Aplicaciones de la Teoría de Matrices en Matemática Discreta

M.A. Fiol
ETSE de Telecomunicació
Departament de Matemàtica Aplicada i Telemàtica
Universitat Politècnica de Catalunya
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.

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. Algunas 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 [4]. 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 [2] 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 de su área. Un ejemplo claro de ésto lo constituye la "forma normal de Smith" para matrices enteras, que tratamos 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

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

La *equivalencia por la izquierda* se define análogamente y exige la presencia 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

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

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 entera 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 $\boldsymbol{M}$ is 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 h_{ij}, $j > i$, pertenece a un conjunto completo de residuos módulo h_{ii}; por ejemplo $h_{ij} \in \{0, 1, \ldots, h_{ii} - 1\}$. Además, se sabe que esta formal normal es única.

2.2 La forma normal de Smith

Para cada entero $k = 1, 2, \ldots, n$, 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 $\binom{n}{k}^2$ de tales submatrices y, como $\boldsymbol{M}$ es no singular, alguna de éllas 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 de $\boldsymbol{M}$. Nótese también que d_k divide a d_{k+1} para todo $k = 0, 1, 2, \ldots, n-1$, 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

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

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

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

(Por tanto, esta forma normal también es única).

2.3 Sistemas lineales diofánticos

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 *permutación-equivalencia*). Para una descripción de éstas y otras aplicaciones, pueden consultarse las referencias [13, 14].

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 ó, equivalentemente, si $a - b$ es un múltiplo de m. Con notación autoexplicativa,

$$a \equiv b \pmod{m} \quad \Longleftrightarrow \quad a - b \in m\mathbb{Z}. \qquad (1)$$

Este concepto de congruencia entre enteros 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 retículos unidimensional de los puntos enteros de la recta:

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

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 se denominada *diagrama de Cayley* de un grupo Γ con respecto a un conjunto de generadores Δ y que se denota por $Cay(\Gamma, \Delta)$. Así, en nuestro ejemplo, $C_m = Cay(\mathbb{Z}_m, \{1\})$.

La questión que nos planteamos ahora es: ¿Cómo representar la periodicidad discreta en un un espacio n-dimensional como, por ejemplo, el plano o el espacio euclideo? 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) $\boldsymbol{M}\mathbb{Z}^n$. Entonces, el concepto de congruencia en $\mathbb{Z}$ tiene la siguiente generalización natural a $\mathbb{Z}^n$: 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,

$$\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{M}} \iff \boldsymbol{a} - \boldsymbol{b} \in \boldsymbol{M}\mathbb{Z}^n. \quad (2)$$

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 éllo seguimos la convención habitual de identificar cada clase de equivlencia por uno cualquiera de sus representantes.
Notar que, cuando $\boldsymbol{M} = \mathrm{diag}(m_1, m_2, \ldots, m_n)$, 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 $\mathbb{Z}_{m_i}$, $i = 1, 2, \ldots, n$.
Sea $\boldsymbol{H} = \boldsymbol{MV}$ la forma normal de Hermite de $\boldsymbol{M}$. Entonces (2) se cumple si y sólo si $\boldsymbol{a}-\boldsymbol{b} \in \boldsymbol{HV}^{-1}\mathbb{Z}^n \in \boldsymbol{H}\mathbb{Z}^n$ ya que $\boldsymbol{V}$ y, por tanto también $\boldsymbol{V}^{-1}$, son unimodulares. Por consiguiente, concluimos que

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

o, en términos de isomorphismo 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 $\boldsymbol{M}$: $\boldsymbol{S} = \mathrm{diag}(s_1, s_2, \ldots, s_n) = \boldsymbol{UMV}$. Entonces se cumple (2) si y sólo si $\boldsymbol{Ua} \equiv \boldsymbol{Ub} \pmod{\boldsymbol{S}}$ o, de forma equivalente,

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

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,

$$\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{M}} \iff \boldsymbol{U}'\boldsymbol{a} \equiv \boldsymbol{U}'\boldsymbol{b} \pmod{\boldsymbol{S}'} \quad (5)$$

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

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

Como resulta que todo grupo abeliano se puede representar como (es isomorfo a) el grupo de vectores módulo una cierta matriz $\boldsymbol{M}$, (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:

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

• El grupo (abeliano) de vectores enteros módulo $\boldsymbol{M}$ es cíclico si y sólo si $d_{n-1} = 1$.
En [6] pueden encontrarse más detalles sobre el tema.

3.1 Redes de doble lazo

Una red de doble lazo consta de n nodos o *vértices* rotulados $0, 1, \ldots, n-1$ y una serie de enlaces unidireccionales o *arcos* de la forma $(i, i+a)$ e $(i, i+b)$, con a y b enteros positivos. Es decir, existen enlaces desde el nodo i hacia los nodos $i+a$ e $i+b$ (las operaciones deben enterderse módulo n). Dicha red se denota entonces por $G(n; a, b)$. En teoría de grafos ésto 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 $i+b$. Estas estructuras 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. 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, la *distancia* entre nodos. Por tanto interesa diseñar redes con reducido *diámetro* (máxima distancia entre vértices). Para tal fin resulta útil 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" (en forma de L) que tesela periódicamente el plano (por translaciones), ver [8]. En la referencia complementaria [7] se describen y estudian varias familias de grafos con esta propiedad geométrica.

