Aplicaciones de la Teoría de Matrices en Problemas de Matemática Discreta *

M.A. Fiol
Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Campus Nord, Barcelona
email: fiol@mat.upc.es

Abstract

Se describen algunas aplicaciones de la teoría de matrices a diversos temas pertenecientes al ámbito de la matemática discreta. En particular, se van a considerar las siguientes áreas de investigación: (a) La teoría de matrices enteras, con las formas normales de Hermite y de Smith, es utilizada en el estudio de la congruencia de vectores enteros, con su generalización del teorema chino del resto y su relación con grupos abelianos. Sus posibles aplicaciones van desde el diseño de ciertas redes de área local, pasando por la teoría de mosaicos y equidescomposición de figuras planas, hasta el desarrollo de métodos de encriptado en criptografía; (b) La teoría espectral de matrices se utiliza ampliamente en diversos temas de la teoría de grafos. En particular, se ha utilizado recientemente para el estudio y caracterización de grafos distancia-regulares, esquemas de asociación, y sus aplicaciones en teoría de códigos completamente regulares; (c) La teoría de matrices circulantes tiene múltiples aplicaciones en diversos campos. Como ejemplos, se pueden citar el estudio de los polígonos anidados, el diseño de osciladores acoplados y la transformada discreta de Fourier.

* *MAT.ES 2005, Valencia, 31 enero–4 febrero 2005.*

1 Introducción

En una primera aproximación, la "matemática discreta" puede describirse como la rama de las matemáticas que trata sobre las estructuras numerables, en contraste con la "matemática del contínuo" que se usa en análisis y geometría clásicos. Algunos de los temas básicos de los que se ocupa la matemática discreta son las técnicas de enumeración, estructuras combinatorias, teoría de grafos, estructuras algebraicas discretas, las versiones discretas de la geometría, y la teoría de códigos. Una introducción a algunos de estos temas puede encontrarse en [7, 15]. Este tipo de matemática ha recibido un gran impulso en las últimas décadas, gracias al desarrollo espectacular de la informática y las telecomunicaciones, por lo que actualmente es una de las ramas de la matemática aplicada con más vitalidad.

La teoría de matrices no necesita presentación y es un tema clásico en matemáticas, con amplias aplicaciones de tipo teórico y práctico. En el prefacio de su libro, Bellman [4] la define como la "aritmética de las matemáticas superiores", justificando su afirmación por el hecho de que las matrices representan las transformaciones más importantes, a saber, las transformaciones lineales.

En este trabajo se pretende dar algunos ejemplos de la interrelación entre la teoría de matrices y algunos temas de la matemática discreta. Estos temas, relacionados a menudo con las aplicaciones, no son necesariamente los temas centrales de dicha matemática, sino que corresponden en general a nuestras líneas de trabajo. Sin embargo, lo que sí ocurre, como cabía esperar, es que los resultados básicos que intervienen en la resolución de nuestros ejemplos, constituyen resultados centrales del área de teoría de matrices. Un ejemplo claro de ésto lo constituye la "forma normal de Smith" para matrices enteras, que presentamos a continuación.

2 Matrices enteras y equivalencia

Denotemos por $\mathbb{Z}^{n\times n}$ el anillo de matrices $n \times n$ enteras, es decir cuyos elementos son números enteros. Dadas $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{Z}^{n\times n}$, se dice que $\boldsymbol{A}$ es *equivalente por la derecha* a $\boldsymbol{B}$ si existe una matriz $\boldsymbol{V} \in \mathbb{Z}^{n\times n}$ unimodular (esto es, con determinante ± 1) tal que

$$\boldsymbol{A} = \boldsymbol{B}\boldsymbol{V}.$$

Análogamente, la *equivalencia por la izquierda* exige la existencia de una matriz unimodular $\boldsymbol{U}$ que cumpla $\boldsymbol{A} = \boldsymbol{U}\boldsymbol{B}$. Por otra parte, se dice que las matrices $\boldsymbol{A}$ y $\boldsymbol{B}$

son *equivalentes* cuando

$$\boldsymbol{A} = \boldsymbol{UBV}$$

para ciertas matrices unimodulares $\boldsymbol{U}, \boldsymbol{V} \in \mathbb{Z}^{n\times n}$.

2.1 La forma normal de Hermite

A partir de ahora supondremos, por sencillez, que $\boldsymbol{M} = (m_{ij})$ denota una matriz $n \times n$, entera y no singular, con columnas $\boldsymbol{m}_j = (m_{1j}, m_{2j}, \dots m_{nj})^\top$, $j = 1, 2, \dots, n$ y determinante (en valor absoluto) $m = |\det \boldsymbol{M}|$. Entonces, el teorema de la *forma normal de Hermite* afirma que $\boldsymbol{M}$ es equivalente por la derecha a una matriz triangular superior $\boldsymbol{H}(\boldsymbol{M}) = \boldsymbol{H} = (h_{ij})$ cuyos elementos de la diagonal h_{ii} son todos positivos (no nulos), y cada elemento sobre la diagonal y en la fila i-ésima; es decir, h_{ij}, $j > i$, pertenece a un conjunto completo de residuos módulo h_{ii}; por ejemplo $h_{ij} \in \{0, 1, \dots, h_{ii} - 1\}$. Además, se sabe que esta formal normal es única.

2.2 La forma normal de Smith

Para cada entero $k = 1, 2, \dots, n$, se define el llamado *k-ésimo divisor determinantal*, denotado por $d_k(\boldsymbol{M}) = d_k$, como el máximo común divisor de los determinantes de los $k\times k$ menores de $\boldsymbol{M}$ (es decir, de las submatrices cuadradas de $\boldsymbol{M}$ cuyos elementos pertenecen a alguna de las k filas y k columnas elegidas previamente). Notar que, fijado k, existen $\binom{n}{k}^2$ menores $k \times k$ y, como $\boldsymbol{M}$ es no singular, alguno de ellos debe tener determinante no nulo. Así, en particular, d_1 es el máximo común divisor de todos los elementos de $\boldsymbol{M}$ y, en el otro extremo, d_n coincide con el determinante m de $\boldsymbol{M}$. Nótese también que d_{k-1} divide a d_k para todo $k = 1, 2, \dots, n$, donde, por conveniencia, definimos $d_0 = 1$. Entonces los *factores invariantes* de $\boldsymbol{M}$, denotados por $s_k(\boldsymbol{M}) = s_k$, son las cantidades

$$s_k = \frac{d_k}{d_{k-1}} \quad (1 \le k \le n)$$

que se sabe cumplen las misma propiedad de divisibilidad que los divisores determinantales, es decir, $s_k | s_{k+1}$ para todo $k = 1, 2, \dots, n-1$. El teorema de la *forma normal de Smith* afirma entonces que la matriz $\boldsymbol{M}$ es equivalente a la matriz diagonal

$$\boldsymbol{S}(\boldsymbol{M}) = \boldsymbol{S} = \operatorname{diag}(s_1, s_2, \dots, s_n).$$

Por consiguiente, esta forma normal también es única.

La forma normal de Smith tiene múltiples aplicaciones en matemáticas. Por ejemplo, se usa en la resolución de sistemas lineales diofánticos (con coeficientes y soluciones enteras); en la teoría de grupos abelianos, ligada como veremos a la congruencia entre vectores enteros; y en el estudio de la equivalencia entre matrices bajo permutación de sus filas y columnas (la llamada *equivalencia por permutación*). Para una descripción de éstas y otras aplicaciones, pueden consultarse las referencias [30, 31].

3 Congruencias y grupos abelianos

Como sabemos, dado un entero positivo m, decimos que los enteros a, b son congruentes módulo m si los restos que se obtienen al dividir a y b por m son iguales o, equivalentemente, si $a - b$ es un múltiplo de m. Con la notación habitual,

$$a \equiv b \pmod{m} \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad a - b \in m\mathbb{Z}. \tag{1}$$

Este concepto de congruencia es bien conocido, y tiene muchas aplicaciones en la resolución de diversos problemas, tanto teóricos como prácticos. Esencialmente, su utilidad radica en el hecho de que representa la periodicidad (con periodo m) en el retículo unidimensional de los puntos enteros de la recta:

$$\ldots - \boldsymbol{m}, -(m-1), \ldots, \mathbf{0}, 1, \ldots, \boldsymbol{m}, m+1, \ldots, \mathbf{2}\boldsymbol{m}, 2m+1, \ldots$$

por lo que podríamos llamarla "periodicidad discreta". Gráficamente, podemos representar esta situación con m puntos equiespaciados sobre una circunferencia, numerados correlativamente desde 0 hasta $m-1$ siguiendo el sentido de las agujas del reloj. Además, si queremos representar el efecto del "generador" $a = 1$, establecemos un arco dirigido desde el punto i al punto $i + 1 \pmod{m}$. Obtenemos así un *ciclo dirigido* con m vértices, C_m, como representación del grupo cíclico de m elementos, $\mathbb{Z}_m$. Esto es un ejemplo de lo que, en teoría de grafos, se denomina *diagrama de Cayley* de un grupo Γ con respecto a un conjunto de generadores Δ y habitualmente se denota por $Cay(\Gamma, \Delta)$. Así, en nuestro ejemplo, $C_m = Cay(\mathbb{Z}_m, \{1\})$.

