Mirando hacia el futuro

Sección a cargo de

Antonio Viruel

En esta entrega disfrutamos de la narrativa de Andrei que nos muestra cómo de difusa y artificial es esa frontera entre lo que se da por llamar matemáticas aplicadas y matemáticas fundamentales. Veremos aquí cómo las técnicas de Teoría de Grupos, ambiente en el que el autor es uno de los referentes mundiales, se muestran tremendamente efectivas en un aspecto combinatorio como la generación de grafos expander, con aplicaciones directas a las ciencias de la computación.

Grafos, grupos y variedades: un punto de encuentro

por

Andrei Jaikin

1. Preludio

La ciencia actual es como nuestro universo que está en continua expansión. En algún lugar de este universo hay una galaxia que se llama Matemáticas. Sus estrellas se llaman Álgebra, Geometría, Teoría de Números... Cada estrella puede tener varios planetas que están habitados por matemáticos. A los matemáticos les gusta viajar a los planetas cercanos. Por ejemplo, los habitantes del planeta Teoría de Grupos son muy amigos de los de Teoría de Anillos. Pero cuando se trata de un viaje a otra estrella, por no decir a otra galaxia, son muy perezosos y siempre encuentran excusas para no ir. Sin embargo, en la galaxia de Matemáticas también hay varios agujeros negros. Allí las reglas y las costumbres cambian y los matemáticos ya no se dividen por los nombres de sus estrellas, y hasta hay visitantes de otras galaxias que comparten su vida con ellos. Dicen que si uno ha entrado en alguno de estos agujeros, nunca más quiere volver a su planeta. Os queremos contar sobre un agujero que se llama «Expanders». Pero tened mucho cuidado porque os podéis quedar atrapados. ¡Os hemos advertido!

2. Grafos expander

Supongamos que queremos diseñar una red (de ordenadores, carreteras, etc.) con muchos nodos. Cada enlace en esta red es muy costoso. Por lo tanto vamos a usar pocas conexiones. Sin embargo, queremos que si, como resultado de una anomalía, algunos enlaces se rompen, sólo un número pequeño de nodos se queden desconectados. Claramente este problema tiene una interpretación en términos de grafos.

Sea $X = (V, E)$ un grafo finito simple (sin lazos y sin aristas múltiples), es decir, V es el conjunto de sus vértices y $E \subseteq P_2(V)$ es el conjunto de aristas, donde $P_2(V)$ denota el conjunto de los pares de los elementos de V. La constante que mide la cantidad de enlaces es $d(X) = \frac{|E|}{|V|}$ y la constante que es responsable de la alta conectividad se llama el *parámetro isoparamétrico* de X y se define como

$$h(X) = \min_{A \subseteq V} \frac{|\partial A|}{\min\{|A|, |V \setminus A|\}},$$

donde ∂A (que se llama *frontera* de A) es el subconjunto de aristas de X que conectan los vértices de A con los que no están en A. Por lo tanto, buscamos los grafos con $d(X)$ pequeño y $h(X)$ grande. Es claro que $d(X)$ no puede ser demasiado pequeño ya que, para ser conexo, el número de aristas tiene que ser, como mínimo, uno menos que el número de vértices.

Para simplificar las cosas nos vamos a centrar sólo en los grafos *k-regulares*, es decir, los grafos con exactamente k aristas saliendo de cada vértice. En este caso $d(X) = \frac{k}{2}$. En estos términos, la pregunta que nos interesa se puede formular de la siguiente manera:

Pregunta principal. *Sea $k \geq 3$. ¿Existe una constante $\epsilon > 0$ y una familia infinita de grafos k-regulares X con $h(X) \geq \epsilon$?*

Una familia infinita de grafos k-regulares $\{X_i\}$ para la cual existe una constante $\epsilon > 0$ con $h(X_i) \geq \epsilon$ para todo i, se llama una familia de *expanders*. El primer interés en familias de grafos expanders surgió en los principios de los años 70. Su existencia para cada $k \geq 3$ fue probada por M. Pinsker [35] en 1973 usando métodos probabilísticos. Sin embargo para aplicaciones reales se necesita una manera explícita de producir estos grafos. El primer resultado en esta dirección lo consiguió G. Margulis en 1975 ([31]). Su construcción usa técnicas de representaciones de grupos. Vamos a explicarlo más tarde. Pero primero intentaremos crear una fuente abundante de ejemplos de grafos regulares.

3. Grafos de Cayley y de Schreier

Sea G un grupo finito y S un subconjunto de G simétrico ($S = S^{-1}$). El *grafo de Cayley* de G con respecto a S es el grafo $\mathrm{Cay}(G, S)$ cuyo conjunto de vértices coincide con G y $\{x, y\} \in P_2(G)$ es una arista de $\mathrm{Cay}(G, S)$ si $xy^{-1} \in S$.

Una generalización natural del concepto de grafo de Cayley es el *grafo de Schreier* $\mathrm{Sch}(G, H, S)$. Aquí H es un subgrupo de G y los vértices de $\mathrm{Sch}(G, H, S)$ son clases

izquierdas $G/H = \{gH : g \in G\}$. Un par $\{xH, yH\} \in P_2(G/H)$ es una arista de $\mathrm{Sch}(G, H, S)$ si $xHy^{-1} \cap S \neq \emptyset$.[1] Si H es un subgrupo normal de G, entonces existe una identificación natural entre $\mathrm{Sch}(G, H, S)$ y $\mathrm{Cay}(G/H, \bar{S})$, donde $\bar{S}$ denota la imagen de S en G/H.

La siguiente definición está motivada por la pregunta principal. Sea G un grupo generado por un conjunto finito simétrico S y $\{H_i\}$ una familia de subgrupos normales de G de índice finito. Decimos que G tiene la *propiedad* (τ) *con respecto a* $\{H_i\}$ si $\{\mathrm{Sch}(G, H_i, S)\}$ es una familia de expanders. Si $\{H_i\}$ es la familia de todos los subgrupos normales de G de índice finito, entonces simplemente decimos que G tiene la *propiedad* (τ).