4 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 transladarlo según un cierto movimiento rígido (ó *isometria*) se superpone a sí mismo (es decir, queda invariante). Una o más baldosas teselan periódicamente cuando constituyen un mosaico (ó *teselación*) periódico. El caso más simple se produce cuando una sola figura tesela usando sólo translaciones, como ocurre con los polígonos regulares triángulo, cuadrado y hexágono. Los mosaicos periódicos han sido objeto de atención y estudio desde muy antiguo. En nuestro país tenemos un mágnifico ejemplo de éllo en los mosaicos de la Alhambra de Granada, que han sido (y son) objeto de numerosos estudios, incluida alguna tesis doctoral. 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 [10].

4.1 Equidescomposición de figuras planas

Dos figuras planas se llaman *equidescomponibles* cuando una de éllas puede dividirse en un número finito de piezas que, resituadas adecuadamente, permiten obtener la otra (sin que se produzcan solapamientos). 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 sólamente cierto tipo de movimientos como, por ejemplo, translaciones y rotaciones. Como dichos movientos 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 afrima 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 demostrarción de estos resultados puede realizarse utilizando las propiedades de las teselaciones periódicas (ver [1]).

5 Teoria 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, denotado por $ij \in V$ 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 consiste en estudiar propiedades (estructurales) del grafo G a partir de propiedades (algebraicas) de la matriz $\boldsymbol{A}$. 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. Posíblemente, 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 [3].

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 éllo calculamos las componentes i-ésimas en la ecuación vectorial anterior y obtenemos:

$$(\boldsymbol{Av})_i = \sum_{j=1}^{n} a_{ij} v_j = \sum_{i \sim j} v_j = \lambda v_i. \qquad (8)$$

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:

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

Un estudio del diámetro de un grafo a partir de su espectro puede encontrarse en [9].

5.1 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, 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 [11].

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 $G = (V, E)$. 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 éllo 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.

6 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

$$\boldsymbol{C} = \mathrm{circ}(c_0, c_1, \ldots, c_{n-1}) = \sum_{k=0}^{n-1} c_k \boldsymbol{A}^k. \qquad (9)$$

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

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

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

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

Otra forma de ver ésto es considerar ciertos vectores que resulten ser autovectores de $\boldsymbol{A}$. A tal fin, denotemos $\omega := \lambda_1 = e^{j\frac{2\pi}{n}}$, 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:

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

con ℓ-ésima componente $\phi_{k\ell} := \omega^{k\ell}$, $0 \le \ell \le n-1$. Así resulta, recordando la interpretación en (8), que

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

es decir,

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

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 (9), 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

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

(Nótese que estos autovalores no son necesariamente distintos).

6.1 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 $\sum_{i=0}^{n-1} c_i = 0$ (esto significa que el centro de gravedad del polígono coincide con el origen de coordenadas) y lados $c_{0i}c_{0,i+1}$, $0 \le i \le n-1$ (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,

$$c_{1i} := sc_{0,i} + tc_{0,i+1} \qquad (0 \le i \le n-1). \tag{10}$$

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 (10) 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 [5]).

6.2 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:

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

y, por tanto, $\{\frac{1}{\sqrt{n}}\boldsymbol{\phi}_k\}_{0\le k\le n-1}$ 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

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

es el coeficiente de Fourier del desarrollo.
La matriz de cambio de base $\boldsymbol{F} = (f_{k\ell})$, con componentes $f_{k\ell} = \frac{1}{\sqrt{n}}\omega^{-k\ell}$, $0 \le k, \ell \le n-1$, 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:

$$\overline{\boldsymbol{F}}\boldsymbol{F} = \boldsymbol{I} \tag{11}$$

(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 (11),

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

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 [12]).

Agradecimientos

Estas notas corresponden a parte de un curso de verano, organizado por la "Càtedra RAMON LLULL" (UB, UIB, EGL), celebrado en Palma de Mallorca (5-9 de julio de 1999), y coordinado por el Prof. Pere Cerdà. Agradezco sinceramente a las institucions involucradas, y especialmente al coordinador del curso, la invitación recibida.

References

[1] F. Aguiló, M.A. Fiol, and M.L. Fiol, Periodic tilings as a dissection method. *Amer. Math. Monthly*, submitted (1999).

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

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

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

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

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

[7] M.A. Fiol, J.L.A. Yebra y M.L. Fiol, Grafos y teselaciones del plano, en: *Actas III JAEM (Jornadas sobre aprendizaje y enseñanza de las Matemáticas)* 69-77, Zaragoza, 1983.

[8] 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.

[9] 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.

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

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

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

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

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