Problemas de combinatoria sobre cuerpos finitos: el método polinomial

Guillermo Matera

Universidad Nacional de General Sarmiento y CONICET

Encuentro Argentino de Cuerpos Finitos y Temas Afines
Córdoba, 19-20 de octubre de 2017

El problema de Kakeya

En 2009, un artículo que resuelve la conjetura de Kakeya atrajo la atención [Dvir, J. AMS, 2009].

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos. Un conjunto $K \subset \mathbb{F}_q^n$ es de Kakeya si contiene una recta en cada dirección.

Ejemplos: $\mathbb{F}_q^n$, $\mathbb{F}_q^n \setminus \{\mathbf{0}\}$.

Pregunta: cuál es el menor cardinal de un conjunto de Kakeya?

Conjetura [Wolff, 1999]: si $K \subset \mathbb{F}_q^n$ es de Kakeya $\Rightarrow |K| \geq c_n q^n$.

El problema clásico de Kakeya

Esta conjetura es el análogo sobre cuerpos finitos de la conjetura de Kakeya en teoría geométrica de la medida.

El problema de la aguja de Kakeya (1917): cuál es el área mínima en el plano necesaria para rotar continua y completamente (360°) una aguja de longitud unitaria y grosor nulo?

Ejemplo 1: un disco unidad ($=$área $\pi/4$).

Ejemplo 2: Usando una curva deltoide se consigue con área $\pi/8$.

El problema clásico de Kakeya

El problema clásico de Kakeya

Se define un conjunto de Kakeya en $\mathbb{R}^2$ como uno que contiene un segmento unitario en cada dirección.

Teorema [Besicovitch, 1919]: existen conjuntos de Kakeya en $\mathbb{R}^2$ de medida Lebesgue arbitrariamente chica.

De hecho, se pueden construir conjuntos de Kakeya de medida cero. Por otro lado, se sabe que estos conjuntos tienen dimensión 2 (en el sentido de dimensión Hausdorff o Minkowski).

Conjetura de Kakeya: un conjunto de Besicovitch en $\mathbb{R}^n$ (es decir, un subconjunto de $\mathbb{R}^n$ que contiene un segmento en cada dirección) tiene dimensión Minkowski y Hausdorff igual a n.

(Problema abierto si $n \geq 3$).

El problema de Kakeya sobre cuerpos finitos

La solución de la conjetura de Kakeya sobre cuerpos finitos es muy simple, y un ejemplo del método polinomial.

El núcleo del argumento de Dvir es el siguiente resultado:

Proposición: Sea $K \subset \mathbb{F}_q^n$ de Kakeya y $P \in \mathbb{F}_q[X_1, \ldots, X_n]$, con $d := \deg P < q$, que se anula en $K \Rightarrow P = 0$.

Demostración: si existiera $P \neq 0$, escribamos

$$P = P_d + \text{términos de menor grado.}$$

Sea $v \in \mathbb{F}_q^n \backslash \{0\}$ una dirección. Como K es de Kakeya $\Rightarrow K$ contiene una recta $\{x + tv : t \in \mathbb{F}_q\} \Rightarrow P(x + tv) = 0$ para cada $t \in \mathbb{F}_q$. Como $\deg P < q$,

$$0 = P(x + Tv) = P_d(v)T^d + \text{términos de menor grado en } T.$$

Como P_d es homogéneo de grado $d > 0$, se anula en $\mathbb{F}_q^n$. Como $\deg P_d < q \Rightarrow P_d = 0$. ■

Corolario: si $K \subset \mathbb{F}_q^n$ es de Kakeya $\Rightarrow |K| \geq \binom{q+n-1}{n} \sim \frac{q^n}{n!}$.

El método polinomial

En resumen, en ciertas clases problemas combinatorios, que involucran conjuntos finitos arbitrarios, se utilizaban métodos "combinatorios".

En los últimos años, muchos problemas importantes se resolvieron utilizando técnicas algebraicas (de geometría o topología algebraica), dando lugar al método polinomial.

La idea es capturar (o al menos partir) los conjuntos en el conjunto de ceros de un o varios polinomios "bajo control" (por ej., de grado bajo). Aplicando herramientas de geometría algebraica se estudia la estructura de este conjunto de ceros, y por lo tanto el conjunto de objetos en cuestión.