La cuestión que nos planteamos ahora es: ¿Cómo representar la periodicidad discreta en un espacio n-dimensional como, por ejemplo, el plano o el espacio euclídeo? La respuesta pasa por considerar un tipo de equivalencia entre vectores (columna) con coordenadas enteras, cuyo conjunto denotaremos por $\mathbb{Z}^n$. Entonces, dada una matriz entera $\boldsymbol{M}$ como en la sección anterior, el conjunto $\boldsymbol{M}\mathbb{Z}^n$, cuyos elementos son

combinaciones lineales con coeficientes enteros de los vectores (columna) $\boldsymbol{m}_j$, es el llamado *retículo* generado por $\boldsymbol{M}$. Notar que $\mathbb{Z}^n$, con la operación suma de vectores, es un grupo commutativo que tiene como subgrupo (normal) $\boldsymbol{M}\mathbb{Z}^n$.

Ahora, el concepto de congruencia en $\mathbb{Z}$ tiene la siguiente generalización natural a $\mathbb{Z}^n$ [12]: Decimos que dos vectores enteros, $\boldsymbol{a}$ y $\boldsymbol{b}$ son *congruentes módulo* $\boldsymbol{M}$ cuando su diferencia $\boldsymbol{a} - \boldsymbol{b}$ pertenece al retículo generado por $\boldsymbol{M}$. Es decir,

$$\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{M}} \quad \stackrel{\text{def}}{\iff} \quad \boldsymbol{a} - \boldsymbol{b} \in \boldsymbol{M}\mathbb{Z}^n. \tag{2}$$

Comparar con (1). De la misma forma que el grupo cociente $\mathbb{Z}_n = \mathbb{Z}/m\mathbb{Z}$ es conocido simplemente por el conjunto de "enteros módulo m", podemos referirnos a $\mathbb{Z}_M^n = \mathbb{Z}^n/\boldsymbol{M}\mathbb{Z}^n$ como el grupo de "vectores enteros módulo $\boldsymbol{M}$". Con ello seguimos la convención habitual de identificar cada clase de equivalencia por uno cualquiera de sus representantes.

Notar que, cuando $\boldsymbol{M} = \operatorname{diag}(m_1, m_2, \ldots, m_n)$, los vectores $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)^\top$ y $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)^\top$ son congruentes módulo $\boldsymbol{M}$ si y sólo si se satisface el sistema de congruencias en $\mathbb{Z}$

$$a_i \equiv b_i \pmod{m_i} \qquad (1 \le i \le n).$$

En este caso, $\mathbb{Z}_M^n$ es el producto directo (o cartesiano) de los grupos cíclicos $\mathbb{Z}_{m_i}$, $i = 1, 2, \ldots, n$.

3.1 Isomorfismos de grupos

Sea $\boldsymbol{H} = \boldsymbol{MV}$ la forma normal de Hermite de $\boldsymbol{M}$. Entonces (2) se cumple si y sólo si

$$\boldsymbol{a} - \boldsymbol{b} \in \boldsymbol{H}\boldsymbol{V}^{-1}\mathbb{Z}^n = \boldsymbol{H}\mathbb{Z}^n$$

ya que $\boldsymbol{V}$, y por tanto también $\boldsymbol{V}^{-1}$, son unimodulares. Por consiguiente, concluimos que

$$\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{M}} \quad \iff \quad \boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{H}} \tag{3}$$

o, en términos de isomorfismo de grupos,

$$\mathbb{Z}^n/\boldsymbol{M}\mathbb{Z}^n \cong \mathbb{Z}^n/\boldsymbol{H}\mathbb{Z}^n.$$

Consideremos ahora la forma normal de Smith de la matriz $\boldsymbol{M}$,

$$\boldsymbol{S} = \operatorname{diag}(s_1, s_2, \ldots, s_n) = \boldsymbol{UMV}.$$

Entonces se cumple (2) si y sólo si $\boldsymbol{U}\boldsymbol{a} \equiv \boldsymbol{U}\boldsymbol{b} \pmod{\boldsymbol{S}}$ o, de forma equivalente,

$$\boldsymbol{u}_i\boldsymbol{a} \equiv \boldsymbol{u}_i\boldsymbol{b} \pmod{s_i} \qquad (1 \leq i \leq n) \tag{4}$$

donde $\boldsymbol{u}_i$ denota la fila i-ésima de $\boldsymbol{U}$. Además, si r representa el entero positivo más pequeño tal que $s_1 = s_2 = \cdots = s_{n-r} = 1$ (si no existe tal entero tomamos $r = n$), las $n - r$ primeras ecuaciones en (4) son irrelevantes, y sólamente necesitamos considerar las r últimas. Es decir, en forma matricial,

$$\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{M}} \iff \boldsymbol{U}'\boldsymbol{a} \equiv \boldsymbol{U}'\boldsymbol{b} \pmod{\boldsymbol{S}'} \tag{5}$$

donde $\boldsymbol{U}'$ denota la matriz $r \times n$ formada por las r últimas filas de $\boldsymbol{U}$, y $\boldsymbol{S}' = \operatorname{diag}(s_{n-r+1}, s_{n-r+2}, \ldots, s_n)$. En consecuencia, la aplicación lineal Ψ desde el conjunto de vectores módulo $\boldsymbol{M}$ al conjunto de vectores módulo $\boldsymbol{S}'$, definida por $\Psi(\boldsymbol{A}) = \boldsymbol{U}\boldsymbol{a}$, es un isomorfismo de grupos que nos permite escribir:

$$\mathbb{Z}^n/\boldsymbol{M}\mathbb{Z}^n \cong \mathbb{Z}^r/\boldsymbol{S}'\mathbb{Z}^r \cong \mathbb{Z}_{s_{n-r+1}} \times \cdots \times \mathbb{Z}_{s_n}. \tag{6}$$

Como todo grupo abeliano finito se puede representar como (es isomorfo a) el grupo de vectores módulo una cierta matriz $\boldsymbol{M}$ (ver, por ejemplo, [13]), nótese que (6) es, en realidad, el enunciado del teorema central sobre descomposición de grupos commutativos. Otras dos consecuencias interesantes de la discusión anterior son las que siguen:

- *El número de vectores distintos módulo $\boldsymbol{M}$ (clases de equivalencia) es:*

$$|\mathbb{Z}^n/\boldsymbol{M}\mathbb{Z}^n| = |\det \boldsymbol{M}| = m. \tag{7}$$

- *El grupo (abeliano) de vectores enteros módulo $\boldsymbol{M}$ es cíclico si y sólo si $d_{n-1} = 1$.*

En [12] pueden encontrarse más detalles sobre el tema. En las dos siguientes secciones se plantean dos aplicaciones de las congruencias entre vectores. Por razón de sencillez, sólo se aborda el caso de dimensión dos, aunque muchos de los resultados expuestos pueden generalizarse a cualquier dimensión.

4 Redes de doble lazo

Una *red de doble lazo* consta de n nodos o *vértices* rotulados $0, 1, \ldots, n-1$ y los enlaces unidireccionales o *arcos* de la forma $(i, i + a)$ e $(i, i + b)$, con a y b enteros positivos llamados "pasos". Es decir, existen enlaces desde el nodo i hacia los nodos $i+a$ e $i+b$

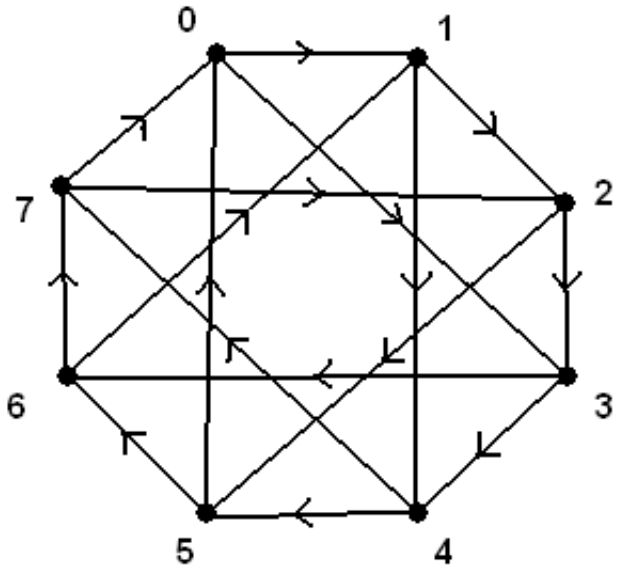

Figure 1: La red de doble lazo $G(8;1,3)$

(las operaciones deben entenderse módulo n). Por tanto, dicha red, que se denota comúnmente por $G(n;a,b)$, corresponde al diagrama de Cayley $Cay(\mathbb{Z}_n,\{a,b\})$. Por ejemplo, la Fig. 1 muestra la red de doble lazo $G(8;1,3)$.

