

El problema finito de Kakeya

Jonathan López Ruiz

Facultad de Ciencias, Universidad Nacional Autónoma de México
e-mail: jonathan_mathfc@ciencias.unam.mx

Resumen

En este trabajo, que surge a partir de [15], se presenta la notable solución de Zeev Dvir al problema finito de Kakeya [8]. Este es un problema en la frontera entre combinatoria y análisis armónico. Por mucho tiempo se consideró un problema muy difícil por los expertos en el área, pero la prueba de Dvir tiene apenas dos páginas de largo y apenas requiere algunos conceptos básicos (nociones elementales de álgebra lineal y polinomios) para su exposición.

1 Introducción.

En su artículo de 1917 [13] el matemático japonés Sôichi Kakeya propuso el siguiente interesante problema con aspecto de acertijo:

Problema de Kakeya. *¿Cuál es la menor área requerida para rotar 180° y de forma continua un segmento de recta de longitud uno en el plano, de modo que vuelva a ocupar su posición original?*

Sería interesante que el amable lector abandonase temporalmente la lectura del presente trabajo y dedicase un momento a buscar su propia solución al problema de Kakeya. Suponiendo que ya se ha dedicado un tiempo a la cuestión, y antes de dar soluciones definitivas, vamos a explorar posibles soluciones que quizá se hayan pensado:

Un primer intento de solución al problema de Kakeya apunta a rotar el segmento a lo largo de media circunferencia de radio uno como se muestra en la figura 1 (a). En efecto, basta tomar el segmento OA como el radio de la semicircunferencia y rotarlo 180° alrededor de O hasta coincidir con el punto B . Después, se puede trasladar horizontalmente hacia la izquierda –esto no modifica el área utilizada– hasta su posición inicial. El área utilizada con este procedimiento es $\frac{\pi}{2} = 1.5707\dots$

Puede mejorarse la solución anterior si consideramos un círculo de diámetro uno como en la figura 1 (b). Haciendo coincidir el diámetro con el segmento AB y girándolo 180° alrededor del centro de la circunferencia, éste queda invertido ocupando un área igual a $\frac{\pi}{4} = 0.7853\dots$ Sin embargo, todavía podemos hacerlo mejor. Consideremos un triángulo equilátero de altura uno, llamémoslo ABC . Coloquemos el segmento sobre el lado AB con uno de sus extremos en el vértice B . Giremos 60° alrededor del extremo del segmento que se ha fijado y deslicemos sobre el lado BC . De nuevo, giremos 60° alrededor del vértice C y avancemos a lo largo de AC . Ahora, podemos rotar de nueva cuenta 60° alrededor del vértice

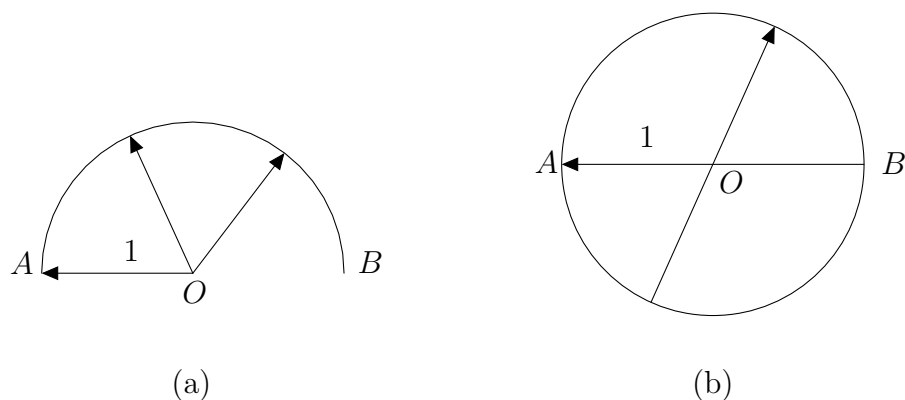


Figura 1: Movimiento de un segmento de longitud uno en (a) Semicírculo de radio 1 y área $\frac{\pi}{2}$ (b) Círculo de diámetro 1 y área $\frac{\pi}{4}$.

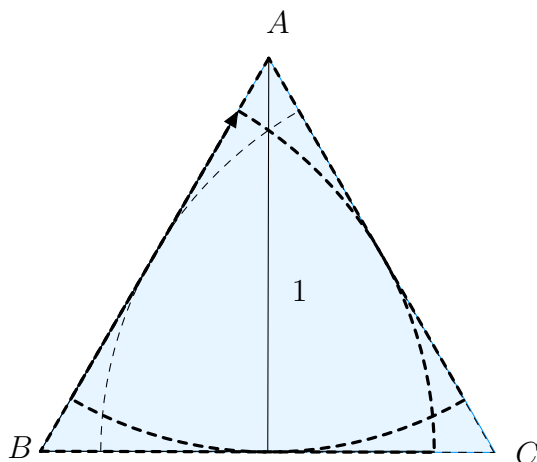


Figura 2: Triángulo equilátero de altura uno y área $\frac{1}{\sqrt{3}}$.

A y, finalmente, desplazarnos hacia abajo sobre AB . Como resultado, hemos invertido el segmento dentro del triángulo ABC . Este procedimiento, en efecto, mejora la solución pues el área del triángulo es $\frac{1}{\sqrt{3}} = 0.5773\dots$. La figura 2 muestra lo anterior.

El mismo Kakeya conjeturó que el triángulo equilátero era la figura que resolvía el problema restringiéndose a la clase de figuras convexas en el plano, mas no presentó una demostración de dicha afirmación. (Esto sería demostrado en 1919 por el matemático húngaro Julius Pál en [19]). En [10] Kakeya, junto con M. Fujiwara, conjetura una nueva solución para el problema de Kakeya: la deltoide ¹ inscrita en una circunferencia de diámetro $\frac{3}{2}$. (Ver

¹Consideremos un circunferencia de radio R (llamada directriz) y en su interior otra circunferencia (lla-

figura 3.) Es fácil convencerse de que un segmento de longitud uno puede rotarse dentro de tal figura pues ésta posee la siguiente interesante propiedad: si γ denota a la deltoide, para cualquier punto P en γ , la tangente en P a γ contiene un segmento AB interior a la figura y de longitud uno, independientemente del punto P que se tome. Sorprendentemente, el área de esta figura es $\frac{\pi}{8} = 0.3926\dots$ (¡incluso mejor que para el caso convexo!), aunque nada daba indicios de que esto no pudiese mejorarse.

