1)}$). Nótese que este resultado no se puede deducir del Teorema 3.10, ni con la palabras "suma" y "producto" intercambiadas.*

Ejercicio 3.14. *Considerando el conjunto $A = [N]$, demostrar que el término $o(1)$ en el exponente del ejercicio precedente es necesario.*

En 2008 Solymosi [Sol09] mejoró aún más el exponente utilizando un argumento distinto, pero igualmente simple y elegante.

Teorema 3.15. *Sea $A \subseteq \mathbb{R}$ un conjunto finito. Entonces*

$$|A+A|^2|A\cdot A| \gg \frac{|A|^4}{\log|A|},$$

y en particular

$$\max(|A+A|,|A\cdot A|) \gg \frac{|A|^{4/3}}{\log^{1/3}|A|}.$$

Demostración: La demostración usa la noción de la *energía multiplicativa*, definida por

$$E^{\times}(A) := |\{(a,b,c,d)\in A^4 : ad=bc\}|.$$

Notése que trivialmente $E^{\times}(A)\leq |A|^3$. Comprobamos también la cota inferior siguiente.

Afirmación 3.16.

$$E^{\times}(A) \geq \frac{|A|^4}{|A\cdot A|}. \tag{3.1}$$

Demostración de la Afirmación 3.16: Para todo $s\in\mathbb{R}$, denotamos por $r_A(s)$ el número de representaciones de s como $s=a\cdot a'$ con $a,a'\in A$. Entonces, por la desigualdad de Cauchy-Schwarz,

$$E^{\times}(A)=\sum_{s\in A\cdot A} r_A(s)^2 \geq \frac{(\sum_{s\in A\cdot A} r_A(s))^2}{|A\cdot A|},$$

y el simple hecho de que $|A|^2=\sum_{s\in A\cdot A} r_A(s)$ completa la demostración. □

En vista de (3.1), esperaríamos poder acotar superiormente la energía multiplicativa por una cantidad que dependiera del cardinal del conjunto suma de A, lo que nos proporcionaría una estimación suma-producto en el sentido de la Conjetura 3.9.

Para ello, definamos primero, para cada $\lambda\in\mathbb{R}$, la función $r_A^*(\lambda)$ cuenta el número de representaciones de λ como $\lambda = a/a'$, como siempre con $a,a'\in A$. Esto nos permite expresar la energía multiplicativa de A como

$$E^{\times}(A)=\sum_{\lambda\in A/A} r_A^*(\lambda)^2 = \sum_{\lambda\in A/A} |\lambda\cdot A\cap A|^2,$$

donde $A/A := \{a/a' : a,a'\in A\}$ y $\lambda\cdot A := \{\lambda a : a\in A\}$. El logaritmo en la cota final tiene su origen en la división en intervalos diádicos que aplicamos al escribir

$$E^{\times}(A)=\sum_{\lambda\in A/A} |\lambda\cdot A\cap A|^2 = \sum_{i=0}^{\log|A|}\sum_{\lambda\in\Lambda_i} |\lambda\cdot A\cap A|^2,$$

donde $\Lambda_i := \{\lambda \in A/A : 2^i \leq |\lambda \cdot A \cap A| < 2^{i+1}\}$. Deducimos que existe un entero i_0 para el cual

$$\frac{E^{\times}(A)}{\log |A|} \leq \sum_{\lambda \in \Lambda_{i_0}} |\lambda \cdot A \cap A|^2. \tag{3.2}$$

Para facilitar la notación, enumeramos los elementos de Λ_{i_0} en orden creciente, es decir $\lambda_1, \lambda_2, \ldots, \lambda_k$ para algún entero k, así que $E^{\times}(A)/\log |A| \leq k2^{2(i_0+1)}$. Llega el momento de considerar la geometría del problema. Por construcción, cada recta de la forma $y = \lambda_j x$, $j = 1, \ldots, k$, contiene entre 2^{i_0} y 2^{i_0+1} puntos de $A \times A$. Para todo $j = 1, \ldots, k$, denotamos el conjunto de estos puntos P_j. Dado que todo par de rectas distintas forma una base de $\mathbb{R}^2$, llegamos a la conclusión que el conjunto $P_j + P_{j'}$ es de cardinal $|P_j||P_{j'}| \geq 2^{2i_0}$ cuando $j \neq j'$. Además, para todos $j \neq j'$, los conjuntos suma $P_j + P_{j+1}$ y $P_{j'} + P_{j'+1}$ son disjuntos. Entonces

$$k2^{2i_0} \leq |\bigcup_{j=1}^{k} (P_j + P_{j+1})| \leq |(A \times A) + (A \times A)| = |A + A|^2,$$

pero de (3.2) y (3.1) tenemos también

$$k2^{2i_0+2} \geq \frac{E^{\times}(A)}{\log |A|} \geq \frac{|A|^4}{|A \cdot A| \log |A|},$$

lo que implica el resultado final. □

3.3. El fenómeno suma-producto en cuerpos finitos. Es natural plantear el mismo problema suma-producto en cuerpos que no sean $\mathbb{R}$. Nos concentramos en esta sección en el caso de cuerpos de característica positiva, en particular un primo p.

Para entender el porqué este problema es más complicado en $\mathbb{F}_p$, tomemos un conjunto $A \subseteq \mathbb{F}_p$ que consista en todo $\mathbb{F}_p$ excepto un conjunto pequeño de elementos (digamos 10). Observar entonces que un tal conjunto A no puede crecer mucho ni bajo adición ni multiplicación, ya que está restringido por el cardinal del cuerpo ambiente. Para poder demostrar cualquier fenómeno suma-producto en un cuerpo finito, hace falta suponer que el cardinal de A no sea del mismo orden que p.

Un primer paso importante en esta dirección, en parte debido a sus implicaciones para el problema de Kakeya que veremos en el Capítulo 4, fue el siguiente resultado de Bourgain, Katz y Tao [BKT04].

Teorema 3.17. *Sea p un primo. Entonces para todo $\delta > 0$, existe $\epsilon = \epsilon(\delta) > 0$ con la propiedad siguiente. Sea $A \subseteq \mathbb{F}_p$ un conjunto de cardinal $p^\delta < |A| < p^{1-\delta}$. Entonces*

$$\max(|A+A|, |A \cdot A|) \gg |A|^{1+\epsilon}.$$

Poco después, Bourgain y Konyagin [BGK06] quitaron la condición $|A| > p^\delta$. No daremos los detalles de la prueba (que es larga y técnica). Queda por remarcar que aunque la demostración del Teorema 3.17 no hacía referencia a la geometría de incidencia, Bourgain, Katz y Tao dedujeron un teorema de incidencia (el Corolario 3.20 más abajo) de su teorema suma-producto, mejorando la estimación primitiva en este caso.