En teoría de grafos esta estructura (y también el ciclo C_m descrito anteriormente) es un ejemplo de *grafo dirigido* o *digrafo* y, en el lenguaje propio del área, se dice que el vértice i es *adyacente hacia* los vértices $i+a$ e $i+b$. Un digrafo es *fuertemente conexo* cuando existe un camino (dirigido) entre cualquier par de vértices. En particular, $G(n;a,b)$ es fuertemente conexo si y sólo si $\{a,b\}$ es un conjunto generador del grupo $\mathbb{Z}_n$; es decir, cuando $\mathrm{mcd}(n,a,b)=1$. Las redes de doble lazo han sido propuestas y estudiadas como modelos para las llamadas "redes de área local", en las que una serie de ordenadores situados a corta distancia intercambian datos a alta velocidad [22]. En particular, el retraso en la transmisión de un mensaje entre dos nodos tiene que ver con el número mínimo de retransmisiones necesarias para llegar a su destino, esto es, con la *distancia* entre nodos. Por tanto interesa diseñar redes con reducido *diámetro* (máxima distancia entre vértices). Para tal fin, es posible utilizar congruencias en $\mathbb{Z}^2$, juntamente con la teoría de matrices enteras. El puente que nos permite pasar de la formulación combinatoria (es decir, la estructura de la red) a la algebraica es la

representación de cada digrafo mediante una "baldosa" (región plana) en forma de L, a la que llamamos *L-forma*, que tesela periódicamente el plano por translaciones. Dicha forma geométrica facilita el estudio de las propiedades del digrafo relacionadas con la distancia, tales como, por ejemplo, su diámetro y su distancia media entre vértices (ver [22]). En la referencia complementaria [23] se describen y estudian varias familias de grafos con esta propiedad geométrica.

Siguiendo un ejemplo, vamos a ver que cada digrafo $G(n; a, b)$ tiene asociada una L-forma, caracterizada por una matriz 2×2 entera, y viceversa.

4.1 De un digrafo a una L-forma

Consideremos el digrafo $G(n; a, b)$ que se supone fuertemente conexo: $\mathrm{mcd}(n, a, b) = 1$. Consideremos el plano dividido en cuadrados unitarios (centrados en los puntos de coordenadas enteras que forman un retículo). A partir de un cuadrado —o punto reticular—marcado con el cero, sumamos $a \pmod n$ cuando nos movemos horizontalmente al cuadrado siguiente; y $b \pmod n$ cuando nos movemos verticalmente. Entonces, el plano queda "recubierto" por los enteros módulo n, elementos del grupo cíclico $\mathbb{Z}_n$, como se muestra en la Fig. 2 con el ejemplo $G(8; 1, 3)$. Nótese que, de esta forma, cada vértice del digrafo $G(n; a, b)$ queda asociado a un punto del retículo.

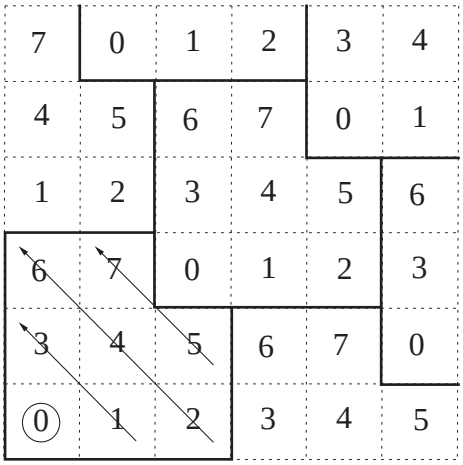

Figure 2: La representación plana de $G(8; 1, 3)$ y su correspondiente L-forma

Ahora escogemos un vértice (o cuadrado) inicial, digamos el 0 (en un círculo en la Fig. 2), lo marcamos y marcamos también todos los vértices desde 1 hasta $n - 1$

que esten a distancia mínima del 0 en el correspondiente digrafo. Notar que, en el retículo, la distancia entre puntos se mide fácilmente con la norma $\|\cdot\|_1$. Por tanto, el marcaje se puede hacer siguiendo un simple algoritmo que considera las diagonales sucesivas, tal como se muestra en la Fig. 2. Entonces se demuestra que los cuadrados marcados forman siempre una L-forma que periódicamente tesela el plano. La baldosa obtenida en nuestro ejemplo se muestra también en la figura. Por la simetría del digrafo, la L-forma obtenida no depende del vértice inicial y, por tanto, lo representa de forma unívoca. En general, una L-forma queda caracterizada por sus dimensiones (l, h, w, y), con $l, h \geq 1$, $0 \leq w \leq l$, $1 \leq y \leq h$, ver Fig. 3. Notar que el diámetro D del digrafo corresponde entonces a la máxima de las distancias desde el 0 hasta los vértices marcados con asterisco; es decir,

$$D = \max\{l + h - w - 2, l + h - y - 2\}.$$

4.2 De una L-forma a un digrafo

A partir de una L-forma con dimensiones (l, h, w, y), $\gcd(l, h, w, y) = 1$, y área $n = lh - wy$, se pueden obtener los pasos a, b del correspondiente digrafo con n vertices de la forma que sigue (ver [11]).

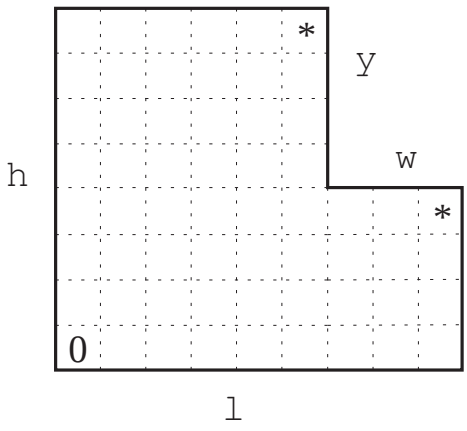

Figure 3: Una L-forma genérica

Consideremos la matriz entera

$$\boldsymbol{M} = \begin{pmatrix} l & -w \\ -y & h \end{pmatrix}$$

con su forma normal de Smith $\boldsymbol{S}(\boldsymbol{M}) = \boldsymbol{U}\boldsymbol{M}\boldsymbol{V} = \mathrm{diag}(1, n)$, donde $\boldsymbol{U}, \boldsymbol{V}$ son matrices unimodulares. Entonces, según los comentarios anteriores y para determinados pasos a, b, tenemos el isomorfismo entre digrafos de Cayley

$$Cay(\mathbb{Z}^2/\boldsymbol{M}\mathbb{Z}^2; \boldsymbol{e}_1, \boldsymbol{e}_2) \cong Cay(\mathbb{Z}_n; a, b) = G(n; a, b),$$

donde $\boldsymbol{e}_1 = (1, 0)$, $\boldsymbol{e}_2 = (0, 1)$. Por consiguiente, según la teoría expuesta en la Subsección 3.1, los pasos a, b son las imágenes, por la aplicación Ψ, de los vectores coordenados $\boldsymbol{e}_1, \boldsymbol{e}_2$. Esto es, si $\boldsymbol{U}$ tiene como segunda fila el vector (α, β), los pasos del digrafo $G(n; a, b)$ son $a = \alpha \pmod n$ y $b = \beta \pmod n$. Este posible par de pasos no es único, ya que la matriz resultante $\boldsymbol{U}$ en la factorización de $\boldsymbol{S}$ tampoco lo es. De hecho, todos los pares posibles son de la forma $a' = \lambda a \pmod n$ y $b' = \lambda b \pmod n$ con $\lambda \in \mathbb{Z}_n^\star$ (es decir, $\mathrm{mcd}(\lambda, n) = 1$), ver [22].

Podemos aplicar este método a nuestro ejemplo previo. Consideremos la L-forma de la Fig. 2, con dimensiones $l = h = 3,\ w = y = 1$. Entonces

$$\boldsymbol{M} = \begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix},$$

y el cómputo de $S(\boldsymbol{M})$, $\boldsymbol{U}$, $\boldsymbol{V}$ da:

$$\boldsymbol{S} = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}, \quad \boldsymbol{U} = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \quad \boldsymbol{V} = \begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}.$$

Así, los pasos son $(a, b) = (3, 1)$ o, más generalmente, $(a, b) = (3\lambda, \lambda)$, $\lambda \in \mathbb{Z}_8^\star$. Esto es, $(a, b) \in \{(3, 1), (1, 3), (7, 5), (5, 7)\}$.