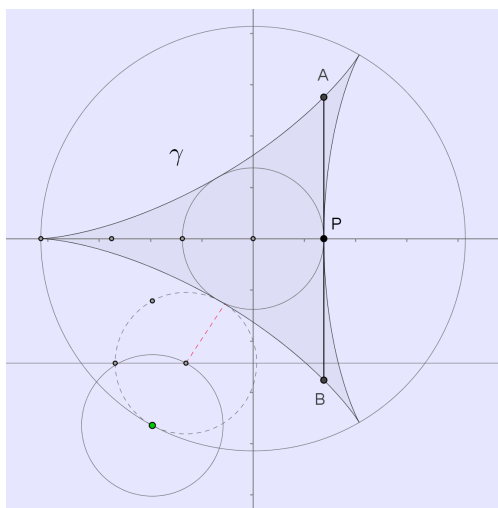


Figura 3: Deltoide de área $\frac{\pi}{8}$ inscrita en una circunferencia de diámetro $\frac{3}{2}$.

Fue en el año de 1928 cuando el matemático ruso Abram S. Besicovitch estableció en [2] una notable solución al problema de Kakeya, dando una respuesta totalmente inesperada: la tarea de rotar continuamente un segmento de longitud uno dentro de un conjunto puede realizarse ocupando un área *tan pequeña como se desee!* Esto es, dado $\epsilon > 0$, existe una figura en el plano, de área menor que ϵ , en la cual se puede rotar un segmento de recta de longitud uno según las condiciones del problema de Kakeya. (Para una detallada exposición de la solución de Besicovitch al problema de Kakeya se sugiere al lector la consulta de [15].)

Uno de los elementos de la sorprendente solución de Besicovitch al problema de Kakeya es la construcción de los ahora llamados *conjuntos de Besicovitch* en el plano. De forma general, un *conjuntos de Besicovitch* se define como sigue:

Definición 1.1. *Un conjunto compacto B de \mathbb{R}^n se llamará **conjunto de Besicovitch** si contiene un segmento de recta de longitud uno en cada dirección. De forma precisa,*

$$\forall e \in \mathbb{S}^{n-1} \exists x_e \in \mathbb{R}^n \text{ tal que } \left\{ x_e + te : t \in \left[-\frac{1}{2}, \frac{1}{2} \right] \right\} \subseteq B,$$

donde $\mathbb{S}^{n-1} = \{x \in \mathbb{R}^n : \|x\| = 1\}$, la esfera unitaria en \mathbb{R}^n .

(mada generatriz) de radio menor, $r = \frac{R}{3}$, tangente a la primera. Una *deltoide* es la curva que describe el movimiento de un punto situado sobre la circunferencia generatriz que gira, sin deslizamiento, por el interior de la circunferencia directriz. Es un caso particular de las *hipocicloides*.

De hecho se pueden construir conjuntos de Besicovitch en \mathbb{R}^n de *medida de Lebesgue* cero [27]. Por otro lado, aun cuando existen conjuntos de Besicovitch de *medida de Lebesgue* cero, Roy O. Davies demostró en [5] que los conjuntos de Besicovitch en el plano tienen *dimensión Hausdorff* igual a 2. (No entraremos en detalles sobre el concepto de *dimensión Hausdorff* aquí, pero, para la consulta de definiciones y demás propiedades, sugerimos al lector consultar [9, 16] y [22].) Lo anterior da pie de manera natural a una conjetura análoga para dimensiones más grandes:

Conjetura de Kakeya. *Un conjunto de Besicovitch en \mathbb{R}^n tiene dimensión Hausdorff igual a n .*

La conjetura de Kakeya permanece abierta para $n \geq 3$ y parece volverse cada vez menos asequible conforme la dimensión aumenta. Hoy en día se considera uno de los mayores problemas abiertos en la teoría geométrica de la medida. En recientes años, la palabra “Kakeya” ha aparecido con mayor frecuencia en la literatura matemática ya que los conceptos relacionados con el problema original han llevado a establecer nuevos vínculos con áreas insospechadas de las matemáticas, entre las que destacan, por mencionar algunas, análisis armónico, transformada de Fourier, combinatoria, teoría de números y hasta ecuaciones de onda. (Excelentes referencias donde se explican las conexiones mencionadas son [27, 4] y [25].) Dadas las numerosas conexiones de la conjetura de Kakeya con otras ramas de las matemáticas, así como los pocos avances significativos en su solución, se han considerado diversos análogos a ésta con la esperanza de obtener nuevas ideas que permitan establecerla de manera completa. Como consecuencia natural, se ha desarrollado una maquinaria de nuevas técnicas que, en muchas ocasiones de forma inesperada, han ayudado a resolver problemas aparentemente pertenecientes a un contexto completamente ajeno.

En este trabajo estaremos interesados en un análogo particular a la conjetura de Kakeya, conocido como *el problema finito de Kakeya*, propuesto por Thomas Wolff en 1999 [27]. El enunciado es un “modelo a escala” de la conjetura de Kakeya, y es extremadamente conveniente pues evita todas las tecnicidades involucradas en el concepto de *dimensión Hausdorff*.

2 El problema finito de Kakeya.

Antes de entrar con todo detalle al *problema finito de Kakeya*, primero establezcamos la notación que utilizaremos a lo largo de la exposición:

Denotaremos por \mathbb{F} a un campo arbitrario y por \mathbb{F}^n al espacio vectorial, sobre el campo \mathbb{F} , de dimensión n . Con esto en cuenta,

Definición 2.1. 1. Para cada par de vectores $x, y \in \mathbb{F}^n$, con $x \neq 0$, definimos la recta $l(y; x) \subseteq \mathbb{F}^n$ que pasa por y en la dirección de x como

$$l(y; x) = \{y + tx : t \in \mathbb{F}\}.$$

2. Sea \mathbb{F} un campo finito. Un conjunto $K \subseteq \mathbb{F}^n$ es un **conjunto finito de Kakeya** si, para cada $x \neq 0$ en \mathbb{F}^n , existe $y = y_x \in \mathbb{F}^n$ tal que $l(y; x) \subseteq K$.

Para todo lo que sigue, nos referiremos a un conjunto finito de Kakeya simplemente como conjunto de Kakeya. La gran ventaja, respecto al caso euclidiano, de considerar estos conjuntos de Kakeya es que la única noción de *tamaño* a considerar es la de cardinalidad. Como estamos trabajando en campos finitos al considerar conjuntos de Kakeya, la cardinalidad de éstos será siempre finita. Podemos entonces enunciar el *problema finito de Kakeya* en este contexto.

