TRES OBSERVACIONES SOBRE EL ALGEBRA LINEAL

por GARRETT BIRKHOFF
(Harvard University, Cambridge, Mass.)

Este artículo está dividido en cuatro partes. Las dos primeras partes contienen notas sobre las matrices; las dos últimas partes, notas sobre las álgebras lineales.

1. *Medias aritméticas de permutaciones.* Por definición, una media aritmética de permutaciones es una matriz

$$A=\sum_{i=1}^{s}\lambda_i P_i \qquad [\lambda_i\geqq 0,\quad \lambda_1+\ldots+\lambda_s=1] \tag{1}$$

en donde las P_i son matrices que representan permutaciones. Es evidente que cada matriz A que satisface (1) satisface también

$$\sum_{i=1}^{s}a_{ij}=\sum_{j=1}^{n}a_{ij}=1, \text{ para todo } i,j=1,\ldots,n. \tag{1'}$$

Estas matrices son interesantes para la probabilidad,[1] y los cuadrados mágicos son múltiplos escalares de estas matrices.

Teorema. Si una matriz $n\times n$ A satisface (1'), entonces es una media aritmética de permutaciones.

Demostración. Ha sido demostrado por P. Hall,[2] que una matriz $n\times n$ B cuyos coeficientes son todos nulos o uno, contiene

---

[1] Cfr. HADAMARD y M. FRÉCHET, *Sur les probabilités discontinues des évènements en chaîne*, Zeits. R. Ang. Math. 13 (1933), 92-7.

[2] *On representatives of subsets*, Jour. Lond. Math. Soc. 10 (1935), 26-30. Este resultado está vinculado con un teorema de D. KONIG, *Ueber Graphen und ihre Anwendungen*, Math. Annalen 77 (1916), p. 453.

una permutación P de unos, o contiene una sub-matriz $(i+1)\times(n-i)$ de ceros. De donde se sigue que cualquier matriz no-negativa C (cada $c_{ij}\geqq 0$) que no contenga una sub-matriz $(i+1)\times(n-i)$ de ceros, contiene un múltiplo escalar positivo cP de una permutación P (es decir, que $c_{ij}\geqq cp_{ij}$, donde $p_{ij}=0$ excepto para un $p_{ij(i)}=1$ en cada fila y cada columna). Si c es igual al máximo c_{ij} con $p_{ij}=1$, obtendremos $C-cP\geqq 0$, donde $R=C-cP$ contiene un cero más que R. Podemos repetir este proceso hasta que obtengamos un residuo que contiene una sub-matriz $(i+1)\times(n-i)$ 0, así que

$$C=\lambda_1 P_1+\ldots+\lambda_s P_s+R \quad [\lambda_i\geqq 0], \tag{2}$$

donde R contiene una sub-matriz $(i+1)\times(n-i)$ 0.

Además, si C satisface (1), R satisfará

$$\sum_{i=1}^{n} r_{ij}=\sum_{j=1}^{n} r_{ij}=\alpha=1-\lambda_1-\ldots-\lambda_s. \tag{3}$$

Aparece de la Figura 1 que la suma de los coeficientes de R_1 es $(i+1)\alpha$; la suma de los coeficientes de R_3 es $(n-i)\alpha$. La suma de todos los coeficientes de R es por consiguiente por lo menos $(n+1)\alpha=(i+1)\alpha+(n-i)\alpha$

$$\begin{array}{c} \\ i \\ n-i \end{array}\begin{array}{c} \begin{array}{cc} i+1 & n-i-1 \end{array} \\ \left(\begin{array}{c|c} R_1 & R_2 \\ \hline 0 & R_3 \end{array}\right) \end{array}$$

Figura 1

Pero la suma es $n\alpha$, de donde $\alpha=0$ y $\lambda_1+\ldots+\lambda_s=1$ en (3). De donde se sigue que $R=0$ en (2), que es equivalente a (1).

No parece existir ninguna representación (1) con propiedades únicas.