Ejercicio 3.18. *Demostrar que la cota del Ejercicio 3.1 vale también en el plano finito $\mathbb{F}_p^2$.*

Ejercicio 3.19. *Demostrar que se puede cumplir la igualdad en la desigualdad del Ejercicio 3.18 cuando $|P| = p^2$.*

Corolario 3.20. *Sea p un primo impar. Entonces para todo $\delta > 0$, existe $\epsilon = \epsilon(\delta) > 0$ con la propiedad siguiente. Para todo conjunto P de puntos y L de rectas en $\mathbb{F}_p^2$ de cardinal $|P|, |L| \leq N = p^\delta$ para algún $0 < \delta < 2$,*

$$I(P, L) \ll N^{3/2-\epsilon}.$$

La deducción del corolario a partir del Teorema 3.17 es tediosa, y le referimos al lector al artículo original [BKT04].

Como ya lo hemos observado, subconjuntos grandes de cuerpos finitos no pueden crecer en el sentido de Erdős-Szemerédi porque están contenidos en un ambiente demasiado restrictivo. El ejemplo siguiente, que se debe a Bourgain [Bou05] y Chang [Cha08], proporciona una versión mas precisa de este enunciado.

Ejemplo 3.21. *Sea g un generador de $\mathbb{F}_p^\times$ y sea M un entero a determinar. Consideramos para todo entero $L \leq p$ el conjunto*

$$A_L := \{g^x : 1 \leq x \leq M\} \cap \{L+1, \ldots, L+M\} \subseteq \mathbb{F}_p.$$

Por el principio del palomar, existe un entero L tal que el cardinal de A_L esta acotado inferiormente por $M/(p/M) = M^2/p$. Ponemos $A := A_L$. Entonces A satisface la relación $|A+A| \ll M$ además de $|A \cdot A| \ll M$, así que poniendo $M := \sqrt{p|A|}$ obtenemos un conjunto cuyo conjuntos suma y producto son de cardinal menor o igual que $\sqrt{p|A|}$. Entonces si $|A| \gg p^{1/3}$, no podemos esperar obtener una estimación del tipo

$$\max(|A+A|, |A \cdot A|) \gg |A|^{2-\epsilon},$$

como lo requiere la Conjetura de Erdős-Szemerédi.

El análogo ingenuo de la Conjetura 3.9 tiene que ser sustituido por la versión siguiente (explicitada por Garaev [Gar08], por ejemplo).

Conjetura 3.22. *Sea $A \subseteq \mathbb{F}_p$. Entonces*

$$\max(|A+A|, |A \cdot A|) \gg \min(|A|^{2-\epsilon}, |A|^{1/2} p^{1/2-\epsilon}).$$

En primer lugar nos concentramos en el caso en el que el cardinal de A es grande, que está completamente resuelto. De hecho, es posible demostrar un teorema de incidencia en este contexto, de lo cual se deduce fácilmente el correspondiente teorema suma-producto.

Teorema 3.23. *Sea p un primo impar. Sea P un conjunto de puntos y L un conjunto de rectas en $\mathbb{F}_p^2$. Entonces*

$$I(P,L) \leq \frac{|P||L|}{p} + \sqrt{p|P||L|}.$$

Demostración: Esta demostración se debe a Vinh [Vin11], y utiliza de nuevo la teoría de grafos. Para simplificar el argumento, trabajaremos en el espacio proyectivo $\mathbb{PF}_p^2$, en el cual consideramos una inmersión de una copia de $\mathbb{F}_p^2$ de manera habitual (identificando un punto $x = (x_1, x_2)$ con la clase de equivalencia de $(x_1, x_2, 1)$, la que denotamos $[x]$). Definimos un grafo $G = (V, E)$ poniendo $V := \mathbb{PF}_p^2$ y conectando $[x]$ y $[y]$ par una arista si y sólo si $x \cdot y := x_1y_1 + x_2y_2 + x_3y_3 = 0$. Dicho de otra manera, $[x]$ está conectado a $[y]$ si el punto representado por $[x]$ se encuentra en la recta representada por $[y]$, y viceversa. Nótese que G tiene $n := p^2 + p + 1$ vértices y es regular de grado $d := p + 1$, con d vértices de G presentando bucles (porque el número de soluciones no nulas de $x_1^2 + x_2^2 + x_3^2 = 0$ sobre $\mathbb{F}_p$ es igual a $p^2 - 1$).

Calculamos los valores propios la matriz de adyacencia de G, es decir, la matriz $A = (a_{ij})_{i,j \in V}$ tal que $a_{ij} = 1$ si y solo si hay una arista entre los vértices i y j, y cero si no. Esta matriz es real y simétrica y por lo tanto admite una base ortonormal de vectores propios. Es bien conocido que el mayor valor propio de la matriz de adyacencia de un grafo regular es igual al grado de regularidad, y que está asociado con el vector propio $\mathbf{1} = (1, 1, \ldots, 1)$ normalizado. En otras palabras, el mayor valor propio de la matriz de adyacencia de nuestro grafo G es $\lambda_0 := d$, correspondiente al vector propio $v_0 := \mathbf{1}/\sqrt{n}$.

Hay varias maneras de acotar la magnitud de los valores propios restantes. Una opción para comprobar que son todos de magnitud como máximo $\sqrt{d}$ se basa en estudiar la descomposición $A^2 = A^T A = J + (d-1)I$, donde J es la matriz $n \times n$ que consiste

sólo en unos, y I es la matriz identidad de dimensión n. (Para ver eso, observamos que para distintos $[x]$ y $[y]$, existe precisamente un trayecto de longitud 2 entre ellos, lo que corresponde al hecho de que cada par de rectas se corta en un sólo punto). Dado que el rango de J es 1 y que J tiene sólo un valor propio no trivial (que corresponde al vector v_0), concluímos que los valores propios restantes son todos iguales a $d-1$.

Es bien conocido también, y de hecho es el núcleo de la prueba, que todo grafo d-regular con n vértices cuyos valores propios no triviales son pequeños se comporta aproximadamente como un grafo aleatorio del modelo $G_{n,d/n}$. Para no dejar nada en el tintero, enunciamos y demostramos el lema siguiente–muy estándar–con tal fin.

