2021 Retos Vitales

para una nueva era

Las autopistas del ciberespacio

Pilar Bayer Isant

Claves para entender y mejorar el mundo

Reial Acadèmia Europea de Doctors
Real Academia Europea de Doctores
Royal European Academy of Doctors
BARCELONA - 1914

Mc Graw Hill

Fundación RAED
Inspirando a través del conocimiento

Las autopistas del ciberespacio

Fotografía: M. Bayer

Dra. Pilar Bayer Isant
Catedrática Emérita de la Universidad de Barcelona.
Académica de Número y Vicepresidenta de la Sección de Ciencias Experimentales de la Real Academia Europea de Doctores (RAED).

INTRODUCCIÓN

Navegamos por internet a diario, con objetivos distintos, y nuestras consultas a la *World Wide Web* (WWW) se relacionan con bases de datos cada vez más complejas. A pesar de que más de la mitad de la población mundial está conectada a la red, los avances técnicos nos permiten acceder a la información de manera rápida y asequible. La quinta generación de estándares de comunicación, proporcionados por la red 5G, cuya implantación generalizada se prevé para el 2025, se orienta a la conexión de un millón de aparatos móviles por kilómetro cuadrado, con una tasa de transmisión de datos de 1,2 gigabits por segundo ($1{,}2\times10^9$ bits/s) y espectros entre los 30 y 300 gigahercios, proporcionados por ondas de radio de frecuencias extremadamente altas (EHF) y longitudes de onda milimétricas de 1 a 10 milímetros (*mm-waves*).

El propósito de este capítulo es dar a conocer, de una manera divulgativa, algunas herramientas matemáticas que forman parte de estos éxitos tecnológicos sin precedentes. Nos limitaremos a las que influyen en la velocidad de transmisión de datos y que están basadas en la teoría de grafos. La teoría de grafos es hoy una rama de la matemática discreta y de las ciencias de la computación. Los grafos intervienen en muchos algoritmos ligados a las nuevas tecnologías. En su desarrollo teórico y práctico confluyen gran varie-

dad de conceptos y logros matemáticos cuya motivación fue en su día el avance del conocimiento matemático.

En matemática discreta y en ciencias de la computación, el concepto de grafo responde a una estructura geométrica muy sencilla. Un grafo se compone de un conjunto finito de puntos, llamados vértices o nodos, y de un conjunto finito de segmentos determinados por pares de estos vértices, llamados lados o aristas (figura 1).

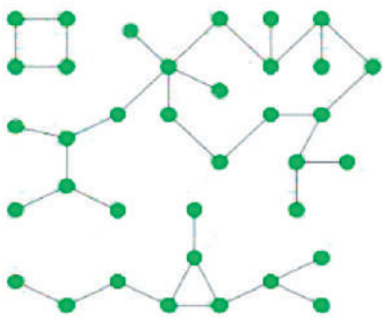

Figura 1. Grafo no conexo y con ciclos. Imagen: Wikimedia Commons.

Los grafos sirven para modelizar multitud de estructuras de la vida real. En la teoría de la información, podemos identificar a los vértices de un grafo con un conjunto de antenas y a sus aristas, con sus canales de conexión. En la estructura de la WWW, podemos identificar los nodos de un grafo con las páginas de hipertexto y las aristas, con los hipervínculos entre ellas. En ciencias de la computación, podemos construir un grafo con nodos dados por distintos ordenadores que trabajan interconectados. En sociología, distintas comunidades pueden estar representadas por los vértices de un grafo; sus interacciones nos darán las aristas del mismo. En economía, los vértices de un grafo pueden responder a distintas sedes bancarias y las aristas, a asociaciones entre las mismas. En medicina, hemos visto grafos que tienen por nodos comunidades afectadas por la COVID–19 y por aristas, las transmisiones por contagio. Los vértices de un grafo no tienen por qué estar todos en el mismo plano. Tal es el caso del grafo asociado a nuestro sistema nervioso, con nodos los puntos gatillo, bien conocidos en fisioterapia.

Dado un grafo, podemos estar interesados en que la transmisión de datos a través de sus aristas se realice de manera rápida o de manera lenta, y de forma completa o bien de forma parcial, dependiendo de la naturaleza de estos. En los primeros casos, hablaremos de grafos expansivos; en los segundos, de grafos contractivos (figura 2).

En este capítulo nos centraremos especialmente en la teoría de los grafos expansivos, con una breve mención al final a los grafos contractivos.

A fin de que los datos circulen con la máxima velocidad posible y sin interrupciones a través de las aristas de un grafo, podríamos pensar que cada nodo debería estar conectado a un gran número de nodos. Ello nos conduciría a establecer un gran número de aristas saliendo de cada nodo, lo cual suele ser costoso de llevar a la práctica. Intuitivamente, serían más rentables los grafos construidos con muchos vértices y pocas aristas. Sin embargo, esta manera de proceder podría conllevar transmisiones mucho más lentas e interrupciones en el suministro de la información. **La teoría matemática subyacente al trazado de lo que podríamos llamar la «red de autopistas del ciberespacio» se encarga de hallar una solución óptima al problema de diseñar grafos con «un gran número de vértices», «pocas aristas», «altamente conexos» y «robustos»**, a fin de que alcance a un gran número de usuarios, su coste sea asequible, y la transmisión de datos fluya con rapidez y sin cortes.

La matemática permite valorar la capacidad de transmisión de un grafo y su robustez, y proceder al diseño de grafos que optimicen las propiedades mencionadas. Desde un punto de vista matemático, debemos distinguir entre la demostración teórica de la *existencia* de grafos expansivos y su *construcción efectiva*, obtenida esta muchos años después de la primera.