Aunque los grafos de Schreier sí dependen del conjunto de generadores S, tener la propiedad (τ) con respecto a una familia de subgrupos sólo depende del grupo y la familia de subgrupos.

A continuación vamos a presentar distintos métodos para construir un grupo finitamente generado G que posee la propiedad (τ) con respecto a una familia infinita de subgrupos normales de índice finito, proporcionando así varias respuestas a la pregunta principal. Notemos que como nos interesan sólo subgrupos de G de índice finito, podemos suponer que G es *residualmente finito*, es decir, la intersección de sus subgrupos de índice finito es trivial. Por ejemplo, los grupos finitamente generados *lineales* (subgrupos de $\mathrm{GL}_n(K)$ para algún cuerpo K) son residualmente finitos. Estos grupos van a jugar un rol especial en nuestra exposición. Si $G \leq \mathrm{GL}_n(K)$ para algún cuerpo K y es finitamente generado, entonces $G \leq \mathrm{GL}_n(R)$ para un subanillo R finitamente generado de K. Para cada ideal I de índice finito en R podemos definir el subgrupo $G(I)$:

$$G(I) = \{g \in G : g \equiv 1 \pmod{I}\}.$$

Claramente $G(I)$ es un subgrupo de índice finito en G. Un *subgrupo de congruencia* de G es un subgrupo que contiene algún $G(I)$ donde I es un ideal de R de índice finito. Está claro que esta definición depende de la representación $G \leq \mathrm{GL}_n(R)$ del grupo G como matrices. A continuación, cuando nos referimos a un subgrupo de congruencia, siempre estará muy claro de qué representación se trata.

4. Expansión en variedades

Un grafo se convierte en un espacio métrico si vemos una arista como un intervalo $[0, 1]$. Vamos a buscar un análogo a la propiedad de expansión en espacios métricos que conocemos muy bien: variedades riemannianas M de volumen finito. La analogía es la siguiente: la frontera ∂A de un conjunto de vértices A corresponde a una hipersuperficie E que divide la variedad en dos partes X y Y, $|\partial A|$ corresponde al área $\mu(E)$ de E, $|A|$ al volumen $\lambda(X)$ de X y $|V \setminus A|$ al volumen $\lambda(Y)$ de Y. Esto nos lleva a la definición de la *constante de Cheeger* de M:

$$h(M) = \inf_E \frac{\mu(E)}{\min\{\lambda(X), \lambda(Y)\}}.$$

[1] Hemos adoptado esta definición para que $\mathrm{Sch}(G, H, S)$ sea un grafo simple.

La constante de Cheeger está muy ligada al operador de Laplace-Beltrami Δ_M. Por ejemplo, J. Cheeger [16] prueba que, para las variedades compactas,

$$\lambda_1(M) \geq \frac{h(M)^2}{4},$$

donde $\lambda_1(M)$ denota el menor autovalor positivo de Δ_M. Por otro lado, P. Buser [15] estableció que si la curvatura de Ricci $R(M)$ satisface $R(M) \geq -(\dim M - 1)a^2$ para algún $a \geq 0$, entonces

$$\lambda_1(M) \leq 2a(\dim M - 1)h(M) + 10h(M)^2.$$

Por lo tanto, la alta expansión en variedades riemannianas compactas corresponde al alto valor de $\lambda_1(M)$. En particular, obtenemos el siguiente resultado.

PROPOSICIÓN 4.1. *Sea M una variedad compacta riemanniana y $\{M_i\}$ una familia de recubrimientos finitos de M. Entonces existe $\epsilon > 0$ tal que $h(M_i) \geq \epsilon$ para todo i si y sólo si existe $\delta > 0$ tal que $\lambda_1(M_i) \geq \delta$ para todo i.*

Vamos a construir una familia de variedades riemannianas con el autovalor del laplaciano uniformemente mayor que cero. Sea

$$\mathcal{H} = \{z = x + iy \in \mathbb{C} : x, y \in \mathbb{R}, y > 0\}$$

el semiplano superior en $\mathbb{C}$. El grupo $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$ actúa sobre $\mathcal{H}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

Esta acción conserva la métrica hiperbólica de $\mathcal{H}$, $ds^2 = \frac{1}{y^2}(dx^2 + dy^2)$. Si G es un subgrupo discreto de $\mathrm{PSL}_2(\mathbb{R})$, entonces el cociente $M = G\backslash\mathcal{H}$ es una variedad riemanniana con laplaciano $\Delta_M = -y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$. Un *subgrupo de congruencia* de $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ es un subgrupo que contiene a

$$\Gamma(m) = \{A \in \mathrm{PSL}_2(\mathbb{Z}) : A \equiv \pm 1 \pmod{m}\}$$

para algún m.

TEOREMA 4.2 (A. Selberg [38]). *Sea G un subgrupo de congruencia de $\mathrm{PSL}_2(\mathbb{Z})$. Entonces $\lambda_1(G\backslash\mathcal{H}) \geq \frac{3}{16}$.*

De hecho, este resultado nos proporciona una familia explícita de expanders.

COROLARIO 4.3. *El grupo $\mathrm{PSL}_2(\mathbb{Z})$ tiene propiedad (τ) con respecto a $\{\Gamma(m)\}$.*

En particular, si

$$S = \left\{ \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\},$$

entonces la familia de grafos 3-regulares $\{\mathrm{Sch}(\mathrm{PSL}_2(\mathbb{Z}), \Gamma(m), S) : m \geq 2\}$ es una familia de expanders.

Idea de la demostración. Aunque $M_m = \Gamma(m)\backslash\mathcal{H}$ no sea compacto, el resultado de la proposición 4.1 se puede también aplicar en esta situación (para los detalles ver [15, sección 7]). Por lo tanto, $h(M_m) \geq c_1$ para una constante que se puede calcular explícitamente.