Cotas superiores y número "esperado" de puntos

Cantidad de soluciones "esperable"

- Si $E_d := \{F \in \mathbb{F}_q[X_1, \ldots, X_n] : \deg F \leq d\}$,

$$\frac{1}{|E_d|} \sum_{F \in E_d} \left| V(F) \cap \mathbb{F}_q^n \right| = q^{n-1},$$

$$\frac{1}{|E_d|} \sum_{F \in E_d} \left(\left| V(F) \cap \mathbb{F}_q^n \right| - q^{n-1} \right)^2 = q^{n-1} - q^{n-2}.$$

Cotas superiores

- [Ore, 1922] Si $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ tiene grado $d > 0$,

$$\left| V(F) \cap \mathbb{F}_q^n \right| \leq d q^{n-1}.$$

($q > d \Rightarrow$ existe $\boldsymbol{x} \in \mathbb{F}_q^n$ tal que $F(\boldsymbol{x}) \neq 0$.)

Estimaciones de la cantidad de puntos

A fin de obtener estimaciones, consideramos la geometría: dado $F \in \mathbb{F}_q[X_1, \ldots, X_n]$, consideramos la hipersuperficie

$$H := V(F) := \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^n : F(\boldsymbol{x}) = 0\}.$$

A. Weil introduce el concepto de absoluta irreducibilidad.

- $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ es absolutamente irreducible si es irreducible como elemento de $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$.

  Ejemplo: en $\mathbb{F}_5$, $F := X_1 + X_2^3$ es, pero $G := X_1^2 - 3X_2^2$ no es.

- $H := V(F) \subset \overline{\mathbb{F}}_q^n$ es absolutamente irreducible si F es absolutamente irreducible.

Estimaciones para hipersuperficies

[Weil, 1948] demuestra la conjetura de Riemann para curvas planas sobre cuerpos finitos y obtiene la siguiente estimación.

Teorema: Si $C := V(F) \subset \overline{\mathbb{F}}_q^2$ es absolutamente irreducible con $F \in \mathbb{F}_q[X_1, X_2]$ de grado d,

$$\big||C(\mathbb{F}_q)| - q\big| \leq (d-1)(d-2)q^{1/2} + d + 1.$$

[Cafure-M, 2006] Dada una hipersuperficie $H := V(F) \subset \overline{\mathbb{F}}_q^n$ absolutamente irreducible definida sobre $\mathbb{F}_q$ de grado $d > 0$:

$$\big||H(\mathbb{F}_q)| - q^{n-1}\big| \leq (d-1)(d-2)q^{n-3/2} + 5d^{13/3}q^{n-2}.$$

Estimaciones para variedades

Para el caso de una variedad algebraica arbitraria
$V := V(F_1, \ldots, F_s) := \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^n : F_1(\boldsymbol{x}) = \cdots = F_s(\boldsymbol{x}) = 0\}$,
se consideran dos invariantes geométricos : dimensión y grado.

- Dimensión= cantidad de "variables libres" =máxima codimensión de una variedad lineal "general" $L \subset \overline{\mathbb{F}}_q^n$ con $V \cap L \neq \emptyset$.
- Grado= $|L \cap V|$, donde L es una variedad lineal "general" de codimensión $\dim V$.

Número "esperado" de puntos: $|V(\mathbb{F}_q)| \approx q^{\dim V}$.

S. Lang y Weil (1954) prueban que si $V \subset \overline{\mathbb{F}}_q^n$ es absolutamente irreducible, definida sobre $\mathbb{F}_q$, de dimensión $r > 0$ y grado $\delta > 0$, existe $C = C(n, r, \delta)$ independiente de q tal que

$$\left| |V(\mathbb{F}_q)| - q^r \right| \leq (\delta - 1)(\delta - 2)q^{r-1/2} + Cq^{r-1}.$$

Estimaciones para intersecciones completas

A fin de hallar una expresión explícita para C, Weil propone considerar la función zeta: $a_j := \left|V \cap (\mathbb{F}_{q^j})^n\right|$, se define

$$\mathcal{Z}(V, T) := \exp\left(\sum_{j=0}^{\infty} a_j \frac{T^j}{j}\right).$$

Dwork (1960) demuestra que $\mathcal{Z}(V, T)$ es una función racional. De una factorización de $\mathcal{Z}(V, T)$ se deduce una estimación para V.

Deligne [IHES, 1974] demuestra la hipótesis de Riemann para intersecciones completas (=las ecuaciones se "cortan bien") en $\mathbb{F}_q$. Como primera aplicación, obtiene una estimación.