Lema 3.24 (Lema de expansores)**.** *Sea $G=(V,E)$ un grafo d-regular con n vértices. Sean B, C subconjuntos de V. Entonces el número de aristas $e(B,C)$ entre B y C satisface*

$$\left| e(B,C) - \frac{d}{n}|B||C| \right| \leq \max_{\lambda \neq \lambda_0} |\lambda| \sqrt{|B||C|}.$$

Demostración del Lema 3.24: Escribimos $v_0, \ldots, v_n$ para la sucesión de vectores propios de la matriz de adyacencia A de G, asociados a la sucesión (en orden no creciente) de valores propios $\lambda_0, \ldots, \lambda_n$. Denotamos 1_B el vector característico del conjunto B, es decir la coordenada i de 1_B vale 1 si $i \in B$, y 0 si no. Desarrollamos $1_B = \sum_{k=0}^{n} b_k v_k$ y $1_C = \sum_{k=0}^{n} c_k v_k$ respecto a la base ortonormal $v_0, \ldots, v_n$. Observamos que $v_0 \cdot 1_B = b_0 = |B|/\sqrt{n}$, y de manera similar $v_0 \cdot 1_C = c_0 = |C|/\sqrt{n}$. Ahora

$$e(B,C) = 1_B^T A 1_C = \left(\sum_{k=0}^{n} b_k v_k \right)^T A \left(\sum_{j=0}^{n} c_j v_j \right) = \sum_{k=0}^{n} \lambda_k b_k c_k$$

por ortonormalidad de los vectores v_i. La discusión precediendo al lema implica que $\lambda_0 b_0 c_0 = d \cdot |B||C|/n$, y entonces

$$|e(B,C) - \frac{d}{n}|B||C|| \leq \max_{\lambda \neq \lambda_0} |\lambda| \sum_{k=1}^{n} b_k c_k \leq \max_{\lambda \neq \lambda_0} |\lambda| \left(\sum_{k=1}^{n} b_k^2 \right)^{1/2} \left(\sum_{k=1}^{n} c_k^2 \right)^{1/2}$$

como queríamos demostrar. □

El lema se aplica inmediatamente al conjunto $B := P$ de puntos y el conjunto $C := L$ de rectas, proporcionando

$$I(P,L) \leq \frac{p+1}{p^2+p+1}|P||L| + \sqrt{d|P||L|} \leq \frac{|P||L|}{p} + \sqrt{p|P||L|},$$

lo que completa la demostración del teorema. □

Por el mismo argumento que en el cuerpo de números reales, obtenemos una variante del teorema suma-producto a partir del teorema de incidencia (el Teorema 3.23).

Corolario 3.25. *Sea p un primo impar, y sea $A \subseteq \mathbb{F}_p$. Entonces*

$$\max(|A+A|, |A \cdot A|) \gg \frac{2|A|^2}{p^{1/2} + (p + 4|A|^3/p)^{1/2}}.$$

Ejercicio 3.26. *Deducir el Corolario 3.25 a partir del Teorema 3.23, imitando la demostración del Teorema 3.10.*

Ejercicio 3.27. *Demostrar que el Corolario 3.25 implica los enunciados siguientes.*

- *Si $p^{1/2} \ll |A| \leq p^{2/3}$, entonces*
$$\max(|A+A|, |A \cdot A|) \gg \frac{|A|^2}{p^{1/2}}.$$
- *Si $p^{2/3} \leq |A| \ll p$, entonces*
$$\max(|A+A|, |A \cdot A|) \gg p^{1/2}|A|^{1/2}.$$
- *Si $|A| \leq \sqrt{p}$, no se puede decir nada que no sea trivial.*

Ejercicio 3.28. *Demostrar que el segundo enunciado del Ejercicio 3.27 es (esencialmente) óptimo.*

Ejercicio 3.29. *(Para los lectores que conocen la teoría básica de las sumas exponenciales.) Establecer una cota superior para la expresión*

$$\frac{1}{p} \sum_{n=0}^{p-1} \sum_{x \in A \cdot A} \sum_{a_1 \in A} \sum_{a_2 \in A} \sum_{y \in A+A} e(n(xa_1^{-1} + a_2 - y)),$$

donde $e(x) := e^{2\pi i x/p}$. Dar una demostración alternativa a los enunciados del Ejercicio 3.27.

Ejercicio 3.30. *Generalizar el Corolario 3.25 al resultado siguiente: para todos conjuntos $A, B, C \subseteq \mathbb{F}_p$,*

$$|A+B||A \cdot C| \gg \min\left(p|A|, \frac{|A|^2|B||C|}{p}\right).$$

En el régimen en el que A tiene tamaño pequeño, los métodos analíticos/espectrales fallan y se requieren herramientas combinatorias más sutiles. Los años recientes han visto una sucesión de avances en cuanto al exponente de crecimiento, empezando por Garaev

[Gar07], que demostró que para todo $|A| < p^{7/13}(\log p)^{-4/13}$,

$$\max(|A+A|, |A\cdot A|) \gg |A|^{15/14-o(1)}.$$

En trabajos posteriores, Katz and Shen [KS08] mejoraron el exponente a $14/13 - o(1)$ para $|A| \leq p$, superado poco después por Bourgain y Garaev [BG09] que consiguieron $13/12 - o(1)$. Unos años más tarde, Rudnev [Rud12] obtuvo un exponente de $12/11 - o(1)$ para $|A| \leq \sqrt{p}$. Por último, hacia un año, Roche-Newton, Rudnev y Shkredov [RNRS14] obtuvieron el siguiente resultado notable:

Teorema 3.31. *Sea p un primo y sea $A \subseteq \mathbb{F}_p$. Suponemos que $|A| < p^{5/8}$. Entonces*

$$\max(|A+A|, |A\cdot A|) \gg |A|^{6/5}.$$

Nótese que cuando $|A| \sim p^{5/8}$, la cota coincide con la del Corolario 3.25. El Teorema 3.31 se deduce del teorema de incidencia siguiente que se debe a Rudnev [Rud14].

Teorema 3.32. *Sea p un primo, P un conjunto de puntos y Π un conjunto de planos en $\mathbb{PF}_p^3$. Sea σ el máximo número de planos incidentes en una sola recta, y supongamos que $|P| \geq |\Pi|$ y que $|\Pi| = O(p^2)$. Entonces*

$$I(P,\Pi) \ll |P||\Pi|^{1/2} + \sigma|P|.$$

La demostración de este teorema de incidencia está basada en los métodos extraordinariamente poderosos de Guth y Katz, que no podemos abarcar en este curso. Aquí sólo mostramos como deducir un teorema de tipo suma-producto.

Demostración del Teorema 3.31 asumiendo el Teorema 3.32: Sea $A \subseteq \mathbb{F}_p$, y para facilitar la notación escribimos $B := A\cdot A$ y $C := A^{-1}$. El número de soluciones de la ecuación

$$a + bc = a + b'c' \tag{3.3}$$

con $a, a' \in A, b, b \in B, c, c' \in C$ se acota inferiormente por $E(A)|A|^2$, donde $E(A)$ es la *energía aditiva* definida por

$$E(A) := |\left\{(a_1,a_2,a_3,a_4) \in A^4 : a_1 + a_2 = a_3 + a_4\right\}|.$$

Pero toda solución de (3.3) corresponde a una incidencia entre un punto de $P := \{(a,c,b') : a \in A, b' \in B, c \in C\}$ y un plano de $\Pi := \{\pi : x+by-c'z = a', a' \in A, b \in B, c' \in C\}$. Cada uno de estos conjuntos es de cardinal $|\Pi| = |P| = |A||B||C| = |A|^2|A\cdot A|$, y el número máximo de planos colineales esta acotado por $\max(|A|,|B|,|C|) = \max(|A|,|A\cdot A|) = |A\cdot A|$.