Fijemos la clausura F de un dominio fundamental para $\mathrm{PSL}_2(\mathbb{Z})$ en $\mathcal{H}$:

$$F = \left\{ z \in \mathcal{H} : |z| \geq 1,\ |\operatorname{Re}(z)| \leq \frac{1}{2} \right\}.$$

Entonces

$$S = \left\{ \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} = \{ g \in \mathrm{PSL}_2(\mathbb{Z}) : g \cdot F \cap F \neq \emptyset \}.$$

Notemos que el grafo de Schreier $X_m = \mathrm{Sch}(\mathrm{PSL}_2(\mathbb{Z}), \Gamma(m), S)$ se puede «dibujar» de forma natural en M_m: las $\mathrm{PSL}_2(\mathbb{Z})$-traslaciones de las caras $\Gamma(m)\backslash\Gamma(m)\cdot F$ en M_m corresponden a los vértices del grafo X_m, y dos vértices están conectados por una arista si las correspondientes caras se intersecan. Claramente, una partición de los vértices del grafo en dos subconjuntos disjuntos A y $V \setminus A$ induce una partición de la variedad M_m en dos partes X e Y, cuya intersección E corresponde a la frontera ∂A. Por lo tanto, la cota inferior para $h(M_m) \geq c_1$ implica una cota inferior $h(X_m) \geq c_2$ para alguna constante positiva c_2 que también se puede calcular explícitamente. □

Es muy llamativo que, para probar este resultado combinatorio, se requiere pasar por el mundo continuo. Recientemente J. Bourgain y A. Gamburd crearon un método que ha permitido demostrar el corolario 4.3 sin uso de geometría. Sin embargo, sigue siendo una demostración complicada. Por lo tanto, esperamos que puedan surgir nuevas ideas y por eso planteamos el siguiente problema.

Problema 1. *Encontrar una demostración «elemental» del corolario 4.3.*

5. Caracterización espectral de grafos expander

En la sección anterior hemos visto que la propiedad de expansión de variedades riemanianas compactas se puede caracterizar en términos de sus laplacianos. Resulta que una caracterización análoga existe para grafos. Sea $X = (V, E)$ un grafo simple k-regular finito y $\mathcal{F}(V) = \{f : V \to \mathbb{C}\}$. El laplaciano de X es el operador $\Delta_X : \mathcal{F}(V) \to \mathcal{F}(V)$ definido como

$$\Delta_X(f)(v) = f(v) - \frac{1}{k} \sum_{\{v,w\} \in E} f(w).$$

Es un operador autoadjunto positivo y las funciones constantes están en el núcleo de Δ_X. Denotemos por $\lambda_1(X)$ el segundo autovalor minimal de Δ_X (que puede ser cero si el grafo no es conexo). Entonces $h(X)$ y $\lambda_1(X)$ están ligados mediante las siguientes desigualdades ([18, 1, 41, 2]):

$$\lambda_1(X) \geq \frac{h(X)^2}{2k^2}, \quad h(X) \geq \frac{k\lambda_1(X)}{2}.$$

Por lo tanto, obtenemos la siguiente caracterización de los expanders.

PROPOSICIÓN 5.1. *Sea $\{X_i\}$ una familia de grafos k-regulares. Entonces existe $\epsilon > 0$ tal que $h(X_i) \geq \epsilon$ para todo i si y sólo si existe $\delta > 0$ tal que $\lambda_1(X_i) \geq \delta$ para todo i.*

Como en el caso de variedades, resulta más fácil obtener una cota para $\lambda_1(X)$ que para $h(X)$. De hecho, es posible construir una familia de expanders $\{X_i\}$ con un valor de $\lambda_1(X_i)$ óptimo.

TEOREMA 5.2.

1. *Para cada $k \in \mathbb{N}$ y $\epsilon > 0$ existe sólo un número finito de grafos k-regulares finitos X con $\lambda_1(X) \geq 1 + \epsilon - \frac{2\sqrt{k-1}}{k}$.*
2. *Si $k = p^m + 1$ con p primo, entonces existe una construcción explícita de una familia infinita $\{X_i\}$ de grafos k-regulares tales que $\lambda_1(X_i) \geq 1 - \frac{2\sqrt{k-1}}{k}$.*

El primer resultado se debe a Alon y Boppana ([28]). El segundo es la famosa construcción de A. Lubotzky, R. Phillps y P. Sarnak [30] (independientemente obtenido también por G. Margulis [32] y posteriormente generalizado por M. Morgenstern [33]), que usa en su solución la conjetura de Ramanujan-Petersson sobre valores de la función τ. Por eso los grafos k-regulares finitos X tales que $\lambda_1(X) \geq 1 - \frac{2\sqrt{k-1}}{k}$ se llaman *grafos de Ramanujan*. Cuando k no es igual a una potencia de un primo más 1, entonces no se conoce si existe una familia infinita de grafos k-regulares de Ramanujan.

PREGUNTA 2. *¿Para qué valores de k existe una familia infinita de grafos k-regulares de Ramanujan?*

Aunque los grafos de Ramanujan son los «mejores» expanders desde el punto de vista del primer autovalor del laplaciano, no tienen por qué ser los «mejores» desde el punto de vista de la constante isoparamétrica. De hecho, todavía no hay construcciones explícitas de familias expanders con la constante isoparamétrica tan «buena» como la de grafos aleatorios.

En el caso de los grafos de Schreier con respecto a subgrupos normales, resulta que la caracterización espectral de grafos expanders se puede interpretar en términos de representaciones de grupos.

PROPOSICIÓN 5.3. *Sea G un grupo generado por un conjunto finito simétrico S y $\{H_i\}$ una familia de subgrupos normales de G de índice finito. Entonces G tiene propiedad (τ) con respecto a $\{H_i\}$ si y sólo si existe $\epsilon > 0$ tal que, para cualquier representación $\pi : G \to U(V)$, de G como operadores unitarios de un espacio de Hilbert V de dimensión finita que satisface*

(a) $V^G = \{v \in V : \pi(g)v = 0 \ \forall g \in G\} = \{0\}$ y

(b) $H_i \leq \ker \pi$ para algún i,

se cumple que $\|\pi(s)v - v\| \geq \epsilon \|v\|$ para todo $s \in S$ y $v \in V$.