5 Mosaicos periódicos

Como es bien sabido, un mosaico está constituido por una serie de baldosas que recubren todo el plano sin solaparse ni dejar huecos. Un mosaico se llama *periódico* cuando al trasladarlo según un cierto movimiento rígido (o *isometria*) se superpone a sí mismo (es decir, queda invariante). Una o más baldosas teselan periódicamente cuando constituyen un mosaico (*embaldosado* o *teselación*) periódico. El caso más simple se produce cuando una sola figura tesela usando sólo translaciones, como ocurre con los polígonos regulares cuadrado y hexágono. Los mosaicos periódicos han sido objeto de atención y estudio desde muy antiguo. En nuestro país tenemos un magnífico ejemplo de ello en los mosaicos de la Alhambra de Granada, que han sido

(y son) objeto de numerosos estudios, incluida alguna tesis doctoral (cuya principal contribución se describe en [32]). Gran parte de su interés radica en la relación que guardan con la teoría de grupos; en particular, el estudio y clasificación de los grupos cristalográficos planos. (El desarrollo de la cristalografía corresponde al siglo XIX, aunque el primer tratamiento matemático de los mosaicos se debe a Kepler). El lector interesado en más detalles sobre el tema, puede consultar el texto de Grünbaum y Shephard [25].

5.1 Equidescomposición de figuras planas

Dos figuras planas se llaman *equidescomponibles* cuando una de ellas puede dividirse en un número finito de piezas que, resituadas adecuadamente, permiten obtener la otra (sin que se produzcan solapamientos ni queden huecos). Por tanto, dos figuras equidescomponibles deben tener la misma área. Lo curioso es que, para figuras poligonales, el resultado converso también es cierto: Según el teorema clásico de Bolyai-Gerwin, *cualquier par de regiones poligonales de igual área son equidescomponibles*. Además, se sabe que la disección puede hacerse utilizando sólo regla y compás. Sin embargo, el resultado análogo para poliedros no se cumple. Por ejemplo, se ha demostrado que un tetraedro regular y un cubo de igual volumen no son equidescomponibles. De forma más restrictiva, a veces se requiere que las figuras no tan sólo sean equidescomponibles, sino que una se pueda transformar en la otra usando solamente cierto tipo de movimientos como, por ejemplo, translaciones y rotaciones. Como dichos movimientos y su composición forman un grupo, digamos G, se dice entonces que las correspondientes figuras son *G-equidescomponibles*. En este contexto, otro resultado clásico es el teorema de Hadwiger-Glur, que afirma que dos regiones poligonales de igual área son siempre G_S-equidescomponibles, siendo G_S el grupo de translaciones y simetrías centrales (o, lo que es lo mismo, giros de 180 grados). De hecho, se sabe que éste es el mínimo subgrupo del grupo completo G_K de isometrías del plano que cumple esta propiedad. Una demostración de estos resultados puede realizarse utilizando las propiedades de las teselaciones periódicas (ver [1]). La idea básica en dicha demostración es la obtención de determinadas equidescomposiciones a partir de la superposición de dos teselaciones formadas con las figuras correspondientes. Un ejemplo interesante se muestra en la Fig. 4, donde se obtiene la conocida equidescomposición mínima (con el mínimo número posible de piezas) de un cuadrado y un triángulo equilatero.

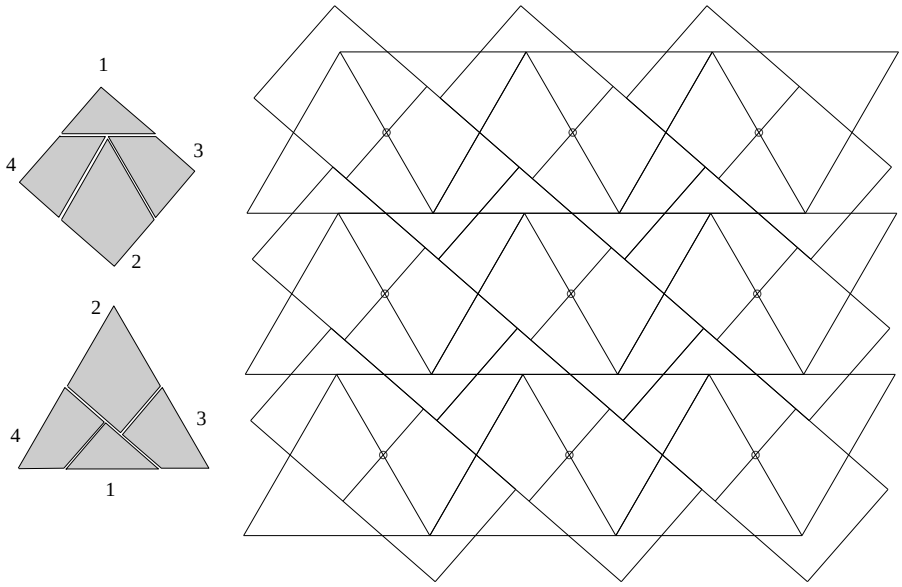

Figure 4: Equidescomposición mínima de un cuadrado y un triángulo equilátero.

6 Una generalización del teorema chino del resto

Dado un elemento $\boldsymbol{a}$ (vector columna) del grupo $\mathbb{Z}^n/\boldsymbol{M}\mathbb{Z}^n$, denotemos por $o(\boldsymbol{a})$ su orden, definido como el menor entero positivo r tal que $r\boldsymbol{a} \equiv 0 \pmod{\boldsymbol{M}}$. Equivalentemente,

$$r\boldsymbol{M}^{-1}\boldsymbol{a} = \frac{m\boldsymbol{M}^{-1}\boldsymbol{a}}{m/r} \in \mathbb{Z}^n.$$

Por ser r mínimo, m/r es el máximo entero positivo tal que divide a m y a todos los números $\boldsymbol{m}_i\boldsymbol{a}$, donde $\boldsymbol{m}_i$ denota ahora la i-ésima fila de la matriz $m\boldsymbol{M}^{-1}$. Entonces,

$$o(\boldsymbol{a}) = \frac{m}{\operatorname{mcd}(m, \boldsymbol{m}_1\boldsymbol{a}, \ldots, \boldsymbol{m}_n\boldsymbol{a})}. \tag{8}$$

Una ligera generalización del teorema chino del resto se enuncia de la siguiente forma:

- *Sean $m_1, m_2, \ldots, m_n$ y $a_1, a_2, \ldots, a_n$ enteros tales que*

$$\operatorname{mcd}(m_i, m_j) = 1 \quad (i \neq j); \qquad \operatorname{mcd}(a_i, m_i) = 1 \quad (1 \leq i \leq n). \tag{9}$$

Entonces, dados enteros cualesquiera $b_1, b_2, \ldots, b_n$, el sistema de congruencias

$$a_i x \equiv b_i \pmod{m_i} \quad (1 \leq i \leq n) \tag{10}$$

tiene exactamente una solución módulo $m = |m_1 m_2 \cdots m_n|$.

En su forma clásica, el teorema chino del resto corresponde al resultado anterior cuando $a_i = 1$ para todo $1 \leq i \leq n$, con lo cual la segunda condición en (9) desaparece.

En nuestro contexto, el sistema de congruencias (10) es equivalente a la congruencia

$$x\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{M}}, \tag{11}$$

donde $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)^\top$, $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)^\top$, y $\boldsymbol{M} = \operatorname{diag}(m_1, m_2, \ldots, m_n)$.

Entonces, estamos interesados en la solución de la congruencia (11) para una matriz genérica $\boldsymbol{M}$. Así, el siguiente resultado, que puede verse como una generalización del teorema chino del resto, es una consecuencia directa de (8).

• *Sea* $\boldsymbol{M}$ *una matriz* $n \times n$ *entera, con determinante* $m = |\det \boldsymbol{M}| > 0$. *Sea* $g = \operatorname{mcd}(m, \boldsymbol{m}_1\boldsymbol{a}, \ldots, \boldsymbol{m}_n\boldsymbol{a})$, *donde* $\boldsymbol{m}_i$ *es la* i*-ésima fila de la matriz* $m\boldsymbol{M}^{-1}$. *Si* $g = 1$, *entonces la congruencia*

$$x\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{M}}, \tag{12}$$

tiene exactamente una solución módulo m *para cualquier* $\boldsymbol{b} \in \mathbb{Z}^n$.

En particular, si $\boldsymbol{M} = \operatorname{diag}(m_1, m_2, \ldots, m_n)$ se tiene la condición

$$g = \operatorname{mcd}\left(m, \frac{a_1 m}{m_1}, \ldots, \frac{a_n m}{m_n}\right) = 1 \tag{13}$$

que, como se puede comprobar, es equivalente a (9).