Observamos que la condición $|A| < p^{5/8}$ garantiza que $|\Pi| = |A|^2|A \cdot A| \ll p^{5/4}|A|^{6/5} < p^2$ siempre que $|A \cdot A| \ll |A|^{6/5}$, lo que evidentemente podemos suponer sin pérdida de generalidad. El teorema de incidencia de Rudnev (el Teorema 3.32) por lo tanto implica que el número de soluciones de (3.3) es

$$\ll (|A|^2|A \cdot A|)^{3/2} + |A|^2|A \cdot A|^2.$$

Es fácil de ver que el primer término en esta expresión es dominante. Además, la energía aditiva $E(A)$ se acota inferiormente por $|A|^4/|A + A|$ (imitando el argumento simple por Cauchy-Schwarz que hemos usado en la demostración del Teorema 3.15 para la energía multiplicativa), lo que resulta en la desigualdad

$$|A + A|^2|A \cdot A|^3 \gg |A|^6.$$

□

4. El método polinomial y el fenómeno Kakeya

4.1. El método polinomial. En esta sección introducimos el método polinomial, que se ha utilizado con gran éxito en el ámbito de la combinatoria aditiva, pero también en informática teórica (para un artículo de revisión reciente y completo, véase [Tao13]). Empezamos por una generalización simple del teorema fundamental del álgebra sobre un cuerpo finito $\mathbb{F}$, que dice que todo polinomio en una variable de grado d posee como máximo d raíces. Dicho de otra manera, si $S \subseteq \mathbb{F}$ es un conjunto tal que $|S| > \text{grad}(P)$, entonces existe $x \in S$ tal que $P(x) \neq 0$.

Ejercicio 4.1 (Lema de Schwartz-Zippel)**.** *Sea $f \in \mathbb{F}_p[x_1, \dots, x_n]$ un polinomio no nulo de grado d. Entonces f posee como máximo dp^{n-1} raíces.*

Observamos que este lema implica inmediatamente que cuando el grado d de un polinomio no nulo f es estrictamente menor p, entonces f posee $< p \cdot p^{n-1} = p^n$ raíces. En otras palabras, un polinomio no nulo de grado estrictamente menor que p tiene que tomar un valor no cero sobre $\mathbb{F}_p^n$.

Una versión más elaborada de este principio es el famoso *Nullstellensatz combinatorio* de Alon [A99].

Teorema 4.2 (Nullstellensatz combinatorio)**.** *Sea $f \in \mathbb{F}_p[t_1, \dots, t_n]$ un polinomio de grado d con un coeficiente no nulo en $t_1^{d_1} \cdots t_n^{d_n}$, con $d_1 + \cdots + d_n = d$, y sean $S_1, \dots, S_n \subseteq \mathbb{F}_p$ conjuntos tales que $|S_i| > d_i$ para todo $i = 1, 2, \dots, n$. Entonces existen $x_1 \in S_1, \dots, x_n \in S_n$ tales que $f(x_1, \dots, x_n) \neq 0$.*

DEMOSTRACIÓN: La demostración se realiza por inducción sobre n. El caso $n = 1$ corresponde al teorema fundamental del álgebra. Supongamos que hemos demostrado el resultado para $n - 1 \geq 1$ variables.

Sea g el polinomio

$$g(t_n) := \prod_{s_n \in S_n} (t_n - s_n),$$

en una variable de grado $|S_n|$. Podemos escribir $P(t_1, \ldots, t_n)$ como

$$P(t_1, \ldots, t_n) = q(t_1, \ldots, t_{n-1})g(t_n) + r(t_1, \ldots, t_n),$$

donde q es un polinomio de grado menor o igual a $d - |S_n|$, y r es un polinomio de grado menor o igual a d. Escribimos

$$r(t_1, \ldots, t_n) = \sum_{j=0}^{|S_n|} r_j(t_1, \ldots, t_{n-1})t_n^j,$$

y desarrollamos qg como la suma de $qt_n^{|S_n|}$ y términos de orden inferior, cada uno de grado como máximo

$$(d - |S_n|) + (|S_n| - 1) < d = d_1 + \cdots + d_n.$$

Concluimos que los términos de orden inferior tienen un coeficiente nulo en $t_1^{d_1} \cdots t_n^{d_n}$. Dado que $|S_n| > d_n$, el polinomio $qt_n^{|S_n|}$ también tiene un coeficiente nulo en $t_1^{d_1} \cdots t_n^{d_n}$. Esto significa que el resto r tiene que tener un coeficiente no nulo en $t_1^{d_1} \cdots t_n^{d_n}$, lo que implica en particular que r_{d_n} tiene un coeficiente no nulo en $t_1^{d_1} \cdots t_{n-1}^{d_{n-1}}$.

Por la hipótesis inductiva, existen $x_1 \in S_1, \ldots, x_{n-1} \in S_{n-1}$ tales que $r_{d_n}(x_1, \ldots, x_{n-1}) \neq 0$. Pero el caso $n = 1$ aplicado a

$$r(t_n) := r(x_1, \ldots, x_{n-1}, t_n),$$

lo cual es un polinomio de grado d_n, nos permite encontrar también $x_n \in S_n$ tal que $r(x_n) \neq 0$. Ya que $g(x_n) = 0$, tenemos

$$P(x_1, \ldots, x_n) = q(x_1, \ldots, x_{n-1})g(x_n) + r(x_1, \ldots, x_n) = r(x_1, \ldots, x_n) \neq 0,$$

la conclusión deseada. □

Como primera aplicación, damos una demostración alternativa del teorema de Cauchy-Davenport del capítulo 2.

DEMOSTRACIÓN ALTERNATIVA DEL TEOREMA 2.4: El caso $|A| + |B| > p$ es trivial, supongamos entonces que $|A| + |B| \leq p$. Nuestro objetivo es demostrar que $|A + B| \geq |A| + |B| - 1$.

Supongamos, a fin de obtener una contradicción, que $|A+B| < |A|+|B|-1$, es decir $K := |A+B| \leq |A|+|B|-2$. Definimos el polinomio $P(t_1,t_2) := \prod_{m\in A+B}(t_1+t_2-m)$ de grado K. Se observa que el coeficiente de $t_1^{|A|-1}t_2^{(K-|A|-1)}$ en P es igual a $\binom{K}{|A|-1}$, lo cual es no nulo modulo p puesto que $K \leq |A|+|B|-2 < |A|+|B| \leq p$. Aplicamos el Teorema 4.2 con $d = d_1+d_2$ y $d_1 = |A|-1$, $d_2 = |B|-1$, así que A y B son conjuntos tales que $|A| > d_1$ y $|B| > d_2$. Se deduce que existen $a \in A$ y $b \in B$ tales que $P(a,b) \neq 0$. Pero por construcción, $P(a',b') = 0$ para todo $a' \in A$ y todo $b' \in B$, lo que proporciona la contradicción que buscábamos. □

Existe una variante inocua del teorema de Cauchy–Davenport que resistía durante muchos años a toda tentativa de resolución; en particular, el método de la e-transformada del Capitulo 2 falla al intentarla aplicar en este caso que mostraremos. El Nullstellensatz combinatorio nos permite dar una solución a este problema (aunque fue resuelta por métodos distintos por da Silva y Hamidoune en 1994).

