

K. RIBNIKOV

---

# ANALISIS COMBINATORIO



## Análisis combinatorio

К.А.Рыбников

**ВВЕДЕНИЕ  
В КОМБИНАТОРНЫЙ АНАЛИЗ**

Издательство Московского университета

K. RÍBNIKOV

# Análisis combinatorio



Editorial Mir Moscú

Traducido del ruso por K.Medkov

Impreso en la URSS

На испанском языке

ISBN 5-03-000610-9

© Издательство Московского университета, 1985  
© traducido al español, editorial Mir, 1988

# ÍNDICE

<b>Prólogo</b>	<b>6</b>
<b>Capítulo 1. Fundamentos teóricos del análisis combinatorio</b>	<b>7</b>
1.1. Qué se estudia en el análisis combinatorio y qué clase de problemas se resuelven	7
1.2. Conocimientos indispensables de la teoría de los conjuntos y del álgebra	9
1.3. Muestras y ordenaciones	17
1.4. Distribuciones y llenados	23
1.5. Sistemas de conjuntos	32
<b>Capítulo 2. Funciones generatrices</b>	<b>37</b>
2.1. Fundamentos del método de funciones generatrices	37
2.2. Tipos de funciones generatrices y de numeradores	40
2.3. Aparato operacional del método de funciones generatrices	52
2.4. Sobre las aplicaciones del método de funciones generatrices	62
2.5. Teoría de Redfield-Polya	66
<b>Capítulo 3. Métodos lógicos</b>	<b>74</b>
3.1. Método de inclusiones y exclusiones	74
3.2. Sistemas de representantes de los conjuntos	78
3.3. Principios de la teoría de Ramsey	83
<b>Capítulo 4. Aparato tabular de matriz del análisis combinatorio</b>	<b>87</b>
4.1. Sistemas de incidencia y matrices especiales	87
4.2. Rectángulos y cuadrados latinos	93
4.3. Bloque-esquemas	101
4.4. Permanentes	113
<b>Capítulo 5. Medios geométricos y gráficos</b>	<b>130</b>
5.1. Evidencia en las interpretaciones de los sistemas discretos	130
5.2. Ideas geométricas finitas	132
5.3. Sobre los grafos	144
<b>Capítulo 6. Métodos de resolución de los problemas extremales</b>	<b>159</b>
6.1. Planteamiento de los problemas combinatorios extremales y accesos a su resolución	159
6.2. Método de ramificaciones y restricciones <sup>1)</sup>	165
6.3. Métodos heurísticos	179
6.4. Optimización en los grafos	189
6.5. Flujos en las redes	192
<b>Capítulo 7. Métodos probabilísticos en el análisis combinatorio</b>	<b>206</b>
7.1. Ejemplos de aplicación de los métodos probabilísticos	206
7.2. Problemas de planificación del experimento	210
7.3. Método de entropía	214
7.4. Método de balance aleatorio	220
7.5. Sistemas separadores de subconjuntos	224
<b>Capítulo 8. Análisis combinatorio en los conjuntos parcialmente ordenados</b>	<b>232</b>
8.1. Conjuntos parcialmente ordenados	232
8.2. Retículos	263
8.3. Funciones de incidencia e inversión de Moebius	248
8.4. Matroides	324
<b>Bibliografía</b>	<b>361</b>
<b>Índice alfabético de materias</b>	<b>367</b>

## PRÓLOGO

En el presente libro se examinan los métodos matemáticos de investigación de los sistemas discretos. Esta clase de sistemas ocupan un notable lugar en la actividad de la gente y existe una diversidad de tipos difícil de examinar (circuitos eléctricos, flujos de transporte e información, sistemas de organización de la producción, tablas, grafos, razonamientos lógicos, etc.).

Pese a que el carácter específico y heterogéneo de los sistemas discretos aparenta ser insuperable, éstos tienen en sus fundamentos mucho de común. Esto se manifiesta con toda evidencia en la semejanza e, incluso, en la coincidencia de los modelos matemáticos que se introducen al resolver problemas de carácter discreto.

Las amplias clases de los sistemas discretos se analizan en nuestro libro como partes de una teoría única. Dentro de los márgenes de dicha teoría (que históricamente conserva su nombre de análisis combinatorio) las clases citadas ocupan su lugar en dependencia de cómo se interpretan sus entes, qué problemas se estudian y cuáles son los métodos que se eligen para resolverlos. Tal exposición, como muestra la experiencia, facilita el estudio del análisis combinatorio y atribuye a esta parte de las matemáticas los rasgos necesarios de universalidad, tanto teórica como práctica.

Para que el lector obtenga una mejor orientación en la moderna teoría combinatoria general, el capítulo ocho del libro, escrito en colaboración con A.M.Reviakin, contiene material referente a la aplicación de problemas y métodos del análisis combinatorio a los conjuntos de naturaleza lo más amplia posible.

Resta por añadir que el autor expresa su más profundo agradecimiento a sus discípulos y colegas que prestaron una valiosa cooperación, y muy especialmente a A.M.Reviakin, quien ayudó activamente al autor en el proceso de preparación de la versión española del libro.

El autor quedará agradecido por las observaciones de los lectores.

# CAPÍTULO I      FUNDAMENTOS TEÓRICOS DEL ANÁLISIS COMBINATORIO

En este capítulo se dan explicaciones que tienen por fin permitir al lector la formación de nociones elementales sobre el análisis combinatorio (combinatoria). Se trata de los objetos que se estudian en el análisis combinatorio (considerado como una asignatura) y de los problemas que en este caso se plantean y se resuelven. Además, se introducen los conceptos principales, operaciones y simbolismo. Por fin, se explican los procedimientos aplicados en la resolución de los problemas combinatorios no complejos que se plantean tanto en la teoría como en la práctica.

## 1.1. QUÉ SE ESTUDIA EN EL ANÁLISIS COMBINATORIO Y QUÉ CLASE DE PROBLEMAS SE RESUELVEN

Enunciemos, para iniciar, unos cuantos problemas. Harémoslo para que el lector perciba intuitivamente el carácter combinatorio de dichos problemas y esté mejor preparado para poder asimilar las formulaciones generales.

a) Uno que ha terminado la enseñanza media y aspira a ingresar en la Universidad tiene que aprobar cuatro exámenes, siendo el sistema de calificación de cinco puntos. Para ingresar es suficiente obtener 17 puntos. ¿Cuántas son las combinaciones que le permiten aprobar los exámenes (por supuesto, sin sacar ni un solo mal)?

b) ¿Cómo se debe buscar el itinerario más corto para un cartero o un operador cinematográfico que atienden un número dado de poblados? La distancia entre cada par de poblados se conoce.

c) ¿Qué número de reinas o de otras piezas de ajedrez es suficiente para que ellas mantengan bajo amenaza todas las casillas del tablero de ajedrez y no se puedan comer una a la otra? ¿Cuántas son las combinaciones de su colocación?

d) ¿ En cuántas partes dividen un espacio  $n$  planos, si de cuatro cualquiera de ellos ninguno pasa por un mismo punto, de tres, ninguno pasa por una misma recta y de dos, ninguno es paralelo, mientras que cualesquiera tres planos tienen un punto común?

Los problemas de esta índole son semejantes por el hecho de que, en primer lugar, en ellos se estudian los conjuntos discretos (compuestos de elementos separados, aislados). En la mayoría de los casos los conjuntos mencionados son finitos. Tampoco se excluyen del análisis combinatorio los conjuntos infinitos, compuestos por un número infinitamente grande

de elementos, siempre que haya una información suficiente sobre las peculiaridades estructurales de estos últimos conjuntos. La estructura de los conjuntos discretos puede ser muy compleja en función de las relaciones y razones existentes entre ellos. La primera principal tarea del análisis combinatorio consiste en estudiar tales estructuras discretas y expresar sus propiedades empleando los métodos adoptados en las matemáticas (analíticos, gráficos, tabulares y geométricos).

Sobre los conjuntos discretos se realizan operaciones. Algunas de ellas originan el cambio de la estructura de los conjuntos, otras modifican la composición de éstos. Como operaciones más simples del primer tipo intervienen las permutaciones habituales de elementos, y del segundo tipo, la separación de los subconjuntos de elementos, o, como suele decirse, sus muestras. Como regla, al resolver los problemas, las operaciones se aplican más de una vez (reiteradamente) y, además, en las combinaciones más diversas, cuando vienen impuestas diferentes condiciones. Esto es una razón por la que se prestan posibilidades prácticamente inagotables de crear construcciones discretas, las cuales se denominan frecuentemente configuraciones (a veces, configuraciones combinatorias).

Según sean el carácter del objeto de investigación y las operaciones a introducir, se determina la totalidad específica de los problemas que se resuelven mediante el análisis combinatorio. Los más antiguos son problemas sobre el número de construcciones discretas que satisfacen las condiciones planteadas. Los métodos de su resolución han recibido el nombre de problemas enumerativos. Además de los problemas de tipo enumerativo, en el análisis combinatorio se estudian cuestiones de existencia o no existencia de una configuración que satisfaga las condiciones prefijadas, se buscan algoritmos de construcción de las configuraciones, como también las cuestiones de selección en una totalidad dada de tales configuraciones o algoritmos que posean, en un mayor o menor grado, las propiedades elegidas (problemas y métodos de optimización).

El análisis combinatorio está asociado con muchos apartados de las matemáticas e incluso tiene partes comunes correlacionadas. Efectivamente, los elementos de los razonamientos combinatorios surgieron en tiempos remotos, antiguamente, en la aurora de la formación de las ciencias matemáticas. No obstante, en el transcurso de la historia estos elementos se desarrollaban junto con otras partes de las matemáticas, integrando en diversos casos la composición de éstas. No es difícil ver que en una serie de ramas de las matemáticas modernas (teoría de los números, álgebra, geometría, lógica matemática y otras) muchos conceptos y métodos fundamentales tienen naturaleza discreta y poseen conexiones estables. Esto permite estudiar los problemas del análisis combinatorio en diferentes interpretaciones, investigar problemas, que a primera vista parecen tener diferente naturaleza, desde un punto de vista único que corresponda del modo más conveniente a la esencia del problema.

Hoy día las posibilidades de los métodos discretos de investigación aumentaron muy bruscamente. Ha crecido también la importancia de estos métodos. A la par con la teoría combinatoria general formada históricamente (análisis combinatorio) existen en las matemáticas modernas: la teoría de los grafos y de los hipergrafos, geometría de los números, análisis discreto y análisis finito, investigación de operaciones, etc. En los libros y artículos se consideran ciertas clases de problemas, lo que es testimonio de amplia ramificación y riqueza de las investigaciones combinatorias.

La tarea de este libro consiste en exponer el análisis combinatorio como una teoría matemática de investigaciones de los conjuntos discretos en sus diferentes interpretaciones, teniendo presente que dicha teoría está basada en principios únicos, es suficientemente rica en lo que se refiere a los métodos que se emplean y puede servir de base teórica general para los métodos discretos de investigación en las matemáticas.

## 1.2. CONOCIMIENTOS INDISPENSABLES DE LA TEORÍA DE LOS CONJUNTOS Y DEL ÁLGEBRA

La información que se incluye en este párrafo del libro se destina para describir las propiedades de los objetos que se estudian en el análisis combinatorio, las operaciones que se realizan sobre ellos y para introducir un simbolismo uniforme. Las definiciones, los términos y los símbolos se eligen, por regla, de los que son de uso general en las matemáticas. La introducción de ellos será paulatina.

El concepto principal es el de *conjunto*. No damos definición de este concepto debido a una tautología inevitable. Todos los conjuntos que se analizan en el libro (si no hay referencias a una precisión especial) son discretos y finitos. Los conjuntos se designarán mediante letras mayúsculas latinas  $A, B, \dots$ , y los *elementos de los conjuntos*, mediante letras minúsculas  $a, b, \dots$ . Escribiremos  $a \in A$ , si el elemento  $a$  pertenece al conjunto  $A$ , y  $a \notin A$ , si  $a$  no pertenece al conjunto  $A$ . Se denomina *subconjunto*  $A$  del conjunto  $S (A \subseteq S)$  cualquier conjunto cuyos elementos pertenecen todos a  $S$ . En otras palabras,  $A \subseteq S$ , si de  $a \in A$  se deduce que  $a \in S$ . Los conjuntos  $A$  y  $B$  *coinciden* o son *iguales* ( $A = B$ ), si están compuestos por unos mismos elementos. Dicho de otro modo,  $A = B$ , cuando y sólo cuando  $A \subseteq B$  y  $B \subseteq A$ . Si  $A \subseteq B$ , pero  $A \neq B$ , suele decirse que  $A$  es un subconjunto *propio* del conjunto  $B$ , y se escribe:  $A \subset B$ .

Los conjuntos, al igual que los subconjuntos, pueden introducirse y designarse mediante diferentes métodos. Por ejemplo, un subconjunto  $A$  del conjunto  $S$  se define frecuentemente como conjunto de todos los elementos  $a \in S$  que poseen cierta propiedad bien determinada. Si designamos esta propiedad mediante  $P(a)$ , la definición de  $A$  puede escribirse simbólicamente así:  $A = \{a \in S \mid P(a)\}$ , o bien (simplemente)  $A = \{a \mid P(a)\}$ . Estas inscripciones se leen del modo siguiente: " $A$  es un conjunto de todos los elementos

$a$  del conjunto  $S$ , para los cuales resulta válida la condición  $P(a)$ ". Por ejemplo, la inscripción  $A = \{a \mid a \in \mathbb{N} \text{ y } a = 2b \text{ para cierto } b \in \mathbb{N}\}$ , donde  $\mathbb{N}$  es un conjunto de números naturales, describe el conjunto de todos los números positivos pares.