Problema finito de Kakeya. *Sea \mathbb{F} un campo finito. Si $K \subseteq \mathbb{F}^n$ es un conjunto de Kakeya, entonces*

$$|K| \geq C_n |\mathbb{F}|^n,$$

donde $C_n > 0$ depende sólo de n , pero no de la cardinalidad de \mathbb{F} .²

Para $n = 1$, el único conjunto de Kakeya es \mathbb{F} y, por tanto, la solución es inmediata; así que el problema se vuelve interesante para $n \geq 2$. El mismo Wolff estableció en [27] una cota de la forma $C_n |\mathbb{F}|^{\frac{n+2}{2}}$ (obsérvese que esto resuelve el problema para $n = 2$). Subsecuentemente esta cota fue mejorada en [20, 3, 17] y [24], tanto para el caso general n como para pequeños valores de éste ($n = 3, 4$). Pese a que importantes matemáticos trabajaron en el problema finito de Kakeya, por ejemplo Terence Tao, ganador de la medalla Fields, el avance era similar al de la conjetura de Kakeya (aunque hay que decirlo, el problema llevaba relativamente poco de haberse propuesto y recibió mucha menos atención que su análogo en el caso euclidiano). Hasta antes del 2009 la mejor cota para el problema finito de Kakeya era de la forma $C_n |\mathbb{F}|^{\frac{4n}{7}}$ ([20] y [17], basados en resultados de [14]). Sin embargo, en ese mismo año, Zeev Dvir sorprendió a la comunidad matemática tras resolver en [8] el problema finito de Kakeya utilizando un breve (¡tan sólo una página de extensión!) y hermoso argumento que explota el comportamiento de ciertos polinomios en los conjuntos de Kakeya; una prueba digna de “El libro” [1]. Lo que nos ocupará de aquí en adelante será presentar la solución de Dvir al problema finito de Kakeya con todo detalle, preservando el espíritu pionero –salvo por algunas observaciones sugeridas a Dvir por Terence Tao y Noga Alon– de la prueba original en todo su esplendor.

3 Resultados preliminares.

En esta sección estaremos especialmente interesados en *polinomios en n variables con coeficientes en el campo \mathbb{F}* . Cabe entonces hacer un breve recordatorio sobre algunos aspectos básicos sobre dichos polinomios. (Sin embargo, para el lector familiarizado, se sugiere continuar la lectura en el párrafo anterior de la proposición 3.1.)

Un *polinomio en n variables x_1, \dots, x_n con coeficientes en el campo \mathbb{F}* se define como una expresión $p(x_1, \dots, x_n)$ de la forma

$$p(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n \geq 0} c_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n},$$

²En el problema finito de Kakeya se debe pensar a n como fijo. Además, algunos autores precisan que se deben considerar valores muy grandes para la cardinalidad del campo \mathbb{F} .

donde los coeficientes c_{i_1, \dots, i_n} están en \mathbb{F} , y sólo un número finito de ellos son diferentes de cero. Con la suma y producto usual de polinomios, éstos últimos forman un anillo, llamado anillo de los polinomios en x_1, x_2, \dots, x_n con coeficientes en \mathbb{F} , que se denotará por $\mathbb{F}[x_1, x_2, \dots, x_n]$.

En n variables, un *monomio* es un polinomio de la forma $x_1^{i_1} \cdots x_n^{i_n}$, donde la suma $i_1 + \dots + i_n$ se llama el *grado* del monomio. El *grado* de un polinomio $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ ³, $\deg(p)$, se define como el máximo de los grados de sus monomios para los que sus coeficientes sean distintos de cero. También diremos que $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ es *homogéneo* si todos sus monomios con coeficientes no cero tienen el mismo grado. Un polinomio $p(x)$ en $\mathbb{F}[x_1, x_2, \dots, x_n]$ se dice ser el *polinomio cero*, denotado por 0 , si todos sus coeficientes son iguales a cero. Se define el grado del polinomio cero $0 \in \mathbb{F}[x_1, x_2, \dots, x_n]$ como -1 . Por último, los siguientes conceptos serán de gran utilidad para todo lo sucesivo: Se dice que un vector $(a_1, \dots, a_n) \in \mathbb{F}^n$ es un *cero* o *raíz* del polinomio $p(x_1, \dots, x_n)$ en $\mathbb{F}[x_1, x_2, \dots, x_n]$ si $p(a_1, \dots, a_n) = 0$; además, diremos que un polinomio $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ *se anula* en un conjunto $A \subseteq \mathbb{F}^n$ si $p(a) = 0$ para cada $a \in A$.

El primer paso en la demostración de Dvir del problema finito de Kakeya es la generalización del siguiente resultado sobre polinomios en una variable:

Proposición 3.1. *Sea $d \geq 1$ un entero.*

- (i) *Si $p(x) \in \mathbb{F}[x]$ es un polinomio no cero de grado a lo más d , entonces $p(x)$ tiene a lo más d raíces en \mathbb{F} .*
- (ii) *Dado un conjunto $A \subseteq \mathbb{F}$ de cardinalidad a lo más d , existe un polinomio diferente de cero $p(x) \in \mathbb{F}[x]$, de grado a lo más d , que se anula en el conjunto A .*

Obsérvese que la proposición anterior permite establecer cotas para la cardinalidad de un subconjunto A del campo \mathbb{F} . En efecto, según el punto (i), para obtener una cota superior para $|A|$ bastará exhibir un polinomio no cero de grado pequeño que se anule en el conjunto A . Por otro lado, utilizando el recíproco del punto (ii), se puede obtener una cota superior para $|A|$ demostrando que el único polinomio de grado pequeño que se anula en el conjunto A es el polinomio cero.

Este tipo de observaciones serán de gran utilidad para resolver el problema finito de Kakeya y, por tanto, motivan la necesidad de generalizar la proposición 3.1 a polinomios en varias variables.

3.1 Lema de DeMillo-Lipton-Zippel-Schwartz.

El punto (i) de la proposición 3.1 establece que un polinomio no cero $p(x) \in \mathbb{F}[x]$ no puede tener más de $\deg(p)$ raíces en \mathbb{F} . Por supuesto, en general, este no es el caso para polinomios en varias variables: por ejemplo, el polinomio $p(x_1, x_2) = x_1 x_2$ con coeficientes en \mathbb{R} se anula

³Para facilitar la notación, cuando sea conveniente escribiremos $p(x)$ en lugar de $p(x_1, \dots, x_n)$ para denotar a un polinomio en $\mathbb{F}[x_1, \dots, x_n]$, entendiéndose que x abrevia (x_1, x_2, \dots, x_n) .

en todas las parejas $(x_1, 0), (0, x_2)$, con $x_1, x_2 \in \mathbb{R}$. Por lo tanto $p(x_1, x_2)$ tiene un número infinito de raíces. En consecuencia, si de alguna forma queremos obtener un análogo de este resultado para polinomios en varias variables –conservando la relación entre el grado y el número de raíces de un polinomio–, un punto central será considerar polinomios con coeficientes en un campo finito. Esto es precisamente lo que asegura el *lema de DeMillo-Lipton-Zippel-Schwartz*, que se a continuación:

Lema 3.2. *Sea \mathbb{F} un campo finito con q elementos. Todo polinomio diferente de cero $p(x)$ en $\mathbb{F}[x_1, x_2, \dots, x_n]$ de grado d tiene a lo más dq^{n-1} raíces en \mathbb{F}^n .*

Se presentan aquí dos pruebas de este resultado. La primera de ellas, debida a Zeev Dvir [8] y a Dana Moshkovitz [18], requiere el siguiente lema previo.