Ejercicio 4.3. *Dado un conjunto $A \subseteq \mathbb{F}_p$, definimos el* conjunto suma restringido $A\widehat{+}B := \{a+b : a \in A, b \in B, a \neq b\}$. *Demostrar que*

$$|A\widehat{+}B| \geq \min\{|A|+|B|-3, p\}.$$

Además, si $|A| \neq |B|$, entonces

$$|A\widehat{+}B| \geq \min\{|A|+|B|-2, p\}.$$

4.2. El problema de Kakeya euclideano. El problema de Kakeya es uno de los grandes problemas abiertos de la matemáticas moderna, en parte porque tiene, a pesar de la simplicidad de su enunciado, importantes y profundas implicaciones en otros áreas, como por ejemplo en el análisis de ecuaciones en derivadas parciales, y en teoría de números. El objeto de estudio son los *conjuntos de Kakeya,* es decir conjuntos en un espacio euclídeo de dimensión n que contengan un segmento unitario de línea en todas las direcciones.

Definición 4.4 (Conjunto de Kakeya)**.** *Un* conjunto de Kakeya *de dimensión n es un subconjunto de $\mathbb{R}^n$ que contiene un segmento unitario de línea en todas las direcciones.*

La cuestión central es si se pueden construir conjuntos de Kakeya "pequeños", en un sentido que desarrollaremos en esta sección. El primer resultado en esta dirección es el famoso teorema de Besicovitch [Bes28], que afirma que existen conjuntos de Kakeya cuya medida de Lebesgue es nula. Referimos al lector a las notas de curso de Green [Gre03] para los detalles de la prueba.

Teorema 4.5. *Existe un conjunto de Kakeya de dimension 2, cerrado y acotado, cuya medida de Lebesgue es nula.*

Mientras los conjuntos de Kakeya pueden ser muy pequeños en el sentido de la medida de Lebesgue, resulta que tienen un fuerte carácter bidimensional. Para dar una caracterización precisa, necesitamos la definición siguiente.

Definición 4.6 (Dimensión de Minkowski)**.** *Sea $B \subseteq \mathbb{R}^n$, y denotamos por $N_\delta(B)$ el δ-entorno de B. Definimos la* dimensión de Minkowski inferior $\underline{d}(B)$ *por*

$$\underline{d}(B) := \text{ínf}\left\{d : \liminf_{\delta\to 0} \frac{|N_\delta(B)|}{\delta^{n-d}} = 0\right\}$$

y la dimensión de Minkowski superior $\overline{d}(B)$ *por*

$$\overline{d}(B) := \text{ínf}\left\{d : \limsup_{\delta\to 0} \frac{|N_\delta(B)|}{\delta^{n-d}} = 0\right\}.$$

Hay otras nociones de dimensión que se han utilizado en este contexto, como por ejemplo la dimensión de Hausdorff. Nosotros nos centraremos en la primera.

Ejemplo 4.7. *El cuadrado $S := [0,1]\times[0,1]\times\{0\}$, como subconjunto de $\mathbb{R}^3$, tiene dimensión de Minkowski superior e inferior igual a $\overline{d}(S) = \underline{d}(S) = 2$. Para ver eso, se observa que $2\delta \leq |N_\delta(S)| \leq 4\delta$, así que*

$$\liminf_{\delta\to 0}\left(n - \frac{\log|N_\delta(S)|}{\log\delta}\right) \geq 2$$

y

$$\limsup_{\delta\to 0}\left(n - \frac{\log|N_\delta(S)|}{\log\delta}\right) \leq 2.$$

Ejercicio 4.8. *Calcular la dimensión de Minkowski superior e inferior del conjunto de Cantor*[5] *como subconjunto de $\mathbb{R}$.*

La célebre conjetura de Kakeya afirma que todo conjunto de Kakeya en $\mathbb{R}^n$ tiene dimensión de Minkowski n.

Conjetura 4.9 (Conjetura de Kakeya)**.** *Sea $d(n) := \text{ínf}_{B\subseteq\mathbb{R}^n}\overline{d}(B)$, donde el ínfimo está definido sobre todos los conjuntos de Kakeya $B \subseteq \mathbb{R}^n$. Entonces*

$$d(n) = n.$$

[5]El conjunto de Cantor es el conjunto de todos los puntos del intervalo real $[0,1]$ que admiten una expresión en base 3 que no utilice el dígito 1.

Esta conjetura permanece abierta salvo el caso $n = 2$, en el cual fue resuelta por Davies.

Teorema 4.10. *Todo conjunto de Kakeya en el plano euclideano es de dimensión de Minkowski superior igual a 2, es decir* $d(2) = 2$.

DEMOSTRACIÓN: Sea $B \subseteq \mathbb{R}^2$ un conjunto de Kakeya. Consideremos su δ-entorno $N_\delta(B)$. Tenemos que demostrar que $|N_\delta(B)| \gg \delta^\epsilon$ para todo ϵ. Dado que B contiene un segmento unitario en cada dirección, $N_\delta(B)$ contiene un rectángulo de tamaño $\delta \times 1$ en cada dirección, y en particular en cada dirección definiendo un ángulo de $\pi j/2k$ con el eje X positivo, donde $j = 1, \ldots, k := \lfloor 1/\delta \rfloor$. Denotamos estos rectángulos $R_1, \ldots, R_k$, y escribimos $A := \cup_j R_j$. Por la desigualdad de Cauchy-Schwarz, obtenemos

$$k^2\delta^2 = \left(\int (1_{R_1} + \ldots 1_{R_k})(x)dx \right)^2 \leq |A| \int (1_{R_1} + \ldots 1_{R_k})(x)^2 dx = |A| \sum_{j,l} |R_j \cap R_l|. \tag{4.1}$$

Pero el área de intersección de cada pareja de rectángulos se calcula fácilmente: es igual a $\delta^2/\sin\theta$, donde $\theta := |j-l|\pi/2k$ es el ángulo entro los dos rectángulos R_j y R_l. Dado que $k \leq 1/\delta$, tenemos $\delta^2/\sin\theta \leq 2\delta/|j-l|$, y pues para cada j,

$$\sum_l |R_j \cap R_l| \leq \delta + 2\sum_{s=1}^{k} \frac{2\delta}{s} \ll \delta \log(1/\delta).$$

Sumando todos los valores de j y sustituyendo en (4.1) proporciona $|A| \gg 1/\log(1/\delta)$ y completa la demostración. □

Considerando de manera similar la intersección de tubos bien separados en dimensión $n \geq 3$, no es demasiado difícil demostrar que $d(n) \geq (n+1)/2$ (para los detalles, véase otra vez [Gre03]). Sin embargo, para n grande esta cota está lejos del enunciado de la conjetura 4.9. Wolff [Wol99] la mejoró ligeramente a $d(n) \geq (n+2)/2$: veremos una versión simplificada de su argumento, sobre un cuerpo finito, en la sección siguiente. Utilizando métodos de la combinatoria aditiva, Bourgain [Bou99] obtuvo $d(n) \geq 13n/25$, y Katz y Tao [KT99, KT02], refinando su método, obtuvieron el récord actual de $d(n) \geq (n-1)/\alpha + 1$, done $\alpha \approx 1{,}675$ es la mayor raíz del polinomio $x^3 - 4x + 2$. (Para una versión simplificada de este argumento, proporcionando la cota $d(n) \geq 4n/7$, véase el artículo de revisión de Dvir [Dvi10]).