Introduzcamos el símbolo  $\emptyset$  para designar con él un conjunto *vacío*, es decir, conjunto sin elementos. Es evidente que cualquier conjunto contiene en calidad de subconjunto un conjunto vacío. Por  $P(S)$  designaremos un conjunto de todos los subconjuntos del conjunto  $S$ , el cual contiene, en calidad de elementos, todos los subconjuntos propios  $A$  que satisfacen la condición  $\emptyset \subset A \subset S$ , como también el conjunto vacío  $\emptyset$  y el mismo conjunto  $S$ . Por ejemplo, si  $S = \{a, b, c\}$ , entonces  $P(S)$  contiene, además de  $\emptyset$  y  $S$ , seis subconjuntos propios  $\{a\}$ ,  $\{b\}$ ,  $\{c\}$ ,  $\{a, b\}$ ,  $\{a, c\}$ ,  $\{b, c\}$ . En general, si  $S$  se compone de  $n$  diferentes elementos, entonces  $P(S)$  contiene  $2^n$  diferentes subconjuntos. Por eso, en la literatura matemática  $P(S)$  se denota también con  $2^S$ .

Diremos que está dada la *aplicación*  $\varphi$  del conjunto  $A$  en el conjunto  $B$ , si a todo elemento del conjunto  $A$  se le ha puesto en correspondencia cierto elemento del conjunto  $B$ . Para designar la aplicación  $\varphi$  de  $A$  en  $B$ , haremos uso del símbolo  $\varphi: A \rightarrow B$ . Si  $a \in A$ , entonces el elemento de  $B$ , que se le ha puesto en correspondencia al elemento  $a$ , se designa mediante  $\varphi(a)$  y se denomina *imagen* del elemento  $a$  en la aplicación  $\varphi$ . Si  $b \in B$ , entonces cualquier elemento  $a$  de  $A$ , para el cual se verifica la igualdad  $b = \varphi(a)$ , se llama *preimagen* (imagen recíproca) del elemento  $b$ . El conjunto  $A$  lleva el nombre de *origen* de la aplicación  $\varphi$ , y el conjunto  $B$  es el *fin* de la aplicación citada. Por supuesto, cada elemento del origen de la aplicación  $\varphi$  tiene exactamente una sola imagen. No obstante, no todo elemento del fin de dicha aplicación tiene necesariamente una preimagen. Por otra parte, el fin de una aplicación puede contener elementos que cuentan con varias preimágenes. Un subconjunto del fin de la aplicación  $\varphi$  compuesto por todos los elementos suyos que tienen preimagen, o bien, lo que es lo mismo, que se representan en la forma  $\varphi(a)$  para cierto  $a \in A$ , se denomina *imagen de la aplicación*  $\varphi$  y se designa  $\text{Im } \varphi$ . Para un conjunto finito  $A = \{a_1, a_2, \dots, a_n\}$  se emplea con frecuencia la inscripción de la aplicación  $\varphi: A \rightarrow B$  en forma de dos filas, a saber

$$\varphi = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \varphi(a_1) & \varphi(a_2) & \dots & \varphi(a_n) \end{pmatrix}.$$

Dos aplicaciones  $\varphi_1: A_1 \rightarrow B_1$ ;  $\varphi_2: A_2 \rightarrow B_2$  se consideran *iguales*, si  $A_1 = A_2$ ,  $B_1 = B_2$ , y  $\varphi_1(a) = \varphi_2(a)$  para cualesquiera  $a \in A_1$ . La aplicación  $\varphi': A' \rightarrow B$  es una *contracción sobre*  $A'$  de la aplicación  $\varphi: A \rightarrow B$ , siempre que  $A' \subseteq A$  y  $\varphi'(a) = \varphi(a)$  para todo  $a \in A'$ .

La aplicación  $\varphi: A \rightarrow B$  lleva el nombre de *encaje* (inmersión), si cada elemento de  $B$  tiene no más de una preimagen, es decir,  $\varphi(a) = \varphi(b)$  lleva

conigo  $a = b$ . Si cada elemento de  $B$  tiene al menos una preimagen, o bien, con otras palabras,  $\text{Im}\varphi = B$ , la aplicación  $\varphi$  se denomina *superposición*. Una superposición  $\varphi : A \rightarrow B$  se llama también aplicación de  $A$  sobre  $B$ . Una aplicación que representa a la vez un encaje y una superposición se denomina *biunívoca* (biyectiva).

Si  $A = B$ , la aplicación biunívoca  $\varphi : A \rightarrow A$  se llama *sustitución*.

Los conjuntos pueden ser *finitos* (es decir, compuestos por un número finito de elementos) e *infinitos*. El número de elementos en un conjunto  $A$  recibe el nombre de *potencia* del conjunto  $A$  y se designa con  $|A|$ . Se dice que los conjuntos  $A$  y  $B$  son *equipotentes*, si existe una aplicación biunívoca  $\varphi : A \rightarrow B$ . Evidentemente, dos conjuntos finitos son equipotentes, cuando y sólo cuando contienen ambos un número igual de elementos. Denominaremos *n-conjunto* a todo conjunto finito  $A$  tal que  $|A| = n$ . Los conjuntos infinitos pueden ser equipotentes a alguno de sus subconjuntos; por ejemplo, el conjunto de los números naturales es equipotente al conjunto de los números positivos pares y al conjunto de sus cuadrados. Entre los conjuntos infinitos se distinguen los conjuntos numerables e innumerables. Se llama *numerable* todo conjunto infinito que sea equipotente con el conjunto de números naturales. En adelante, cuando se trate de conjuntos infinitos, éstos se considerarán numerables.

Definamos ciertas operaciones que se realizan en el conjunto  $P(S)$ .

Se llama *unión* (reunión o suma)  $A \cup B$  de los conjuntos  $A$  y  $B$  el conjunto de todos los elementos pertenecientes o bien a  $A$ , o bien a  $B$  (o bien a  $A$  y  $B$  simultáneamente):

$$A \cup B = \{a \in S \mid a \in A, \text{ o bien } a \in B\}.$$

Se llama *intersección* (o *producto*)  $A \cap B$  de los conjuntos  $A$  y  $B$  el conjunto de todos los elementos pertenecientes tanto a  $A$ , como a  $B$ :

$$A \cap B = \{a \in S \mid a \in A \text{ y } a \in B\}.$$

De un modo análogo se definen las uniones e intersecciones de un sistema arbitrario (incluido el infinito) de conjuntos.

Se llama *complemento* del conjunto  $A$  el conjunto

$$\bar{A} = \{a \in S \mid a \notin A\}.$$

Se llama *diferencia* de los conjuntos  $A$  y  $B$  el conjunto  $A \setminus B = \{a \in S \mid a \in A \text{ y } a \notin B\}$ . Es evidente que  $A \setminus B = A \cap \bar{B}$ .

Se llama *diferencia simétrica* de los conjuntos  $A$  y  $B$  el conjunto

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

El conjunto  $P(S)$  con las operaciones de unión, intersección y de complemento definidas sobre él recibe el nombre de *booleano*. Quedan válidas en este caso las siguientes leyes algebraicas:

1.  $A \cap A = A$ ;  $A \cup A = A$  (idempotencia);
2.  $A \cap B = B \cap A$ ;  $A \cup B = B \cup A$  (conmutatividad);
3.  $A \cap (B \cap C) = (A \cap B) \cap C$ ;  $A \cup (B \cup C) = (A \cup B) \cup C$  (asociatividad);
4.  $A \cap (A \cup B) = A$ ;  $A \cup (A \cap B) = A$  (absorción);
5. Si  $A \subseteq C$ , se tiene  $A \cup (B \cap C) = (A \cup B) \cap C$  (modularidad);
6.  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;  
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$  (distributividad);
7.  $A \cap \emptyset = \emptyset$ ;  $A \cup \emptyset = A$ ;  
 $A \cap \bar{S} = \bar{A}$ ;  $A \cup \bar{S} = \bar{S}$  (fronteras universales);
8.  $A \cap \bar{A} = \emptyset$ ;  $A \cup \bar{A} = S$  (complementariedad);
9.  $\overline{\bar{A}} = A$
10.  $\overline{A \cap B} = \bar{A} \cup \bar{B}$ ;  $\overline{A \cup B} = \bar{A} \cap \bar{B}$  (leyes de De Morgan).

Si  $A \cap B = \emptyset$ , entonces  $A$  y  $B$  se llaman conjuntos *disjuntos*. La representación del conjunto  $S$  en forma de una unión de los subconjuntos disjuntos dos a dos recibe el nombre de *partición* del conjunto  $S$ . En otras palabras,  $A_1, A_2, \dots, A_k$  es una partición del conjunto  $S$ , si  $S = \bigcup_{i=1}^k A_i$ , y  $A_i \cap A_j = \emptyset$  para cualesquiera  $i \neq j$ . Una totalidad de todos los pares ordenados  $(a, b)$  tales que  $a \in A$ ,  $b \in B$ , se denomina producto *directo* (*cartesiano*) de los conjuntos  $A$  y  $B$  y se designa por  $A \times B$ , es decir,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Si  $A = B$ , el producto directo  $A \times A$  se denota con  $A^2$ . Análogamente se determina el producto directo de  $k$  conjuntos:

$$A_1 \times A_2 \times \dots \times A_k = \{(a_1, a_2, \dots, a_k) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_k \in A_k\},$$

y, al coincidir los conjuntos, tenemos:  $A^k = A \times A \times \dots \times A$ .

Enunciemos las reglas evidentes que yacen en la base de muchos cálculos y estimaciones combinatorios.

**Regla de la suma.** Si  $S$  es un conjunto finito y  $S = \bigcup_{i=1}^k A_i$ , donde  $A_i \in P(S)$ ,  $i = 1, 2, \dots, k$ , entonces

$$|S| = \left| \bigcup_{i=1}^k A_i \right| \leq \sum_{i=1}^k |A_i|,$$

con la particularidad de que la igualdad tiene lugar cuando  $A_1, A_2, \dots, A_k$  forman una partición del conjunto  $S$ .

**Regla del producto.** Para los conjuntos finitos  $A_1, A_2, \dots, A_k$  tenemos

$$|A_1 \times A_2 \times \dots \times A_k| = \prod_{i=1}^k |A_i|.$$

Llamemos *correspondencia binaria* entre los conjuntos  $A$  y  $B$  cualquier subconjunto  $A \subseteq A \times B$ . Si  $(a, b) \in \alpha$ , suele decirse que  $a$  se encuentra en

Fig.1.1



relación  $\alpha$  respecto a  $b$ , y esto se expresa en la forma  $a\alpha b$ . La noción de correspondencia binaria entre  $A$  y  $B$  sirve de generalización del concepto de la aplicación  $\varphi : A \rightarrow B$ . En efecto, cada aplicación  $\varphi : A \rightarrow B$  define la correspondencia binaria  $\alpha_\varphi$  entre  $A$  y  $B$ : la expresión  $a\alpha_\varphi b$  significa que  $b = \varphi(a)$ . Viceversa, sea dada una correspondencia binaria  $\alpha$  entre los conjuntos  $A$  y  $B$ . Analicemos para todo  $a \in A$  el conjunto de todos los  $b \in B$  que se caracteriza por la propiedad  $a\alpha b$ . Dicha correspondencia define la aplicación  $\varphi : A \rightarrow B$ , cuando y sólo cuando para todo  $a \in A$  existe exactamente un solo elemento  $b \in B$  que se caracteriza por las propiedades  $a\alpha b$ . Así pues, la noción de correspondencia binaria incluye el concepto de aplicación como un caso particular (muy importante).

Cuando  $A = B$ , la correspondencia binaria  $\varrho \subseteq A \times A$  lleva el nombre de *relación binaria* en el conjunto  $A$ . Son ejemplos de relación binaria la relación de igualdad  $\Delta = \{(a, a) \mid a \in A\}$ , llamada *diagonal* del conjunto  $A$ , y la relación que coincide con todo el conjunto  $A \times A$ , denominada *relación unidad*.

A una relación binaria  $\varrho$  sobre el conjunto finito  $A$  se le puede poner en correspondencia un ente geométrico llamado grafo orientado o diagrama. A todo elemento  $a \in A$  se le pone en correspondencia un punto en el plano que lleva el nombre de vértice. Si para  $a$  y  $b$  tenemos  $a\varrho b$ , los puntos marcados con  $a$  y  $b$  se unen por una flecha que parte de  $a$  y llega a  $b$  y que se denomina arco. La totalidad de vértices y arcos construidos del modo mencionado representan el diagrama  $\Gamma(A, \varrho)$  de la relación  $\varrho$ . En la fig. 1.1 se exponen los diagramas  $\Gamma(A, \Delta)$  y  $\Gamma(A, I)$ , respectivamente, donde  $A = \{a, b, c\}$ ,  $I = A \times A$ .

Sea  $A'$  un subconjunto no vacío del conjunto  $A$ , sobre el cual viene dada la relación binaria  $\varrho$ : de la relación  $\varrho'$  en  $A'$ , definida mediante la condición

$$a\varrho' b = a\varrho b \text{ para cualesquiera } a, b \in A',$$

se dice que ella está *inducida* mediante la relación  $\varrho$ .

Formulemos las propiedades que pueden tener las relaciones binarias. Una relación  $\varrho$  se denomina *reflexiva*, si  $a\varrho a$  para todo  $a \in A$ . Dicho de otro modo, una relación es reflexiva, siempre que  $\Delta \subseteq \varrho$ . Si la expresión  $a\varrho b$  lleva consigo  $b\varrho a$ , la relación  $\varrho$  se llama *simétrica*. En cambio, si  $a\varrho b$  y  $b\varrho a$  tienen por resultado  $a = b$ , la relación  $\varrho$  se llama *antisimétrica*. Una relación  $\varrho$  se llama *transitiva*, si  $a\varrho b$  y  $b\varrho c$  conducen a  $a\varrho c$ . No es difícil

convencerse de que la diagonal posee todas las cuatro propiedades citadas, mientras que la relación unidad tiene todas estas propiedades, a excepción de la antisimetría. Pero, si  $A$  se compone sólo de un elemento, la relación unidad coincide con la diagonal.

Se denomina *clase contigua* de la relación binaria  $\rho$ , definida por un elemento  $a \in A$ , el conjunto de todos los elementos  $b \in A$  tales que  $b\rho a$ .