De hecho, en la proposición anterior podemos considerar sólo representaciones irreducibles. Por lo tanto, hemos construido un puente que relaciona la propiedad (τ) de G con representaciones irreducibles de sus cocientes finitos.

6. La propiedad (T) de Kazhdan

Viendo la proposición 5.3, la definición de la *propiedad* (T) que vamos a presentar en breve nos parecerá bastante natural. Sin embargo, el desarrollo histórico ha sido muy distinto de como hemos contado las cosas. D. Kazhdan introdujo la propiedad (T) a mediados de los años 60 [27] motivado por una pregunta completamente diferente. Quería demostrar que los retículos (subgrupos discretos de covolumen finito) en grupos de Lie simples de rango alto son finitamente generados. Para resolver este problema define una propiedad de representaciones de grupos localmente compactos que dice que, en la topología de Fell, la representación trivial de G está aislada de las representaciones unitarias que no tienen vectores G-invariantes no triviales. A esta propiedad la llama propiedad (T). También D. Kazhdan observa que, para grupos discretos, la propiedad (T) implica que el grupo es finitamente generado; y, si un grupo localmente compacto posee la propiedad (T), entonces sus retículos la tienen también. Finalmente, D. Kazhdan demuestra que los grupos de Lie de rango mayor que dos la tienen. Posteriormente, L. Vaserstein extiende el método de D. Kazhdan también a los grupos de Lie de rango 2.

Teorema 6.1 ([27, 46]). *Sea G un retículo de un grupo de Lie simple de rango como mínimo 2. Entonces G satisface la propiedad (T) de Kazhdan.*

Resulta sorprendente que una propiedad tan técnica haya encontrado sus aplicaciones no sólo en el problema que hemos descrito, sino en una amplia variedad de cuestiones en muy distintas áreas de las matemáticas. En este artículo sólo vamos a definir la propiedad (T) para grupos discretos finitamente generados.

Sea G un grupo generado por un conjunto finito simétrico S. Definamos la *constante de Kazhdan de G con respecto a S* como

$$\kappa(G,S) = \inf_{\substack{\pi: G\to U(V)\\ 0\neq v\in V}} \max_{s\in S} \frac{\|\pi(s)v - v\|}{\|v\|},$$

donde $\pi : G \to U(V)$ recorre todas las representaciones unitarias de G tales que $V^G = \{0\}$. Decimos que G tiene la propiedad (T) si $\kappa(G,S) > 0$ para algún conjunto finito S de G. La proposición 5.3 nos dice que la propiedad (τ) es una forma débil de la propiedad (T). En 1975, G. Margulis [31] se dio cuenta que los grupos que tienen la propiedad (T) proporcionan una fuente de ejemplos de familias de expanders.

Corolario 6.2. *Sea $G = \mathrm{SL}_3(\mathbb{Z})$, $G(m) = \{A \in G : A \equiv 1 \pmod m\}$ y*

$$S = \{\mathrm{Id} \pm E_{ij} : 1 \leq i \neq j \leq 3\}.$$

Entonces $\{\mathrm{Sch}(G, G(m), S) : m \geq 2\}$ es una familia de expanders.

Demostración. Como $\mathrm{SL}_3(\mathbb{Z})$ es un retículo en $\mathrm{SL}_3(\mathbb{R})$, por el teorema 6.1, $\mathrm{SL}_3(\mathbb{Z})$ posee la propiedad (T) y por lo tanto tiene la propiedad (τ). □

Notemos que el corolario sólo dice que $\kappa(G,S) > 0$, sin proporcionar ninguna cota explícita. Esto se debe a que el método de Kahdan no es constructivo: la propiedad (T) de $\mathrm{SL}_3(\mathbb{Z})$ es consecuencia de la propiedad (T) del grupo de Lie $\mathrm{SL}_3(\mathbb{R})$.

La primera cota explícita para $\kappa(G,S)$ fue conseguida por Y. Shalom [39]. El método de Shalom se puede caracterizar como algebraico porque usa directamente la estructura del grupo $\mathrm{SL}_3(\mathbb{Z})$ y no el hecho de ser retículo en un grupo de Lie.

En los últimos años, con los métodos algebraicos (algunos distintos de los de Shalom) se ha conseguido demostrar la propiedad (T) para grupos «grandes». El siguiente ejemplo es un resultado de M. Ershov y A. Jaikin.

TEOREMA 6.3 ([20]). *Sea R un anillo asociativo unitario generado por*

$$T = \{1 = t_0, t_1, \ldots, t_k\}.$$

Sea $n \geq 3$ y $G = \mathrm{EL}_n(R)$ el grupo generado por matrices

$$\{\mathrm{Id} + rE_{i,j} : 1 \leq i \neq j \leq n,\, r \in R\}.$$

Sea $S = \{\mathrm{Id} \pm tE_{i,j} : 1 \leq i \neq j \leq n,\, t \in T\}$. Entonces existe una constante explícita c tal que

$$\kappa(G,S) \geq \frac{c}{\sqrt{n+k}}.$$

El método introducido en [20] permitió desarrollar una técnica para demostrar la propiedad (T) en grupos graduados por sistemas de raíces [21], o demostrar que grupos de Golod-Shafarevich tienen una imagen infinita que posee la propiedad (T) y, por lo tanto, no son amenables [19]. Es muy probable que estos grupos «grandes» con la propiedad (T) puedan servir de contraejemplos a algunas preguntas que hasta ahora estaban fuera de nuestro alcance. Como ejemplo podemos mencionar la siguiente pregunta que relaciona el crecimiento de subgrupos con la propiedad (T).