Lema 3.3. *Sea \mathbb{F} un campo finito, con $|\mathbb{F}| = q$, y sea $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ un polinomio de grado $d < q$. Si $p(x) = 0$ para cada $x \in \mathbb{F}^n$, entonces, $p(x)$ es el polinomio cero.*

Demostración: La prueba se realizará por inducción matemática sobre n , el número de variables de $p(x)$. Caso base: $n = 1$. Sea $p(x) \in \mathbb{F}[x]$. Si $p(x)$ no es el polinomio cero, entonces, sabemos que éste tiene a lo más $d < q$ raíces en \mathbb{F} . Así, existe $a \in \mathbb{F}$ tal que $p(a) \neq 0$. Con esto queda demostrado el resultado para $n = 1$. Analicemos ahora el caso $n \geq 2$:

Hipótesis de inducción: para cualquier polinomio $f(x)$ en $\mathbb{F}[x_1, x_2, \dots, x_{n-1}]$ de grado menor que q se cumple que, si $f(x) = 0$ para cada $x \in \mathbb{F}^{n-1}$, entonces $f(x)$ es el polinomio cero. Sea $p(x_1, \dots, x_n) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ un polinomio de grado $d < q$. Supongamos, además, que $p(x_1, \dots, x_n) = 0$ para todo $(x_1, \dots, x_n) \in \mathbb{F}^n$. Así, tenemos que mostrar que $p(x_1, \dots, x_n)$ es el polinomio cero. Para esto, vamos a descomponer a $p(x_1, \dots, x_n)$ en sumandos de acuerdo a las potencias de la variable x_n como sigue:

$$p(x_1, \dots, x_n) = \sum_{i=0}^k f_i(x_1, \dots, x_{n-1})x_n^i,$$

donde $f_i \in \mathbb{F}[x_1, \dots, x_{n-1}]$ para $0 \leq i \leq k \leq d$, con k la mayor potencia a la cual aparece la variable x_n en $p(x)$. Ahora bien, sea $a = (a_1, \dots, a_{n-1}) \in \mathbb{F}^{n-1}$, y definamos $p_a(x_n) \in \mathbb{F}[x_n]$ como $p_a(x_n) = p(a_1, \dots, a_{n-1}, x_n)$. Sabemos que $p_a(x_n) = 0$ para cada $x_n \in \mathbb{F}$; además, $\deg(p_a) \leq k \leq d < q$, por lo que volvemos al caso $n = 1$. Luego, $p_a(x_n)$ es el polinomio cero, es decir, $f_i(a_1, \dots, a_{n-1}) = 0$, para toda $0 \leq i \leq k$. Pero la elección de $a \in \mathbb{F}^{n-1}$ fue arbitraria, por lo cual, en realidad, $f_i(x) = 0$ para cada $x \in \mathbb{F}^{n-1}$. También se cumple que $\deg(f_i) \leq d < q$, así que, utilizando la hipótesis de inducción, para cada $0 \leq i \leq k$, $f_i(x)$ debe ser el polinomio cero. En otras palabras, todos los coeficientes de $f_i(x)$, y por lo tanto de $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$, son cero. En consecuencia, $p(x)$ es el polinomio cero.

Por lo tanto, por el principio de inducción matemática, se concluye que el resultado es verdadero para cada $n \in \mathbb{N}$. \square

Demostración del lema 3.2. Sea $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ de grado d . El caso $n = 1$ del lema está considerado en el punto (i) de la proposición 3.1, así que podemos suponer que $n \geq 2$.

Más aún, sin pérdida de generalidad, podemos suponer que $1 \leq d < q$ ⁴. La demostración se hará reduciendo al caso $n = 1$. Escribamos $p(x) = f(x) + g(x)$, donde $f(x)$ es un polinomio, no cero, homogéneo de grado d y $g(x)$ tiene sólo monomios de grado estrictamente menores que d . Por el lema 3.3, $f(w) \neq 0$ para algún vector w en \mathbb{F}^n . Más aún, como $f(x)$ es homogéneo de grado $d \geq 1$, $w \neq 0$ (pues $f(0) = 0$ al ser $f(x)$ homogéneo). Ahora, a cada vector $u \in \mathbb{F}^n$ asociémosle la recta $l_u = \{u + tw : t \in \mathbb{F}\}$ por u en la dirección w . Así, $l_u \cap l_v = \emptyset$ siempre que $v \notin l_u$. En efecto, si $y \in l_u \cap l_v$, entonces existen $t_1, t_2 \in \mathbb{F}$ tales que $y = u + t_1w$ y $y = v + t_2w$. De donde, $u + t_1w = v + t_2w$, o bien, $v = u + (t_1 - t_2)w$. Luego, $v \in l_u$, lo cual es una contradicción a la suposición inicial.

Obsérvese que al ser $w \neq 0$, cada recta l_u contiene $|l_u| = q$ puntos. De este modo, el espacio \mathbb{F}^n puede partirse en $\frac{q^n}{q} = q^{n-1}$ rectas. Queda, por tanto, demostrar que el número de raíces del polinomio $p(x)$ en cada recta l_u es a lo más d .

Para probar esto, nótese que, para cada $u \in \mathbb{F}^n$, la función $p_u(t) = p(u + tw)$ es un polinomio en t de grado a lo más d . Más aún, este polinomio es diferente de cero ya que el coeficiente del término t^d en $p_u(t)$ es $f(w) \neq 0$. Por lo tanto, $p_u(t)$ tiene a lo más d raíces. En otras palabras, el polinomio $p(x)$ se puede anular en a lo más d puntos de la recta l_u . Como sólo hay q^{n-1} rectas en la partición de \mathbb{F}^n , el número total de raíces de $p(x)$ no puede exceder dq^{n-1} , como buscábamos probar. \square

Un resultado ligeramente más general fue demostrado independientemente por Richard A. DeMillo y Richard J. Lipton [6], Richard Zippel [28] y Jacob T. Schwartz [21].