Entre los grafos expansivos construibles y óptimos se encuentran los *grafos de Ramanujan*. Su nombre es en reconocimiento a la labor pionera de Srinivasa Ramanujan (1887-1920), un matemático indio que afianzó su formación matemática en Cambridge, bajo la dirección de Godfrey H. Hardy (1877-1947)[6]. Uno de los problemas resueltos por Ramanujan a instancias de Hardy versó sobre las sumas de cuadrados; se trataba de un problema aritmético, independiente de la teoría de grafos[3]. Sin embargo, y tal como veremos,

Figura 2. Expansor de entrenamiento. Imagen: Wikimedia Commons.

ciertos planteamientos y propiedades numéricas descubiertas por Ramanujan en este estudio han resultado de la máxima importancia para la resolución del problema que nos ocupa.

Entre los primeros grafos de Ramanujan construidos explícitamente se encuentran los grafos *LPS*, introducidos por Lubotzky, Phillips y Sarnak en un brillante artículo de finales de la década de 1980.[17] La construcción de estos grafos conjuga propiedades aritméticas de los números enteros descubiertas por Ramanujan con propiedades aritméticas de los números cuaternios, cuya construcción se remonta a Richard Hamilton (1805-1865) y Adolf Hurwitz (1859-1919).

GRAFOS EXPANSIVOS

El objetivo de esta sección es proporcionar los elementos necesarios para la comprensión del concepto de grafo expansivo y, en particular, de los grafos de Ramanujan. Nos limitaremos a dar las definiciones específicas imprescindibles, omitiendo las de carácter general que forman parte del lenguaje científico matemático habitual.

Conceptos básicos de la teoría de grafos

Un grafo G se define por medio de un par ordenado (V, E), formado por un conjunto finito V cuyos elementos llamaremos *vértices*, y por un conjunto finito de pares (no ordenados) de vértices, cuyos elementos llamaremos *aristas*. Vértices *adyacentes* o *vecinos* son, por definición, los que determinan una arista. El *orden* n de un grafo viene dado por el número de sus vértices. El *grado* d de un vértice de un grafo viene dado por el número de aristas que en él concurren. Un grafo se dice que es *d-regular* si todos sus vértices son del mismo grado, d. Un grafo de orden $n \geq 3$ se dice que es un *ciclo* si es regular y de grado $d = 2$. Un *lazo* es una arista que une un nodo consigo mismo. Un *camino* de un grafo es un conjunto de vértices interconectados por aristas. Un grafo se de-

nomina *conexo* si para cada par de vértices existe al menos un camino que los une. Un *árbol* es, por definición, un grafo conexo y sin ciclos (figura 3). Una reunión disjunta de árboles constituye lo que se denomina un *bosque*.

Dado un subconjunto F de vértices de un grafo $G = (V, E)$, definimos la *frontera* de F por la fórmula

$$\partial(F) := \{x \in V \mid d(x, F) = 1\}.$$

Es decir, la frontera de un conjunto de vértices F está formada por aquellos vértices del grafo que, no siendo de F, son vecinos de algún elemento de F.

La *tasa de transmisión* de un grafo se define por

Figura 3. Árbol.
Imagen: Wikimedia Commons.

$$h(G) := \inf\left\{\frac{|\partial(F)|}{|F|} \,\middle|\, F \subset V,\ 0 < |F| \leq n/2\right\},$$

en donde |-| denota el número de elementos de un conjunto finito dado. El valor de h se relaciona con el carácter conexo del grafo. Así, G es conexo si y solo si $h(G) > 0$; y G es altamente conexo cuanto mayor es el valor de h. De la definición de $h(G)$ se deduce que, en los grafos altamente conexos, cualquier subconjunto de vértices tiene un número elevado de vecinos. Coloquialmente se expresa diciendo que en ellos los rumores se difunden con rapidez.

Un grafo se denomina *bipartido* si sus vértices se pueden separar en dos conjuntos disjuntos A, B, de manera que sus aristas sólo conectan vértices de A con vértices de B.

El espectro de un grafo

Designaremos por $\mathbb{R}$ al conjunto de todos los números reales, con su estructura habitual de cuerpo dada por la suma y por el producto. Los elementos de $\mathbb{R}$ se identifican con los puntos de una recta, llamada la recta numérica real. Los números enteros, $\mathbb{Z}$, y los números naturales, $\mathbb{N}$, son parte de esta recta. Introducimos a continuación el espectro de un grafo de orden n, que constará de n números reales.

Podemos caracterizar un grafo $G = (V, E)$ por un cuadro de números, denominado su *matriz de adyacencia* $A_G = (a_{ij})$. Si $V = \{x_1, ..., x_n\}$ denota el conjunto de vértices numerados del grafo, dicha matriz consiste en un conjunto de $n \times n$ números naturales que cuentan el número de aristas que unen los distintos pares de vértices (x_i, x_j):

$$a_{ij} = |\{y \in E \mid o(y) = x_i, t(y) = x_j\}|.$$

En la figura 4 se aprecian tres grafos distintos, no regulares, de orden 4, con las correspondientes matrices de adyacencia:

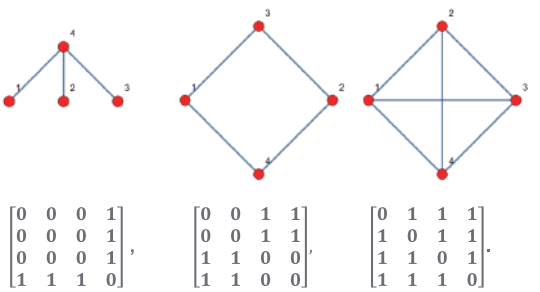

Figura 4. Matrices de adyacencia.