La relación binaria  $\rho$  en el conjunto  $A$  se llama relación de equivalencia, si es reflexiva, simétrica y transitiva a la vez. Las relaciones de equivalencia son de gran importancia en el análisis combinatorio, puesto que están estrechamente ligadas con las particiones de los conjuntos. Efectivamente, puede demostrarse con facilidad que una totalidad de clases contiguas de relaciones de equivalencia sobre un conjunto  $S$  representa la partición de este último y que a toda partición del conjunto  $S$  le corresponde la relación de equivalencia  $\rho$ , cuyas clases coinciden con los bloques de la partición indicada (la afirmación  $a\rho b$  tiene lugar, si y sólo si  $a$  y  $b$  pertenecen a un mismo subconjunto de la partición del conjunto  $S$ ).

Una relación binaria  $\rho$  sobre el conjunto  $A$  se denomina relación de orden parcial, si es reflexiva, antisimétrica y transitiva. La relación de orden parcial se denotará con el símbolo  $\leq$ . La notación  $a \geq b$  significa que  $b \leq a$ . A veces diremos que  $A$  (o bien  $(A, \leq)$ ) es un conjunto parcialmente ordenado, suponiendo que la relación de orden parcial ya es conocida (esta afirmación, sin embargo, no es bien correcta, por cuanto en un solo conjunto pueden fijarse órdenes diferentes).

Un conjunto parcialmente ordenado se denomina *trivial*, siempre que  $a \leq b$ , cuando y sólo cuando  $a = b$ . Un conjunto parcialmente ordenado  $(A, \leq)$ , que posee la propiedad de que para cualesquiera  $a, b \in A$  se verifica o bien  $a \leq b$ , o bien  $b \leq a$ , lleva el nombre de *cadena* (lo llaman también conjunto *linealmente ordenado*).

Recordemos, además, algunos conceptos algebraicos que nos harán falta ulteriormente. Se denomina *operación binaria* sobre el conjunto  $A$  la aplicación  $f: A \times A \rightarrow A$ . Si  $f(a, b) = c$ , donde  $a, b, c \in A$ , se escribe  $a * b = c$ . Una operación binaria se llama *asociativa*, si para cualesquiera  $a, b, c \in A$ :

$$(a * b) * c = a * (b * c).$$

Si una operación binaria satisface la condición

$$a * b = b * a$$

para cualesquiera  $a, b \in A$ , se denomina *conmutativa*. El elemento  $e \in A$  se denomina elemento *unidad* (elemento *neutro*) respecto de la operación  $*$ , si para todo  $a \in A$ :

$$a * e = e * a = a.$$

Si tal elemento existe, es único. Supongamos que un conjunto  $A$  con operación prefijada posee un elemento unidad  $e$ . En este caso el elemento  $a^{-1}$

se denomina *inverso* (o *simétrico*) del elemento  $a \in A$  con relación a dicha operación, siempre que  $a * a^{-1} = a^{-1} * a = e$ . El conjunto  $A$  con operación binaria  $*$ , en el cual las ecuaciones  $a * x = b$ , e  $y * a = b$  son resolubles unívocamente respecto de  $x$  e  $y$  para cualesquiera  $a, b \in A$  se llama *casi grupo*. Un conjunto no vacío  $A$ , sobre el cual viene definida la operación binaria asociativa, recibe el nombre de *semigrupo*. Si la operación es conmutativa, el semigrupo se llama *abeliano*. Un semigrupo, en el que existe un elemento unidad y para cada elemento existe uno inverso, se denomina *grupo*. El número de elementos en el grupo se llama *orden* del grupo. Un grupo cuyos elementos son todos la potencia de un elemento  $a$  (es decir, pueden obtenerse por la aplicación sucesiva de la operación, empleando un mismo elemento  $a$  distinto del elemento neutro) se llama *cíclico*. Los grupos cíclicos son siempre abelianos.

Sean  $A$  y  $B$  los grupos finitos de órdenes arbitrarios con las operaciones binarias  $*$  y  $\circ$ , respectivamente, y supongamos que  $\varphi: A \rightarrow B$  es una aplicación, con la cual para cualesquiera  $a, a' \in A$  se verifica la igualdad

$$\varphi(a * a') = \varphi(a) \circ \varphi(a'),$$

Tal aplicación  $\varphi$  se llama *homomorfismo* del grupo  $A$  en el grupo  $B$ . Si  $\varphi$  es una aplicación biunívoca, el homomorfismo recibe el nombre de *isomorfismo*.

**Ejemplo.** Un conjunto de sustituciones  $\varphi: X \rightarrow X$  forma un grupo, si la operación  $*$  se define como resultado de la actuación sucesiva de dos sustituciones, es decir  $\varphi * \psi = \pi$ , donde  $\forall x \in X: \pi(x) = \psi(\varphi(x))$ . Dicho grupo lleva el nombre de *grupo simétrico de potencia  $n = |X|$* . Es fácil mostrar que todos los grupos simétricos de un mismo orden son isomorfos. Observemos que los grupos simétricos no son abelianos cuando  $n \geq 3$ .

Si en un subconjunto  $B \subseteq A$  el resultado de una operación de dos cualesquiera elementos de  $B$  pertenece también a  $B$ , suele decirse que  $B$  está *cerrado* respecto de la operación dada. Se llama *subgrupo* a un subconjunto no vacío del grupo que está cerrado respecto de la operación binaria y que para cada elemento contiene un elemento inverso.

Un conjunto  $A$  con dos operaciones binarias  $+ y \circ$  se denomina *anillo*, siempre que forma un grupo abeliano respecto de la operación  $+$ , un semigrupo respecto de la operación  $\circ$ , y si  $\circ$  es distributiva respecto de la operación  $+$ , es decir, si para cualesquiera  $a, b, c \in A$  se tiene

$$\begin{aligned}(a + b) \circ c &= a \circ c + b \circ c, \\ c \circ (a + b) &= c \circ a + c \circ b.\end{aligned}$$

En un anillo los elementos neutros respecto de las operaciones  $+$  y  $\circ$  se denominan *nulo* y *unidad*, respectivamente. Un elemento del anillo se llama *invertible*, si para dicho elemento existe un elemento inverso respecto de la operación  $\circ$ .

Si un conjunto de elementos de un anillo, distintos de cero, forma res-

pecto de la operación  $\circ$  un grupo abeliano, entonces el anillo se llama en este caso *campo*. Un campo en el que se contienen un número finito de elementos se llama *finito*. Un campo finito de  $n$  elementos existe, cuando y sólo cuando  $n = p^\alpha$ , donde  $p$  es un número primo y  $\alpha$ , un número natural. Tal campo es único con exactitud hasta un isomorfismo en el que se conservan ambas operaciones binarias. Este campo se denomina *de Galois* y se designa, de ordinario, con la expresión  $GF(p^\alpha)$ . Si  $\alpha = 1$ ,  $GF(p)$  es isomorfo al campo de residuos respecto al módulo primo (o irreducible)  $p$ .

Como ejemplos de un anillo infinito y de un campo infinito sirven el anillo de números enteros  $\mathbf{Z}$  y el campo de números reales  $\mathbf{R}$ . Las operaciones binarias son aquí operaciones corrientes de adición y multiplicación.

Se denomina *espacio lineal*  $L$  sobre el campo  $P$  el conjunto dotado de la operación binaria  $\varphi: L \times L \rightarrow L$ , la cual se designa habitualmente como adición  $\varphi(a, b) = a + b$  para  $a, b \in L$ , y de la operación binaria externa  $f: P \times L \rightarrow L$ , la cual se designa habitualmente como multiplicación  $f(p, a) = pa$ , con la particularidad de que dichas operaciones satisfacen los siguientes axiomas:

a) con respecto a la operación de adición el espacio  $L$  es un grupo abeliano. El elemento neutro de este grupo se denota con 0; el elemento inverso de  $a$  se designa corrientemente con  $-a$ :

b) la multiplicación de los vectores por los elementos del campo  $P$ , o por los escalares, es unitaria, es decir,  $1 \cdot a = a$  para todos los  $a$ , y asociativa, es decir,  $p(qa) = (pq)a$  para cualesquiera  $p, q \in P$ ;  $a \in L$ :

c) la adición y la multiplicación están unidas mediante las leyes de distributividad, es decir,

$$p(a + b) = pa + pb,$$

$$(p + q)a = pa + qa$$

para cualesquiera  $p, q \in P$ ;  $a, b \in L$ .

La expresión del tipo  $p_1 a_1 + \dots + p_n a_n$  lleva el nombre de *combinación lineal* de los vectores  $a_1, a_2, \dots, a_n$ ; los escalares  $p_i$  se llaman *coeficientes* de dicha combinación lineal.

Se denomina *álgebra* sobre el campo  $P$  el anillo asociativo con la unidad  $A$  que contiene el campo  $P$  y es tal que  $P$  yace en el centro de  $A$ , es decir, que conmuta con todos los elementos de  $A$ . En particular,  $A$  es un espacio lineal sobre el campo  $P$ .

Los conceptos nuevos se introducirán más adelante a medida que surja la necesidad. Paseinos, ahora, a la explicación del sentido de las operaciones combinatorias más simples. Nos limitaremos, para empezar, al análisis de los conjuntos linealmente ordenados. Sin embargo, estudiaremos también, en forma paulatina, los conjuntos de estructura más compleja.

### 1.3. MUESTRAS Y ORDENACIONES

Con el concepto de *muestra* se asocian tanto la propia operación de selección de un subconjunto del conjunto dado, como también el resultado de la operación citada, es decir, el subconjunto elegido. En lo sucesivo se tendrá en cuenta precisamente la segunda interpretación, siempre que no se diga lo contrario.

Supongamos que de un  $n$ -conjunto  $A_n$  se ha obtenido una  $r$ -muestra:

$$(a_1, a_2, \dots, a_r), \text{ donde } a_i \in A_n; i = 1, 2, \dots, r; r \leq n.$$

El número  $r$  se llama *volumen* de la muestra.

Según sean las condiciones del problema, en las muestras puede tomarse en consideración el orden de sucesión de los elementos en ellas (y en este caso las  $r$ -muestras se llaman *r-permutaciones*), o bien dicho orden no se toma en consideración (en este último caso se denominan *r-combinaciones*). Por ejemplo, dos 5-muestras del conjunto  $A_n (n \geq 5)$ :

$$(a_1, a_2, a_3, a_4, a_5) \text{ y } (a_5, a_4, a_3, a_2, a_1)$$

representan en sí 5-combinaciones iguales y al mismo tiempo 5-permutaciones diferentes. En general, dos  $r$ -permutaciones  $a = (a_1, a_2, \dots, a_r)$  y  $b = (b_1, b_2, \dots, b_r)$  son iguales:  $a = b$  únicamente si  $a_i = b_i; i = 1, 2, \dots, r$ . En las muestras es posible la aparición reiterada de los elementos, y en tal caso ellas se denominan *r-combinaciones con repetición* y *r-permutaciones con repetición*, respectivamente. Una  $r$ -permutación (con repetición) de elementos del conjunto  $A$  se llama también *palabra de longitud  $r$  sobre el alfabeto  $A$* .

Es evidente que los conceptos de  $r$ -permutaciones y  $r$ -combinaciones, al igual que sus combinaciones, abarcan todos los tipos posibles de muestras. Por eso no hay necesidad de dar el concepto de arreglo (variación), aunque dicho concepto aparece todavía en la literatura, principalmente en los manuales.

La multiformidad de la solución de los problemas combinatorios observada en las etapas iniciales del desarrollo de las matemáticas condujo a una cuestión natural: ¿cuántos son los procedimientos, por medio de los cuales puede realizarse la requerida disposición combinatoria? En particular, el cálculo del número de  $r$ -muestras de un  $n$ -conjunto fue históricamente uno de los primeros problemas de la combinatoria.

Hallemos el número de todas las  $r$ -permutaciones posibles (sin repetición) de un  $n$ -conjunto. Denotemos el número que se busca mediante  $P(n, r)$ . El problema se reduce a una aplicación sucesiva de la regla del producto. En efecto, en el  $n$ -conjunto se tienen  $n$  posibilidades para elegir el primer elemento de la  $r$ -permutación. Una vez realizada tal elección, quedan  $n - 1$  posibilidades para la elección del segundo elemento, luego quedan  $n - 2$  posibilidades para elegir el tercer elemento, etc.: para la elección del  $r$ -ésimo

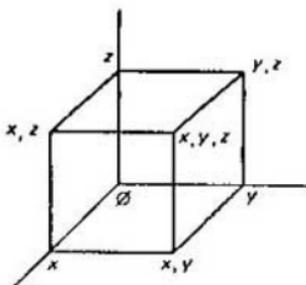


Fig 1.2.

elemento tendremos  $n - r + 1$  posibilidades. De acuerdo con la regla del producto,

$$P(n, r) = n(n - 1) \dots (n - r + 1),$$

de donde se deduce

$$P(n, n) = n!$$

Para que el resultado sea más completo, admitamos

$$P(n, 0) = 0! = 1.$$

Calculemos ahora el número de  $r$ -permutaciones posibles con repetición. En este caso, después de elegir cualquier elemento de la  $r$ -permutación quedan las mismas  $n$  posibilidades para elegir el elemento siguiente. Por consiguiente, según la regla del producto, el número de  $r$ -permutaciones con repetición del  $n$ -conjunto es igual a  $n^r$ .

Los razonamientos aducidos aquí se ilustran fácilmente con un ejemplo del esquema de urna, cuyos diferentes tipos se emplean en la teoría de las probabilidades: se tiene una urna dentro de la cual se encuentran colocadas  $n$  bolas iguales y de la cual se sacan por turno  $r$  bolas. En tal caso resultan posibles dos casos: la bola sacada o bien se retorna a la urna (elección con retorno) o bien no se retorna (elección sin retorno).