Estimaciones para intersecciones completas

Sean $F_1, \ldots, F_{n-r} \in \mathbb{F}_q[X_0, \ldots, X_n]$ homogéneos de grados $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ y consideremos la variedad proyectiva

$$V := \{\boldsymbol{x} \in \mathbb{P}^n : F_1(\boldsymbol{x}) = 0, \ldots, F_{n-r}(\boldsymbol{x}) = 0\}.$$

Teorema: Si V es una intersección completa no singular

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_r\, q^{r/2},$$

donde $p_r := |\mathbb{P}^r(\mathbb{F}_q)| = q^r + q^{r-1} + \cdots + 1$ y $b'_r(n, \mathbf{d})$ es un invariante (nro. de Betti) asociado a V.

Ghorpade y Lachaud [Moscow Math J, 2002] extienden el enfoque de Weil a intersecciones completas singulares (usan estimaciones de Katz (2001) sobre sumas de números de Betti).

Teorema: Si V es singular, $s := \dim \mathrm{Sing}(V)$ y $d := \max_i d_i$,

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_{r-s-1}\, q^{\frac{r+s+1}{2}} + 9 \cdot 2^r \cdot ((n-r)d + 3)^{n+1} q^{\frac{r+s}{2}}.$$

Estimaciones para intersecciones completas

Sean $F_1, \ldots, F_{n-r} \in \mathbb{F}_q[X_0, \ldots, X_n]$ homogéneos de grados $d_1, \ldots, d_{n-r}$ que definen una intersección completa $V := V(\mathbf{F}) \subset \mathbb{P}^n$ (de dimensión r) con $s := \dim \operatorname{Sing} V \leq r-2$.
Sean $\delta := \prod_i d_i$ y $D := \sum_{i=1}^{n-r}(d_i - 1)$.

Con A. Cafure y M. Privitelli [FFA 31, 2015] usamos herramientas de geometría proyectiva clásica para demostrar:

Teorema: Si $V \subset \mathbb{P}^n$ es normal (i.e., $s \leq r-2$), entonces

$$\left| |V(\mathbb{F}_q)| - p_r \right| \leq (\delta(D-2)+2)q^{r-\frac{1}{2}} + 14D^2\delta^2 q^{r-1}.$$

Más aun, si V es regular en codimensión 2 (i.e., $s \leq r-3$),

$$\left| |V(\mathbb{F}_q)| - p_r \right| \leq 14D^3\delta^2 q^{r-1}.$$

Por último, con M. Pérez y M. Privitelli [JNT, 2016], probamos:

Teorema: Para $q \gtrsim 2sD^{r-s}\delta$,

$$\left| |V(\mathbb{F}_q)| - p_r \right| \leq \left(b'_{r-s-1} + 2\sqrt{\delta} + 1\right) q^{\frac{r+s+1}{2}}.$$

Distribución de patrones de factorización

Sea $M(n)$ el conj. de polinomios mónicos de $\mathbb{F}_q[T]$ de grado n.
Sea $\lambda := (\lambda_1, \ldots, \lambda_n)$ un patrón de factorización, esto es,

$$n = \lambda_1 + 2\lambda_2 + \cdots + n\lambda_n.$$

Un polinomio $f \in M(n)$ tiene patrón de factorización λ si tiene λ_i factores irreducibles de grado i en $\mathbb{F}_q[T]$ para $1 \leq i \leq n$.

Para $A \subset M(n)$, sea $\mathcal{T}_\lambda(A) := |\{f \in A : f \text{ tiene patrón } \lambda\}|$.

Cohen [Acta Arith., 1970] relaciona la distribución de patrones de factorización con el de ciclos en el n-ésimo grupo simétrico. Más precisamente, demuestra que, para n fijo,

$$\mathcal{T}_\lambda(M(n)) = \mathcal{T}(\lambda)\, q^n + \mathcal{O}(q^{n-\frac{1}{2}}),$$

donde $\mathcal{T}(\lambda)$ es la proporción de elementos en el n-ésimo grupo simétrico cuyo patrón es λ.

Distribución de patrones de factorización

Ejemplos

- Si $\lambda := (0, \ldots, 0, 1)$ (polinomios irreducibles), entonces

$$\mathcal{T}(\lambda) = \frac{1}{n} \quad \text{y} \quad \mathcal{T}_\lambda(M(n)) \approx \frac{q^n}{n} \text{ (Gauss)}.$$

- Para $\lambda := (n, 0, \ldots, 0)$ (factores lineales),

$$\mathcal{T}(\lambda) = \frac{1}{n!} \quad \text{y} \quad \mathcal{T}_\lambda(M(n)) \approx \frac{q^n}{n!}.$$

Una cuestión importante es saber si estos resultados valen para familias de polinomios en $M(n)$. En particular, consideramos

$$A_s := \left\{ T^n + a_{n-1} T^{n-1} + \cdots + a_0 : a_{n-s-1}, \ldots, a_0 \in \mathbb{F}_q \right\}.$$

Distribución de patrones de factorización

Se trata del análogo en cuerpos de funciones de los resultados de distribución de primos de intervalos.