Lema 3.4 (DeMillo-Lipton-Zippel-Schwartz). *Sea \mathbb{F} un campo y d un entero positivo. Para cada conjunto finito $A \subseteq \mathbb{F}$ tal que $|A| \geq d$, se cumple que cualquier polinomio no cero $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ de grado d tiene a lo más $d|A|^{n-1}$ raíces en A^n .*

Demostración: Sea $A \subseteq \mathbb{F}$ un conjunto finito tal que $|A| \geq d$. Vamos a demostrar el resultado utilizando inducción matemática sobre n , el número de variables de $p(x)$.

Para $n = 1$, el polinomio no cero en una variable $p(x)$ tiene a lo más d raíces en \mathbb{F} (punto (i) de la proposición 3.1). Ahora analicemos el caso $n \geq 2$. Supongamos que el resultado es verdadero para cualquier polinomio de $n - 1$ variables, y consideremos $p(x)$ un polinomio diferente de cero en $\mathbb{F}[x_1, x_2, \dots, x_n]$. Para contar el número de raíces de $p(x)$ en A^n , primero vamos descomponerlo en sumandos de acuerdo a las potencias de la variable x_n como sigue:

$$p(x) = \sum_{i=0}^k g_i(x_1, x_2, \dots, x_{n-1}) x_n^i,$$

donde $g_i(x_1, x_2, \dots, x_{n-1}) \in \mathbb{F}[x_1, x_2, \dots, x_{n-1}]$ para $0 \leq i \leq k \leq d$. Con esto en cuenta, escribamos cada $v \in A^n$ en la forma $v = (a, b)$ con $a \in A^{n-1}$, $b \in A$, y estimemos el número de raíces $p(a, b) = 0$. Se pueden distinguir los siguientes dos casos:

⁴En efecto, si $d \geq q$ entonces $dq^{n-1} \geq q^n$, lo cual da lugar a una cota superior inmediata para el número de raíces posibles.

Caso 1. Raíces (a, b) tal que $g_k(a) = 0$. Como $g_k(x_1, x_2, \dots, x_{n-1})$ es distinto del polinomio cero y $\deg(g_k) \leq d - k \leq d$ —pues el grado del polinomio $g_i(x_1, x_2, \dots, x_{n-1})x_n^i$ es a lo más d —, el polinomio $g_k(x_1, x_2, \dots, x_{n-1})$ tiene a lo más $(d - k)|A|^{n-2}$ raíces en A^{n-1} , por hipótesis de inducción. Ahora bien, para cada $a \in A^{n-1}$ hay a lo más $|A|$ diferentes posibles elecciones para el elemento b . Esto quiere decir que el número de raíces de $p(x)$ en A^n que caen en este primer caso son a lo más $(d - k)|A|^{n-1}$.

Caso 2. Raíces (a, b) con $g_k(a) \neq 0$. Observemos que $p(a, x_n) \in \mathbb{F}[x_n]$ es un polinomio distinto de cero, de una sola variable, x_n , y de grado k . Así, para cada elemento a , hay a lo más k posibles elecciones de b en A de modo que $p(a, b) = 0$. Ya que existen a lo más $|A|^{n-1}$ posibles elecciones para el elemento a , tenemos a lo más $k|A|^{n-1}$ raíces de $p(x)$ en este caso.

Sumando el número máximo de raíces posibles en ambos casos, se sigue que hay a lo más

$$(d - k)|A|^{n-1} + k|A|^{n-1} = d|A|^{n-1}$$

raíces de $p(x)$ en A^n . Por lo tanto, por el principio de inducción matemática, se concluye que el resultado es verdadero para cada $n \in \mathbb{N}$. \square

Observaciones 3.1. Aunque la demostración, utilizando inducción matemática, del lema 3.4 parezca menos intuitiva (en el sentido geométrico) que la prueba del lema 3.2, la primera tiene la ventaja de no requerir el lema 3.3. De hecho, este último resultado puede deducirse a partir del lema 3.4.

3.2 Lema de anulación.

Pasemos ahora a formular la generalización de la parte (ii) de la proposición 3.1; nos referiremos a ella de aquí en adelante como el *lema de anulación*. Para esto, nos valdremos del siguiente lema que versa sobre el espacio de los polinomios de grado acotado.

Lema 3.5. El \mathbb{F} -espacio vectorial $\text{Poly}_d(\mathbb{F}^n)$ de polinomios en $\mathbb{F}[x_1, x_2, \dots, x_n]$ de grado a lo más d tiene dimensión $\binom{d+n}{d}$.

Demostración: Una base para el espacio $\text{Poly}_d(\mathbb{F}^n)$ está dada por el conjunto de los monomios $x^{i_1}x^{i_2}\dots x^{i_n}$, con $i_1 + i_2 + \dots + i_n \leq d$:

$$\{1, x_1, \dots, x_n, x_1^2, x_1x_2, \dots, x_1^3, \dots, x_n^d\}.$$

Así, necesitamos contar el número total de monomios en la base. En este sentido, lo anterior es equivalente a contar el número de sucesiones (i_1, i_2, \dots, i_n) de enteros no negativos restringidos a la condición $i_1 + i_2 + \dots + i_n \leq d$. Consideremos pues la función f definida por

$$f(i_1, i_2, \dots, i_n) = (i_1 + 1, i_1 + i_2 + 2, \dots, i_1 + i_2 + \dots + i_n + n).$$

Es decir, la imagen de cada sucesión (i_1, i_2, \dots, i_n) es la sucesión estrictamente creciente

$$i_1 + 1 < i_1 + i_2 + 2 < \dots < i_1 + i_2 + \dots + i_n + n,$$

lo cual determina el subconjunto $\{i_1 + 1, i_1 + i_2 + 2, \dots, i_1 + i_2 + \dots + i_n + n\}$ de n elementos (el hecho que la sucesión sea estrictamente creciente asegura esto) del conjunto $\{1, 2, \dots, n + d\}$. Nótese que f es una función biyectiva en su imagen, por lo cual el número de monomios es igual al número de subconjuntos de n elementos escogidos de uno con $n + d$, es decir, igual a $\binom{n + d}{n}$.

$$\text{Por lo tanto, } \dim [Poly_d(\mathbb{F}^n)] = \binom{n + d}{n}.$$

□

Lema 3.6 (Lema de anulación). *Sea $d \geq 0$ un número entero. Dado un conjunto $A \subseteq \mathbb{F}^n$ de cardinalidad $|A| < \binom{n + d}{d}$, existe un polinomio no cero $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ de grado a lo más d que se anula en A .*