6.1 Algunas aplicaciones: Esquemas para compartir secretos

Históricamente, el problema chino del resto se planteó por la necesidad de confeccionar calendarios teniendo en cuenta diferentes eventos que sucedían con periodicidades diferentes. En la actualidad, el teorema chino del resto, en sus diferentes versiones, tiene aplicaciones en casi todas las áreas de la matemática. Como ejemplos, tenemos la teoría de autómatas finitos, temas de computación (cálculo modular, computación simbólica), algorítmica (convolución cíclica, transformada rápida de Fourier, interpolación de polinomios sobre cuerpos), la teoría de códigos (códigos bloque, códigos de residuo redundantes), y criptografía (esquemas para compartir secretos, esquemas de clave pública). El lector interesado en éstas y otras aplicaciones puede consultar la referencia [9]. En particular, en dicho trabajo se discuten dos aplicaciones de la generalización expuesta anteriormente del teorema en cuestión,

que hacen referencia al diseño de códigos de residuo redundantes y esquemas para compartir secretos. Veamos algunos detalles sobre dichos esquemas.

En un *esquema para compartir secretos*, hay un conjunto de n participantes, cada uno de los cuales recibe un *fragmento* del secreto, de manera que sólo determinados subconjuntos "autorizados" pueden reconstruir el secreto (ver [34]). Estos esquemas son útiles, por ejemplo, en procesos en los que, en una red distribuida o de área local, se pretende realizar cálculos a partir de datos que deben mantenerse confidenciales. La *estructura de acceso* de un esquema para compartir secretos es la familia de tales subconjuntos. Como es lógico, se requiere que cualquier conjunto que contenga un subconjunto autorizado sea también autorizado. Por ejemplo, la llamada *estructura de* (t, n)*-umbral*, correspondiente a un *esquema de* (t, n)*-umbral* [28], está constituida por todos los subconjuntos con al menos t elementos de un conjunto con n elementos.

Veamos, por ejemplo, como la versión clásica del teorema chino del resto proporciona, por sí mismo, un esquema muy simple (con $t = n$) para compartir secretos. Sea $m_1, m_2, \ldots, m_n$ enteros positivos primos entre sí a pares, y $m = \prod_{i=1}^{n} m_i$. Consideremos el mencionado teorema con respecto a estos módulos. Supongamos que el secreto es un entero s, tal que $0 \leq s < n$, que es compartido por t participantes P_i, $1 \leq i \leq n$, de la siguiente forma: Al participante P_i se le da el residuo $s_i \equiv s \pmod{m_i}$. Entonces, por el teorema chino del resto, los t fragmentos de información s_i son suficientes para determinar el secreto original s, pero resulta imposible a partir de cualquier subconjunto con menos de t residuos s_i.

7 Teoría espectral de grafos

Como ya se ha dicho anteriormente, un digrafo consta simplemente de una serie de vértices y arcos que los unen. La versión no dirigida de este concepto es el llamado grafo $G = (V, E)$, con conjunto de vértices $V = V(G)$, y ramas $E = E(G)$ que son pares no ordenados de vértices. Si los vértices $i, j \in V$ forman una rama, se denota por $ij \in E$ ó $i \sim j$, y se dice que i y j son *adyacentes*.

Una forma usual de representar un grafo (o digrafo) G es a través de su *matriz de adyacencia* $\boldsymbol{A} = (a_{ij})$, con filas y columnas indexadas por los vértices de G, y elementos

$$a_{ij} = \begin{cases} 1 & \text{si } i \sim j \\ 0 & \text{en caso contrario.} \end{cases}$$

El problema genérico de la teoría algebraica de grafos consiste en estudiar propiedades (estructurales) del grafo G a partir de propiedades (algebraicas) de la matriz $\boldsymbol{A}$ (y

viceversa). Por ejemplo, se demuestra que el elemento ij de la potencia k-ésima de $\boldsymbol{A}$, $a_{ij}^{(k)} = (\boldsymbol{A}^k)_{ij}$, coincide con el número de caminos de longitud k (longitud = número de ramas) que van del vértice i al vértice j.

Como la matriz de adyacencia depende del orden en que se consideran los vértices, solemos centrar nuestra atención sobre aquellas propiedades de $\boldsymbol{A}$ que son invariantes bajo una permutación de sus filas y columnas. Posiblemente, la más conocida de tales propiedades es el espectro de la matriz, o conjunto de sus autovalores y multiplicidades, que se denota por

$$\operatorname{sp} G = \{\lambda_0^{m_0}, \lambda_1^{m_1}, \ldots, \lambda_d^{m_d}\}.$$

(Los exponentes indican las multiplicidades). Así, la teoría espectral de grafos trata de dilucidar hasta que punto el espectro de la matriz de adyacencia de un grafo contiene información sobre su estructura. En un primer momento se pensó que dicho espectro podría caracterizar unívocamente el grafo, pero pronto se descubrió la existencia de grafos distintos (es decir, no isomorfos) con el mismo espectro, a los que se les llamó *grafos coespectrales*. Una buena introducción a la teoría algebraica (y, en particular, espectral) de grafos puede encontrarse en el texto clásico de Biggs [5].

Una idea muy simple, pero muy útil, en este campo es la siguiente interpretación de los autovectores y autovalores como un proceso dinámico de "desplazamiento de cargas". Supongamos que $\boldsymbol{A}$, la matriz de adyacencia de un grafo o digrafo, tiene autovector $\boldsymbol{v}$ con autovalor λ: $\boldsymbol{Av} = \lambda\boldsymbol{v}$. Si cada componente v_i de $\boldsymbol{v}$ se interpreta como una carga inicial del vértice i, nos interesa averiguar que ocurre cuando aplicamos la transformación (movimiento de cargas) representado por $\boldsymbol{A}$. Para ello calculamos las componentes i-ésimas en la ecuación vectorial anterior y obtenemos:

$$(\boldsymbol{Av})_i = \sum_{j=1}^{n} a_{ij} v_j = \sum_{i \sim j} v_j = \lambda v_i. \tag{14}$$

Por tanto, el efecto resultante es que cada vértice i recibe las cargas de sus vecinos para quedar con una carga final igual a λ veces la que tenía inicialmente. En otras palabras, el autovalor λ es la razón, común a todos los vértices, entre las cargas final e inicial:

$$\lambda = \frac{1}{v_i} \sum_{i \sim j} v_j \qquad \text{para todo } i \in V \text{ con } v_i \neq 0.$$

Entre los parámetros de un grafo estudiados a partir de su espectro, podemos mencionar: el *número de independencia* α (máximo número de vértices no adyacentes

entre sí); el *número cromático* χ (mínimo número de colores necesarios para colorear los vértices de manera que vértices adyacentes tengan distinto color); y el *diámetro* D (misma definición que en el caso de digrafos, pero ahora la distancia es una métrica pues los caminos son no dirigidos). Por ejemplo, en cuanto a los dos primeros parámetros, se sabe que, si G es un grafo regular (es decir, cada vértice tiene el mismo número—llamado *grado*—de vértices adyacentes) con n vértices y autovalores $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$, entonces,

$$\alpha \leq \frac{n}{1 - \frac{\lambda_1}{\lambda_n}}, \qquad \chi \geq 1 - \frac{\lambda_1}{\lambda_n}.$$

(Para las demostraciones, ver [5]). Resultados similares también se aplican en el caso no regular (ver [14]). En cuanto al diámetro, si G es un grafo conexo con $d+1$ autovalores distintos, $\lambda_0 > \lambda_1 > \cdots > \lambda_d$ (notar el cambio de notación), entonces $D \leq d$. Además, si G es regular con n vértices,

$$\sum_{i=0}^{d} \frac{\pi_0}{\pi_i} > n \quad \Rightarrow \quad D \leq d-1,$$

donde los $\pi_i's$ son parámetros tipo-momento que se calculan a partir de las distancias entre autovalores en la forma $\pi_i = \prod_{j=0(j\neq i)}^{d} |\lambda_i - \lambda_j|$, $0 \leq i \leq d$, (ver [21]).

8 Distancia-regularidad

Según se comenta en [2], nadie sabe quién formuló por primera vez el siguiente resultado o le dió su "toque humano":

- *Si en una reunión de tres o más personas, cada dos personas tienen precisamente un amigo en común, entonces hay una persona (el "político") que es amigo de todos.*

Actualmente se le conoce como el "teorema de la amistad". La primera demostración (por contradicción) se debe a Erdös, Rényi y Sós [10], y está considerada aún como la más conseguida. Básicamente, consta de dos partes: primero se demuestra que si el grafo G que modela tal reunión (donde, por supuesto, las amistades se representan por ramas) es un contraejemplo con más de 3 vértices, entonces debe ser regular, digamos de grado k. Como consecuencia de ello, resulta que G debe ser "fuertemente regular" con parámetros $(n, k; 1, 1)$ (es decir, cada par de vértices son adyacentes a

exactamente un vértice común). En segundo lugar usamos de nuevo la teoría espectral para demostrar que G no puede existir.