Desde un punto de vista informático, es muy interesante observar que todo grafo puede reconstruirse a partir de su matriz de adyacencia, ya que esta permite estudiar numéricamente los grafos prescindiendo de figuras.

Si G es un grafo d-regular, entonces se satisface que $A_G(u) = du$, siendo $u = (1,1,...,1)$. Es decir, u es un vector propio de la matriz de adyacencia del grafo, con valor propio igual al grado d del mismo. La matriz de adyacencia define un operador simétrico A_G en $\mathbb{R}^n$, pues la misma arista que une x_i con x_j une también x_j con x_i. Por propiedades bien conocidas, este operador simétrico diagonaliza en una base ortogonal de vectores propios y sus valores propios son todos números reales. Llamando espectro de un operador lineal, como es habitual, al conjunto de sus valores propios, tendremos que

$$\mathrm{Spec}\,(\mathrm{A}_G) = \{\, d = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_n \geq -d\}.$$

La diferencia $d - \lambda_2$ recibe el nombre de *brecha espectral* y es una cantidad que influye en la tasa de transmisión del grafo, tal como veremos a continuación.

El operador lineal $\Delta_G = \mathrm{Id} - \mathrm{A}_G$ se conoce como el *laplaciano* del grafo G. En una base de vectores propios tendrá por matriz

$$\Delta_G = \begin{bmatrix} 0 & \cdots & 0 \\ 0 & d-\lambda_2 & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d-\lambda_n \end{bmatrix}.$$

El operador de Laplace es una herramienta muy común en el análisis matemático, que interviene en la modelización de fenómenos vibratorios. Su estudio se inició en 1747 a raíz de la obtención de la ecuación que rige el movimiento de una cuerda vibrante, deducida de las leyes de Newton por el matemático y enciclopedista francés Jean le Rond d'Alembert. Estos estudios fueron continuados por Pierre-Simon de Laplace, Jean-Joseph Fourier y Sophie Germain, entre muchos otros. El operador de Laplace interviene en distintas ecuaciones en derivadas parciales que regulan la propagación del sonido, la luz, el calor, los terremotos y fenómenos atómicos. Su análogo en teoría de grafos nos servirá para controlar la propagación de la información.

Expansores

Una sucesión $(G_m)_{m\geq 1}$ de grafos d-regulares, con $d \geq 3$, se dice que es una *sucesión expansiva* si existe una constante $C > 0$ tal que $h(G_m) > C$, para todo $m \geq 1$. Las sucesiones expansivas de grafos se conocen también con el nombre de *expansores*.

La desigualdad de Cheeger-Buser. La tasa de transmisión $h(G)$ de un grafo se relaciona con la brecha espectral $d - \lambda_2$.[10] Más concretamente, para todo grafo G que sea d-regular, conexo y sin lazos se satisfacen las desigualdades

$$\frac{d-\lambda_2}{2} \leq h(G) \leq \sqrt{2d(d-\lambda_2)}.$$

En consecuencia, una brecha espectral grande nos garantizará un grafo con una elevada tasa de transmisión. Y, fijado el grado de un grafo, una tasa de transmisión elevada solo podrá conseguirse mediante un segundo valor propio pequeño del laplaciano.

Grafos de Ramanujan. Un grafo G, d-regular, se denomina de Ramanujan si

$$\lambda(G) \leq 2\sqrt{d-1},$$

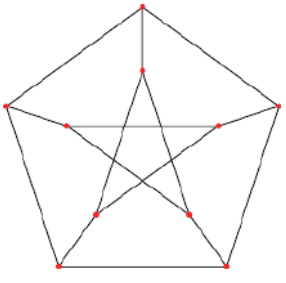

Figura 5. Grafo de Petersen. Imagen: Wikimedia Commons.

en donde $\lambda(G)$ denota el máximo de los valores absolutos $|\lambda_i|$ de los elementos del espectro de G para $i \geq 2$.

Los cálculos siguientes ponen de manifiesto que el grafo de Petersen, P, de orden 10 y 3-regular, que se muestra en la figura 5, es un grafo de Ramanujan, puesto que en él se satisface que

$$\text{Spec}\,(A_p) = \{3, 1, 1, 1, 1, 1, -2, -2, -2, -2\}; \quad \lambda(P) \leq 2.82843\ldots$$

Notemos que el grafo anterior tiene muy pocos nodos, por lo que no es útil para nuestros propósitos. Lubotzky, Phillips y Sarnak[17] y Morgenstern[19] construyeron sucesiones expansivas de grafos de Ramanujan, regulares, de grado $d = p^f + 1$, para todo número primo p y entero $f \geq 1$. Los grafos que forman estas sucesiones adquieren asintóticamente (cuando $p \to \infty$) el valor mayor posible de la brecha espectral. Puesto que, desde el siglo III a.C., sabemos por Euclides que el conjunto de los números primos es infinito, la construcción mencionada permite obtener sucesivamente grafos de Ramanujan con tantos nodos como se quiera.

SUMAS DE CUADRADOS: MOTIVACIÓN Y RESULTADOS DE RAMANUJAN

En esta sección se exponen brevemente la motivación y los resultados del trabajo de Ramanujan[21].