PREGUNTA 3. *Sea $a_n(G)$ el número de subgrupos de índice n en G. ¿Es cierto que, si G tiene la propiedad (T), entonces*

$$\lim_{n\to\infty} \sqrt[n]{a_n(G)} = 1\,?$$

7. EL MÉTODO DE BOURGAIN-GAMBURD

Hay una gran diferencia entre las familias de expanders que aparecen en las secciones 4 y 6. Los que construimos usando la propiedad (T) tienen carácter local. Es decir, la propiedad de expansión de grafos es consecuencia de la estructura de un entorno grande de un vértice (notemos que, en un grafo de Cayley, todos las bolas del mismo radio son isomorfas, porque el grupo de automorfismos del grafo actúa transitivamente sobre sus vértices). Esto se debe a un resultado de Y. Shalom [40] que dice que, para un grupo discreto G con la propiedad (T), existe un grupo finitamente presentado $\tilde{G}$ tal que $\tilde{G}$ tiene la propiedad (T) y G es un cociente de $\tilde{G}$.

Los ejemplos de la sección 4 son completamente diferentes. Por ejemplo, usando los métodos de la sección 4 se puede producir una familia de expanders $\{X_i\}$ tal que, para cada n, cualquier bola de radio n en X_i con $i \geq n$ es isomorfa a un árbol (recordemos que un *árbol* es un grafo en el que dos vértices cualesquiera están

conectados por exactamente un camino). Por lo tanto, la propiedad de expansión de los grafos X_i es una consecuencia de la estructura global de estos grafos. En la sección 4 la propiedad de expansión se ha obtenido analizando unas variedades riemannianas. En [5], J. Bourgain and A. Gamburd han introducido un método directo para probar la propiedad de expansión que no sólo es aplicable para los ejemplos de la sección 4, sino que proporciona una gran colección de familias de expanders a partir de grafos de Scheier de grupos lineales sobre cuerpos de números ([5, 6, 7, 9, 37, 45]). El siguiente teorema es un ejemplo de los resultados de este tipo:

Teorema 7.1. *Sea G un subgrupo de $\mathrm{SL}_n(\mathbb{Z})$ finitamente generado y denso en sentido de Zariski (es decir, si $f(a_{11},\dots,a_{nn})$ es un polinomio con coeficientes complejos que se anula sobre todos los elementos de G, entonces f es múltiplo de $\det((a_{ij}))-1$). Entonces G tiene la propiedad (τ) con respecto a subgrupos de congruencia*

$$\big\{G(m)=\{g\in G : g\equiv 1 \pmod m\}\big\}_{m\in\mathbb{N}}.$$

Vamos a describir brevemente en qué consiste el método de Bourgain-Gamburd. Sea $\{X_i=\mathrm{Cay}(G_i,S_i)\}$ una familia de grafos de Cayley con $k=|S_i|$. Queremos ver que estos grafos forman una familia de expanders. El punto de partida es considerar una distribución μ_i en G_i que toma valores $\frac{1}{k}$ en puntos de S_i y 0 en los demás puntos. La idea de Bourgain y Gamburd consiste en analizar el comportamiento de las distribuciones $\mu_i^{(s)}$ en G_i, donde $\mu_i^{(s)}$ se define como

$$\mu_i^{(s)}(g)=(\mu^{(s-1)}*\mu)(g)=\sum_{h\in G_i}\mu^{(s-1)}(gh^{-1})\mu(h)\qquad (g\in G_i).$$

El valor de $\mu_i^{(s)}(g)$ es la probabilidad de llegar a g desde 1 en el grafo X_i en s pasos.

Resulta que si la $[c\log_2|G_i|]$-potencia de μ_i, para una constante c fija, es aproximadamente igual a la distribución uniforme U_{G_i} ($U_{G_i}(g)=\frac{1}{|G_i|}$ para todo $g\in G_i$), entonces $\{X_i=\mathrm{Cay}(G_i,S_i)\}$ es una familia de expanders.

Proposición 7.2. *Los grafos $\{X_i=\mathrm{Cay}(G_i,S_i)\}$ forman un familia de expanders si y sólo si existen constantes $c>0$ y $\epsilon>0$ tales que*

$$\|\mu_i^{([c\log_2|G_i|])}-U_{G_i}\|_2^2=\sum_{g\in G_i}\Big|\mu_i^{([c\log_2|G_i|])}(g)-\frac{1}{|G_i|}\Big|^2\le|G_i|^{-1-\epsilon}.$$

Para aplicar el criterio anterior, Bourgain y Gamburd propusieron dividir el análisis del comportamiento de $\mu_i^{(s)}$ en los siguientes pasos.

Paso 1: Demostrar que existe una constante $c_1>0$ y $\epsilon_1>0$ tales que

$$\mu_i^{(2[c_1\log_2|G_i|])}(1)=\|\mu_i^{([c_1\log_2|G_i|])}\|_2^2\le|G_i|^{-\epsilon_1}.$$

En grafos de Schreier de grupos lineales este resultado se obtiene como consecuencia de la alternativa de Tits [44], que dice que un grupo lineal contiene un grupo libre o es *virtualmente resoluble* (es decir, contiene un subgrupo de índice finito resoluble).

Este paso se puede interpretar como que, en $2[c_1 \log_2 |G_i|]$ pasos, la concentración en 1 es pequeña.

Paso 2: Demostrar que existe una constante $c_2 > 0$ y $\epsilon_2 > 0$ tales que, para cada subgrupo H de G_i,

$$\mu_i^{(2[c_2 \log_2 |G_i:H|])}(H) = \sum_{h \in H} \mu_i^{(2[c_2 \log_2 |G_i:H|])}(h) \leq |G_i : H|^{-\epsilon_2}.$$

Este paso dice que la concentración de una potencia controlada de μ_i en subgrupos propios de G_i es pequeña. En el primer caso donde se aplicó el método de Bourgain-Gamburd ([5]), la prueba de este paso no era mucho más complicada que la del paso 1. Sin embargo, para resultados posteriores ([6, 7, 9, 37, 45]) la demostración de este paso requiere unos resultados muy potentes y sofisticados ([4, 34, 8]).