2. *Algebras lineales asociativas completas.* Nuestra primera nota sobre las álgebras es casi trivial. Por analogía con la terminología usada para los grupos, llamaremos *completa,* a un álgebra lineal asociativa A con la propiedad siguiente: si A está contenida como sub-álgebra invariable en otra álgebra G, entonces B es la suma directa $B = A + C$ de A con otra sub-álgebra invariable C de B.

Teorema. Para que A sea completa, es necesario y suficiente que A contenga un elemento unitario e.

Demostración. Si A contiene un elemento e, y es invariable en B, entonces $A = eBe$ y el sub-conjunto C de elementos $c = b - ebe = b - eb = b - be$ $(b \in B)$ son sub-álgebras invariables complementarias. (Para ver que $ebe = eb$, nótese que $eb \in A$, ya que A es invariable, y por consiguiente $eb = (eb)e = ebe$).

Recíprocamente, podemos formar de cualquier A el álgebra B de toda $a + \lambda e$, con $ea = ae = a$. Es evidente que A es una sub-álgebra invariable de B. Si existe una sub-álgebra C invariable complementaria, contendrá un elemento $c = e - a_0$ tal que $ca = ac = 0$ para todo a. Eso implica que

$$0 = (e - a_0)a = ea - a_0 a = a - a_0 a, \tag{4}$$

así que $a = a_0 a$ y (dualmente) $a = a a_0$. De aquí se sigue que A contiene un elemento unidad a_0.

3. *Extensiones escalares de álgebras lineales.* Sea Γ una definición que determine un *sub-espacio* $C(A) = C$ de cada álgebra lineal A con base finita de una clase fija A; las A pueden no ser asociativas. Supongamos también que $\alpha(C) = C$ para cada automorfismo α de A como *anillo,* es decir para cada correspondencia biunívoca de A tal que

$$\alpha(a+b) = \alpha(a) + \alpha(b) \quad \text{y} \quad \alpha(ab) = \alpha(a)\,\alpha(b) \tag{5}$$

para cada $a, b \in A$, pero no necesariamente $\alpha(\lambda a) = \lambda\alpha(a)$ para cada escalar λ. Además supongamos que si A^* es una *extension* escalar[3] cualquiera de A, entonces

[3] Usaremos la terminología de A. A. ALBERT, *Structure of Algebras,* N. Y., 1939, excepto que conservaremos la distinción entre sub-anillo y sub-álgebra.

(6) $$C(A) = C(A^*) \frown A,$$

lo que dice que los elementos de $C(A)$ son los elementos de A que pertenecen a $C(A^*)$.

Estas condiciones se satisfacen en los casos siguientes: (i) el *radical* de un álgebra lineal asociativa, (ii) el *centro* de un álgebra lineal asociativa, (iii) la más grande sub-álgebra invariante *integrable* de un álgebra de Lie, (iv) la sub-álgebra generada por los *conmutatores* en un álgebra de Lie. En general, si se satisfacen estas condiciones, diremos que la operación $A \longrightarrow C(A)$ define *subespacios realmente característicos* de las $A \varepsilon \mathbf{A}$.

Sin embargo, no podemos concluir de (6) que $C(A^*)$ es la extensión escalar $[C(A)]^*$ de $C(A)$; aunque es trivial que $C(A^*)$ contiene $[C(A)]^*$. Por ejemplo, sea A el álgebra lineal asociativa con base $(1, y)$ y con $y^2 = -\gamma$, sobre el cuerpo $F = J_2(\gamma)$ obtenido del cuerpo J_2 de los enteros módulo dos, por la adjunción de una indeterminada γ. El radical $R(A)$ de A se reduce al elemento 0; en efecto A es un cuerpo. Mientras que si F^* es la extensión algebraica de F por $\sqrt{\gamma}$, entonces $(\sqrt{\gamma} \cdot 1 + y) \varepsilon R(A^*)$, porque $(\sqrt{\gamma} \cdot 1 + y)^2 = \gamma + y^2 = \gamma - y^2 = 0$ y A es conmutativa.

Notamos que F^* es una extensión *inseparable* de F. Nuestro resultado principal es que en efecto

(7) $$C(A^*) = [C(A)]^* \qquad \text{(que implica (6))},$$

a menos que A^* contenga una extensión inseparable de A.