Si $\pi(x) := |\{0 < p \leq x : p \text{ es primo}\}|$, el Teorema de los números primos (TNP) afirma que

$$\pi(x) \sim \frac{x}{\ln x}.$$

Es razonable pensar que, si $I := (x, x + \Phi(x)]$, entonces

$$\pi(I) = \pi(x + \Phi(x)) - \pi(x) \sim \frac{\Phi(x)}{\ln x}. \tag{1}$$

- Si $\Phi(x) \sim c \cdot x$ con $0 < c < 1$, es el TNP.
- Aceptando la hipótesis de Riemann, vale para $\Phi(x) \sim \sqrt{x} \log x$ (Selberg, 1943).

Distribución de patrones de factorización

Para potencias menores de x, en el ICM'94 Granville conjetura:

$$\text{Si } \Phi(x) > x^{\epsilon} \ (0 < \epsilon < 1), \text{ entonces (1) es cierta .}$$

Granville (2010): "We know of no approach to prove that there are primes in all intervals $(x, x + \sqrt{x}]$".

Discutimos resultados análogos a (1) en $\mathbb{F}_q[T]$. Para esto, es necesario definir "intervalos" en $\mathbb{F}_q[T]$.

Si $f \in \mathbb{F}_q[T]$ es de grado k, definimos $\|f\| := q^k$. Así,

$$\left|[0, q^n] \cap \{\text{mónicos}\}\right| = |\{f \in \mathbb{F}_q[T] : f \text{ mónico}, \|f\| \leq q^n\}| = q^n.$$

Si $\pi_q(n) := |\{g \in M(n) : g \text{ es irreducible}\}|$, el análogo al TNP es el resultado de Gauss:

$$\pi_q(n) \sim \frac{q^n}{n}.$$

Distribución de patrones de factorización

El análogo al intervalo $[x, x + x^\epsilon)$ $(0 < \epsilon < 1)$ es

$$\begin{aligned} I(f, \epsilon) :=& \{g \in \mathbb{F}_q[T] : \|f - g\| < \|f\|^\epsilon\} \\ =& f + \{h \in \mathbb{F}_q[T] : \deg g < n - s\}, \end{aligned}$$

donde $n - s := \lfloor \epsilon \deg f \rfloor$. Si $f := T^n + a_{n-1} T^{n-1} + \cdots + a_0$, otra forma de describir esta familia

$$A_s := \left\{ T^n + a_{n-1} T^{n-1} + \cdots + a_0 : a_{n-s-1}, \ldots, a_0 \in \mathbb{F}_q \right\}.$$

Sería de esperar que

$$|A_s \cap \{irreducibles\}| \sim \frac{q^{n-s}}{n}.$$

Más generalmente, vamos a discutir la distribución de patrones de factorización entre los elementos de A_s.

Distribución de patrones de factorización

Un ejemplo simple: consideramos $\lambda := (n, 0, \ldots, 0)$ y la familia

$$A_s := \left\{ T^n + a_{n-1} T^{n-1} + \cdots + a_0 : a_{n-s-1}, \ldots, a_0 \in \mathbb{F}_q \right\}.$$

Sean $X_1, \ldots, X_n$ indeterminadas, $\boldsymbol{X} := (X_1, \ldots, X_n)$ y

$$G(\boldsymbol{X}, T) := (T + X_1) \cdots (T + X_n) = T^n + \Pi_1 T^{n-1} + \cdots + \Pi_n,$$

donde $\Pi_1, \ldots, \Pi_n \in \mathbb{F}_q[\boldsymbol{X}]$ son los polinomios simétricos elementales.

- $f \in M(n)$ tiene patrón $\lambda \Leftrightarrow \exists\, \boldsymbol{x} \in \mathbb{F}_q^n$ con $f = G(\boldsymbol{x}, T)$.
- $G(\boldsymbol{x}, T) \in A_s \Leftrightarrow \Pi_j(\boldsymbol{x}) = a_{n-j}$ para $1 \leq j \leq s$.