Demostración: Sea $Poly_d(\mathbb{F}^n) \subseteq \mathbb{F}[x_1, x_2, \dots, x_n]$ el \mathbb{F} -espacio vectorial de los polinomios de grado a lo más d . Por el lema 3.5, sabemos que $\dim [Poly_d(\mathbb{F}^n)] = \binom{n + d}{d}$. Consideremos también al espacio vectorial $\mathbb{F}^{|A|}$ de todas las sucesiones finitas $(y_a)_{a \in A}$. Éste tiene dimensión igual a $|A|$, la cual por hipótesis es menor que $\dim [Poly_d(\mathbb{F}^n)]$. Ahora bien, consideremos la transformación lineal $T : Poly_d(\mathbb{F}^n) \rightarrow \mathbb{F}^{|A|}$ definida por $T(p) = (p(a))_{a \in A}$. Como el rango de T , $R(T)$, es un subespacio vectorial de $\mathbb{F}^{|A|}$, se sigue que $\dim [R(T)] \leq \dim (\mathbb{F}^{|A|})$. En consecuencia,

$$\begin{aligned} 0 &< \binom{n + d}{d} - |A| \\ &= \dim [Poly_d(\mathbb{F}^n)] - \dim (\mathbb{F}^{|A|}) \\ &\leq \dim [Poly_d(\mathbb{F}^n)] - \dim [R(T)]. \end{aligned}$$

Esto es, la transformación T tiene núcleo no trivial. Por lo tanto, existe un polinomio no cero $p(x) \in Poly_d(\mathbb{F}^n)$ que se anula en el conjunto A . □

4 Solución al problema finito de Kakeya.

Vamos a comenzar la solución al problema finito de Kakeya con la prueba del caso particular $n = 2$ debida a Keith M. Rogers [20]. (Recordemos que este caso ya se había establecido desde la publicación del artículo de Wolff [27].) Análogamente a lo que ocurre actualmente con la conjetura de Kakeya, es interesante que por muchos años fuese el único avance contundente en la conjetura finita de Kakeya. La demostración de Rogers es un argumento relativamente sencillo de conteo y, aunque la prueba es notable por sí misma, es de nuestro interés exponerla al lector para ejemplificar la diferencia conceptual entre los argumentos combinatorios utilizados hasta antes de la solución de Dvir y las técnicas novedosas introducidas por éste.

4.1 Conjuntos finitos de Kakeya en dos dimensiones.

Rogers toma como base para su prueba la siguiente observación.

Observaciones 4.1. Sea \mathbb{F} un campo, con $|\mathbb{F}| = q$.

- (i) Hay $\frac{q^n - 1}{q - 1}$ distintas direcciones para orientar una recta en \mathbb{F}^n .
- (ii) Cualesquiera dos rectas distintas en \mathbb{F}^n se intersecan en a lo más un punto.

Estas propiedades se establecen, respectivamente, en los lemas 4.1 y 4.2.

Lema 4.1. Sea \mathbb{F} un campo finito. Dados dos vectores $x_1, x_2 \in \mathbb{F}^n \setminus \{0\}$ y $y \in \mathbb{F}^n$, entonces, $l(y; x_1) = l(y; x_2)$ si, y sólo si, existe $\alpha \neq 0$ en \mathbb{F} tal que $x_1 = \alpha x_2$.

Demostración: Supongamos primero que existe $\alpha \neq 0$ en \mathbb{F} tal que $x_1 = \alpha x_2$.

1. Si $y + tx_1 \in l(y; x_1)$, con $t \in \mathbb{F}$, entonces $y + tx_1 = y + (t\alpha)x_2$, donde $t\alpha \in \mathbb{F}$. Luego, $y + tx_1 \in l(y; x_2)$.
2. Si $y + tx_2 \in l(y; x_2)$, con $t \in \mathbb{F}$, entonces $y + tx_2 = y + \left(\frac{t}{\alpha}\right)x_1$, donde $\frac{t}{\alpha} \in \mathbb{F}$ (note que se puede dividir entre α pues éste es diferente de cero). Luego, $y + tx_2 \in l(y; x_1)$.

De 1 y 2, se sigue que $l(y; x_1) = l(y; x_2)$.

Recíprocamente, si $l(y; x_1) = l(y; x_2)$, entonces, para $1 = t_1 \in \mathbb{F}$, existe $t_2 \in \mathbb{F}$ tal que $y + x_1 = y + t_2 x_2$. De donde, $x_1 = t_2 x_2$, con $\alpha = t_2$ (note que $\alpha = t_2 \neq 0$, pues, si lo fuera, $x_1 = 0$ contradiciendo que $x_1 \in \mathbb{F}^n \setminus \{0\}$). \square

De aquí en adelante se dirá que dos vectores $x_1, x_2 \in \mathbb{F}^n \setminus \{0\}$ apuntan en direcciones distintas si $x_1 \neq \alpha x_2$ para todo $\alpha \neq 0$ en \mathbb{F} . Ahora bien, si $|\mathbb{F}| = q$, entonces hay $q^n - 1$ vectores no cero en \mathbb{F}^n ; además, según el lema anterior, para un vector no cero dado hay otros $q - 1$ que apuntan en la misma dirección. Por lo tanto, el número de posibles direcciones para orientar una recta es $\frac{q^n - 1}{q - 1}$.

Lema 4.2. Sea \mathbb{F} un campo finito. Dos rectas distintas $l(y_1; x_1)$ y $l(y_2; x_2)$ en \mathbb{F}^n o son ajenas o se intersecan en un punto.

Demostración: Supongamos que $a, b \in l(y_1; x_1) \cap l(y_2; x_2)$. Entonces

$$y_1 + t_a x_1 = a = y_2 + s_a x_2 \tag{1}$$

y

$$y_1 + t_b x_1 = b = y_2 + s_b x_2, \tag{2}$$

con $t_a, s_a, t_b, s_b \in \mathbb{F}$, y donde $t_a \neq t_b, s_a \neq s_b$ (si ocurriese la igualdad en algún caso, se llegaría a que $a = b$). De 1 y 2 se obtiene, respectivamente, que

$$y_1 - y_2 = s_a x_2 - t_a x_1$$

y

$$y_1 - y_2 = s_b x_2 - t_b x_1.$$

De donde, $s_a x_2 - t_a x_1 = s_b x_2 - t_b x_1$, o bien, $(t_b - t_a) x_1 = (s_b - s_a) x_2$. En consecuencia,

$$x_1 = \frac{s_b - s_a}{t_b - t_a} x_2,$$

con $\frac{s_b - s_a}{t_b - t_a} \in \mathbb{F}$ diferente de cero. Por lo tanto, por el lema 4.1, $l(y_1; x_1) = l(y_2; x_2)$; lo cual contradice nuestra suposición inicial. Se concluye entonces que dos rectas distintas en \mathbb{F}^n , si se cortan, lo hacen en tan sólo un punto. \square

Con esto ya podemos establecer el problema finito de Kakeya para $n = 2$.