Lema: Sea F^* alguna extensión de F tal que cada $\lambda \varepsilon (F^* - F)$ tenga por lo menos otro elemento conjugado $\alpha(\lambda) \neq \lambda$. Entonces se satisface (7).

Demostración. Sea $x_1, \ldots, x_m$ una base de $C(A)$; luego existe una base $x_1, \ldots, x_m, y_1, \ldots, y_n$ de A. Si existiera un elemento z de $C(A^*) - [C(A)]^*$, podríamos escribir

$$z = \lambda_1 x_1 + \ldots + \lambda_m x_m + \mu_1 y_1 + \ldots + \mu_n y_n,$$

donde algún $\mu_k \neq 0$. Además, $\mu_1 y_1 + \ldots + \mu_n y_n \varepsilon C(A^*)$, puesto que $z \varepsilon C(A^*)$ y por (6) $\lambda_1 x_1 + \ldots + \lambda_m x_m \varepsilon C(A^*)$. Sea ahora

(8) $$z' = \mu_1 y_1 + \ldots + \mu_n y_n \varepsilon C(A^*) - [C(A)]^*,$$

en donde el número de $\mu_i \neq 0$ es *mínimo*. Después de una multiplicación de (8) por un escalar μ_k^{-1} conveniente y de una permutación de índices, (8) se cambiará en

$$(8') \qquad z'' = y_1 + \mu_2 y_2 + \ldots + \mu_r y_r \, \varepsilon \, C(A^*) \quad (r \text{ mínimo, } 0 < r \leqq n)$$

Supongamos ahora que algún $\mu_j \, \varepsilon \, (F^* - F)$; por hipótesis, $\alpha(\mu_j) \neq \mu_j$ para algún automorfismo de F^*/F. Entonces

$$(8'') \qquad \alpha(z'') = y_1 + \mu'_2 y_2 + \ldots + \mu'_r y_r \, \varepsilon \, C(A^*) \quad [\mu_i = \alpha(\mu_i)]$$

es el trasformado de z'' por un automorfismo de anillo (5) de A. Ya que $C(A)$ es un sub-espacio, y que $\mu_j - \mu'_j \neq 0$,

$$(9) \quad z' - z'' = (\mu_2 - \mu'_2) y_1 + \ldots + (\mu_r - \mu'_r) y_r \, \varepsilon \, C(A^*) - [C(A)]^*.$$

Sin embargo, el número de $(\mu_i - \mu'_i) \neq 0$ es *menos* de r, lo que es una contradicción a (8). Se sigue que la hipótesis que algún $\mu_j \, \varepsilon \, (F^* - F)$ es imposible, de donde cada $\mu_j \, \varepsilon \, F$, de donde $z'' \, \varepsilon \, A \cdot C(A^*) = C(A)$ en (8'), de donde $z' = \mu_k z'' \, \varepsilon \, [C(A)]^*$ en (8); ésta es otra contradicción. No es sostenible la hipótesis de que pueda existir $z \, \varepsilon \, C(A^*) - [C(A)]^*$, lo que implica (7), q. e. d.

Ahora anotaremos tres hechos. Primero, la hipótesis del Lema se satisface para cada extensión algebraica normal y separable. Además, desde ξ y $\xi + 1$ son elementos conjugados, la hipótesis se satisface también para cada extensión trascendente simple, $F^* = F(\xi)$. Finalmente, la hipótesis del Lema se satisface para la unión VF^*_α de una sucesión infinita o transfinita

$$F < F^*_1 < F^*_2 < F^*_3 < \ldots < VF^*_n = F^*_\omega < F^*_{\omega+1} < \ldots,$$

si se satisface para cada $F^*_{\alpha+1} / F^*_\alpha$. Se sigue por inducción transfinita el siguiente teorema.

Teorema. Si F^* puede obtenerse de F por una sucesión finita o transfinita de extensiones separables o trascendentes, entonces

$$(7) \qquad C(A^*) = [C(A)]^*$$

para cada definición de sub-espacio realmente característica.

Corolario. Se satisface (11) si F es un cuerpo de característica infinita.