Las sumas de dos cuadrados

En el siglo XVII, Pierre de Fermat se dio cuenta de que los enteros primos de la forma $p = 4k + 1, k > 0$, podían descomponerse como suma de dos cuadrados:

$$5 = 1^2 + 2^2, \qquad 13 = 2^2 + 3^2,$$
$$17 = 1^2 + 4^2, \qquad 29 = 2^2 + 5^2, \ldots$$

También $2 = 1^2 + 1^2$. Sin embargo, este no era el caso para los enteros primos de la forma $p = 4k + 3,\ k > 0,$ como el $3, 7, 11, 19, \ldots$

Estos hechos pudieron explicarse y demostrarse a partir de las propiedades aritméticas de los números enteros de Gauss.

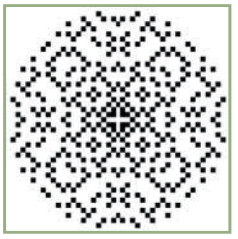

Figura 6. Primos de Gauss. Imagen: Wikimedia Commons.

Los enteros de Gauss

Recordemos que los números complejos $\mathbb{C}$ se escriben en la forma $a + bi$, con números reales e $i^2 = -1$. Por tanto, el cuerpo complejo $\mathbb{C}$ extiende el cuerpo real $\mathbb{R}$. Sus elementos se representan por los puntos del plano. Se denominan números enteros de Gauss los números complejos de componentes enteras; es decir, los números que se escriben en la forma $a + bi$ con a, b pertenecientes a $\mathbb{Z}$. Se representa su conjunto por $\mathbb{Z}[i]$. De manera análoga a lo que ocurre en $\mathbb{Z}$, todo entero de Gauss (no nulo y no unitario) descompone de manera única (salvo el orden y unitarios) en producto de enteros de Gauss primos. Los primos de $\mathbb{Z}$ que permanecen primos en $\mathbb{Z}[i]$ son, precisamente, los que no son suma de dos cuadrados[13]. Los primeros enteros de Gauss que son primos, representados por puntos de la figura 6, son (en el primer cuadrante): $1 + i, 3, 2 + i, 7, 11, 3 + 2i, 4 + i,...$ Como en el caso de los números enteros, el conjunto de los primos de Gauss es, también, infinito.

Si escribimos $r_2(n)$ para expresar el número de maneras en que un entero $n \geq 1$ descompone como suma de dos cuadrados enteros, al tener en cuenta el orden y los signos posibles, obtenemos que

$$r_2(5) = 8, \qquad r_2(7) = 0, \qquad r_2(4) = 4, \qquad r_2(100) = 12,...$$

En general, dados dos enteros $n > 0, k > 0$, consideremos el número $r_k(n)$ de maneras en que n puede expresarse como suma de k cuadrados. A lo largo de los siglos XVIII y XIX, se demostraron las fórmulas exactas siguientes, que determinan estos números a partir de los divisores de n

$$r_2(n) = 4(d_1(n) - d_3(n)),$$

$$r_4(n) = 8 \sum_{d|n} d, \quad d \neq 4k,$$

$$r_8(n) = 16 \sum_{d|n} (-1)^{n+d} d^3.$$

En donde $d_i(n)$ denota el número de divisores de n congruentes con i módulo 4. La primera fórmula es debida a Euler y a Gauss; la segunda y la tercera son debidas a Jacobi.

Las sumas de 24 cuadrados

El problema que Hardy propuso a Ramanujan fue el hallazgo de una fórmula para el cálculo de $r_{24}(n)$. Es decir, Ramanujan debía calcular de cuántas maneras un entero n dado podía descomponerse como suma de 24 cuadrados. La solución que Ramanujan dio a este problema es espectacular y puede calificarse como uno de los momentos estelares de la historia de las matemáticas. Ello es debido no solo a la naturaleza de la fórmula obtenida por Ramanujan sino también a los descubrimientos a los que su deducción condujo:

$$r_{24}(n) = \frac{16}{621}\sigma_{11}^{*}(n) + \frac{128}{691}\left[(-1)^{n-1}259\tau(n) - 512\tau\left(\frac{n}{2}\right)\right].$$

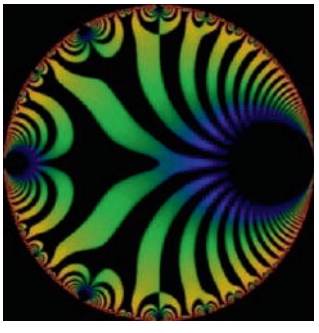

Figura 7. |Re (Δ)|.
Imagen: Wikimedia Commons.

En esta fórmula, la función σ_{11}^{*} es una función que depende de la suma de las potencias onceavas de los divisores de un número. La función τ que aparece se conoce con el nombre de función *tau* de Ramanujan y está ligada a las funciones elípticas de Jacobi. Concretamente, $\tau(n)$ es el n-ésimo coeficiente de Fourier de la función Δ:

$$2\pi^{-12}\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n,$$
$$q = e^{2\pi iz},\ \ Re(z) > 0.$$

La función Δ denota aquí la *función modular discriminante* de las *curvas elípticas*. En la figura 7 se representa el módulo de su parte real como función definida sobre el disco unidad.

El conocimiento que hoy tenemos de las funciones modulares, con simetrías provenientes de la acción del *grupo modular* $SL(2, \mathbb{Z})$, permite obtener una demostración de la fórmula de Ramanujan completamente transparente[2].

Las conjeturas de Ramanujan

En 1916, Ramanujan había calculado los 30 primeros valores de la función tau y, a la vista de los resultados obtenidos, conjeturó las siguientes propiedades de esta función:

i)	$\tau(mn) = \tau(m)\tau(n)$, si $\gcd(m, n) = 1$.
ii)	$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$, si p es primo y $n \geq 1$.
iii)	$\lvert\tau(p)\rvert \leq 2p^{\frac{11}{2}}$, para todo primo p.