Teorema 4.3. *Sea \mathbb{F} un campo finito con q elementos. Si K es un conjunto de Kakeya en \mathbb{F}^2 , entonces*

$$|K| \geq \frac{q^2}{2}.$$

Demostración: Por (i) de la observación 4.1 sabemos que hay $\frac{q^2 - 1}{q - 1} = q + 1$ direcciones para orientar una recta en \mathbb{F}^2 . Como K debe contener al menos una recta en cada dirección, éste debe contener al menos $q + 1$ rectas distintas; sean l_1, l_2, \dots, l_{q+1} dichas rectas. Además, recordemos que cada una de estas rectas tiene q elementos y que dos rectas distintas se cortan a lo más en un punto. Por lo tanto,

$$\begin{aligned} |K| &\geq |l_1| + |l_2 - l_1| + |l_3 - (l_1 \cup l_2)| + \dots + |l_{q+1} - (l_1 \cup l_2 \cup \dots \cup l_q)| \\ &\geq q + (q - 1) + \dots + 1 + 0 \\ &= \frac{q(q + 1)}{2} \\ &\geq \frac{q^2}{2} \end{aligned}$$

\square

4.2 El caso general: la demostración de Dvir.

El segundo punto clave en la demostración de Dvir es una notable observación sobre el comportamiento de ciertos polinomios que se anulan en los conjuntos finitos de Kakeya. La idea es la siguiente: el recíproco del lema de anulación (lema 3.6) permite acotar inferiormente

la cardinalidad de un conjuntos $A \subseteq \mathbb{F}^n$ demostrando que ningún polinomio no cero de grado pequeño se anula en el conjunto A . De forma precisa, si ningún polinomio no cero de grado menor que d se anula en el conjunto A , entonces

$$|A| \geq \binom{n+d}{d} = \binom{n+d}{n}.$$

Nos interesa, pues, el caso $d = q - 1$. Esto motiva el siguiente teorema.

Teorema 4.4. *Sea \mathbb{F} un campo, con $|\mathbb{F}| = q$, y $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ un polinomio de grado a lo más $q - 1$. Si $p(x)$ se anula en un conjunto de Kakeya $K \subseteq \mathbb{F}^n$, entonces $p(x)$ es el polinomio cero.*

Demostración: Supongamos, por el contrario, que $p(x)$ no es el polinomio cero. Escribamos a éste de la siguiente manera:

$$p(x) = \sum_{i=0}^d p_i(x), \quad (3)$$

donde $0 \leq d \leq q - 1$ es el grado del polinomio $p(x)$ y $p_i(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ es un polinomio homogéneo de grado i , para cada $0 \leq i \leq d$. Podemos notar que $p_d(x)$ no es el polinomio cero pues d es justo el grado de $p(x)$. Además, como sabemos que este último se anula en el conjunto no vacío K , se sigue que $d > 0$.

Sea $v \in \mathbb{F}^n \setminus \{0\}$ un vector arbitrario. Como K es un conjunto de Kakeya, sabemos que éste contiene a la recta $\{u + tv : t \in \mathbb{F}\}$, para algún $u = u_v \in \mathbb{F}^n$. Luego, como el polinomio $p(x)$ se anula en todo K , en particular, se tiene que $p(u + tv) = 0$ para cada $t \in \mathbb{F}$. Observemos que el lado izquierdo de la ecuación $p(u + tv) = 0$ es un polinomio en la variable t de grado a lo más $q - 1$ – ya que $\deg(p) \leq q - 1$ – que se anula en todo el campo \mathbb{F} . Esto implica que $p(u + tv)$ es exactamente el polinomio cero pues, de no serlo, por el punto (i) de la proposición 3.1, éste tendría a lo más $q - 1$ raíces en \mathbb{F} , pero hemos dicho ya que se anula en \mathbb{F} , el cual contiene q elementos.

Ahora, el coeficiente del monomio t^d que resulta de sustituir $u + tv$ en la ecuación (3) es exactamente $p_d(v)$; así, el hecho que $p(u + tv)$ sea el polinomio cero permite concluir que $p_d(v) = 0$. Pero al ser la elección del vector v arbitraria, resulta que $p_d(v) = 0$ para cada $v \in \mathbb{F}^n \setminus \{0\}$. Además, $p_d(0) = 0$ ya que $d > 0$ y $p_d(x)$ es homogéneo de grado d . Así, el polinomio $p_d(x)$ se anula en todo el espacio \mathbb{F}^n . En consecuencia de lo anterior se sigue que $p_d(x)$ debe ser el polinomio cero por el lema 3.3. Sin embargo, establecimos al principio de la prueba que el polinomio $p_d(x)$ era distinto de cero ya que d es el grado del polinomio $p(x)$. Así hemos llegado a una contradicción y el resultado queda demostrado. \square

Combinando el lema 3.6 y el teorema 4.4 se obtiene de manera inmediata la solución al problema finito de Kakeya.

Corolario 4.5 (Zeev Dvir). *Sea \mathbb{F} un campo finito. Si $K \subseteq \mathbb{F}^n$ es un conjunto de Kakeya, entonces*

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

Demostración: Supongamos que $|\mathbb{F}| = q$. La segunda desigualdad se sigue de la definición del coeficiente binomial:

$$\binom{q + n - 1}{n} = \frac{1}{n!} q(q + 1) \dots (q + n - 1) \geq \frac{q^n}{n!}.$$

Vamos a concentrarnos, pues, en la primera desigualdad. Si

$$|K| < \binom{q + n - 1}{n} = \binom{q + n - 1}{q - 1},$$

entonces, por el lema 3.6 existe un polinomio no cero $p(x) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ de grado $d \leq q - 1$ que se anula en el conjunto K . Pero esto contradice al teorema 4.4. \square