El (supuesto) grafo G es, de hecho, un ejemplo de grafo "distancia-regular", en este caso con diámetro 2. En general, y hablando de forma intuitiva, decimos que un grafo es distancia-regular cuando, al ser observado (o "colgado") desde cualquiera de sus vértices, siempre se obtiene la misma estructura por "capas" (constituidas por los vértices a distancia $0, 1, 2, \ldots$ del vértice base), y los vértices de cada capa resultan indistinguibles entre sí. Como ejemplos sencillos de grafos distancia-regulares podemos citar, por ejemplo, los 1-esqueletos de los poliedros regulares. Una definición más precisa de la distancia-regularidad es la siguiente: Un grafo G con diámetro D es distancia-regular si, para cada par de vértices (u, v) y enteros $0 \leq i, j \leq D$, el número $p_{ij}(u, v)$ de vertices a distancia i de u y a distancia j de v sólo depende de $k = \mathrm{dist}(u, v)$, y entonces escribimos $p_{ij}(u, v) = p_{ij}^k$ para ciertas constantes p_{ij}^k llamadas "números de intersección". De hecho, debido a las muchas relaciones existentes entre dichos números, se puede dar una definición mucho más económica que, para cada distancia k, involucra solamente los pares de distancias $(i, j) = (k-1, 1)$, $(k, 1)$, y $(k+1, 1)$. (Sucede que los correspondientes números de intersección son suficiente para determinar todos los demás; ver, por ejemplo, [5]). Así, la definición más usual de distancia-regularidad reza de la siguiente forma: *Un grafo* Γ *es distancia-regular cuando, para cualquier par de vértices* u, v *a distancia* $\mathrm{dist}(u, v) = k$*, los números* c_k*,* a_k*,* b_k*, de vertices que son adyacentes a* v*, y están a distancia* $k-1$*,* k*,* $k+1$*, respectivamente, de* u *sólo dependen de* k*.*

Desde su introducción (por Biggs, a principios de los años 70), los grafos distancia-regulares, y su principal generalización los "esquemas de asociación", han demostrado ser un concepto clave en combinatoria algebraica. Dichos grafos tienen conexiones importantes con otras ramas de las matemáticas, tales como geometría, teoría de códigos, teoría de grupos, teoría de diseños, así como también con otras áreas de la teoría de grafos. Tal como apuntan Brouwer, Cohen y Neumaier en su extenso texto sobre el tema [6], ello es debido a que la mayor parte de objetos finitos que gozan de "suficiente regularidad" están relacionados estrechamente con los grafos distancia-regulares.

Una reciente caracterización de estos grafos, obtenida por el autor y Garriga [18], es la siguiente:

• *Un grafo regular* Γ *con matriz de adyacencia* $\boldsymbol{A}$*, con* $d+1$ *autovalores distintos, es distancia-regular si y sólo si el número* $n_d(u)$ *de vértices a distancia* d *de cada vértice* u *es constante y depende solamente del espectro de* $\boldsymbol{A}$*.*

Más precisamente, si Γ tiene n vertices y espectro $\operatorname{sp} \boldsymbol{A} = \{\lambda_0^1, \lambda_1^{m_1}, \ldots, \lambda_d^{m_d}\}$ (recuérdese que los supraíndices denotan multiplicidades; λ_0 es simple—$m_0 = 1$—porque, al ser G conexo, la matriz $\boldsymbol{A}$ es irreducible) entonces se requiere que, para todo vértice u,

$$n_d(u) = n \left(\sum_{i=0}^{d} \frac{\pi_0^2}{m_i \pi_i^2} \right)^{-1} \qquad (u \in V), \tag{15}$$

donde, como antes, $\pi_i = \prod_{j=0(j\neq i)}^{d} |\lambda_i - \lambda_j|$, $0 \leq i \leq d$. De hecho, la caracterización anterior sigue siendo válida si las n igualdades en (16) se sustituyen por una sola:

$$\sum_{u \in V} n_d(u)^{-1} = \sum_{i=0}^{d} \frac{\pi_0^2}{m_i \pi_i^2}, \tag{16}$$

(ver [16]). Nótese que $n \sum_{u \in V} n_d(u)^{-1}$ corresponde a la media harmónica de los números $n_d(u)$.

Como ejemplo, consideremos el grafo (1-esqueleto) del cubo $G = \mathsf{Q}_3$, que tiene $n = 8$ vertices, espectro $\operatorname{sp} \mathsf{Q}_3 = \{3^1, 1^3, -1^3, -3^1\}$ y diámetro $d = 3$. Además, cada vértice u tiene exactamente un vértice a distancia máxima, $n_d(u) = 1$. Entonces, por la simetría de la malla de autovalores, obtenemos $\pi_0 = \pi_3 = 2 \cdot 4 \cdot 6$ y $\pi_1 = \pi_2 = 2 \cdot 2 \cdot 4$, de donde $\frac{\pi_0}{\pi_1} = \frac{\pi_0}{\pi_2} = 3$ y $\frac{\pi_0}{\pi_3} = 1$, y el sumatorio en (16) da

$$8 \left(2 + \frac{2}{3} \cdot 3^2 \right)^{-1} = 1 = n_d(u).$$

Por tanto, se concluye que Q_3 es un grafo distance-regular (llamado 2-*antipodal* porque cada vértice tiene exactamente un vértice a distancia máxima).

8.1 Aplicaciones en teoría de códigos

En lenguaje amplio, podemos entender una cierta cantidad de información como una serie de palabras concatenadas. En la práctica sucede a menudo que, al transmitir dicha información, se producen errores que enmascaran su significado (al modificar las palabras que la constituyen). La teoría de códigos, iniciada por Shannon en su famoso artículo [33] (ver http://antoine.iies.es/Papeles/Shanon.PDF), estudia la manera de solucionar este problema. Básicamente, se trata de añadir "redundancia" a cada palabra para hacerla "insensible" a posibles alteraciones. Un ejemplo sencillo lo constituye el lenguaje común, en el que la mayoría de palabras "conservan" su significado

aún que estén escritas o pronunciadas erróneamente. Para una introducción a la teoría de códigos, ver por ejemplo el texto de Van Lint [27].

Como ya se ha mencionado anteriormente, la teoría sobre grafos distancia-regulares tiene múltiples aplicaciones en teoría de códigos. En teoría de grafos, un código dado C (conjunto de palabras permitidas o *palabras-código*) puede representarse simplemente como un cierto subconjunto de vértices $C \subset V$ de un grafo G, normalmente distancia-regular [24, 27]. El conjunto de vértices representa el "universo" de palabras que uno puede recibir (tengan significado o no); y se establece una rama entre dos palabras cuando, con una cierta probabilidad, una puede transformarse en la otra en el proceso de la transmisión. Así, cuanto menor es la distancia entre dos palabras (medida en G) más se asemejan. Si una palabra-código no ha sufrido demasiadas alteraciones, la palabra resultante no está demasiado lejos de la original y ello permite recuperarla (criterio de decisión por proximidad). Por tanto un código es tanto mejor cuanto más alejadas están entre sí las palabras que lo constituyen. En el estudio y diseño de buenos códigos, se usan técnicas algebraicas que, como ya se ha explicado, nos dan información sobre la estructura del grafo G y, en particular, del subconjunto de vértices C que representa al código. En las aplicaciones son especialmente importantes los llamados códigos "completamente regulares", para los cuales el grafo que los contiene se estructura en una especie de distancia-regularidad alrededor del conjunto que constituye el código. Sucede entonces que dichos códigos pueden caracterizarse algebráicamente de forma similar a como se caracterizan los grafos distancia-regulares, a través de su espectro, según la fórmula (16), (ver [19, 20]).