La demostración de las dos primeras conjeturas de Ramanujan fue obtenida por Louis Mordell en 1917.[18] Posteriormente fue generalizada por Eric Hecke mediante la creación de la teoría de los operadores que llevan su nombre[14]. Estas demostraciones implicaron ahondar en la teoría de las funciones modulares y, en su generalización, la teoría de las *funciones automorfas*. Se trata de funciones de variable compleja con altos grados de simetría procedentes de grupos de movimientos de la geometría hiperbólica[5].

La conjetura iii) de Ramanujan permite interpretar la fórmula de los 24 cuadrados de la manera siguiente: su primer sumando proporciona el término principal y el segundo corresponde a un término de error, pequeño con relación al término principal (del orden de su raíz cuadrada). Su demostración exigió un trabajo mucho más arduo y exhaustivo que el de las dos primeras.

En 1968, Pierre Deligne[11] probó que la demostración de la conjetura iii) de Ramanujan podía obtenerse como consecuencia de unas profundas conjeturas que habían sido formuladas por André Weil en 1949.[25] Las conjeturas de Weil se referían al espectro del automorfismo de Frobenius, $\mathrm{Spec}(\mathrm{Frob}_q)$.

El automorfismo de Frobenius es un operador que actúa sobre la cohomología $\mathrm{H}^*(\mathrm{X})$ de las variedades algebraicas $X|\mathrm{F}_q$ definidas sobre cuerpos finitos F_q. A lo largo de las *décadas* de 1950 y 1960 se demostraron todas las conjeturas de Weil, salvo una, gracias a un trabajo monumental de fundamentación de la geometría algebraica moderna realizado por Alexander Grothendieck durante 14 años al frente del IHES (*Institut des Hautes Études Scientifiques*). La demostración de la conjetura de Weil que quedaba pendiente fue obtenida por el propio Deligne en 1973,[12] con lo cual las conjeturas i), ii) y iii) de Ramanujan sobre la función tau quedaron todas probadas. Estos resultados le valieron a Deligne la obtención de la Medalla Fields (1978) y del Premio Abel (2013), los dos reconocimientos máximos que se conceden en matemáticas[4]. Podemos sintetizar los resultados citados de Deligne mediante las fórmulas:

$$\tau(p) = \lambda_p + \overline{\lambda}_p,\ \lambda_p = \mathrm{vap}\left(\mathrm{Frob}_p, H^{11}\right),$$

$$\lambda_p = \mathrm{vap}\left(\mathrm{Frob}_p, H^i\left(X/\overline{\mathrm{F}}_p, \mathbb{Q}_l\right)\right) \Rightarrow \left|\lambda_p\right| \leq 2p^{i/2}.$$

Una observación crucial para la construcción efectiva de grafos expansivos fue la siguiente: el hecho de que una tasa de transmisión alta de un grafo estuviera ligado a valores propios pequeños del espectro del operador de Laplace podía quizá relacionarse con la última conjetura de Weil, por cuanto que esta conjetura garantizaba la existencia de valores propios pequeños en el espectro del operador de Frobenius. Estos razonamientos fueron materializados, como veremos, mediante la construcción de los grafos *LPS*.

NÚMEROS HIPERCOMPLEJOS Y LA CONSTRUCCIÓN *LPS*

La construcción *LPS* está basada en propiedades aritméticas de los números hipercomplejos. Los números hipercomplejos nos permitirán enlazar el laplaciano de un grafo con el operador de Frobenius de una variedad algebraica.

Los cuaternios de Hamilton

Designaremos por $\mathrm{H}(R) := \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in R\}$ al conjunto de los cuaternios de Hamilton con coeficientes en un anillo numérico R, dado. El cuerpo $H(\mathbb{R})$ de los cuaternios de Hamilton es una extensión del cuerpo complejo $\mathbb{C}$. Por definición, en los cuaternios, se satisfacen las reglas de cálculo

$$i^2 = j^2 = k^2 = -1,$$

$$ij = -ji = k;\ \ jk = -kj = i,\ ki = -ik = j.$$

Observemos que el orden en que se multiplican cuaternios importa para la determinación de su producto; es decir, se trata de una estructura algebraica de cuerpo no conmutativo.

Dado un cuaternio q, representaremos por $\overline{q}$ su cuaternio conjugado y por $N(q)$, su norma, definidos por

$$q = a_0 + a_1 i + a_2 j + a_3 k, \qquad \overline{q} := a_0 - a_1 i - a_2 j - a_3 k,$$
$$N(q) := q\overline{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

Se denominan cuaternios enteros de Hamilton a los elementos de $\mathrm{H}(\mathbb{Z})$, es decir a los cuaternios de coordenadas enteras. Como en el caso de los enteros de Gauss, todo entero de Hamilton (no nulo y no unitario) descompone en producto de enteros de Hamilton primos, si bien estas descomposiciones no tienen por qué ser únicas. De hecho, ningún primo de $\mathbb{Z}$ permanece primo en $\mathrm{H}(\mathbb{Z})$. Veamos un ejemplo:

$$13 = (1 + 2i + 2j + 2k)(1 - 2i - 2j - 2k) = (3 + 2i)(3 - 2i).$$

A continuación consideraremos congruencias con números cuaternios, que imitan las congruencias habituales con números enteros. Para ello sea $q \neq 2$

un entero primo y sea $\mathrm{F}_q := \mathbb{Z}/q\mathbb{Z}$ el cuerpo finito de q elementos. Podemos considerar el homomorfismo de reducción $\mathrm{r}_q : \mathrm{H}(\mathbb{Z}) \longrightarrow \mathrm{H}(\mathrm{F}_q)$, y derivar a partir de él la siguiente representación matricial para los cuaternios con componentes en el cuerpo finito. Dado un elemento $\alpha = a_0 1 + a_0 i + a_2 j + a_3 k$ de $\mathrm{H}(\mathrm{F}_q)$, le asignaremos la matriz

$$m_{q(\alpha)} = \begin{bmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{bmatrix},$$

en donde los elementos x, y son soluciones en F_q de la ecuación $x^2 + y^2 + 1 = 0$. Esta asignación permite reemplazar las operaciones de suma y producto de cuaternios reducidos por las operaciones de suma y producto de matrices en $\mathrm{M}(2, \mathrm{F}_q)$.