Se deduce que

$$\mathcal{T}_\lambda(A_s) \sim \frac{1}{n!} \cdot \left| \{ \Pi_1 = a_{n-1}, \ldots, \Pi_s = a_{n-s} \} \cap \mathbb{F}_q^n \right|.$$

Distribución de patrones de factorización

Junto con A. Cafure, E. Cesaratto, M. Pérez y M. Privitelli ([Adv Math Comm, 2012], [JCT-A, 2014], [Acta Arith, 2014]) estudiamos el lugar singular de intersecciones completas definidas por polinomios simétricos.

Teorema: Sea V una variedad definida por polinomios simétricos $F_i := G_i(\Pi_1, \ldots, \Pi_s)$ $(1 \leq i \leq n-r)$. Si $V(G_1, \ldots, G_{n-r})$ es una intersección completa no singular, entonces V es una intersección completa con $\operatorname{Sing} V \leq s-1$.

Combinando resultados de este tipo con estimaciones para intersecciones completas proyectivas singulares obtenemos:

Teorema: Si $p > 2$ y $n - s \geq 3$, entonces

$$\left| \mathcal{T}_\lambda(A_s) - \frac{q^{n-s}}{n!} \right| \leq \frac{(s+2)!}{n!} q^{n-s-\frac{1}{2}} + 6 \frac{((s+2)!)^2}{n!} q^{n-s-1}.$$

(precisa para $s \lesssim n/2$)

Cardinal promedio del conjunto de valores

También aplicamos esta metodología a otro clásico problema combinatorio: estimar el cardinal promedio del conjunto de valores.

Si $f \in \mathbb{F}_q[T]$, su conjunto de valores es $f(\mathbb{F}_q)$. Sea $\mathcal{V}(f) := |f(\mathbb{F}_q)|$.

Birch y Swinnerton–Dyer (1959): si $f \in \mathbb{F}_q[T]$ es "genérico",

$$\mathcal{V}(f) = \mu_n\, q + \mathcal{O}(q^{1/2}),$$

donde $n := \deg f$ y $\mu_n := \sum_{r=1}^{n} (-1)^{r-1}/r!$.

Cohen (1972): Si $\mathcal{V}(n,0) := \dfrac{1}{|M(n)|} \displaystyle\sum_{f \in M(n)} \mathcal{V}(f)$, entonces

$$\mathcal{V}(n,0) = \mu_n\, q + \mathcal{O}(1).$$

Cardinal promedio del conjunto de valores

Pregunta: qué se puede decir del promedio si algunos de los coeficientes de $f := T^n + a_{n-1}T^{n-1} + \cdots + a_0$ se fijan?

Sea $A_s := A_s(a_{n-1}, \ldots, a_{n-s})$ la familia

$$A_s := \left\{ f := T^n + a_{n-1}T^{n-1} + \cdots + a_0 : a_{n-s-1}, \ldots, a_0 \in \mathbb{F}_q \right\},$$

y consideremos $\mathcal{V}(n,s) := \dfrac{1}{|A_s|} \displaystyle\sum_{f \in A_s} \mathcal{V}(f)$.

Cohen (1973): Sea $\mathcal{V}(n,s)$ el cardinal promedio del conjunto de valores cuando $a_n, \ldots, a_{n-s} \in \mathbb{F}_q$ están fijos. Para $\mathrm{car}(\mathbb{F}_q) > n$,

$$\mathcal{V}(n,s) = \mu_n\, q + \mathcal{O}(q^{1/2}).$$

Cardinal promedio del conjunto de valores

Trabajo con E. Cesaratto, M. Pérez y M. Privitelli: reducción a estimaciones para intersecciones completas singulares.

Teorema 1: si $s \leq \frac{n}{2}$, entonces

$$\mathcal{V}(n,s) = \sum_{r=1}^{n-s} (-1)^r \binom{q}{r} q^{1-r} + \frac{1}{q^{n-s-1}} \sum_{r=n-s+1}^{n} \frac{(-1)^r}{r!}\, \chi_{n,s,r} + \mathcal{O}(1),$$

donde $\chi_{n,s,r}$ es el número de puntos $\mathbb{F}_q$–racionales de cierta intersección completa proyectiva singular de dimensión $n-s$ definida sobre $\mathbb{F}_q$.

Teorema 2: Para $s \leq n/2$ y cualquier característica de $\mathbb{F}_q$,

$$\mathcal{V}(n,s) = \mu_n\, q + c(n),$$

donde $c(n)$ es explícita y con "buen comportamiento".

Gracias!!!