9 Matrices circulantes

Una matriz cuadrada $\boldsymbol{C}$ se llama *circulante*, y se denota por $\boldsymbol{C} = \mathrm{circ}(c_0, c_1, \ldots, c_{n-1})$, si cada una de sus filas se obtiene desplazando cíclicamente una posición la fila anterior. Esto es:

$$\boldsymbol{C} = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & \ldots & c_0 \end{pmatrix}.$$

Así, por ejemplo, el ciclo dirigido de n vértices C_n tiene como matriz de adyacencia $\boldsymbol{A} = \mathrm{circ}(0, 1, 0, \ldots, 0)$, cuyo elemento ij es $a_{ij} = 1$ si $j = i + 1 \pmod n$ (j adyacente desde i), y $a_{ij} = 0$ en caso contrario. Análogamente, la potencia k-ésima es $\boldsymbol{A}^k = \mathrm{circ}(0, 0, \ldots, 1, \ldots, 0)$, con el 1 en la posición k ya que indica un único camino entre

vértices a distancia k. De lo anterior, vemos que cualquier matriz circulante se puede escribir en la forma

$$\boldsymbol{C} = \mathrm{circ}(c_0, c_1, \ldots, c_{n-1}) = \sum_{k=0}^{n-1} c_k \boldsymbol{A}^k. \tag{17}$$

Por otra parte, el polinomio característico de $\boldsymbol{A}$ es

$$\phi(C_n, \lambda) = \det \begin{pmatrix} \lambda & -1 & 0 & \cdots & 0 \\ 0 & \lambda & -1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \cdots & \lambda \end{pmatrix} = \lambda^n - 1.$$

con lo cual los autovalores de $\boldsymbol{A}$ son las raíces n-ésimas de la unidad

$$\lambda_k = \sqrt[n]{1} = e^{i\frac{k2\pi}{n}} \quad (0 \leq k \leq n-1).$$

Otra forma de ver ésto es considerar ciertos vectores que resulten ser autovectores de $\boldsymbol{A}$. A tal fin, denotemos $\omega = \lambda_1 = e^{i\frac{2\pi}{n}}$, con lo cual $\lambda_k = \omega^k$ y $\overline{\lambda_k} = \omega^{-k}$. Entonces definimos los n vectores columna $\boldsymbol{\phi}_k$ de la forma siguiente:

$$\boldsymbol{\phi}_k = (\omega^0, \omega^k, \omega^{2k}, \ldots, \omega^{(n-1)k})^\top \quad (0 \leq k \leq n-1)$$

con ℓ-ésima componente $\phi_{k\ell} = \omega^{k\ell}$, $0 \leq \ell \leq n-1$. Así resulta, recordando la interpretación en (14), que

$$\begin{aligned} (\boldsymbol{A}\boldsymbol{\phi}_k)_\ell &= \sum_{\ell \sim j} \phi_{kj} = \phi_{k,\ell+1} \\ &= \omega^{k(\ell+1)} = \omega^k \omega^{k\ell} \\ &= \lambda_k (\boldsymbol{\phi}_k)_\ell \quad (0 \leq \ell \leq n-1) \end{aligned}$$

es decir,

$$\boldsymbol{A}\boldsymbol{\phi}_k = \lambda_k \boldsymbol{\phi}_k \qquad (0 \leq k \leq n-1).$$

Por tanto, hemos comprobado que cada vector $\boldsymbol{\phi}_k$ es autovector de $\boldsymbol{A}$ con autovalor $\lambda_k = \omega^k$.

Esto nos permite calcular los autovectores y autovalores de cualquier matriz circulante. En efecto, a la vista de (17), y para cada vector $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1})$, definimos, el polinomio $p_{\boldsymbol{c}}$ como

$$p_{\boldsymbol{c}}(x) = \sum_{k=0}^{n-1} c_k x^k.$$

Entonces los autovalores θ_k de la matriz circulante $\boldsymbol{C} = \mathrm{circ}(c_0, c_1, \ldots, c_{n-1})$ son de la forma

$$\theta_k = p_{\boldsymbol{c}}(\lambda_k) = p_{\boldsymbol{c}}(\omega^k) \qquad (0 \leq k \leq n-1).$$

(Nótese que estos autovalores no son necesariamente distintos). En las siguientes subsecciones discutimos algunas posibles aplicaciones de las matrices circulantes.

9.1 Polígonos anidados

Consideremos un polígono P_0, cuyos n vértices se representan mediante las componentes de un vector (columna) complejo $\boldsymbol{c}_0 = (c_{00}, c_{01}, \ldots, c_{0,n-1})^\top$ tal que $\sum_{i=0}^{n-1} c_{0i} = 0$ (esto significa que el centro de gravedad del polígono coincide con el origen de coordenadas) y lados $c_{0i}c_{0,i+1}$, $0 \leq i \leq n-1$ (con aritmética módulo n). Dados dos números reales $s, t \in [0,1]$ tales que $s + t = 1$, consideramos ahora el polígono P_1 con vértices los elementos del vector $\boldsymbol{c}_1 = (c_{10}, c_{11}, \ldots, c_{1,n-1})^\top$, tales que el punto c_{1i} está situado sobre el lado $c_{0i}c_{0,i+1}$ y la razón entre las distancias a sus extremos es precisamente s/t:

$$\frac{\mathrm{dist}(c_{1i}, c_{0,i+1})}{\mathrm{dist}(c_{1i}, c_{0,i})} = \frac{|c_{1i} - c_{0,i+1}|}{|c_{1i} - c_{0,i}|} = \frac{s}{t};$$

es decir,

$$c_{1i} = sc_{0,i} + tc_{0,i+1} \qquad (0 \leq i \leq n-1). \tag{18}$$

La cuestión general que se plantea es averiguar la relación entre ambos polígonos P_1 y P_0 o, entendido como un proceso dinámico, cómo se ven modificadas las propiedades (por ejemplo, área, perímetro, centro de gravedad, etc.) de P_0 al transformarse en P_1? Más aún, podemos iterar el procedimiento para obtener un tercer polígono P_2 a partir de P_1, y así sucesivamente obtener una sucesión infinita

$$\mathsf{P}_0, \mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3, \ldots, \mathsf{P}_k, \ldots$$

cuyos elementos reciben, debido a su aspecto geométrico, el nombre de *polígonos anidados*. Entonces interesa conocer si existe, y que aspecto tiene, el "polígono-límite" $\lim_{k\to\infty} \mathsf{P}_k$. Resulta que la transformación considerada (18) admite la representación matricial

$$\boldsymbol{c}_{k+1} = \boldsymbol{C}\boldsymbol{c}_k, \qquad k = 0, 1, 2, \ldots$$

donde $\boldsymbol{C} = \mathrm{circ}(0, s, t, 0, 0, \ldots, 0)$. Esto permite resolver el problema planteado utilizando la teoría de matrices circulantes anteriormente descrita (ver [8]).

9.2 La transformada discreta de Fourier

Resulta que los vectores $\boldsymbol{\phi}_k$, estudiados al principio de esta sección, son ortogonales entre sí con respecto al producto escalar usual para vectores complejos:

$$\langle \boldsymbol{\phi}_k, \boldsymbol{\phi}_h \rangle = \sum_{\ell=0}^{n-1} \phi_{k\ell} \overline{\phi}_{h\ell} = \begin{cases} 0, & k \neq h \\ n, & k = h \end{cases}$$

y, por tanto, $\{\frac{1}{\sqrt{n}}\boldsymbol{\phi}_k\}_{0 \leq k \leq n-1}$ es una base ortonormal de $\mathbb{C}^n$. Esto sugiere representar cualquier vector complejo $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})^\top$ en términos de dicha base:

$$\boldsymbol{x} = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \gamma_k \boldsymbol{\phi}_k$$

donde

$$\begin{aligned} \gamma_k &= \frac{1}{\sqrt{n}} \langle \boldsymbol{x}, \phi_k \rangle = \frac{1}{\sqrt{n}} \sum_{\ell=0}^{n-1} x_\ell \overline{\phi_{k\ell}} \\ &= \frac{1}{\sqrt{n}} \sum_{\ell=0}^{n-1} x_\ell \omega^{-k\ell} = \frac{1}{\sqrt{n}} \sum_{\ell=0}^{n-1} x_\ell e^{-i\frac{2\pi k}{n}\ell} \end{aligned}$$

es el coeficiente de Fourier del desarrollo.

La matriz de cambio de base $\boldsymbol{F} = (f_{k\ell})$, con componentes $f_{k\ell} = \frac{1}{\sqrt{n}}\omega^{-k\ell}$, $0 \leq k, \ell \leq n-1$, es la llamada *matriz de Fourier*. Notar que es una matriz simétrica, con filas (y columnas) los vectores normalizados $\frac{1}{\sqrt{n}}\overline{\boldsymbol{\phi}_k}$, que cumple:

$$\overline{\boldsymbol{F}}\boldsymbol{F} = \boldsymbol{I} \tag{19}$$

(es decir, es una matriz unitaria). La *transformada discreta de Fourier* del vector $\boldsymbol{x}$, denotada por $\boldsymbol{X}$ ó $\mathcal{F}\boldsymbol{x}$, es simplemente el vector transformado (o vector de coeficientes)

$$\boldsymbol{X} = \mathcal{F}\boldsymbol{x} = \boldsymbol{F}\boldsymbol{x}.$$

Por tanto, la fórmula de la transformada inversa, que "recupera" $\boldsymbol{x}$ a partir de $\boldsymbol{X}$, es, según (19),

$$\boldsymbol{x} = \mathcal{F}^{-1}\boldsymbol{x} = \overline{\boldsymbol{F}}\boldsymbol{x}.$$

Esta transformación se usa en teoría de la señal para el análisis de señales discretas (obtenidas, por ejemplo, al muestrear una señal continua) y periódicas (para más detalles, ver [29]).