4.3. El problema de Kakeya sobre un cuerpo finito. Como ya vimos en el capítulo 2, muchas veces conviene transferir un problema difícil a un cuerpo finito. En el caso de Kakeya la cuestión sobre un cuerpo finito fue planteada por primera vez por Wolff [Wol99]. Para empezar, aclaremos lo que significa un conjunto de Kakeya sobre un cuerpo finito.

Definición 4.11 (Conjunto de Kakeya en $\mathbb{F}_p^n$)**.** *Un* conjunto de Kakeya *en* $\mathbb{F}_p^n$ *es un conjunto que contiene una recta en cada dirección.*

Una recta es simplemente un conjunto de la forma $\{x_0 + tx : t = 0, 1, \ldots, p-1\}$, así que la dirección x de la recta está definida únicamente (hasta equivalencia proyectiva).

Como antes, nuestro objetivo es establecer la mínima dimensión de un conjunto de Kakeya.

Definición 4.12 (Dimensión de Besicovitch)**.** *Definimos la* dimensión de Besicovitch $d_{\mathbb{F}_p}(n)$ *como el ínfimo de todo* d *tal que existe una constante* $C = C(d)$ *y un conjunto de Kakeya en* $\mathbb{F}_p^n$ *de cardinal menor o igual a* Cp^d*.*

Ejercicio 4.13. *Considerando el número de incidencias entre puntos y rectas en* $\mathbb{F}_p^n$*, demostrar que*

$$d_{\mathbb{F}_p}(n) \geq \frac{1}{2}(n+1).$$

Después de alguna reflexión, llegamos a la conjetura siguiente.

Conjetura 4.14 (Conjetura Kakeya en $\mathbb{F}_p^n$)**.** *Se cumple la igualdad*

$$d_{\mathbb{F}_p}(n) = n.$$

Resulta que en dimensión 2, es fácil de demostrar.

Teorema 4.15. *Todo conjunto de Kakeya en* $\mathbb{F}_p^2$ *es de cardinal mayor o igual a* $p(p+1)/2$*, así que*

$$d_{\mathbb{F}_p}(2) = 2.$$

Demostración: Ya hemos utilizado este tipo de argumentos en el caso euclideano, pero aquí es todavía más fácil. Dado que el conjunto de Kakeya $A \subseteq \mathbb{F}_p^2$ contiene una recta en cada una de las $p+1$ direcciones, se puede suponer sin pérdida de generalidad que A es la unión de estas rectas, denotadas $\ell_1, \ldots, \ell_{p+1}$. Obsérvese que

$$p^2(p+1)^2 = \left(\sum_{x \in \mathbb{F}_p^2} (1_{\ell_1} + \cdots + 1_{\ell_{p+1}})(x) \right)^2 \leq |A| \sum_{x \in \mathbb{F}_p^2} (1_{\ell_1} + \cdots + 1_{\ell_{p+1}})(x)^2 = |A| \sum_{i,j} |\ell_i \cap \ell_j|.$$

Pero cada pareja de rectas se interseca en precisamente un punto, excepto cuando son iguales, en cual caso el cardinal de la intersección es igual a p. Concluímos que

$$p^2(p+1)^2 \leq 2|A|p(p+1),$$

lo que completa la prueba. □

De hecho, el ejercicio siguiente muestra que la constante 1/2 en el Teorema 4.15 es óptima.

Ejercicio 4.16. *Sea $p > 2$. Considerando el conjunto*

$$S := \{(x,t) \in \mathbb{F}_p^2 : x + t^2 \text{ es un cuadrado en } \mathbb{F}_p\},$$

demostrar que existe un conjunto de Kakeya en $\mathbb{F}_p^2$ de cardinal menor o igual a $p(p+3)/2$.

Presentamos otro argumento que mejora la cota básica del Ejercicio 4.13. Este argumento, conocido bajo el nombre *argumento de cepillo de Wolff*, fue importante en el contexto euclideano (véase la sección 4.2).

Teorema 4.17. *Se cumple la desigualdad*

$$d_{\mathbb{F}_p}(n) \geq \frac{1}{2}(n+2).$$

Más precisamente, todo conjunto de Kakeya en $\mathbb{F}_p^n$ es de cardinal mayor o igual a

$$\frac{1}{8}p^{(n+2)/2}.$$

Antes de empezar, planteamos un ejercicio en dimensión 2 cuyo resultado utilizamos más tarde.

Ejercicio 4.18. *Sea $A \subseteq \mathbb{F}_p^2$ una unión de k rectas en direcciones distintas. Demostrar que $|A| \geq pk/2$.*

Demostración del Teorema 4.17: Supongamos que $A \subseteq \mathbb{F}_p^n$ es un conjunto de Kakeya de tamaño $|A| \leq p^{(n+2)/2}$, o sea , supongamos que A consiste en una unión de k rectas, con $p^{n-1} \leq k \leq 2p^{n-1}$. Afirmamos que existe alguna recta que se corta con un mínimo de $p^{n/2}/4$ rectas. Para ver eso, denotamos las k rectas $\ell_1, \ldots, \ell_k$, y observamos que

$$p^2k^2 = \left(\sum_{x \in \mathbb{F}_p^n} (1_{\ell_1} + \cdots + 1_{\ell_k})(x)\right)^2 \leq |A| \sum_{x \in \mathbb{F}_p^n} (1_{\ell_1} + \cdots + 1_{\ell_k})(x)^2,$$

lo que es igual a

$$|A| \sum_{i,j=1}^{k} |\ell_i \cap \ell_j| \leq p^{(n+2)/2} \sum_{i,j=1}^{k} |\ell_i \cap \ell_j|.$$

Deducimos que existe $1 \leq i \leq k$ tal que

$$\sum_{j \neq i} |\ell_i \cap \ell_j| \geq \frac{1}{2} p^{n/2} - p \geq \frac{1}{4} p^{n/2}.$$

A partir de ahora nos concentramos en $\ell := \ell_i$ y el conjunto de rectas que se cortan con ℓ, las que enumeramos $\ell'_1, \ldots, \ell'_m$, donde $m \geq p^{n/2}/4$. Nos referiremos a esta colección de rectas como el cepillo, y lo denotamos H.