Un ejemplo más. ¿Cuántos subconjuntos tiene un  $n$ -conjunto  $S$ , es decir, a qué es igual  $|P(S)|$ ? La respuesta será  $|P(S)| = 2^n$ . Efectivamente, cualquier  $r$ -muestra  $R = (s_{i_1}, s_{i_2}, \dots, s_{i_r})$ , donde  $r = 1, 2, \dots, n$ , figura en  $P(S)$ . A esta  $r$ -muestra se le puede poner en correspondencia una  $n$ -muestra, compuesta por elementos de dos tipos: ceros, si el elemento no integra la  $r$ -muestra  $R$ , y unidades, si el elemento figura en  $R$ . De este modo, las unidades deben disponerse en los lugares correspondientes a  $i_1, i_2, \dots, i_r$ , mientras que los ceros, en los demás lugares. Pero, el número de tales  $n$ -muestras (es decir, de  $n$ -permutaciones con repetición) de 2-conjunto  $\{0, 1\}$  es igual a  $2^n$ , lo que constituye precisamente el resultado buscado. Este mismo problema puede interpretarse como el problema sobre el número de vértices de un hipercubo en el espacio de  $n$  dimensiones (el caso de  $n = 3$ ,  $S = \{x, y, z\}$  se muestra en la fig. 1.2, donde todos los subconjuntos  $P(S)$  son vértices del cubo).

**Ejercicio.** ¿Cuál es el número de matrices de dimensión  $k \times l$ , compuestas por ceros y unidades?

Calculemos ahora el número de  $r$ -combinaciones, designándolo con  $\binom{n}{r}$  o con  $C_n^r$ . Comencemos por el caso en que todos los elementos en las  $r$ -combinaciones son diferentes. Es fácil ver que el número de  $r$ -combinaciones del  $n$ -conjunto es  $r!$  veces inferior al número de  $r$ -permutaciones de los elementos del mismo conjunto. Por consiguiente,

$$\binom{n}{r} = \frac{P(n, r)}{r!} = \frac{n(n-1) \dots (n-r+1)}{r!} = \frac{n!}{r!(n-r)!};$$

de aquí se deduce que  $\binom{n}{r} = \binom{n-r}{r}$ ; en particular,

$$\binom{n}{n} = \binom{n}{0} = 1.$$

Observemos que las  $r$ -combinaciones del  $n$ -conjunto son sus  $r$ -subconjuntos. Con este motivo estudiemos el problema sobre el número de  $(r_1, r_2, \dots, r_k)$ -particiones del  $n$ -conjunto  $S$ , es decir, de particiones ordenadas del tipo  $S = T_1 \cup T_2 \cup \dots \cup T_k$ , en las cuales  $T_i \cap T_j = \emptyset$  para  $i \neq j$ ;  $i, j = 1, 2, \dots, k$ , con la particularidad de que  $T_i$  es un  $r_i$ -subconjunto del conjunto  $S$ ,  $i = 1, 2, \dots, k$ . Obviamente,  $\sum_{i=1}^k r_i = n$ . Razonemos igual que lo

hemos hecho al buscar el número  $P(n, r)$ . Para elegir el  $r_1$ -subconjunto  $T_1$  de  $S$  se tienen  $\binom{n}{r_1}$  posibilidades: entonces el  $r_2$ -subconjunto  $T_2$  puede elegirse sólo de  $n - r_1$  elementos restantes (ya que  $T_1 \cap T_2 = \emptyset$ ), y, por lo tanto, se tienen  $\binom{n-r_1}{r_2}$  métodos para la elección de  $T_2$ , etc.; el  $r_k$ -subconjunto  $T_k$  puede ser elegido sólo después de haber elegido los  $r_i$ -conjuntos  $T_i$ ,  $i = 1, 2, \dots, k-1$ , por consiguiente de  $n - \sum_{i=1}^{k-1} r_i$  elementos restantes

puede elegirse, sirviéndose de  $\binom{n - \sum_{i=1}^{k-1} r_i}{r_k}$  métodos. Aplicando ahora

la regla del producto, obtendremos que el número buscado de  $(r_1, r_2, \dots, r_k)$ -particiones del  $n$ -conjunto  $S$  es igual a

$$R = \binom{n}{r_1} \binom{n-r_1}{r_2} \dots \binom{n - \sum_{i=1}^{k-1} r_i}{r_k} = \frac{n!}{r_1! r_2! \dots r_k!},$$

(tomando en consideración la expresión para  $\binom{n}{r}$ ). La  $r$ -combinación

del  $n$ -conjunto puede ser interpretada como una  $(r, n - r)$ -partición, y la  $(1, 1, \dots, 1)$ -partición representa simplemente una permutación. Calculemos, por fin, el número de  $r$ -combinaciones con repetición del  $n$ -conjunto  $S$ . Daremos a conocer tres métodos distintos de obtención de este número con el objeto de mostrar los rasgos específicos de los razonamientos combinatorios.

**1<sup>er</sup> método.** Admitamos que los elementos del conjunto  $S$  están numerados por medio de los números  $1, 2, \dots, n$  (es decir,  $S$  se encuentra en una correspondencia biunívoca con el conjunto de los primeros  $n$  números naturales). Entonces, en lugar de las  $r$ -muestras del conjunto  $S$  podemos analizar las  $r$ -muestras (biunívocas) del conjunto  $S' = \{1, 2, \dots, n\}$  que corresponden a las primeras. Toda  $r$ -muestra del conjunto  $S'$  puede ser escrita en la forma  $A = (a_1, a_2, \dots, a_r)$ , donde  $a_1 \leq a_2 \leq \dots \leq a_r$  (la igualdad de los números responde al caso de elementos iguales en la  $r$ -muestra correspondiente de  $S$ ). A la  $r$ -muestra  $A$  (los elementos en esta muestra no son forzadamente diferentes) le ponemos en correspondencia el  $r$ -conjunto  $A' = \{a_1 + 0, a_2 + 1, \dots, a_r + r - 1\}$ , en el cual todos los elementos son, evidentemente, diferentes.

Como es fácil de ver, dicha correspondencia es biunívoca, con la particularidad de que los  $r$ -conjuntos  $A'$  son  $r$ -combinaciones sin repetición del  $(n + r - 1)$ -conjunto  $\{1, 2, \dots, n, n + 1, \dots, n + r - 1\}$ , cuyo número es igual (como quedó demostrado) a  $\binom{n + r - 1}{r}$ . Esta es precisamente la respuesta que buscábamos.

El 2<sup>o</sup> método consiste en la obtención de una fórmula recurrente<sup>1)</sup>.

Denotemos mediante  $f(n, r)$  el número de  $r$ -combinaciones con repeticiones del  $n$ -conjunto  $S$ . Está claro que

$$f(n, 1) = n \quad \text{y} \quad f(1, r) = 1.$$

(para cualquier  $n > 0$  entero de  $n$  elementos pueden elegirse  $n$  diferentes 1-combinaciones, es decir,  $n$  diferentes elementos; mientras tanto para cualquier  $r > 0$  entero de un elemento se puede obtener solamente una  $r$ -combinación: una  $r$ -muestra compuesta por  $r$  elementos iguales). Fijemos en  $S$  cierto elemento, entonces cada  $r$ -combinación o bien contiene este elemento o no lo contiene. Si tiene lugar el primer caso, los demás  $r - 1$  elementos de esta  $r$ -combinación (y, por tanto, las  $r$ -combinaciones que contienen el elemento fijado) pueden ser elegidos empleando los  $f(n, r - 1)$  métodos. Si tiene lugar el segundo caso, la  $r$ -combinación se elige de  $n - 1$  elementos, y entonces, el número de tales  $r$ -combinaciones es igual a  $f(n - 1, r)$ . Empleando la regla de la suma, obtendremos

<sup>1)</sup> Se denominan fórmulas (relaciones) recurrentes aquellas que permiten calcular los valores de una magnitud buscada paso a paso, partiendo de los valores «iniciales» conocidos y de los calculados de antemano.

$$f(n, r) = f(n, r-1) + f(n-1, r). \quad (1)$$

En particular, al conocer  $f(n, 1)$  y  $f(1, r)$ , tenemos

$$f(n, 0) = f(n, 1) - f(n-1, 1) = 1,$$

lo que concuerda con el resultado obtenido anteriormente. Ahora obtenemos sucesivamente

$$f(n, 2) = f(n, 1) + f(n-1, 2) = f(n, 1) + f(n-1, 1) + f(n-2, 2) = \dots$$

$$\dots = n + (n-1) + (n-2) + \dots + 1 = \frac{n(n+1)}{2} = \binom{n+1}{2};$$

$$\begin{aligned} f(n, 3) &= f(n, 2) + f(n-1, 2) + \dots + f(1, 3) = \\ &= \binom{n+1}{2} + \binom{n}{2} + \dots + 1 = \binom{n+2}{3} \end{aligned}$$

etc. Es fácil convencerse de que

$$f(n, r) = \binom{n+r-1}{r}$$

satisface la correlación (1) y las condiciones iniciales:

$$f(n, 1) = n; f(1, r) = 1.$$

**3<sup>er</sup> método.** A una  $r$ -combinación con repetición del  $n$ -conjunto  $S$  (por ejemplo, a  $bcb$  de  $S = \{a, b, c, d, e\}$ ) agreguemos todos los  $n$  elementos del conjunto  $S$ , y escribamos por orden los  $n+r$  elementos obtenidos, disponiendo juntos los elementos iguales: ( $abbccde$ ). A continuación, dividamos los subconjuntos de elementos iguales mediante  $n-1$  rayas: ( $a | bb | b | cc | d | e$ ). Por fin, sustituyamos por puntos todos los elementos dispuestos entre las rayas: ( $. | \dots | .. | . | .$ ). De este modo, a la  $r$ -combinación se le asigna (equipara) la colocación de  $n-1$  rayas en  $n+r-1$  intervalos entre  $n+r$  puntos. Inversamente en cada colocación de esta índole se restaura inóvamente la  $r$ -combinación que le corresponde. Por ejemplo,

$$(. | . | .. | . | .) \rightarrow (aa | b | cc | d | ee) \rightarrow (aabccdee) \rightarrow \{a, c, e\}.$$

Existen en total  $\binom{n+r-1}{n-1} = \binom{n+r-1}{r}$  métodos de colocar  $n-1$  rayas en  $n+r-1$  lugares. Por consecuencia, existe exactamente la misma cantidad de  $r$ -combinaciones con repetición del  $n$ -conjunto.

Como conclusión de este párrafo, analicemos un concepto relacionado con la operación de ordenación, es decir, la permutación. Esta última puede ser examinada desde dos puntos de vista: a) como una totalidad ordenada de elementos del conjunto dado, o bien b) como una perturbación del orden estándar llamado, habitualmente, natural (por ejemplo, alfabético, numérico). El caso a) conduce a las  $r$ -permutaciones,  $r \leq n$ , ya descritas anteriormente. El caso b) conduce a las  $n$ -permutaciones (en relación con la defini-

ción de la  $r$ -permutación) denominadas simplemente permutaciones (o sustituciones), que se estudian en la teoría de los grupos.

Sea, por ejemplo una permutación

$$P = (4, 3, 7, 5, 6, 9, 2, 8, 1, 12, 11, 10),$$

que representa una perturbación del orden natural de los primeros 12 números de la serie natural. Puede ser escrita en forma de una sustitución (en la primera fila se pone el orden natural y en la segunda, el perturbado).

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 3 & 7 & 5 & 6 & 9 & 2 & 8 & 1 & 12 & 11 & 10 \end{pmatrix}.$$

Esta notación muestra que, al realizarse la permutación  $P$ , el elemento 1 se convierte en 4, el elemento 2 en 3, el 3 en 7, etc. La permutación  $P$  puede escribirse también de otro modo:

$$P = (1, 4, 5, 6, 9)(2, 3, 7)(10, 12)(8)(11), \quad (2)$$

donde cada paréntesis es una permutación que actúa sólo contra los elementos encerrados dentro del paréntesis dado y no toca los elementos no encerrados en él (por ejemplo, la sustitución  $(2, 3, 7)$  convierte 2 en 3, 3 en 7, y 7, de nuevo en 2). La representación de una permutación en la forma (2) lleva el nombre de descomposición *en ciclos*. Cualquier permutación puede ser descompuesta en ciclos. Esta descomposición es única, con una exactitud de hasta las permutaciones cíclicas de los elementos dentro de los ciclos. Por ejemplo,  $(2, 3, 7)$ ,  $(3, 7, 2)$   $(7, 2, 3)$  son notaciones diferentes de un mismo ciclo.

Supongamos que una permutación contiene  $k_1$  ciclos compuestos por un solo elemento, es decir, 1-ciclos, luego  $k_2$  2-ciclos,  $k_3$  3-ciclos, etc. En este caso se denomina  $(k_1, k_2, \dots, k_n)$ -permutación, o bien permutación de la forma

$$1^{k_1} 2^{k_2} \dots n^{k_n}, \quad (3)$$

donde, evidentemente,

$$\sum_{i=1}^n ik_i = n.$$

**Teorema.** El número de permutaciones del tipo (3) es igual a

$$P(k_1, k_2, \dots, k_n) = \frac{n!}{1^{k_1} k_1! 2^{k_2} k_2! \dots n^{k_n} k_n!}. \quad (4)$$

*Demostración.* Examinemos la notación de una descomposición en ciclos para la permutación del tipo (3), a saber: primero  $k_1$  paréntesis para la notación de los ciclos de longitud 1, luego  $k_2$  paréntesis para la notación de los ciclos de longitud 2, etc. En  $n$  posiciones dispuestas dentro de todos los paréntesis podemos poner  $n$  elementos, sirviéndonos de  $n!$  métodos, y cada vez obtendremos la notación de la permutación del tipo (3). Sin em-

bargo, entre dichas  $n!$  notaciones se encuentran diferentes notaciones de una misma permutación. Aclaremos cuántas notaciones diferentes tiene una permutación. En primer lugar como hemos observado anteriormente, cada ciclo de longitud  $i$  puede escribirse dentro de los márgenes del paréntesis dado mediante  $i$  métodos. En segundo lugar, sirviéndose de  $k_i$  métodos se pueden reordenar los paréntesis donde están escritos los ciclos de longitud  $i$ . Según la regla del producto obtenemos, que una familia de ciclos de longitud  $i$  puede ser representada por  $i^{k_i} \cdot k_i!$  métodos. Al hacer  $i$  recorrer los valores de 1 a  $n$ , y al aplicar otra vez la regla del producto, concluimos que existen

$$N = 1^{k_1} k_1! 2^{k_2} k_2! \dots n^{k_n} k_n!$$

métodos para escribir cada permutación del tipo (3). Por consiguiente, se tienen en total  $n!/N$  de tales permutaciones, lo que era necesario demostrar.