9.3 Acoplamiento modal

La formulación general de n circuitos resonantes acoplados permite unificar el estudio de diferentes problemas de la física electromagnética [26]. Citemos, como ejemplos, el estudio de filtros de banda de paso, circuitos combinadores de potencia (u osciladores con n elementos activos idénticos), sistemas de onda lenta (como los ánodos de magnetrones), y la formación de arrays de antenas. Cuando el acoplamiento es cíclico; es decir, cuando todos los circuitos son idénticos y el sistema es invariante bajo una permutación cíclica (el ejemplo más simple es el de una cadena en anillo de resonadores idénticos); las propiedades matemáticas de estos sistemas se derivan fácilmente del carácter circulante de la matriz que describe el acoplamiento. Un estudio de tales propiedades, así como de algunas topologías geométricamente realizables (a nivel físico, los acoplamientos sólo se realizan entre elementos adyacentes y no existen cruces entre ellos), se puede encontrar en [3, 17]. Un ejemplo de tales estructuras es la toroidal, de la que se muestra un caso particular, con $n = 15$, en la Fig. 5 (donde los vértices y ramas del grafo representan a los osciladores y a sus acoplamientos, respectivamente). Nótese que la matriz de adyacencia del grafo es una matriz circulante, a saber $\boldsymbol{A} = \mathrm{circ}(0,0,0,1,0,1,0,0,0,0,1,0,1,0,0)$, ya que cada vértice i es adyacente a los vértices $i \pm 3$, $i \pm 5$, (mod 15) (red—no dirigida—de paso fijo).

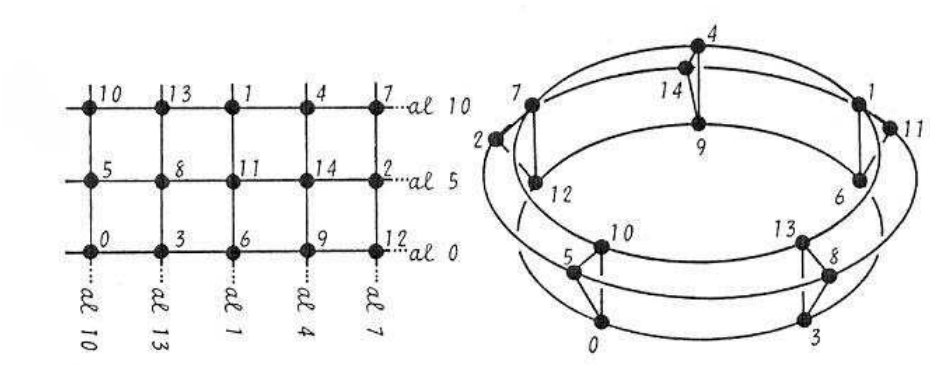

Figure 5: Estructura toroidal de osciladores acoplados.

Agradecimientos

Estas notas corresponden a una conferencia plenaria impartida en el *Primer Congreso Conjunto de Matemáticas RSME-SCM-SEIO-SEMA, MAT.ES 2005*, Facultad de Matemáticas de la Universidad de Valencia, Valencia, 31 enero–4 febrero de 2005. El autor agradece a los organizadores la invitación recibida.

Trabajo subvencionado por la *Comisión Interministerial de Ciencia y Tecnología* (CICYT) y el *Fondo Europeo de Desarrollo Regional* (FEDER) en el marco del proyecto *"Transporte y Gestión de la Información en Sistemas Distribuidos: Modelización de Redes y Diseño de Algoritmos"* (TIC-2001-2171).

El autor agradece también a los profesores Ernest Garriga y José Luis Andrés Yebra los comentarios que permitieron mejorar una versión previa de este trabajo.

References

[1] F. Aguiló, M.A. Fiol, and M.L. Fiol, Periodic tilings as a dissection method. *Amer. Math. Monthly* **107** (2000), no. 4, 341–352.

[2] M. Aigner y G. M. Ziegler, *Proofs from THE BOOK*. Springer, Berlin, 1998.

[3] J. Bará y M.A. Fiol, Matrices circulantes en problemas de acoplamiento modal. Parte I: Análisis. *Actas GEM, IV Reunión*, Comisión: Electricidad y Magnetismo, Murcia, 29–30 sep. 1983, pp. 13–18.

[4] R. Bellman, *Introducción al Análisis Matricial*. Reverté, Barcelona, 1965.

[5] N. Biggs, *Algebraic Graph Theory*. Cambridge University Press, Cambridge, UK, 1993.

[6] A.E. Brouwer, A.M. Cohen y A. Neumaier, *Distance-Regular Graphs*. Springer-Verlag, Berlin, 1989.

[7] F. Comellas, J. Fàbrega, A.S. Lladó i O. Serra, *Matemàtica Discreta*. Politext 26, Edicions UPC, Barcelona, 1994.

[8] P. J. Davis, *Circulant Matrices*. John Wiley & Sons, New York, 1979.

[9] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem. Applications in Computing, Coding, Cryptography*. World Sci. Pub., River Edge, NJ, 1996.

[10] P. Erdös, A. Rényi and V. T. Sós, On a problem of graph theory. *Studia Sci. Math. Hungar.* **1** (1966), 215–235.

[11] P. Esqué, F. Aguiló and M.A. Fiol, Double commutative-step digraphs with minimum diameters, *Discrete Math.* **114** (1993) 147–157.

[12] M.A. Fiol, Congruences in $\mathbb{Z}^n$, finite Abelian groups and the Chinese remainder theorem. *Discrete Math.* **67** (1987) 101–105.

[13] M.A. Fiol, On congruence in $\mathbb{Z}^n$ and the dimension of a multidimensional circulant, *Discrete Math.*, **141** (1995), no. 1-3, 123–134.

[14] M.A. Fiol, Eigenvalue interlacing and weight parameters of graphs, *Linear Algebra Appl.* **290** (1999), no. 1-3, 275–301.

[15] M.A. Fiol, Relaciones, *en: Fotografiando las Matemáticas*, 194–197, Carrogio S.A. de Ediciones, Barcelona, 2000.

[16] M.A. Fiol, Algebraic characterizations of distance-regular graphs. *Discrete Math.* **246** (2002), no. 1-3, 111–129.

[17] M.A. Fiol y J. Bará, Matrices circulantes en problemas de acoplamiento modal. Parte II: Toplogias asociadas. *Actas GEM, IV Reunión*, Comisión: Electricidad y Magnetismo, Murcia, 29–30 sep. 1983, pp. 19–23.

[18] M.A. Fiol y E. Garriga, From local adjacency polynomials to locally pseudo-distance-regular graphs. *J. Combin. Theory Ser. B* **71** (1997), 162–183.

[19] M.A. Fiol y E. Garriga, On the algebraic theory of pseudo-distance-regularity around a set. *Linear Algebra Appl.* **298** (1999), no. 1-3, 115–141.

[20] M.A. Fiol and E. Garriga, An algebraic characterization of completely regular codes in distance-regular graphs. *SIAM J. Discrete Math.*, **15** (2002), no. 1, 1–13.

[21] M.A. Fiol, E. Garriga and J.L.A. Yebra, On a class of polynomials and its relation with the spectra and diameters of graphs. *J. Combin. Theory Ser. B* **67** (1996) 48–61.

[22] M.A. Fiol, J.L.A. Yebra, I. Alegre and M. Valero, A discrete optimization problem in local networks and data alignment. *IEEE Trans. Comput.* **C-36** (1987) 702–713.

[23] M.A. Fiol, J.L.A. Yebra y M.L. Fiol, Grafos y teselaciones del plano. *Actas III JAEM (Jornadas sobre Aprendizaje y Enseñanza de las Matemáticas)* 69–77, Zaragoza, 1983.

[24] C.D. Godsil, *Algebraic Combinatorics*. Chapman and Hall, New York, 1993.

[25] B. Grünbaum and G.C. Shephard, *Tilings and Patterns*. W. H. Freeman and Company, New York, 1987.

[26] C.C. Johnson, *Field and Wave Electrodynamics*. McGraw-Hill, New York, 1969.

[27] J. H. van Lint, *Introduction to Coding Theory*, Third edition. Springer, Berlin, 1999.

[28] P. Morillo, C. Padró, G. Sáez and J.L. Villar, Weighted threshold secret sharing schemes, *Inf. Proc. Letters* **70** (1999), 211–216.

[29] H.P. Neff Jr., *Continuos and Discrete Linear Systems*. Harper & Row, 1984.

[30] M. Newman, *Integral Matrices*. Pure and Applied Mathematics, Vol. 45. Academic Press, New York, 1972.

[31] M. Newman, The Smith normal form. *Linear Algebra Appl.* **254** (1997), 367–381.

[32] R. Pérez-Gómez, The four regular mosaics missing in the Alhambra. *Comput. Math. Appl.* **14** (1987), no. 2, 133–137.

[33] C.E.Shannon, A mathematical theory of communication. *Bell System Tech. J.* **27** (1948), 379–423, 623–656.

[34] D.R. Stinson, An explication of secret sharing schemes, *Des. Codes Cryptogr.* **2** (1992), 357–390.