Cada una de las rectas $\ell'_1, \ldots, \ell'_m$ está ubicada en un único plano de dimensión 2 que contiene también ℓ. Trabajaremos con la colección completa de estos planos $(\Pi_j)_{j=1,\ldots,t}$, y supondremos que cada plano Π_j contiene $\beta_j \geq 1$ de las líneas $\ell'_1, \ldots, \ell'_m$. Del Ejercicio 4.18 sabemos que para todo $j = 1, \ldots, t$,

$$|\Pi_j \cap H| \geq \frac{1}{2}(\beta_j + 1)p \geq (\frac{1}{4}\beta_j + 1)p.$$

En particular, se ve que todo plano Π_j contiene como mínimo $\beta_j p/4$ puntos de H que no están en ℓ, y estas colecciones de puntos son disjuntas cuando j varia entre 1 y m. Concluimos que

$$|A| \geq |H| \geq \frac{1}{4} p \sum_{j=1}^{t} \beta_j = \frac{1}{4} pm \geq \frac{1}{8} p^{(n+2)/2},$$

lo que completa la demostración. □

En dimensión 3, la cota inferior 5/2 para la dimensión de un conjunto Kakeya permanecía el récord durante mucho tiempo. El trabajo de Bourgain, Katz and Tao [BKT04], que ya mencionamos en la sección 3.3, la mejoró por un epsilon (a $5/2 + \epsilon$!) Otros artículos, que no tenemos tiempo para detallar aquí pero que estuvieron basados en el método de Katz y Tao [KT99], mejoraron la cota a

$$d_{\mathbb{F}_p}(n) \geq \frac{1}{7}(4n + 3).$$

Fue en este punto que Dvir [Dvi09] anunció una resolución completa de la conjetura 4.14, utilizando un método completamente distinto, a saber el método polinomial. Antes de dar la prueba (sorprendentemente corta), introducimos la noción del *conjunto de Nikodym*.

Definición 4.19 (Conjunto de Nikodym)**.** *Un conjunto $N \subseteq \mathbb{F}_p^n$ se dice* conjunto de Nikodym *si para todo $x \notin N$, existe una recta por x que interseca N en todo punto salvo uno. En otras palabras, para todo $x \notin N$, existe $y \in \mathbb{F}_p^n$ tal que $\{x + ty : t = 1, \ldots, p-1\} \subseteq N$.*

Está claro que los conjuntos de Nikodym están relacionados con los conjuntos de Kakeya.

Ejercicio 4.20. *Sea $B \subseteq \mathbb{F}_p^n$ un conjunto de Kakeya. Demostrar que existe un conjunto de Nikodym $N \subseteq \mathbb{F}_p^n$ de cardinal menor o igual a $p|B|$.*

¿Cuál es el propósito de definir los conjuntos de Nikodym? Supongamos que existiera un conjunto de Kakeya B (y pues un conjunto de Nikodym N) pequeño en $\mathbb{F}_p^n$. Si pudiésemos encontrar un polinomio f de grado $d < p-1$ cuyos valores en N se conocieran, entonces podríamos recuperar los valores de f en todo punto de $\mathbb{F}_p^n$. En particular, si f fuese no trivial pero nulo en N, entonces podríamos concluir que f es nulo en todo el espacio. Pero esta conclusión estaría en contradicción con el Lema de Schwartz-Zippel, ségun el cual un tal polinomio tiene que tomar al menos un valor no cero.

Teorema 4.21. *Sea $B \subseteq \mathbb{F}_p^n$ un conjunto de Kakeya. Entonces $|B| \gg p^{n-1}/(n!)$.*

Demostración: Sea $d := p-2$, y supongamos, a fin de obtener una contradicción, que

$$|B| < \binom{n-1+d}{n-1}.$$

Entonces el número de monomios en $\mathbb{F}_p[x_1, \ldots, x_n]$ de grado d, igual al número de asignaciones no negativas $j_1, \ldots, j_n$ tales que $j_1 + \cdots + j_n = d$, es estrictamente mayor que el cardinal de B. Se deduce que existe un polinomio homogéneo no trivial $g \in \mathbb{F}_p[x_1, \ldots, x_n]$ de grado d que se anula en todo punto de B. Dado que g es homogéneo, g se anula también en el conjunto de Nikodym $N := \{tx : x \in B\}$ asociado con B.

Consideramos ahora un punto $x \notin N$ y la recta perforada $\ell^* := \{x + ty : t = 1, \ldots, p-1\}$ que para algún $y \in \mathbb{F}_p^n$ está contenida en N. Restringido a ℓ, el polinomio g es un polinomio de grado d que se anula en $p-1 > d$ puntos, así que g es nulo en todo punto de $\ell := \{x + ty : t \in \mathbb{F}_p\}$; en particular, $g(x) = 0$. Pero x fue arbitrario, lo que implica que g se anula en todo $\mathbb{F}_p^n$, contradiciendo el Lema de Schwartz-Zippel (el Lema 4.1) según el cual un polinomio no trivial g de grado d puede poseer como máximo dp^{n-1} raíces. □

Ejercicio 4.22. *Sea $B \subseteq \mathbb{F}_p^n$ un conjunto Kakeya. Formando un producto cartesiano iterado, demostrar que $|B| \gg_{\epsilon,n} p^{n-\epsilon}$.*

Poco después de la primera publicación del trabajo de Dvir, Alon y Tao remarcaron que el argumento de Dvir se podría adaptar para resolver la conjetura completa, con un exponente de n en vez de $n-1$. Lo dejamos como ejercicio (véase el teorema 3 del artículo original de Dvir [Dvi09]).

Ejercicio 4.23. *Sea $B \subseteq \mathbb{F}_p^n$ un conjunto Kakeya. Entonces $|B| \geq p^n/(n!)$.*

Esta cota ha sido mejorada a $p^n/2^n$ [DKSS09]. La construcción siguiente, que se debe a Mockenhaupt y Tao [MT04] para $n = 2$, y Dvir y Saraf y Sudhan [SS08] para $n > 2$ en el caso de característica impar y par, respectivamente, muestra que esta cota es óptima (salvo el factor de 2).

Ejercicio 4.24. *Sea p un primo impar. Considerando el conjunto*

$$B' := \{(x_1^2/4 + x_1 t, \dots x_{n-1}^2/4 + x_{n-1} t, t) : x_1, \dots, x_{n-1}, t \in \mathbb{F}_p\},$$

demostrar que existe un conjunto de Kakeya de cardinal menor o igual a

$$\frac{p^n}{2^{n-1}} + O(p^{n-1}).$$

Agradecimientos. Estoy muy agradecida a Juanjo Rué por haber revisado este texto.