La representación de las permutaciones en forma de un producto de ciclos sirve de fuente para muchos problemas combinatorios, por ejemplo: hallar el número de permutaciones del  $n$ -conjunto que tengan un número prefijado de ciclos (sin tomar en consideración la longitud de los ciclos); que dejen los elementos dados inmóviles; que tengan un número dado de ciclos de longitud prefijada, etc.

#### 1.4. DISTRIBUCIONES Y LLENADOS

En muchos problemas cierta totalidad de elementos (por ejemplo de granos, pernos, tuercas, etc.) se distribuye por cierto conjunto de células (cajas, cajones, etc.) que, como consecuencia, se llenan. Ambos conceptos principales, esto es, distribución (su sinónimo es la partición) y llenado, se emplean tanto para designar las operaciones, como para expresar el resultado de ellas, es decir, la situación obtenida.

Los problemas de esta clase existen desde hace mucho tiempo y cuentan con un procedimiento de resolución elaborado. El interés hacia estos problemas no se extingue, pues tienen gran importancia práctica. Ellos se manifiestan en los más diversos planteamientos: particiones de conjuntos, cortes de grafos y de redes, agrupaciones de tornos y de mecanismos automáticos y robots, etc.

En el aspecto teórico dichos problemas pueden interpretarse como aplicaciones de un conjunto (de elementos) sobre otro conjunto (de células). Pueden ser tratados también como elección de muestras.

Los medios adoptados de resolución de esta clase de problemas dependen de las condiciones impuestas sobre los tipos de elementos a distribuir, métodos de distribución y capacidad de las células. Es evidente, que la riqueza de las condiciones posibles determina la diversidad de los procedimientos aplicados para la resolución de los problemas. Más abajo se da cierta información que introduce al lector en esta esfera de problemas.

Para el cálculo del número de distribuciones hace falta precisar si los ele-

mentos del conjunto dado y las células son distinguibles (por ejemplo, numerados) o no. De acuerdo con ello los problemas se dividen en las siguientes cuatro clases.

(A) los elementos del conjunto son distinguibles, como también lo son las células;

(B) los elementos del conjunto no son distinguibles, las células, son distinguibles;

(C) los elementos del conjunto son distinguibles, las células no son distinguibles;

(D) tanto los elementos del conjunto, como las células no se distinguen entre sí.

Dentro de cada una de estas clases los problemas se diferencian, a su vez, por la forma de las aplicaciones prefijadas por las condiciones concretas. Convengamos en que a continuación  $N$  siempre servirá de designación para un  $n$ -conjunto de elementos, y  $R$  será un  $r$ -conjunto de células. Por cuanto en este párrafo hablamos sólo de los fundamentos teóricos de la operación de distribución y llenado, estudiemos estas clases de problemas en rasgos generales, sin tratar de exponer completa y detalladamente todos los accesos a la resolución de los problemas correspondientes.

(A) Según lo dicho anteriormente, todos los elementos del conjunto  $N$  y todas las células del conjunto  $R$  son distinguibles. Aquí no tiene importancia si se diferencian por la forma, el color, volumen o, incluso, por el número. Tiene importancia sólo el hecho de distinción. He aquí algunas formas equivalentes de este problema: a) formación de las palabras de longitud  $r$ , a partir del alfabeto compuesto por  $n$  letras; b) extracción sucesiva de  $r$  bolas de una urna que contiene  $n$  bolas, con su retorno inmediato; c) formación de las  $r$ -permutaciones con repetición de  $n$  símbolos.

El carácter de la aplicación que por ahora está libre de limitaciones algunas, permite indicar en seguida el número de distribuciones posibles:

$$P = n^r,$$

por cuanto para cada una de  $r$  células se tiene la posibilidad de colocar en ella cualquiera de  $n$  elementos. La forma particular de las aplicaciones (biunívocas) corresponde a una limitación adicional: en cada célula cabe uno, y sólo un elemento. En este caso

$$P = n(n-1) \dots (n-r+1) = \frac{n!}{(n-r)!}.$$

A la clase (A) pertenecen, en particular, los siguientes casos de distinción de los elementos y de las células.

(A<sub>1</sub>) El conjunto  $N$  tiene la  $(k_1, k_2, \dots, k_m)$ -especificación, si cuenta con  $k_1$  elementos del primer tipo (por ejemplo, de color),  $k_2$  elementos del segundo tipo, ...,  $k_m$  elementos del  $m$ -ésimo tipo (además,  $k_1 + k_2 + \dots + k_m = n$ ).

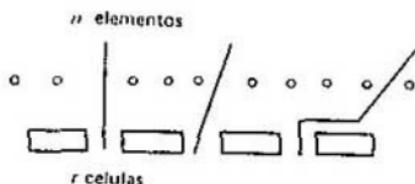


Fig.1.3.

(A<sub>2</sub>) El  $r$ -conjunto  $R$  tiene la  $(n_1, n_2, \dots, n_r)$ -especificación, si en la  $i$ -ésima célula se disponen  $n_i$  elementos,  $i = 1, 2, \dots, r$ .

(A<sub>3</sub>) Los elementos dentro de las células están ordenados, es decir, dos células se consideran llenas de una manera diferente, si es distinta la ordenación de los elementos (incluso de los mismos) alojados en ellas; no hay limitaciones para el volumen de las células.

Sin pretender dar una descripción completa de todas las situaciones posibles, aduzcamos un solo ejemplo. Supongamos, por ejemplo, que el conjunto  $N$  tiene una  $(p, q)$ -especificación, es decir, contiene  $p$  elementos del primer tipo y  $q$  elementos del segundo tipo;  $p + q = n$ . Se necesita determinar cuántas son las distribuciones de los elementos del conjunto  $N$  en  $r$  células diferentes sin limitaciones para el número de elementos en cada una de las células. Los elementos del primer tipo pueden distribuirse en  $r$  células por

$$\binom{p+r-1}{r-1} = \binom{p+r-1}{p}$$

métodos, y los elementos del segundo tipo, por

$$\binom{q+r-1}{r-1} = \binom{q+r-1}{q}$$

métodos. El número total de distribuciones es igual, en virtud de la regla del producto, a

$$\binom{p+r-1}{p} = \binom{q+r-1}{q}.$$

Si tiene lugar la  $(k_1, k_2, \dots, k_m)$ -especificación del conjunto  $N$ , el número de distribuciones de  $n$  elementos suyos en  $r$  células diferentes será

$$\prod_{i=1}^m \binom{r+k_i-1}{i}.$$

Pasemos a los problemas de la clase (B). Como se ha dicho, en los problemas de este tipo los elementos del conjunto  $N$  no son distinguibles y los del conjunto  $R$ , distinguibles. Examinemos diferentes casos:

1. Los elementos del conjunto  $N$  están distribuidos en las células del conjunto  $R$  de una manera tal que ninguna célula está vacía (en la fig. 1.3. se muestra la distribución de  $n = 10$  elementos en  $r = 4$  células).

Según se ve, el problema se reduce a la determinación del número de métodos mediante los cuales se pueda trazar  $r - 1$  líneas en  $n - 1$  intervalos entre los elementos: este número es igual a  $\binom{n-1}{r-1}$ . A este mismo tipo de problemas se refieren los siguientes: hallar el número de métodos para pintar, usando  $r$  colores,  $n$  objetos iguales (por ejemplo, bolas); hallar el número de  $r$ -combinaciones con repetición, en las cuales se emplea cada elemento.

2. Los elementos del conjunto  $N$  de distribuyen en las células de  $R$  de tal modo, que pueden haber células vacías. El método de resolución de los problemas de este tipo es, en lo principal, el mismo. Al conjunto de elementos  $N$  se le agregan  $r$  "elementos vacíos" simbólicos. En este caso el problema se reduce a la determinación del número de métodos de trazar  $r - 1$  líneas en  $n + r - 1$  intervalos entre los elementos. Este número será

$$\binom{n+r-1}{r-1} = \binom{n+r-1}{n}.$$

Entre los problemas de este tipo hay, por ejemplo, el siguiente: hallar el número de soluciones de la ecuación

$$x_1 + x_2 + \dots + x_r = n$$

en  $x_i$ :  $i = 1, 2, \dots, r$  enteros no negativos.

3. En fin, a esta clase se refieren los problemas relacionados con el cálculo del número de muestras de un  $n$ -conjunto.

Los dos tipos restantes de problemas, (C) y (D), donde resultan no distinguibles las células para el llenado, representan, al tratar de resolverlos, dificultades mucho más considerables. Se llaman, habitualmente, por el nombre colectivo de particiones no ordenadas. Los problemas del tipo C, donde son indistinguibles sólo las células, mientras que los elementos a distribuir son distinguibles, permiten, por otra parte, su resolución. Indicemos algunas fórmulas.

1. En aquellos casos en que no se admite, al realizar el llenado, células vacías y cuando se toma en consideración el orden en que los elementos caen en las células, el número buscado de distribuciones es igual a

$$A_n^r = \frac{n!}{r!} \binom{n-1}{r-1}. \quad (1)$$

2. Si la partición antecedente se modifica de tal modo que se admiten 1, 2, ...,  $r$  células vacías, entonces el número buscado de distribuciones es

$$(A')_n^r = A_n^r + A_n^{r-1} + \dots + A_n^1. \quad (2)$$

3. Si no hay células vacías, mientras que el orden de disposición de los elementos en las células no se toma en consideración, el número de distribuciones será

$$B_n^r = \frac{1}{r!} \sum_{\substack{s_1 + \dots + s_r = n \\ s_j \geq 1}} \frac{n!}{s_1! s_2! \dots s_r!} = S(n, r). \quad (3)$$

El número  $S(n, r)$  se llama número de Stirling de 2º género (véase más abajo § 2.3).

4. Cuando en el caso 3 se admiten 1, 2, ...,  $r$  células vacías, el número de distribuciones es igual a

$$(B^r)_n = B_n^r + B_n^{r-1} + \dots + B_n^1. \quad (4)$$

Aduzcamos un esbozo de la demostración de las afirmaciones citadas. Efectivamente, supongamos que en el caso 1 se distribuyen elementos de un conjunto  $N = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ . Las distribuciones  $L$  tienen la forma  $L = \{\alpha_1, \alpha_2, \dots, \alpha_{i_1} \mid \alpha_{i_1+1}, \alpha_{i_1+2}, \dots, \alpha_{i_2} \mid \dots \alpha_{i_{r-1}+1}, \dots, \alpha_{i_{r-1}+2}, \dots, \alpha_n\}$ . El número  $|L|$  de estas distribuciones se puede calcular mediante dos procedimientos:

a)  $|L| = n! \binom{n-1}{r-1}$ , es decir, el número de permutaciones en el conjunto  $N$  se multiplica por el número de distribuciones de  $r-1$  líneas en  $n-1$  intervalos;

b)  $|L| = A_n^r \cdot r!$ , es decir, el número buscado se multiplica por el número de reenumeraciones posibles de las células.

Al igualar entre sí  $a)$  y  $b)$ , obtenemos la fórmula (1). Apliquemos en el caso 3, al igual que en el caso 1, dos métodos para calcular el número de distribuciones en diferentes células:

$$\begin{aligned} B_n^r \cdot r! &= \sum_{\substack{s_1 + \dots + s_r = n \\ s_i \geq 0}} \binom{n}{s_1} \binom{n-s_1}{s_2} \dots \binom{n-s_1-s_2-\dots-s_{r-1}}{s_r} = \\ &= \sum \frac{n!}{s_1!(n-s_1)!} \frac{(n-s_1)!}{s_2!(n-s_1-s_2)!} \dots \frac{(n-s_1-s_2-\dots-s_{r-1})!}{s_r!(n-s_1-s_2-\dots-s_r)!} = \\ &= \sum \frac{n!}{s_1! s_2! \dots s_r!}, \end{aligned}$$

de donde se deduce (3).

Las fórmulas (2) y (4) se desprenden, evidentemente, de las (1) y (3), respectivamente.

Estudiemos, por fin, el caso  $(D)$ , es decir, la clase de problemas sobre las distribuciones, cuando los conjuntos  $N$  y  $R$  se componen ambos de elementos indistinguibles. Dichos problemas resultaron ser más difíciles y la teoría de su resolución aún no está elaborada completamente. La interpretación más conocida del caso dado la representa el problema teórico-numérico sobre la partición de los números naturales en sumandos naturales.

Notemos, ante todo, que los problemas de la clase (D) no pueden equipararse con los problemas de las clases anteriores, como se ha hecho más arriba: las conexiones resultan ser mucho más complejas y no se logra hallar una expresión analítica conveniente para obtener el número buscado.

Para calcular el número de particiones referentes a los problemas de tipo (D), sirve por ahora de medio principal el siguiente método recurrente.

Supongamos que un  $n$ -conjunto  $S$  se divide en  $k$  partes no vacías  $a_1, a_2, \dots, a_k$ , con la particularidad de que  $|a_i| \geq 1, i = 1, 2, \dots, k$ . Denotemos con  $P_k(n)$  el número de tales particiones. Es obvio, que  $P_1(n) = 1; P_k(k) = 1, P_k(n) = 0$  para  $n < k$ .

$$\sum_{i=1}^k a_i = n. \quad (5)$$

Admitamos que  $|a_1| \geq |a_2| \geq \dots \geq |a_k|$  (renumeremos, si es necesario, las partes de la partición). Está claro que

$$\sum_{i=1}^k (a_i - 1) = n - k. \quad (6)$$

Se ha obtenido la partición del  $(n - k)$ -conjunto en partes cuyo número es  $\leq k$  (la igualdad tiene lugar, si cualquier  $a_i$  contiene no menos de 2 elementos). Según la regla de la suma, el número de tales particiones es igual a  $\sum_{i=1}^k P_i(n - k)$ , y, en virtud de la igualdad (6), dicho número es igual al número de particiones del  $n$ -conjunto en  $k$  partes, es decir, a

$$\sum_{i=1}^k P_i(n - k) = P_k(n). \quad (7)$$

Teniendo en cuenta los valores (5), esta fórmula recurrente permite obtener sucesivamente los valores para  $P_k(n)$ , reuniéndolos, si es necesario, en la tabla 1.1.