El algoritmo *LPS*

En este párrafo supondremos que $p \neq 2$, q son enteros primos y que $q > 2\sqrt{p}$. Los *grafos de Cayley* se construyen a partir de la teoría de grupos mediante el uso de grupos finitos G y de subconjuntos S de los mismos[5]. Los vértices del grafo (G, S) coinciden con los elementos del grupo G y las aristas son de la forma (g, gs), con g en G y s en S.

El formato de los grafos *LPS* corresponde a un caso específico de grafos de Cayley. En este caso, los grupos finitos que se consideran son los grupos proyectivos lineales $\mathrm{PGL}(2, q) := \mathrm{GL}(2, q)/\mathrm{F}_q^*$, definidos a partir de las matrices invertibles con coeficientes en el cuerpo finito F_q y los grupos proyectivos especiales lineales $\mathrm{PSL}(2, q)$ definidos a partir de las matrices anteriores con determinante igual a 1.

Consideramos el conjunto siguiente de cuaternios enteros de norma p:

$$\mathrm{S}_p := \{\alpha \in \mathrm{H}(\mathbb{Z}) : \mathrm{N}(\alpha) = p, \alpha \equiv 1, \text{ o bien } \alpha \equiv i + j + k \bmod(2)\}$$

$$= \{\alpha_1, \bar{\alpha}_1, \alpha_2, \bar{\alpha}_2, \ldots, \alpha_s, \bar{\alpha}_s, \beta_1, \ldots, \beta_t\}, \qquad 2s + t = p + 1.$$

Sus elementos son cuaternios primos divisores de p. En ellos supondremos que $a_0(\alpha_i) > 0, a_0(\beta_i) = 0$. Y designaremos por $S_{p,q}$ las imágenes de estos conjuntos obtenidas por reducción r_q módulo un primo q de sus componentes, seguida de su interpretación matricial m_q y proyección pr_q en el grupo proyectivo lineal:

$$S_{p,q} \coloneqq \left(pr_q \circ m_q \circ r_q\right)\left(S_p\right) \subseteq \mathrm{PGL}(2,q).$$

Se trata de un subconjunto simétrico de $p + 1$ elementos. Consideramos ahora los grafos de Cayley

$$LPS(p,q) \coloneqq G\left(\mathrm{PGL}(2,q), S_{p,q}\right), \text{ si } p \text{ es un residuo cuadrático módulo } q,$$
$$LPS(p,q) \coloneqq G\left(\mathrm{PSL}(2,q), S_{p,q}\right), \text{ si } p \text{ no es residuo cuadrático módulo } q.$$

En el primer caso, $LPS(p,q)$ es un grafo no bipartido de $q\,(q^2-1)/2$ vértices y de grado $p + 1$. En el segundo, se trata de un grafo bipartido de $q\,(q^2-1)$ vértices y también de grado $p + 1$. El grafo $LPS(3,7)$ de la figura 8, cuyo cálculo fue programado por Klara Stokes, es un grafo de Ramanujan, no bipartido, de 336 nodos, situados en la circunferencia, y en el que cada nodo está conectado únicamente con 4 vecinos[24].

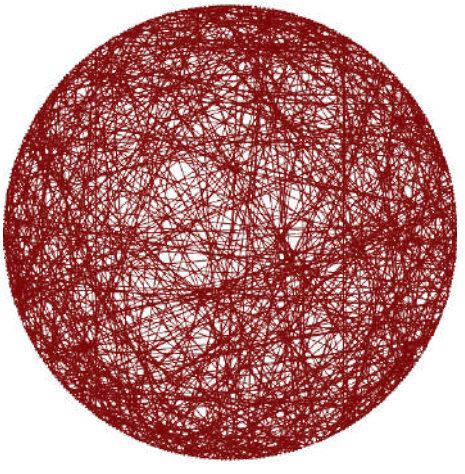

Figura 8. El grafo *LPS*(3,7).
Imagen gentileza de Klara Stokes.

Verificación de la condición de Ramanujan

Para indicar someramente cómo se procede para demostrar que los grafos LPS son de Ramanujan, necesitamos introducir la función zeta de un grafo.

La función zeta de un grafo. Dado un grafo G conexo y d-regular, sea $q = d - 1$. Designemos por N_m el número de sus ciclos de longitud m. Su función zeta es la serie formal definida por

$$Z(G,t) := \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} t^m\right).$$

A esta serie formal se asocia la función de variable compleja $\zeta(G, s) := Z(G, q^{-s})$ resultante de hacer la sustitución $t = q^{-s}$. La fórmula que escribimos a continuación nos expresa la función zeta de un grafo en términos de la matriz de adyacencia del mismo, lo cual explicará *a posteriori* el motivo por el cual la función zeta de un grafo da cuenta de sus propiedades espectrales:

$$\zeta(G,s) = (1-q^{-2s})^{-\chi(G)} \det(I - A_G\, q^{-s} + q^{1-2s} I)^{-1}, \qquad \chi(G) := |V| - |E|.$$

G es un grafo de Ramanujan si, y solo si, los polos de la función $\zeta(G, s)$ contenidos en la franja vertical $0 < Re(s) < 1$ satisfacen que $Re(s) = 1/2$. Es decir, un grafo dado es de Ramanujan si, y solo si, su función zeta satisface el análogo de la hipótesis de Riemann en el estudio de los números primos[7].