Paso 3: Demostrar que para cada $\delta > 0$ existe una constante $\epsilon_3(\delta) > 0$ tal que, si $s \geq [c_1 \log_2 |G_i|]$ y $\|\mu_i^{(s)}\|_2^2 \geq |G_i|^{-1+\delta}$, entonces

$$\|\mu^{(2s)}\|_2^2 \leq \|\mu^{(s)}\|_2^2 \, |G_i|^{-\epsilon_3(\delta)}.$$

La prueba de este paso usa el lema de Balog-Szemerédi-Gowers ([43]) y la estructura de grupos K-aproximados lineales ([24, 36, 13]).

Paso 4: Demostrar que existen constantes $c_4 > 0$ y $\epsilon_4 > 0$ tales que

$$\|\mu_i^{([c_4 \log_2 |G_i|])} - U_{G_i}\|_2^2 \leq |G_i|^{-1-\epsilon_4}.$$

El paso final se obtiene como consecuencia de los pasos anteriores y la información sobre grados de representaciones irreducibles de grupos G_i (la idea que tiene origen en el trabajo de T. Gowers [23]).

El método de Bourgain y Gamburd ha sido un tremendo avance en la teoría de expanders. Sin embargo, para la realización de algunos pasos se requieren técnicas muy sofisticadas que no son siempre aplicables en otras situaciones. Por lo tanto, es de esperar que, con el tiempo, van a surgir nuevas ideas que ayuden a extender los resultados a situaciones todavía no alcanzables hasta ahora. Por ejemplo, es muy de esperar que la siguiente pregunta tendrá pronto una respuesta afirmativa.

PREGUNTA 4. *Sea G un subgrupo de $\mathrm{GL}_n(\mathbb{Z}[\frac{1}{f}])$ y supongamos que cualquier subgrupo de índice finito de G tiene abelianización finita. ¿Es cierto que G tiene la propiedad (τ) con respecto a subgrupos $\{G(m) : (m, f) = 1\}$?*

Sin embargo, queda muchísimo por hacer en característica positiva. Podemos empezar, por ejemplo, con el siguiente problema.

PREGUNTA 5. *Sea G un subgrupo de $\mathrm{SL}_2(\mathbb{F}_p[t])$ y supongamos que G es denso en $\mathrm{SL}_2(\mathbb{F}_p[[t]])$. ¿Es cierto que G tiene la propiedad (τ) con respecto a subgrupos*

$$\big\{G(i) = \{g \in G : g \equiv 1 \pmod{t^i}\}\big\}\,?$$

8. Grupos finitos y expansión

Como vimos en las secciones anteriores los grafos de Cayley son una fuente principal de familias de expanders. Por lo tanto, es muy natural intentar entender cuándo un grupo finito se puede usar para construir un grafo con buenas propiedades de expansión. Esto nos lleva a la siguiente definición.

Definición. *Sea $\{G_i\}$ una familia de grupos finitos. Decimos que es una* familia de expanders *si existe k y si para cada i existe un sistema generador S_i de G_i con k elementos tales que $\{\mathrm{Cay}(G_i, S_i)\}$ es una familia de grafos expanders.*

No es muy difícil establecer algunas condiciones necesarias para que una familia de grupos sea una familia de expanders. Por ejemplo, tienen que tener el número de generadores acotado o no ser resolubles con longitud derivada acotada. Sin embargo, no es de esperar que se puedan caracterizar completamente estas familias. La familia más famosa de grupos finitos es, por supuesto, la familia de grupos simples no abelianos. Como resultado de una serie de trabajos se ha conseguido demostrar que estos grupos forman una familia de expanders:

Teorema 8.1 (E. Breuillard, B. Green, M. Kassabov, A. Lubotzky, N. Nikiolov, T. Tao). *La familia de grupos finitos simples no abelianos es una familia de expanders.*

El empuje principal a la demostración de este teorema lo ha dado M. Kassabov, que demostró el teorema para $\mathrm{PSL}_n(\mathbb{F}_q)$ y los grupos alternados. Posteriormente, junto con A. Lubotzky y N. Nikolov han conseguido demostrar el teorema para todos los grupos simples salvo para los grupos de Suzuki (las referencias y una descripción más amplia se pueden consultar en [26]). El caso de los grupos de Suzuki ha sido resuelto en [14] usando el método de Bourgain-Gamburd. La construcción de sistemas de generadores en las demostraciones de Kassabov, Lubotzky y Nikolov es explícita. Sin embargo, no lo es en la demostración de Breuillard, Green y Tao. Por lo tanto, formulamos el siguiente problema.

Problema 6. *Construir explícitamente generadores con respecto de los cuales los grupos de Suzuki forman una familia de expanders.*

Otra pregunta natural cuya solución daría una nueva demostración del teorema 8.1 es la siguiente.

Pregunta 7. *¿Es cierto que existe un grupo finitamente generado que posee la propiedad (τ) y tiene como imagen cualquier grupo finito simple no abeliano?*

Algunos casos de la pregunta anterior se conocen. Por ejemplo, en [21] se construye un grupo que posee la propiedad (T) y que tiene como imagen cualquier grupo finito simple de tipo Lie de rango ≥ 2.

9. La expansión uniforme

Sea G un grupo generado por un conjunto simétrico finito S. Podemos considerar la función $r_S(n)$ que cuenta el número elementos de G que se pueden expresar como producto de, como mucho, n elementos de S. Esta función se llama

la *función de crecimiento de palabras* de G y claramente depende de S. Sin embargo, muchas propiedades de $r_S(n)$ sólo dependen de G. Por ejemplo, pongamos $l_S = \liminf_{n\to\infty} \sqrt[n]{r_S(n)}$. La constante l_S depende de S, pero la propiedad de ser l_S positiva o igual a cero sólo depende del grupo G. En el caso que l_S sea positiva, decimos que G tiene *crecimiento de palabras exponencial*. En el caso que exista $\epsilon > 0$ tal que $l_S \geq \epsilon$ para todo sistema generador S, decimos que G tiene *crecimiento de palabras exponencial uniforme*. La alternativa de Tits [44] implica que un grupo finitamente generado lineal tiene crecimiento exponencial o es virtualmente resoluble. En la última década se han producido unos resultados espectaculares en esta área. En 2005, A. Eskin, S. Mozes y H. Oh [22] prueban que un grupo lineal sobre un cuerpo de característica cero que no es virtualmente resoluble tiene crecimiento de palabras exponencial uniforme. Este resultado ha sido mejorado en los trabajos de E. Breuillard y T. Gelander [12, 10].