Para los valores pequeños de  $k$  podemos obtener fórmulas de  $P_k(n)$ , por ejemplo

$$P_1(n) = 1; P_2(2) = 1; P_2(1) = 0; \\ P_2(n) = P_2(n - 2) + P_1(n - 2) = P_2(n - 2) + 1;$$

de donde

$$P_2(n) = \frac{n}{2}, \text{ si } n \text{ es par;} \\ P_2(n) = \frac{n-1}{2}, \text{ si } n \text{ es impar.}$$

Pero, ya para  $k = 3$  las fórmulas se hacen bastante engorrosas. La investigación del comportamiento de las magnitudes  $P_k(n)$  y  $P(n) = \sum_{k=1}^n P_k(n)$  (el

Tabla 1.1

k	n	Números $P_k(n)$									
		1	2	3	4	5	6	7	8	9	10
1		1	1	1	1	1	1	1	1	1	1
2			1	1	2	2	3	3	4	4	5
3				1	1	2	3	4	5	7	8
4					1	1	2	3	5	6	9
5						1	1	2	3	5	7
6							1	1	2	3	5
7								1	1	2	3
8									1	1	2
9										1	1
10											1
$P(n) = \sum_k P_k(n)$		1	2	3	5	7	11	15	22	30	42

número de toda clase de particiones del número  $n$ ) para grandes valores de  $k$  está ligada con dificultades considerables. Se ha hallado el valor aproximado

$$P_k(n) \sim \frac{1}{k!} \binom{n-1}{k-1},$$

el cual en la práctica resulta suficiente. Para  $P(n)$  queda determinada una relación recurrente

$$P(n) = P(n-1) + P(n-2) - P(n-5) - P(n-7) + \dots \\ \dots + (-1)^{k-1} P\left(n - \frac{3k^2 \pm k}{2}\right) + \dots$$

y están calculados los primeros valores sucesivos de esta magnitud.

Todas estas cuestiones y otras semejantes se analizan en la teoría de las particiones (véase [16]).

Aproximadamente desde la mitad del siglo anterior, merced a los esfuerzos de Darfi, Ferrers, Sylvester, y más tarde, de MacMahon, en la teoría de las particiones entró la interpretación de las mismas con ayuda de los grafos puntuales. Por ejemplo, la partición  $29 = 7 + 7 + 5 + 3 + 3 + 2 + 2$  está expuesta en la fig. 1.4.

Las partes de las particiones se disponen, como regla, de arriba abajo en el orden de decrecimiento. Del análisis de los correspondientes grafos  $n$ -puntuales (llamados también grafos de Ferrers) pueden directamente obtenerse los resultados siguientes.

1. El número de particiones de un  $n$ -conjunto en las que la mayor parte

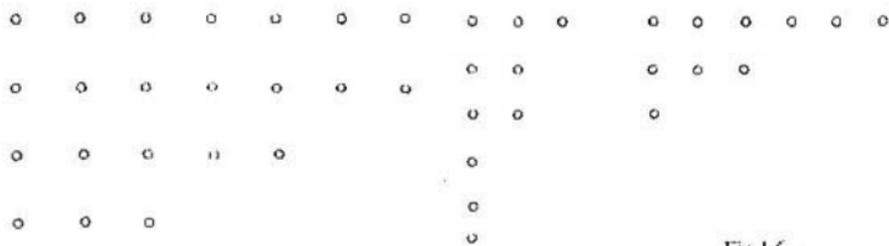


Fig. 1.4.

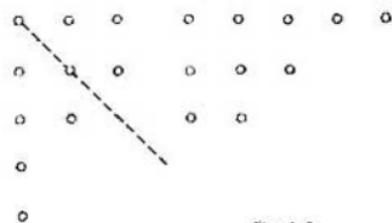


Fig. 1.5

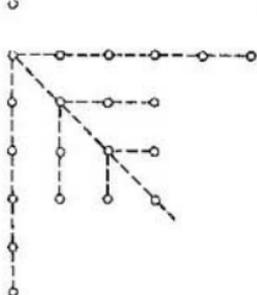


Fig. 1.6.

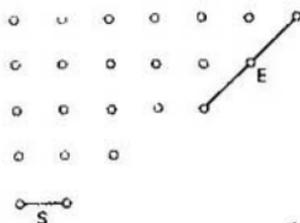


Fig. 1.7.

Fig. 1.8.

tiene  $k$  elementos, es igual al número de partes, es decir, a  $P_k(n)$ . Este teorema se demuestra por transposición del grafo de Ferrers respecto de la diagonal principal; tales grafos se denominan conjugados. Así, por ejemplo, en la fig. 1.5 el conjunto de 10 elementos está partido en 5 partes:  $10 = 3 + 3 + 2 + 1 + 1$ ; al efectuar la transposición, obtenemos:  $10 = 5 + 3 + 2$ , es decir, la partición del 10-conjunto en la cual la parte mayor contiene 5 elementos (una situación análoga se muestra en la fig. 1.6:  $10 = 3 + 2 + 2 + 1 + 1 + 1$  antes de la transposición, y  $10 = 6 + 3 + 1$ , después de la transposición).

2. El número de particiones autoconjugadas de un  $n$ -conjunto (una partición se llama autoconjugada, si el grafo de Ferrers que le corresponde es simétrico respecto de la diagonal principal) es igual al número de particiones del mismo conjunto en subconjuntos desiguales que se componen de un número impar de elementos. El teorema recíproco es también lícito.

Así, por ejemplo, a la partición autoconjugada del 20-conjunto  $20 = 6 + 4 + 4 + 4 + 1 + 1$  (fig. 1.7) le corresponde biunívocamente la partición  $20 = 11 + 5 + 3 + 1$ , si los puntos de la primera columna dispuestos debajo de la diagonal los trasladamos a la primera fila, de la segunda columna, a la segunda fila, etc.

3. El número de particiones de un  $n$ -conjunto en partes diferentes es igual al número de particiones del mismo conjunto en partes, compuestas de un número impar de elementos.

Sea dada una partición del  $n$ -conjunto (por ejemplo,  $n = 34$ ) en componentes impares ( $34 = 5 + 5 + 5 + 5 + 3 + 3 + 3 + 1 + 1 + 1 + 1$ ). Todas las componentes impares iguales se reúnen en grupos (4 de cinco, 3 de tres y 5 unidades) y se escriben los números de sus repeticiones (4, 3 y 5) en el sistema binario ( $4 = 2^2$ ;  $5 = 2^2 + 2^0$ ;  $3 = 2^1 + 2^0$ ). Escribamos la nueva partición, teniendo en cuenta la representación binaria obtenida ( $34 = 5 \cdot 4 + 3 \cdot 3 + 1 \cdot 5 = 5 \cdot 2^2 + 3 \cdot 2^1 + 3 \cdot 2^0 + 1 \cdot 2^2 + 1 \cdot 2^2 + 1 \cdot 2^0 = 20 + 6 + 3 + 4 + 1$ ). Este procedimiento es siempre factible, pues cualquier número se escribe de un modo único en el sistema binario. Siempre se puede razonar también del modo inverso.

4. Si  $Q_n$  y  $Q'_n$  son los números de particiones del  $n$ -conjunto en un número par e impar, respectivamente, de las partes desiguales entre sí, entonces

$$Q_n = \begin{cases} Q'_n, & \text{si } n \neq \frac{k}{2} (3k \pm 1); \\ Q'_k + (-1)^k, & \text{si } n = \frac{n}{2} (3k \pm 1); \end{cases}$$

donde  $k = 1, 2, \dots$

Supongamos que el grafo de Ferrers de la partición del  $n$ -conjunto en partes desiguales tiene la forma mostrada en la fig. 1.8.  $S$  es la parte menor de la partición y  $E$ , un conjunto de puntos (línea) dispuestos, a partir de la parte mayor, bajo un ángulo de  $45^\circ$ . Si  $|S| \leq |E|$ , entonces  $S$  se traslada al conjunto  $E$ ; en cambio, si  $|S| > |E|$ , viceversa,  $E$  se traslada a la parte menor  $S$ . Como resultado de tales traslaciones, tendremos el cambio de la paridad del número de partes desiguales de la partición. A toda partición par se le pone en correspondencia una impar y, además, biunívocamente:  $Q_n = Q'_n$ . Recomendamos que el lector mismo realice dicha operación con el siguiente ejemplo:  $7 + 6 + 5 + 3 + 2 \leftrightarrow 8 + 7 + 5 + 3$ .

Sin embargo, la operación no será posible, si las líneas  $S$  y  $E$  se intersecan y

$$|S| = |E|, \text{ o bien } |S| = |E| + 1.$$

Sea  $|E| = k$ . Entonces, en el primero de los casos exclusivos tendremos

$$n = k + (k + 1) + \dots + (2k - 1) = \frac{k}{2} (3k - 1);$$

y en el segundo:

$$n = (k + 1) + (k + 2) + \dots + 2k = \frac{k}{2} (3k + 1);$$

lo que demuestra nuestra afirmación.

## 1.5. SISTEMAS DE CONJUNTOS

Más arriba definimos la asignatura del análisis combinatorio, dimos una determinada información referente a la teoría de los conjuntos discretos finitos, indicamos las operaciones principales en las investigaciones combinatorias, explicamos los métodos de cálculo del número de entes combinatorios fundamentales, es decir, de muestras y ordenaciones, distribuciones y llenados. Todo lo dicho se realizó sólo para los conjuntos linealmente ordenados, y no para todos los casos posibles. Estas limitaciones fueron determinadas por el carácter introductor del capítulo.

No sería justo, sin embargo, concluir que los problemas tratados en el capítulo presente también son de importancia limitada y que el papel de los mismos es puramente pedagógico. La teoría general de los conjuntos discretos finitos es una asignatura matemática en desarrollo con sus propios problemas específicos. Además ocurre frecuentemente que a las investigaciones teóricas de los conjuntos finitos se reducen los problemas altamente prácticos.

Tomemos, por ejemplo, uno de los problemas sobre las particiones de un  $n$ -conjunto finito  $S$  en subconjuntos disjuntos. Analicemos las particiones  $\pi_1$  y  $\pi_2$ . Designemos, para un elemento  $s \in S$  por  $f_i(s)$  el número de elementos en el bloque de partición  $\pi_i$ , el cual contiene el elemento  $s$  ( $i = 1, 2$ ). Llamemos conjugadas las particiones  $\pi_1$  y  $\pi_2$ , si los pares ordenados de números  $(f_1(s), f_2(s))$  son distintos para todo  $s \in S$ .

**Ejemplo.** Sea  $S = \{1, 2, 3, 4, 5, 6\}$ . Definamos dos particiones:

$$\pi_1 : S = \{1, 2, 3\} \cup \{4, 5\} \cup \{6\};$$

$$\pi_2 : S = \{1, 4, 6\} \cup \{2, 5\} \cup \{3\}.$$

Obtendremos para ellas

$i$	1	2	3	4	5	6
$f_1(i), f_2(i)$	{3, 3}	{3, 2}	{3, 1}	{2, 3}	{2, 2}	{1, 3}

Por cuanto todos los pares ordenados  $\{f_1(i), f_2(i)\}$  son distintos,  $\pi_1$  y  $\pi_2$  serán particiones conjugadas del conjunto  $S$ . Con relación a estas particiones conjugadas se ha demostrado [35] que un par de estas particiones existe, si y sólo si  $n \neq 2, 5, 9$ . Este resultado se ha obtenido al resolver el siguiente problema sobre la identificación de los cables telefónicos multifilares.

Sea dado un cable de  $n$  conductores indistinguibles. Se pide fijar en sus extremos  $A$  y  $B$  los bornes  $A_i, B_i; i = 1, 2, \dots, n$ , que correspondan a cada conductor. El método de resolución consiste en unir los grupos de extremos de los conductores por un lado del cable y en probar el paso de la corriente que se mide por otro lado del cable. Expliquemos esto más detalladamente con un ejemplo de un cable de seis conductores.

Tomemos el extremo  $A$  con bornes  $A_1, A_2, \dots, A_6$ , y unamos sus bornes de acuerdo con la partición  $\pi_1$  (posición I en la fig. 1.9). Supongamos que

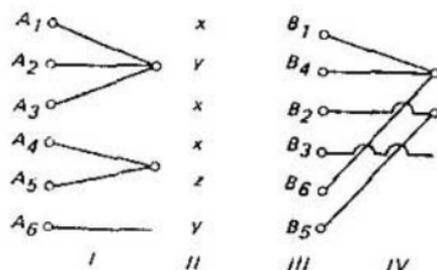


Fig. 1.9.

como resultado de la comprobación por el lado del extremo  $B$  (con bornes  $B_1, B_2, \dots, B_6$ ) se ha obtenido la situación que se indica en la fig. 1.9 mediante la posición II. Los bornes indistinguibles  $B_1, B_2, B_3$  se denotan con  $x$ , los bornes  $B_4$  y  $B_5$  con  $y$ , y el  $B_6$  con  $z$ ; unamos los bornes en el extremo  $B$  de acuerdo con la partición  $\pi_2$  (posición III). A continuación, al desconectar los bornes en el extremo  $A$ , comprobamos cuántos y cuáles conductores por el lado  $A$  quedan conectados en el extremo  $B$ . Admitamos, por ejemplo, que el conductor  $A_1B_1$  resultó conectado con un solo borne en el extremo  $B$ . Por cuanto sabemos que el borne  $A_1$  pertenece al conjunto  $\{A_1, A_2, A_3\}$ , mientras que el borne en el extremo  $B$  integra el conjunto de dos bornes unidos (a saber,  $B_2$  y  $B_3$ ), y por cuanto el par  $\{f_1(i), f_2(i)\} = \{3, 2\}$  corresponde solamente a  $i = 2$ , concluimos que  $A_1$  está conectado con  $B_2$ . Análogamente, si el borne  $A_5$  está conectado con dos otros bornes por el lado  $B$  (es decir, el conductor  $A_5B_5$  pertenece al conjunto de tres conductores que quedaban conectados), entonces  $A_5$  debe ser conectado con  $B_4$  (dado que al par  $(2, 3)$  corresponde  $i = 4$ ), etc.