Polinomios de Chebyshev. Los polinomios de Chebyshev intervienen como herramienta auxiliar en la verificación de la condición de Ramanujan de los grafos *LPS*. Se definen de manera recurrente por las fórmulas

$$U_0(x) = 1,\ U_1(x) = 2x,\ U_2(x) = 4x^2 - 1, \ldots,\ U_{m+1}(x) = 2xU_m(x) - U_{m-1}(x).$$

Y su función generadora es $\sum_{m=0}^{\infty} U_m(x)t^m = \frac{1}{1-2xt+t^2}$.

Una fórmula de trazas. Si consideramos los operadores definidos por

$$T_m := (d-1)^{\frac{m}{2}} U_m\left(\frac{A_G}{2\sqrt{d-1}}\right),$$

obtenemos una fórmula análoga a la fórmula de trazas de los operadores de Hecke[14] en la que interviene el espectro del grafo:

$$\mathrm{Tr}(T_m) = (d-1)^{\frac{m}{2}} \sum_{j=1}^{n} U_m\left(\frac{\lambda_j}{2\sqrt{d-1}}\right), \qquad \mathrm{Spec}(A_G) = \{\lambda_j\}.$$

De nuevo, sumas de cuadrados. Consideremos ahora la forma cuadrática $Q(x_0, x_1, x_2, x_3) := x_0^2 + q^2(x_1^2 + x_2^2 + x_3^2)$ y el siguiente número de representaciones por esta forma de las potencias *m-ésimas* del primo dado p:

$$r_Q(p^m) = |\{\alpha = (a_i) \in H(\mathbb{Z}): Q(a_0, \ldots, a_3) = p^m,$$

a_0 impar y $a_i, i > 0$, par, o bien a_0 par y $a_i, i > 0$, impar$\}|$.

Una fórmula semejante a la de Ramanujan para los 24 cuadrados, basada en propiedades de las funciones automorfas, permite reescribir el número anterior como un término principal más un término de error:

$$r_Q(p^m) = C\,\sigma(p^m) + O_\varepsilon\left(p^{m\left(\frac{1}{2}+\varepsilon\right)}\right),$$

en donde la función sigma denota la suma de divisores, C es una constante positiva y > 0 un número real tan pequeño como se quiera.

A partir de las expresiones obtenidas para la función zeta de un grafo, aplicadas a los grafos $LPS(p, q)$, se obtienen la relación $\frac{2}{n}\mathrm{Tr}(\mathrm{T_m}) = \mathrm{r_Q}(p^{\mathrm{m}})$. Y de ello se deducen las acotaciones deseadas, que prueban que los grafos LPS son de Ramanujan:

$$|\lambda_j| \leq 2\sqrt{p} \leq 2\sqrt{d-1},\ \ 2 \leq j \leq n-2, \text{ en el caso bipartido,}$$
$$|\lambda_j| \leq 2\sqrt{p} \leq 2\sqrt{d-1},\ \ 2 \leq j \leq n-1, \text{ en el caso no bipartido.}$$

Al considerar $q \longrightarrow \infty$ con p fijo, obtendremos el expansor deseado.

Otras aplicaciones

Los grafos, y en particular los grafos expansivos, han sido usados en el diseño de grafos contractivos que mejoran algoritmos de compresión de datos, así como en el de algoritmos de recuperación de los mismos[1,15,22].

Daniel Spielman y Shang Hua Teng aplicaron los grafos expansivos a la mejora del diseño de algoritmos eficientes en programación lineal[23]. En el ICM (*International Congress of Mathematicians*) 2010, celebrado en Hyderabad, India, Daniel Spielman fue galardonado con el Premio Nevanlinna por sus contribuciones a este tema.

Hoy por hoy, los grafos expansivos desempeñan un importante papel en la programación de funciones *hash,* al proporcionar un método eficiente para el cifrado de mensajes y detección de corrupción de datos. De acuerdo con Kristin Lauter, investigadora principal del *Cryptography Group at Microsoft Research*, los grafos de Ramanujan, obtenidos esta vez a través de isogenias de curvas elípticas supersingulares, podrían estar llamados a tener un papel en el desarrollo de la criptografía de la era poscuántica[16].

Presencia en los medios. La figura 9 corresponde a un fotograma de la película *El hombre que conocía el infinito*, de 2015. La película describe el encuentro de Hardy (interpretado por Jeremy Irons) con Ramanujan (Dev Patel), y hay referencias matemáticas a uno de sus trabajos en colaboración: el relativo al comportamiento asintótico del número de particiones de un entero dado[6].

Figura 9. *The man who knew infinity.* La película describe el encuentro de Hardy (Jeremy Irons) con Ramanujan (Dev Patel), y hay referencias matemáticas a uno de sus trabajos en colaboración. Imagen: Wikimedia Commons.

La figura 10 corresponde a un fotograma de la película *Good Will Hunting,* estrenada en 1997, cuyo protagonista (Matt Damon) está intentando dibujar el bosque formado por todos los árboles de orden 10. La figura 11 corresponde a un fotograma de la serie televisiva *Numb3rs*, cuya protagonista femenina en la ficción se llama, por cierto, Amita Ramanujan.