TEOREMA 9.1 (E. Breuillard). *Para cada entero d, existe una constante $N(d)$ tal que, si K es un cuerpo y S es un conjunto finito de $\mathrm{GL}_d(K)$ que genera un grupo no virtualmente resoluble, entonces $S^{N(d)}$ contiene dos elementos que generan un grupo libre no abeliano.*

La propiedad de expansión en grupos se puede ver como una forma fuerte de crecimiento exponencial. Por eso, a la vista de los resultados anteriores es muy natural conjeturar la existencia también de un tipo de expansión uniforme en grupos lineales. Casi nada se conoce todavía al respecto. Vamos a formular algunas preguntas que representan los tipos de resultados que se esperan.

PREGUNTA 8. *¿Es cierto que existe $\epsilon > 0$ tal que, para cualquier primo p y para cualquier sistema generador S de $\mathrm{SL}_n(\mathbb{F}_p)$,*

$$h(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S)) \geq \epsilon\,?$$

Un resultado parcial en esta dirección se ha obtenido en [11].

PREGUNTA 9. *Sea p un primo. ¿Es cierto que existe $\epsilon > 0$ tal que, para cualquier k y para cualquier sistema generador S de $\mathrm{SL}_n(\mathbb{Z}/(p^k))$, se cumple*

$$h(\mathrm{Cay}(\mathrm{SL}_n(\mathbb{Z}/(p^k)), S)) \geq \epsilon\,?$$

Aunque no sea evidente, la respuesta positiva a una de las dos preguntas implica que los subgrupos finitamente generados y Zariski densos en $\mathrm{SL}_n(\mathbb{C})$ tienen crecimiento de palabras exponencial uniforme. La pregunta 9 también se puede formular en términos de grupos profinitos.

PREGUNTA 10. *Sea S un sistema generado finito de $G = \mathrm{SL}_n(\mathbb{Z}_p)$. ¿Es*

$$\{\mathrm{Sch}(G, G(p^k), S) : k \geq 1\}$$

una familia de expanders?

Aunque parezca que la pregunta 10 es más débil que la pregunta 9, porque no fija ninguna cota inferior, en realidad, usando que $\mathrm{SL}_n(\mathbb{Z}_p)$ es compacto se puede demostrar que las dos preguntas son equivalentes.

El hecho de que los generadores en la pregunta 10 los consideramos en $\mathrm{SL}_n(\mathbb{Z}_p)$, y no en $\mathrm{SL}_n(\mathbb{Z})$ como en el teorema 7.1, dificulta por ahora la aplicación del método de Bourgain-Gamburd para la resolución del problema.

Es muy de esperar que la propiedad uniforme también tenga lugar en característica positiva.

Pregunta 11. *Sea S un sistema generador finito de $G = \mathrm{SL}_n(\mathbb{F}_p[[t]])$. ¿Es*

$$\{\mathrm{Sch}(G, G(t^k), S) : k \geq 1\}$$

una familia de expanders?

10. Epílogo

Claramente, en un espacio tan limitado como este artículo hemos podido presentar sólo los resultados y problemas que nos parecen los más interesantes (y, por supuesto, cercanos a nuestros intereses matemáticos). Como consecuencia, muchos aspectos se han quedado fuera de nuestra consideración. Por lo tanto, recomendamos al lector interesado mirar también los siguientes libros y exposiciones.

Para una introducción a grafos expanders y sus aplicaciones en matemáticas y ciencias de computación se puede ver [17, 28, 29, 25]. Para más información sobre la propiedad (T) se puede consultar el libro [3]. Una buena exposición del método de Bourgain-Gamburd está en la página web de T. Tao [42].

Aquí termina nuestra excursión al agujero negro «Expanders». Como vimos, allí han construido sus palacios matemáticos tan ilustres como Bourgain, Kazhdan, Lubotzky, Margulis, Sarnak, Selberg, Tao, y Wigderson, entre otros. Sin embargo todavía queda mucho terreno libre donde podemos plantar nuestras casas.

Referencias

[1] N. Alon, Eigenvalues and expanders, *Combinatorica* **6** (1986), 83–96.

[2] N. Alon y V.D. Milman, λ_1, isoperimetric inequalities for graphs, and superconcentrators, *J. Combin. Theory B* **38** (1985), 78–88.

[3] B. Bekka, P. de la Harpe y A. Valette, *Kazhdan's property* (T), New Mathematical Monographs, 11, Cambridge University Press, Cambridge, 2008.

[4] P. Bougerol y J. Lacroix, *Products of Random Matrices with Applications to Schrödinger Operators*, Progress in Probability and Statistics, vol. 8, Birkhäuser, Boston, 1985.

[5] J. Bourgain y A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, *Ann. of Math.* **167** (2008), 625–642.

[6] J. Bourgain y A. Gamburd, Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. I, *J. Eur. Math. Soc.* **10** (2008), 987–1011.

[7] J. Bourgain y A. Gamburd, Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. II, with an appendix by J. Bourgain, *J. Eur. Math. Soc.* **11** (2009), 1057–1103.

[8] J. BOURGAIN, A. FURMAN, E. LINDENSTRAUSS y S. MOZES, Stationary measures and equidistribution for orbits of non-abelian semigroups on the torus, *J. Amer. Math. Soc.* **24** (2011), 231–280.

[9] J. BOURGAIN y P.P. VARJÚ, Expansion in $\mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$, q arbitrary, *Invent. Math.* **188** (2012), 151–173.