Este algoritmo fue extendido también al caso general. Sea  $I$  un  $n$ -conjunto de números enteros  $I = \{1, 2, \dots, n\}$ . Supongamos que para  $I$  existen dos particiones conjugadas:

$$\pi_1 : I = P_1 \cup P_2 \cup \dots \cup P_k;$$

$$\pi_2 : I = P'_1 \cup P'_2 \cup \dots \cup P'_k.$$

En el extremo  $A$  unamos primeramente los conductores de acuerdo con la partición  $\pi_1$ , es decir, conductores en los cuales los números de los bornes pertenecen a cierto  $P_l \in \pi_1$ ;  $l = 1, 2, \dots, k$ . En el extremo  $B$  elegimos por comprobación los subconjuntos  $S_1, S_2, \dots, S_k$  de bornes de aquellos conductores que fueron conectados en el extremo  $A$ , y enumeramos los bornes en el extremo  $B$  de un modo tal que, cualquiera que sea  $S_r$ , el conjunto de índices de los bornes  $B_i$  que se encuentran en  $S_r$  sea exactamente un subconjunto de  $\pi_1$ . Ahora unamos los conductores en el extremo  $B$  en grupos  $T_1, T_2, \dots, T_k$ , donde  $T_j$  consta de todos aquellos conductores con bornes  $B_i$ , para los cuales  $i \in P'_j$ . Separando todas las conexiones en el extremo  $A$ , escogemos los conductores por el lado de  $A$  que están conectados en el extremo  $B$ .

Realizada esta operación, podemos encontrar los bornes "izquierdo" y "derecho" para un mismo conductor. En efecto, sea  $A_u$  algún conductor

que hemos cogido, y supongamos que en el extremo  $B$  dicho conductor integra el grupo  $T_j$ , el cual tiene, digamos,  $p$  elementos (de donde hallamos este número  $p$ ). Por cuanto se sabe el número de elementos en el subconjunto  $S_i$ , en el que está contenido  $A_u$  (admitamos que es igual a  $q$ ), entonces, basándonos en el procedimiento de construir  $S_i$  y  $T_j$ , y en que todos los pares  $(p, q) = [f_1(u), f_2(u)]$  son diferentes, podemos encontrar el único  $B_{iu}$  tal que  $A_u$  y  $B_{iu}$  sean extremos de un mismo conductor.

En muchas ramas de las matemáticas y en sus aplicaciones se plantean y se resuelven problemas que no sólo se reducen al análisis de los conjuntos discretos y de sus sistemas, sino que, además se enuncian en términos de los mismos. Así, por ejemplo, sucede en la teoría de los autómatas finitos, en la técnica de cómputo discreta, problemas aplicados del álgebra, etc. Describamos unos cuantos problemas tipo que se encuentran muy a menudo.

**Familias de Sperner.** Se dice que los subconjuntos  $S_1, S_2, \dots, S_m$  de un conjunto finito  $S$  forman una familia de Sperner, siempre que ninguno de ellos está contenido en el otro. Sea  $|S| = n$ . ¿Cuál será el número máximo posible  $m$  de términos en la familia de Sperner? La respuesta a esta pregunta lleva el nombre del teorema de Sperner (véase cap. 8):  $m = \binom{n}{[n/2]}$ <sup>1)</sup>.

**Sistemas separadores.** Este concepto fue introducido por A. Rényi [36] al analizar los problemas de la teoría de información. Un sistema de subconjuntos  $\{S_1, S_2, \dots, S_m\}$  de un conjunto finito  $S$  se denomina separador, si en el mismo, para cualesquiera dos elementos distintos del conjunto  $S$ , existe un subconjunto  $S_i$  que contiene sólo un elemento de todos los mencionados. A. Rényi planteó el problema de hallar un sistema separador mínimo bajo la condición de que cada subconjunto de este sistema consta exactamente de un número dado de elementos. Este problema fue analizado en [37].

**Problemas sobre los subconjuntos que se intersecan.** Existen varios problemas en los que se introducen limitaciones en la potencia de los propios subconjuntos  $S_1, S_2, \dots, S_m \subseteq S$  y de sus intersecciones. Se requiere determinar el número máximo ( $m$ ) de subconjuntos que satisfagan dichas condiciones para  $n = |S|$  fijo. Con este motivo recomendamos la obra [38]. Demos a conocer el resultado clásico de Erdős, Chao Ko, Rado [39]. Supongamos que

- 1) cada uno de los subconjuntos  $S_1, S_2, \dots, S_m$  contiene no más de  $k$  elementos, donde  $k \leq n/2$ ;
- 2) ninguno de los subconjuntos está contenido en el otro;
- 3) cualesquiera dos subconjuntos se intersecan. En este caso el número

<sup>1)</sup> Con  $[x]$  se denota el número máximo entero que no sobrepasa  $x$ ; con  $\{x\}$ , el número entero mínimo, superior o igual a  $x$ .

máximo posible de subconjuntos será  $\binom{n-1}{k-1}$ . Precisamente este número de términos tiene el sistema de todos los  $k$ -subconjuntos del  $n$ -conjunto  $S$  en los que está contenido cierto elemento fijo  $s \in S$ .

**Recubrimientos y empaques.** El problema de construcción de los mejores códigos conduce al siguiente problema combinatorio: hallar el número máximo  $m$ , para el cual existe un sistema de subconjuntos  $\{S_1, S_2, \dots, S_m\}$  de  $r$  elementos del  $n$ -conjunto  $S$ , donde  $|S_i \cap S_j| < t$  para cualesquiera  $1 \leq i < j \leq m$ . Dicho de otro modo, se requiere que cada  $t$ -subconjunto del conjunto  $S$  se contenga a lo sumo en uno de los subconjuntos del sistema. Este problema se denomina *problema de empaques*. También se analiza con frecuencia el problema inverso. Exijamos que cada  $t$ -subconjunto se contenga no menos que en uno de los subconjuntos del sistema; se pregunta qué cantidad mínima de  $r$ -subconjuntos del  $n$ -conjunto  $S$  es necesaria para que se pueda formar tal sistema. Este problema se denomina *problema de recubrimientos*. Al igual que el problema de empaques, él está resuelto por ahora sólo en algunos casos particulares (por ejemplo, para  $r = 3, t = 2$ ;  $r = 4, t = 2$ ). Si en lugar de los subconjuntos  $S_1, S_2, \dots, S_m$  estudiamos complementos de los mismos  $S'_1, S'_2, \dots, S'_m$ , donde  $S'_i = S \setminus S_i$ , y ponemos  $k = n - t, l = n - r$ , obtendremos otra forma del problema de recubrimientos: ¿qué número mínimo de  $l$ -subconjuntos del  $n$ -conjunto  $S$  es necesario para que en cualquier  $k$ -subconjunto de conjunto  $S$  se contenga por lo menos uno de los  $l$ -subconjuntos elegidos. Este número lleva el nombre de *número de Turán*  $T(n, k, l)$ . En el año 1941 Turán [40] demostró que

$$T(n, k, 2) = mn - \frac{m(m+1)}{2} (k-1) \text{ para } m \leq \frac{n}{k-1} \leq m+1.$$

Pese a que la formulación es sencilla, el problema de hallar los números de Turán resulta ser, en el caso general, exclusivamente difícil. Para  $l \geq 3$  se han obtenido pocos resultados. Se conoce (véase [41]) que

$$T(n, k, l) = n - (k-1) \text{ para } 1 \leq \frac{n}{k-1} \leq \frac{l}{l-1}.$$

$$T(n, k, l) = \left\lfloor \frac{\left( \left\lfloor \frac{3l}{2} \right\rfloor - 1 \right) n - \left\lfloor \frac{3l}{2} \right\rfloor (k-1)}{\left\lfloor \frac{l}{2} \right\rfloor} \right\rfloor$$

$$\text{para } \frac{l}{l-1} \leq \frac{n}{k-1} \leq \frac{\left\lfloor \frac{3l}{2} \right\rfloor \left\lfloor \frac{l}{2} \right\rfloor}{\left\lfloor \frac{3l}{2} \right\rfloor - 2}.$$

La propiedad  $\emptyset$ . Suele decirse que un sistema de subconjuntos  $S_1, S_2,$

...,  $S_m \subseteq S$  posee la propiedad  $\mathcal{B}$ , si existe tal partición del conjunto  $S = S' \cup S''$  ( $S' \cap S'' = \emptyset$ ), que  $S_i \not\subseteq S'$ ,  $S_i \not\subseteq S''$  ( $i = 1, 2, \dots, m$ ). Se imponen las restricciones  $|S| = n$ , y  $|S_1| = |S_2| = \dots = |S_m| = k$ , y se busca el número mínimo  $m = m(n, k)$  de subconjuntos en un sistema que no posea la propiedad  $\mathcal{B}$ . Este problema se analiza en el cap. 7.

Una clase importante más de problemas sobre los sistemas de conjuntos está relacionada con el teorema de Ramsey al que se dedica un párrafo aparte del capítulo 3.

El estudio de los sistemas de conjuntos es el problema principal en el análisis combinatorio. De los éxitos de dicho estudio depende tanto el enriquecimiento de la teoría de la combinatoria, como también la ampliación de los campos de aplicación.

## CAPÍTULO 2 FUNCIONES GENERATRICES

Durante mucho tiempo el contenido del análisis combinatorio lo constituía el cálculo del número de configuraciones de determinados tipos. Una parte de la teoría combinatoria que estudia estos problemas sigue jugando hoy día un papel importante en las aplicaciones.

En §§ 1.3 y 1.4 hemos considerado los métodos directos ("elementales") de cálculo. El presente capítulo se dedica a los métodos indirectos, con ayuda de los cuales se calcula la cantidad de configuraciones combinatorias.

### 2.1. FUNDAMENTOS DEL MÉTODO DE FUNCIONES GENERATRICES

El método de las funciones generatrices (generadoras) es uno de los más desarrollados en el análisis combinatorio. Las ideas fundamentales de este método fueron enunciadas por primera vez al final del siglo XVIII en las obras de Laplace referentes a la teoría de las probabilidades. Expliquemos las mismas con el siguiente ejemplo sencillo. Veamos el producto del número finito de binomios lineales

$$\prod_{r=1}^n (1 + x_r t) = \sum_{r=0}^n a_r t^r, \quad (1)$$

donde

$$a_r(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq n} x_{i_1} x_{i_2} \dots x_{i_r}$$

no son nada más que funciones simétricas elementales de las variables  $x_1, \dots, x_n$ . Observemos que a los sumandos del coeficiente  $a_r$  se les puede asignar las  $r$ -combinaciones de  $n$  elementos  $x_1, \dots, x_n$ . La expresión (1) se llamará *numerador* de las  $r$ -combinaciones de  $n$  elementos. Si ponemos en (1)  $x_i = 1$  para  $i = 1, \dots, n$ , obtendremos

$$\sum_{r=0}^n \binom{n}{r} t^r = (1 + t)^n, \quad (2)$$

puesto que  $a_r(1, \dots, 1)$  es el número de  $r$ -combinaciones de  $n$  elementos. Desarrollemos la función  $(1 + t)^n$  en potencias de  $t$  según la fórmula de Taylor:

$$(1 + t)^n = \sum_{r=0}^n \frac{n!}{r!(n-r)!} t^r. \quad (3)$$

(Este mismo resultado puede ser demostrado también por inducción respecto de  $n$ .)

De (2) y (3) se deduce

$$\sum_{r=0}^n \binom{n}{r} t^r = \sum_{r=0}^n \frac{n!}{r!(n-r)!} t^r. \quad (4)$$

Al igualar entre sí los coeficientes de iguales potencias de  $t$  en (4), obtenemos de nuevo (esta vez, analíticamente) el resultado del capítulo 1: el número de  $r$ -combinaciones de  $n$  elementos es igual a  $\frac{n!}{r!(n-r)!}$ . Al aplicar este resultado del capítulo 1 a la fórmula (2), obtendremos una demostración más de la identidad (3). Semejante método de determinar los coeficientes del desarrollo de las funciones era generalmente aceptado en la primera mitad del siglo XIX y se llamaba análisis combinatorio, a diferencia del análisis matemático al cual se referían los métodos analíticos de obtención de los desarrollos.

En la expresión (2) la función  $f(t) = (1+t)^n$  está biunívocamente relacionada con una sucesión de los números

$$\left\{ \binom{n}{r} \right\}, \quad r = 0, 1, 2, \dots, n.$$

Tal relación resulta muy útil: atribuyendo en la fórmula (2) diferentes valores particulares a la variable  $t$ , se pueden obtener muchas identidades importantes. Así, por ejemplo, para  $t = 1$  y  $t = -1$  tenemos

$$2^n = \sum_{r=0}^n \binom{n}{r} = 1 + n + \binom{n}{2} + \binom{n}{3} + \dots + \binom{n}{n},$$

$$0 = \sum_{r=0}^n (-1)^r \binom{n}{r} = 1 - n + \binom{n}{2} - \binom{n}{3} + \dots + (-1)^n \binom{n}{n};$$

respectivamente. La adición y sustracción de estas expresiones término a término nos da

$$\sum_{r=0}^n \binom{n}{2r} = \sum_{r=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2r+1} = 2^{n-1},$$

mientras que la simple división de los factores

$$(1+t)^n = (1+t)^m (1+t)^{n-m}$$

conduce a la identidad

$$\binom{n}{r} = \sum_{k=0}^r \binom{n-k}{k} \binom{m}{r-k},$$

que se conoce como convolución de Vandermonde. Por fin, al sustituir en (2)  $t = a/b$ , y al multiplicar por  $b^n$  los miembros primero y segundo, obtenemos seguidamente el *teorema binomial* (la fórmula binomial):

$$(a + b)^n = \sum_{r=0}^n \binom{n}{r} a^r b^{n-r}.$$

debido a lo cual los números  $\binom{n}{r}$  se llaman *coeficientes binomiales*.