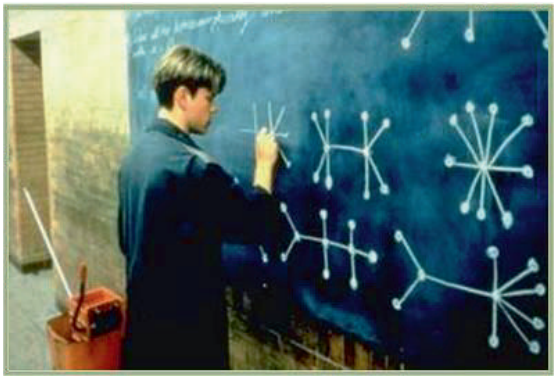

Figura 10. *Good Will Hunting*. Imagen: Wikimedia Commons

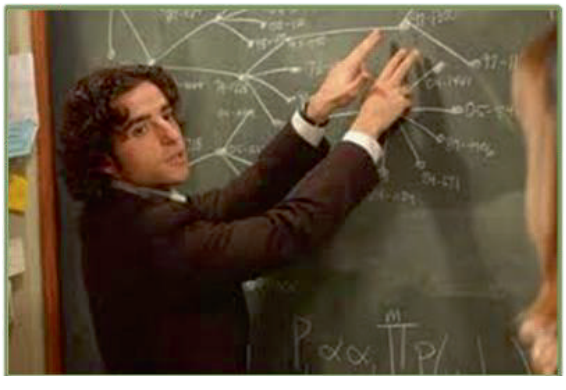

Figura 11. Numb3rs. Imagen: Wikimedia Commons.

REFERENCIAS

1. Adler M., Mitzenmacher A.M. Towards compressing web graphs. *Proceedings of the Data Compression Conference* (DCCí01) 1068-0314/01 (2001), IEEE.
2. Arenas A. On the summation of the singular series. *Manuscripta Mathematica* 1987; 57: 469-75.
3. Bayer P. Sobre una llibreta d'apunts (Ramanujan). *Butll. Soc. Catalana Mat.* 1986; 1: 7-13.
4. Bayer P. Premi Abel 2013 per a Pierre Deligne. *SCM Notícies* 2014; 35: 53-64.
5. Bayer P. La matemàtica de les simetries. *RAD. Tribuna plural* 2014; 4: 29-82.
6. Bayer P. The Man who knew Infinity. *SCM Notícies* 2016; 39: 81-3.
7. Bayer P. The Riemann hypothesis: The great pending challenge. *Mètode Science Studies Journal* 2018; 8: 34-41.
8. Bayer P., Blanco-Chacón I. Quadratic modular symbols on Shimura curves. *J. Théor. Nombres Bordeaux* 2013; 25: 261-83.
9. Bayer P., Remón D. A reduction point algorithm for cocompact Fuchsian groups and applications. *Adv. Math. Commun.* 2014; 8: 223-39.
10. Davidoff G., Sarnak P., Valette A. *Elementary number theory, group theory, and Ramanujan graphs*. Volume 55 of London Mathematical Society Student Texts. Cambridge: Cambridge University Press, 2003.
11. Deligne P. Formes modulaires et représentations l-adiques. *Séminaire Bourbaki* vol. 1968/69, *Lecture Notes in Math* (Springer) 1971; 179.
12. Deligne P. La conjecture de Weil I. *Inst. Hautes Etudes Sci. Publ. Math.* 1974; 43: 273-307.
13. Hardy G.H., Wright E.M. *An introduction to the theory of numbers.* 6th ed. Oxford: Oxford University Press, 2008. (First edition: Oxford University Press, 1938.)

14. Hecke E. Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung I. *Math. Ann.* 1937; 114: 1-28.

15. Jafarpour S., Xu W., Hassibi B., Calderbank R. Efficient and robust compressed sensing using optimized expander graphs. *IEEE Transaccions on Information Theory* 2009; 55: 4299-308.

16. Lauter K. How to keep your secrets in a post-quantum world. *Notices Amer. Math. Soc.* 2020; 67 (1): 22-9.

17. Lubotzky A., Phillips R., Sarnak P. Ramanuajan graphs. *Combinatorica* 1988; 8: 261-77.

18. Mordell L. On Mr. Ramanujan's empirical expansions of modular functions. *Proceedings of the Cambridge Philosophical Society* 1917; 19: 117-24.

19. Morgenstern M. Existence and explicit constructions of q + 1 regular Ramanujan Graphs for every prime power q. *Journal of Combinatorial Theory* 1994; Series B 62.1: 44-62.

20. Murty M.R. Ramanujan graphs. *J Ramanujan Math. Soc.* 2003; 18: 1-20.

21. Ramanujan S. On certain arithmetical functions. *Trans. Cambridge Philos. Soc.* 1916; 22 (9): 159-84. También en *Collected papers of Srinivasa Ramanujan*, pp. 136-62. Providence, RI: AMS Chelsea Publ., 2000.

22. Rossi R.A., Zhou R. GraphZIP: a clique-based sparse graph compression method. *J. Big Data* 2018; 5: 1-14.

23. Spielman D.A., Teng S.H. Nearly linear time algorithms for preconditioning and solving symmetric, diagonally dominant linear systems. *SIAM J. Matrix S.H. Anal. Appl.* 2014; 35 (3): 835-85.

24. Stokes K. *Arithmetic construction of Ramanujan graphs.* Trabajo de Máster en Matemática Avanzada y Profesional. Dirección: P. Bayer. Universidad de Barcelona, 2010.

25. Weil A. Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society* 1949; 55 (5): 497-508.