[10] E. BREUILLARD, A strong Tits alternative. Prepublicación, `http://arxiv.org/abs/0804.1395`.

[11] E. BREUILLARD y A. GAMBURD, Strong uniform expansion in $\mathrm{SL}(2,p)$, *Geom. Funct. Anal.* **20** (2010), 1201–1209.

[12] E. BREUILLARD y T. GELANDER, Uniform independence in linear groups, *Invent. Math.* **173** (2008), 225–263.

[13] E. BREUILLARD, B. GREEN y T. TAO, Approximate subgroups of linear groups, *Geom. Funct. Anal.* **21** (2011), 774–819.

[14] E. BREUILLARD, B. GREEN y T. TAO, Suzuki groups as expanders, *Groups Geom. Dyn.* **5** (2011), 281–299.

[15] P. BUSER, A note on the isoperimetric constant, *Ann. Sci. École Norm. Sup.* **15** (1982), 213–230.

[16] J. CHEEGER, A lower bound for the smallest eigenvalue of the Laplacian, *Problems in Analysis: A Symposium in Honor of Salomon Bochner* (R.C. Gunning, ed.), 195–199, Princeton Univ. Press, Princeton, 1970.

[17] G. DAVIDOFF, P. SARNAK y A. VALETTE, *Elementary number theory, group theory and Ramanujan graphs*, LMS Student Texts 55, Cambridge University Press, Cambridge, 2003.

[18] J. DODZIUK, Difference equations, isoperimetric inequality and transience of certain random walks, *Trans. Amer. Math. Soc.* **284** (1984), 787–794.

[19] M. ERSHOV, Kazhdan quotients of Golod-Shafarevich groups, with appendices by Andrei Jaikin-Zapirain, *Proc. Lond. Math. Soc.* **102** (2011), 599–636.

[20] M. ERSHOV y A. JAIKIN-ZAPIRAIN, Property (T) for noncommutative universal lattices, *Invent. Math.* **179** (2010), 303–347.

[21] M. ERSHOV, A. JAIKIN-ZAPIRAIN y M. KASSABOV, Property (T) for groups graded by root systems. Prepublicación.

[22] A. ESKIN, S. MOZES y H. OH, On uniform exponential growth for linear groups, *Invent. Math.* **160** (2005), 1–30.

[23] W.T. GOWERS, Quasirandom groups, *Combin. Probab. Comput.* **17** (2008), 363–387.

[24] H.A. HELFGOTT, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math. (2)* **167** (2008), 601–623.

[25] S. HOORY, N. LINIAL y A. WIGDERSON, Expander graphs and their applications, *Bull. Amer. Math. Soc. (N.S.)* **43** (2006), 439–561.

[26] M. KASSABOV, A. LUBOTZKY y N. NIKOLOV, Finite simple groups as expanders, *Proc. Natl. Acad. Sci. USA* **103** (2006), 6116–6119.

[27] D.A. KAZHDAN, Connection of the dual space of a group with the structure of its closed subgroups, *Funct. Anal. Appl.* **1** (1967), 63–65.

[28] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures, with an appendix by Jonathan D. Rogawski*, Progress in Mathematics, 125, Birkhäuser Verlag, Basel, 1994. Reeditado en Modern Birkhäuser Classics, 2010.

[29] A. Lubotzky, Expander graphs in pure and applied mathematics, *Bull. Amer. Math. Soc. (N.S.)* **49** (2012), 113–162.

[30] A. Lubotzky, R. Phillips y P. Sarnak, Ramanujan graphs, *Combinatorica* **8** (1988), 261–277.

[31] G.A. Margulis, Explicit constructions of concentrators, *Problems Inform. Transmission* **10** (1975), 325–332.

[32] G.A. Margulis, Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators, *Problems Inform. Transmission* **24** (1988), 39–46.

[33] M. Morgenstern, Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q, *J. Combin. Theory Ser. B* **62** (1994), 44–62.

[34] M.V. Nori, On subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$, *Invent. Math.* **88** (1987), 257–275.

[35] M. Pinsker, On the complexity of a concentrator, *7th International Teletraffic Conference* (Stockholm, June 1973), 318/1–318/4.

[36] L. Pyber y E. Szabó, Growth in finite simple groups of Lie type of bounded rank. Prepublicación, `http://arxiv.org/abs/1005.1858`.

[37] A. Salehi Golsefidy y P.P. Varjú, Expansion in perfect groups, *Geom. Funct. Anal.* **22** (2012), 1832–1891.

[38] A. Selberg, On the estimation of Fourier coefficients of modular forms, *Proc. Symp. Pure Math.* **VIII** (1965), 1–15.

[39] Y. Shalom, Bounded generation and Kazhdan's property (T), *Inst. Hautes Études Sci. Publ. Math.* **90** (1999), 145–168.

[40] Y. Shalom, Rigidity of commensurators and irreducible lattices, *Invent. Math.* **141** (2000), 1–54.

[41] R.M. Tanner, Explicit concentrators from generalized N-gons, *SIAM J. Alg. Discr. Meth.* **5** (1984), 287–294.

[42] T. Tao, Expansion in groups, `http://terrytao.wordpress.com/category/teaching/254b-expansion-in-groups/`.

[43] T. Tao y V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, 105, Cambridge University Press, Cambridge, 2006.

[44] J. Tits, Free subgroups in linear groups, *J. Algebra* **20** (1972), 250–270.

[45] P.P. Varjú, Expansion in $\mathrm{SL}_d(O_K/I)$, I square-free, *J. Eur. Math. Soc.* **14** (2012), 273–305.

[46] L.N. Vaserstein, Groups having the property (T), *Funct. Anal. Appl.* **2** (1968), 174.

Andrei Jaikin, Departamento de Matemáticas, Universidad Autónoma de Madrid, Instituto de Ciencias Matemáticas CSIC-UAM-UC3M-UCM
Correo electrónico: `andrei.jaikin@uam.es`
Página web: `http://www.uam.es/andrei.jaikin`