Referencias

[A99] Noga Alon, *Combinatorial Nullstellensatz*, Combinatorics, Probability and Computing, **8**(1-2), 7–29 (1999).

[Bes28] A S Besicovitch, *On Kakeya's problem and a similar one*, Math. Z. **27** (1928), no. 1, 312–320.

[BG09] Jean Bourgain and M Z Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 1, 1–21.

[BGK06] Jean Bourgain, A A Glibichuk, and S V Konyagin, *Estimates for the Number of Sums and Products and for Exponential Sums in Fields of Prime Order*, J. Lond. Math. Soc. (2) **73** (2006), no. 2, 380–398.

[BGT12] Emmanuel Breuillard, Ben J. Green, and Terence Tao, *The structure of approximate groups*, Publ.math.IHES **116** (2012), no. 1, 115–221.

[BKT04] Jean Bourgain, N Katz, and Terence Tao, *A sum-product estimate in finite fields, and applications*, Geometric & Functional Analysis GAFA (2004).

[Bou99] Jean Bourgain, *On the Dimension of Kakeya Sets and Related Maximal Inequalities*, Geom. Funct. Anal. **9** (1999), no. 2, 256–282.

[Bou05] ———, *More on the sum-product phenomenon in prime fields and its applications*, International Journal of Number Theory **1** (2005), 1–32.

[Cha08] Mei-Chu Chang, *Some problems in combinatorial number theory*, Integers **8** (2008), no. 2, A1–11.

[DKSS09] Z Dvir, S Kopparty, S Saraf, and M. Sudan, *Extensions to the Method of Multiplicities, with Applications to Kakeya Sets and Mergers*, Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on (2009), 181–190.

[Dvi09] Zeev Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc. **22** (2009), no. 4, 1093–1097.

[Dvi10] ———, *Incidence theorems and their applications*, Found. Trends Theor. Comput. Sci. **6** (2010), no. 4, 257–393 (2012).

[Ele97] G Elekes, *On the number of sums and products*, Acta Arith. **81** (1997), no. 4, 365–367.

[ES83] Paul Erdös and Endre Szemerédi, *On sums and products of integers*, Studies in pure mathematics (1983).

[EZ12] Chaim Even-Zohar, *On Sums of Generating Sets in* $\mathbb{Z}_2^n$, Combin. Probab. Comput. **21** (2012), no. 06, 916–941.

[EZL14] Chaim Even-Zohar and Shachar Lovett, *The Freiman–Ruzsa theorem over finite fields*, Journal of Combinatorial Theory **125** (2014), 333–341.

[Fre73] G. A. Freiman, *Foundations of a structural theory of set addition*, American Mathematical Society, Providence, R. I., 1973.

[Gar07] M Z Garaev, *An Explicit Sum-Product Estimate in* $\mathbb{F}_p$, International Mathematics Research Notices (2007).

[Gar08] ———, *The sum-product estimate for large subsets of prime fields*, Proceedings of the American Mathematical Society, 2008.

[Gre03] Ben J. Green, *Lecture notes on Restriction and Kakeya Phenomena*, October 2003.

[Gre05] ———, *Finite field models in additive combinatorics*, Surveys in combinatorics 2005 (Bridget S Webb, ed.), Cambridge Univ. Press, Cambridge, Cambridge, 2005, pp. 1–27.

[Gre14] ———, *Approximate algebraic structure*, To appear, Proceedings of the ICM (2014).

[GT09] Ben J. Green and Terence Tao, *Freiman's theorem in finite fields via extremal set theory*, Combin. Probab. Comput. **18** (2009), no. 3, 335–355.

[Hel13] Harald Andres Helfgott, *Growth in groups: ideas and perspectives*, arXiv (2013).

[JRN12] Timothy G F Jones and Oliver Roche-Newton, *Improved bounds on the set A(A+1)*, arXiv (2012).

[KS08] N H Katz and C Y Shen, *A slight improvement to Garaev's sum product estimate*, Proceedings of the American Mathematical Society, 2008.

[KT99] Nets Hawk Katz and Terence Tao, *Bounds on arithmetic projections, and applications to the Kakeya conjecture*, Mathematical Research Letters **6** (1999), no. 6, 625–630.

[KT02] ———, *New bounds for Kakeya problems*, J. Anal. Math. **87** (2002), no. 1, 231–263.

[MT04] Gerd Mockenhaupt and Terence Tao, *Restriction and Kakeya phenomena for finite fields*, Duke Math. J. **121** (2004), no. 1, 35–74.

[Nat10] Melvyn B. Nathanson, *Additive number theory: inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, May 2010.

[Pet12] Giorgis Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, Combinatorica (2012), 1–14.

[Plü69] Helmut Plünnecke, *Eigenschaften und Abschätzungen von Wirkungsfunktionen*, BMwF-GMD-22, Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 1969.

[PS98] Janos Pach and Micha Sharir, *On the Number of Incidences Between Points and Curves*, Combin. Probab. Comput. **7** (1998), no. 01, 121–127.

[RNRS14] Oliver Roche-Newton, Misha Rudnev, and Ilya Shkredov, *New sum-product type estimates over finite fields*, arXiv (2014).

[Rud12] Misha Rudnev, *An improved sum-product inequality in fields of prime order*, Int. Math. Res. Not. IMRN (2012), no. 16, 3693–3705.

[Rud14] ———, *On the number of incidences between planes and points in three dimensions*, arXiv (2014).

[Ruz99] Imre Z. Ruzsa, *An analog of Freiman's theorem in groups*, Astérisque (1999), no. 258, xv, 323–326.

[San12] Tom Sanders, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE **5** (2012), no. 3, 627–655.

[San13] ———, *The structure theory of set addition revisited*, Bull. Amer. Math. Soc. (N.S.) **50** (2013), no. 1, 93–127.

[Sol05] József Solymosi, *On the number of sums and products*, Bull. Lond. Math. Soc. **37** (2005), no. 4, 491–494.

[Sol09] ———, *Bounding multiplicative energy by the sumset*, Adv. Math. (2009).

[SS08] Shubhangi Saraf and Madhu Sudan, *An improved lower bound on the size of Kakeya sets over finite fields*, Anal. PDE **1** (2008), no. 3, 375–379.

[STJ83] Endre Szemerédi and W T Trotter Jr, *Extremal problems in discrete geometry*, Combinatorica **3** (1983), no. 3-4, 381–392.

[Tao13] Terence Tao, *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*, arXiv (2013).

[Vin11] Le Anh Vinh, *The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields*, European J. Combin. **32** (2011), no. 8, 1177–1181.

[Wol99] T Wolff, *Recent work connected with the Kakeya problem, Prospects in Mathematics, H. Rossi, ed*, American Mathematical Society, 1999.

[WYZ13] Hong Wang, Ben Yang, and Ruixiang Zhang, *Bounds of incidences between points and algebraic curves*, arXiv (2013).

School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom
E-mail address: julia.wolf@bristol.ac.uk