5 Conclusión.

Las técnicas introducidas por Zeev Dvir en su solución al problema finito de Kakeya significaron el principio de una nueva técnica, ahora conocida como **el método polinomial**, que en recientes años se ha ganado el interés de la comunidad matemática pues ha tenido una inesperada aplicación en muchos problemas en combinatoria ([23, 7]); además ha tenido una influencia importante en las ciencias de la computación ([12, 11]). A muy grandes rasgos, el *método polinomial* busca imponer una estructura algebraica a problemas geométricos-combinatorios (es decir, problemas que involucran puntos, rectas, curvas e *incidencias*) utilizando polinomios en varias variables. Y éste, quizás, sea el elemento más interesante del método pues, como vimos en el problema finito de Kakeya, el planteamiento de dichos problemas no involucra polinomios, sin embargo, éstos últimos brindan una estructura crucial en la solución del problema. *Grosso modo*, el *método polinomial* se puede resumir como sigue: El problema que se busca resolver es entender ciertas propiedades de un subconjunto A de un espacio vectorial finito. Para esto, se encuentra un polinomio, de grado conveniente, que se anule en el conjunto A ; después se usa dicho polinomio para estudiar el problema original. Lo verdaderamente atractivo, la sorpresa, de esta nueva estrategia es que al estudiar conjuntos finitos, la transición del problema original al estudio de polinomios requiere únicamente argumentos elementales de álgebra lineal. Intuitivamente, el *método polinomial* es una técnica eficaz, pues, como ya vimos en el punto (ii) de la proposición 3.1 y en el lema 3.2, el número de raíces de un polinomio está estrechamente relacionado con el grado del mismo.

Ahora bien, regresando a la conjetura de Kakeya que, recordemos, fue el punto de partida para considerar el análogo finito, como menciona Terence Tao en [26], en este sentido es una pena que el *método polinomial* sea fundamentalmente dependiente de la estructura algebraica

de los campos finitos ya que dificulta una aplicación directa para resolver la conjetura de Kakeya en el caso euclidiano. Sin embargo, el *método polinomial* es interesante por sí mismo y, aunque de manera introductoria, se espera haber resaltado lo atractivo de esta nueva técnica a lo largo del presente trabajo.

Referencias

- [1] Aigner, M. and Ziegler, G.M., Proofs from the Book, 5th. Edition, Springer-Verlag Berlin Heidelberg, (2014).
- [2] Besicovitch, A. S., On Kakeya's problem and a similar one, *Mathematische Zeitschrift*, Vol. 27, no. 1, pp. 312-320, (1928).
- [3] Bourgain, J., Katz, N. and Tao, T., A sum-product estimate in finite fields, and applications, *Geometric and Functional Analysis*, Vol. 14, no. 1, pp.27-57, (2004).
- [4] Bourgain, J., Harmonic analysis and combinatorics: how much may they contribute to each other, *Mathematics: Frontiers and Perspectives* (V. Arnold. et al., eds.), pp. 13-32, (2000).
- [5] Davies, R. O., Some remarks on the Kakeya problem, *Mathematical Proceedings of the Cambridge Philosophical Society*, Vol. 69, no. 3, pp. 417-421, (1971).
- [6] DeMillo, R. A., and Lipton, R. J., A probabilistic remark on algebraic program testing, *Information Processing Letters* Vol. 7, no. 4, pp. 193-195, (1978).
- [7] Dvir, Z., Incidence theorems and their applications, *Foundations and Trends® in Theoretical Computer Science*, Vol. 6, no.4, pp. 257-393, (2012).
- [8] Dvir, Z., On the size of Kakeya sets in finite fields, *Journal of the American Mathematical Society* Vol. 22, no. 4, pp. 1093-1097, (2009).
- [9] Falconer, K. J., *The geometry of fractal sets*, Vol. 85. Cambridge university press, (1986).
- [10] Fujiwara, M. and Kakeya, S., On some problems of maxima and minima for the curve of constant breadth and the in-revolvable curve of the equilateral triangle, *Tohoku Mathematical Journal*, Vol. 11, pp. 92-110, (1917).
- [11] Guth, L., *Polynomial methods in combinatorics*, Vol. 64, American Mathematical Soc. (2016).
- [12] Jukna, S., *Extremal combinatorics: with applications in computer science*, 2nd. Edition, Springer-Verlag Berlin Heidelberg, (2011).
- [13] Kakeya, S., Some problems on maxima and minima regarding ovals, *Tohoku Science Reports*, Vol. 6, pp. 71-88, (1917).

- [14] Katz, N. H., and Tao., T. Bounds on arithmetic projections, and applications to the Kakeya conjecture, *Mathematical Research Letters*, Vol. 6, no. 5-6, pp. 625-630, (1999).
- [15] López Ruiz, Jonathan, A 100 años del problema de Kakeya: origen y perspectivas, Tesis de licenciatura, Universidad Nacional Autónoma de México, 2017.
- [16] Mattila, P., *Fourier analysis and Hausdorff dimension*, Vol. 150, Cambridge University Press, (2015).
- [17] Mockenhaupt, G. and Tao, T., Restriction and Kakeya phenomena for finite fields, *Duke Mathematical Journal*, Vol. 121, no. 1, pp. 35-74, (2004).
- [18] Moshkovitz, D., An Alternative Proof of The Schwartz-Zippel Lemma, *Electronic Colloquium on Computational Complexity (ECCC)*, Vol. 17. no. 96, p. 34, (2010).
- [19] Pál, J., Ein minimumproblem für Ovale, *Mathematische Annalen*, Vol. 83, no. 3, pp. 311-319, (1921).
- [20] Rogers, K. M., The finite field Kakeya problem, *The American Mathematical Monthly*, Vol. 108, no. 8, pp. 756-759, (2001).
- [21] Schwartz, J. T., Fast probabilistic algorithms for verification of polynomial identities, *Journal of the ACM (JACM)* Vol. 27, no. 4, pp. 701-717, (1980).
- [22] Stein, E. M. and Shakarchi, R., *Real analysis: measure theory, integration, and Hilbert spaces*, Princeton University Press, (2009).
- [23] Tao, T., Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory, arXiv preprint arXiv:1310.6482 <https://arxiv.org/abs/1310.6482> (2013). Accessed 16 October 2017.
- [24] Tao, T., A new bound for finite field Besicovitch sets in four dimensions, *Pacific journal of mathematics*, Vol. 222, no. 2, pp. 337-363, (2005).
- [25] Tao, T., From Rotating Needles to Stability of Waves: Emerging connections between combinatorics, analysis and PDE, *Notices of the AMS*, Vol. 48, no 3, pp. 294-303, (2001).
- [26] Tao, T., Poincaré's Legacies, Part II: pages from year two of a mathematical blog, *American Mathematical Soc.*, (2009).
- [27] Wolff, T., Recent work connected with the Kakeya problem. *Prospects in mathematics* (Princeton, NJ, 1996), Vol. 2, pp. 129-162, (1999).
- [28] Zippel, R., Probabilistic algorithms for sparse polynomials, Ng E.W. (eds) *Symbolic and Algebraic Computation. EUROSAM. Lecture Notes in Computer Science*, Vol. 72, Springer, Berlin, Heidelberg, pp. 216-226, (1979).