**Ejercicio.** Demuéstrese, por inducción respecto a  $m$ , el teorema binomial:

$$\left( \sum_{r=1}^m a_r \right)^n = \sum_{n_1! n_2! \dots n_m!} \frac{n!}{n_1! n_2! \dots n_m!} a_1^{n_1} a_2^{n_2} \dots a_m^{n_m},$$

donde la suma se calcula respecto a todas las soluciones de la ecuación  $n_1 + n_2 + \dots + n_m = n$  en números enteros no negativos; los coeficientes en el segundo miembro se llaman polinomiales y ya aparecieron en el capítulo I como números de las  $(n_1, n_2, \dots, n_m)$ -particiones del  $n$ -conjunto.

La función  $f(t) = (1 + t)^n$  se denomina *función generatriz* de una sucesión de números  $\left\{ \binom{n}{r} \right\}$ , o bien, más brevemente, función generadora del número de  $r$ -combinaciones de  $n$  elementos,  $r = 0, 1, 2, \dots, n$ .

Examinemos ahora una sucesión numérica  $a = (a_0, a_1, a_2, \dots)$ , o bien, de otro modo, la función  $a_n$  de un argumento de número entero  $n$ . A esta función le corresponde biunívocamente la serie

$$f_a(t) = \sum_{n=0}^{\infty} a_n t^n, \quad (5)$$

la cual es más cómoda y simple en las operaciones, particularmente cuando ella converge a una función que posee una forma analítica conveniente. La serie  $f_a(t)$  se llama *función generatriz* de la sucesión  $a$ . Así pues, las funciones generatrices permiten pasar del análisis de magnitudes aisladas (por ejemplo, de las  $r$ -combinaciones para un valor particular  $r$ ) al análisis de sus sucesiones e, incluso, de las clases de sucesiones.

Para la mayoría de los problemas combinatorios la serie (5) es finita. Si esta serie es, sin embargo, infinita y el radio de su círculo de convergencia es igual a cero, las operaciones con ella son posibles sólo dentro del álgebra de las series de potencias formales, el cual se analizará en el párrafo que viene.

## 2.2. TIPOS DE FUNCIONES GENERATRICES Y DE NUMERADORES

Sea  $R$  cierto anillo con la unidad. El anillo  $S(R)$  de sucesiones sobre  $R$  y el anillo  $R[[t]]$ , isomorfo a  $S(R)$ , de series de potencias formales sobre  $R$  se definen del modo siguiente. Los elementos del anillo  $S(R)$  son las sucesiones

$$\{a\} = \{(a_0, a_1, a_2, \dots)\}, \quad (1)$$

y los elementos correspondientes del anillo  $R[[t]]$  son las series

$$\{F_a(t)\}, F_a(t) = \sum_{r=0}^{\infty} a_r t^r. \quad (2)$$

Se llama suma de las sucesiones  $a = (a_0, a_1, \dots)$  y  $b = (b_0, b_1, \dots)$  a la sucesión

$$c = a + b = (a_0 + b_0, a_1 + b_1, \dots) = (c_0, c_1, \dots),$$

y se llama suma de las series  $F_a(t)$  y  $F_b(t)$ , pertenecientes a la clase (2), a la serie  $F_c(t) = F_a(t) + F_b(t)$ :

$$F_c(t) = \sum_{r=0}^{\infty} c_r t^r,$$

donde  $c_r = a_r + b_r$ .

Se denomina producto (o convolución) de las sucesiones  $a$  y  $b$  de la clase (1) a la sucesión  $a \times b = d = (d_0, d_1, \dots)$ , en la cual

$$d_r = a_0 b_r + a_1 b_{r-1} + \dots + a_r b_0, \quad r = 0, 1, \dots, \quad (3)$$

y producto (convolución) de las series  $F_a(t)$  y  $F_b(t)$  de la clase (2), a la serie

$$F_a(t) = F_a(t) \times F_b(t) = \sum_{r=0}^{\infty} d_r t^r,$$

donde  $d_r$  se determina según la fórmula (3).

Definamos ahora: el cero en la clase (1) como una sucesión (nula)

$$0 = (0, 0, \dots),$$

entonces el cero en la clase (2) es la serie correspondiente a  $O$

$$F_0(t) = 0;$$

la unidad en la clase (1) como una sucesión (unitaria)

$$e = (1, 0, 0, \dots),$$

entonces la unidad en la clase (2) será una serie correspondiente a  $e$ :

$$F_e(t) = 1.$$

Por fin, un elemento inverso para  $a \in S(R)$  respecto de la adición en la clase (1) es  $-a = (-a_0, -a_1, \dots)$ , y el elemento correspondiente inverso pa-

ra  $F_a(t)$  en la clase (2) será

$$-F_a(t) = F_{-a}(t) = \sum_{r=0}^{\infty} (-a_r)t^r.$$

Es fácil ver que todos los axiomas del anillo para  $S(R)$  y  $R[[t]]$  tienen lugar.

Sea  $a_0$  un elemento invertible del anillo  $R$ ; buscamos  $a^{-1} = a'$ , partiendo de la condición  $a \times a' = e$ , es decir,

$$\begin{aligned} a_0 a'_0 &= 1, \\ a_1 a'_0 + a_0 a'_1 &= 0, \\ &\dots \dots \dots \\ a_k a'_0 + a_{k-1} a'_1 + a_{k-2} a'_2 + \dots + a_0 a'_k &= 0, \\ &\dots \dots \dots \end{aligned}$$

de donde encontramos  $a'_k$  ( $k = 0, 1, \dots$ ) de las primeras  $k + 1$  ecuaciones, empleando el cálculo sucesivo por el método de Gauss (o bien por el de Cramer). Por consiguiente, sólo para las sucesiones  $a$ , tales que  $a_0$  es invertible, existen  $a^{-1}$  y  $F_a^{-1}(t)$  en los anillos  $S(R)$  y  $R[[t]]$ .

En los anillos  $S(R)$  y  $R[[t]]$  puede introducirse la diferenciación  $D$ : para  $a = (a_0, a_1, \dots)$ ,  $Da = (a_1, 2a_2, \dots, na_n, \dots)$ ,

$$DF_a(t) = \sum_{n=1}^{\infty} n a_n t^{n-1},$$

y la integración  $\int$ :

$$\int a = \left(0, a_0, \frac{a_1}{2}, \dots, \frac{a_n}{n+1}\right), \quad \int F_a(t) = \sum_{n=0}^{\infty} \frac{a_n}{n+1} t^{n+1}.$$

**Ejercicio 1.** Demuéstranse las siguientes propiedades de las aplicaciones  $D$  y  $\int$  en  $S(R)$ :

- 1)  $D(a + b) = Da + Db$ ; 2)  $\int(a + b) = \int a + \int b$ ;
- 3)  $D \int a = a$ ; 4)  $\int Da = a$ ;
- 5)  $D(a \times b) = (Da) \times b + a \times Db$ ;

y las propiedades correspondientes en el anillo  $R[[t]]$ .

Si el anillo  $R$  es un álgebra sobre el campo  $P$ , entonces, al introducir en  $S(R)$  y en  $R[[t]]$  las operaciones de multiplicación por  $\alpha \in P$ :

$$\alpha a = (\alpha a_0, \alpha a_1, \dots), \quad \alpha F_a(t) = \sum_{r=0}^{\infty} (\alpha a_r) t^r,$$

convertimos  $S(R)$  y  $R[[t]]$  en álgebras isomórfas.

Volvamos ahora a las sucesiones que aparecen en los problemas combinatorios, es decir, al álgebra  $S(\mathbf{R})$  de sucesiones sobre el campo  $\mathbf{R}$  de números reales. Para la sucesión  $a \in S(\mathbf{R})$ , la serie  $F_a(t) \in R[[t]]$  lleva el nombre de *función generatriz ordinaria*, mientras que la propia álgebra  $R[[t]]$  se deno-

mina álgebra de Cauchy. Las funciones generatrices ordinarias se usan al analizar las familias de sucesiones cuyos elementos están constituidos por las funciones de las  $r$ -muestras no ordenadas ( $r$ -combinaciones).

Para la construcción de los mismos objetos combinatorios (de las  $r$ -combinaciones) emplearemos el álgebra  $\mathbf{R}(x; t) = \mathbf{R}[x_1, x_2, \dots][[t]]$  de series de potencias formales sobre el álgebra  $\mathbf{R}[x_1, x_2, \dots]$  de polinomios de las variables  $x = \{x_1, x_2, \dots\}$  sobre el campo de números reales. El álgebra  $\mathbf{R}(x; t)$  se llamará *numeradora*, y las series, cuyos coeficientes serán polinomios que enumeran los objetos combinatorios construidos por nosotros, *numeradores* de dichos objetos.

Recordemos que la aplicación  $M: A_1 \rightarrow A_2$ , realizada del álgebra  $A_1$  sobre el campo  $P$  en el álgebra  $A_2$  sobre  $P$ , se denomina *operador lineal*, si  $M(a + b) = Ma + Mb$  y  $M(\alpha a) = \alpha Ma$  para cualesquiera  $a, b \in A_1, \alpha \in P$ . La aplicación  $M$  se denomina *operador multiplicativo*, si  $M(ab) = (Ma)(Mb)$  para cualesquiera  $a, b \in A_1$ . Usaremos con frecuencia la aplicación  $T: \mathbf{R}(x; t) \rightarrow \mathbf{R}[[t]]$  que convierte todos los  $x_i$  en 1.

Ejercicio 2. Demuéstrase que la aplicación  $T$  es un operador multiplicativo lineal.

Ejercicio 3. Demuéstrase que las aplicaciones  $D$  y  $\int$  sobre el álgebra  $\mathbf{R}(x; t)$  son operadores lineales.

EJEMPLO 1. Hállense el numerador y la función generatriz para las  $r$ -combinaciones de  $n$  elementos.

Este problema ya lo hemos resuelto en el § 2.1: el numerador de las  $r$ -combinaciones de  $n$  elementos está dado por la serie (1) en el álgebra numeradora  $\mathbf{R}(x; t)$ , y la función generatriz, por la serie (4) en la subálgebra  $\mathbf{R}[[t]]$  de la misma.

EJEMPLO 2. Hállense el numerador y la función generatriz para las  $r$ -combinaciones con repeticiones del tipo  $(\Lambda_1, \dots, \Lambda_n)$  de  $n$  elementos, donde  $\Lambda_i$  es un subconjunto del conjunto  $\mathbf{N}_0$  de números enteros no negativos; el elemento  $a_i$  puede estar presente en las  $r$ -combinaciones  $\lambda$  veces, siempre que  $\lambda \in \Lambda_i$ .

Al elemento  $a_i$  del  $n$ -conjunto  $S$  pongámosle en correspondencia una variable  $x_i$  en  $\mathbf{R}(x; t)$ , entonces, a la aparición del elemento  $a_i$  en la  $r$ -combinación corresponderá, o bien  $\lambda_1$  veces, ..., o bien  $\lambda_2$  veces, la serie  $x_i^{\lambda_1} t^{\lambda_1} + x_i^{\lambda_2} t^{\lambda_2} + \dots$ . Por eso, el numerador buscado tendrá la expresión

$$\sum_{r=0}^{\infty} a_r t^r = \prod_{i=1}^n \sum_{\lambda \in \Lambda_i} x_i^{\lambda} t^{\lambda}. \quad (4)$$

La función generatriz tiene en este caso la forma

$$F(t) = \prod_{i=1}^n \sum_{\lambda \in \Lambda_i} t^{\lambda} \quad (5)$$

(a los miembros primero y segundo de (4) se ha aplicado el operador lineal  $T$ , que convierte todos los  $x_i$  en 1). Al desarrollar (5) en potencias de  $t$ , llegamos a que el número de  $r$ -combinaciones del tipo  $(\lambda_1, \dots, \lambda_n)$  de  $n$  elementos

es igual al número de soluciones de la ecuación  $y_1 + \dots + y_n = r$  con las incógnitas  $y_i \in \Lambda_i$ ,  $i = 1, \dots, n$ .

**EJEMPLO 3.** Hállense el numerador y la función generatriz, para las  $r$ -combinaciones con repeticiones ilimitadas de  $n$  elementos.

Reduciremos nuestro problema al anterior, si ponemos  $\Lambda_i = \mathbf{N}_0$ ,  $i = 1, \dots, n$ . El numerador (4) adopta la forma:

$$\sum_{r=0}^{\infty} a_r t^r = \prod_{i=1}^n (1 + x_i t + x_i^2 t^2 + \dots) = \sum_{i=1}^n \frac{1}{1 - x_i t}.$$

De aquí (ó de (5)) encontramos la función generatriz:

$$\begin{aligned} f(t) &= (1 + t + t^2 + \dots)^n = (1 - t)^{-n} = \\ &= \sum_{r=0}^{\infty} \frac{(-n)(-n-1)\dots(-n-r+1)}{n!} (-1)^r t^r = \\ &= \sum_{r=0}^{\infty} \binom{n+r-1}{r} t^r = \sum_{r=0}^{\infty} \binom{-n}{r} (-t)^r, \end{aligned}$$

donde se ha puesto por definición

$$\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}.$$

De aquí tenemos la sucesión  $b = (b_0, b_1, \dots)$ , donde  $b_r = \binom{n+r-1}{r}$  es el número de  $r$ -combinaciones con repetición de  $n$  elementos. Este resultado concuerda con el obtenido antes (véase § 1.3).

**EJEMPLO 4.** Hállense el numerador y la función generatriz de las  $r$ -combinaciones con repetición, en las cuales figura por lo menos un elemento de cada tipo.

Pongamos, en las condiciones del ejemplo 2,  $\Lambda_i = \mathbf{N} = \{1, 2, \dots\}$ ,  $i = 1, \dots, n$ . Entonces, de (4) obtenemos el numerador buscado:

$$\sum_{r=0}^{\infty} a_r t^r = \prod_{i=1}^n (x_i t + x_i^2 t^2 + \dots) = t^n \prod_{i=1}^n \frac{x_i}{1 - x_i t}.$$

De aquí tenemos la función generatriz:

$$f(t) = (t + t^2 + \dots)^n = t^n (1 - t)^{-n} = t^n \sum_{r=0}^{\infty} \binom{n+r-1}{r} t^r.$$

Al realizar la sustitución  $n + r = k$ , obtenemos

$$f(t) = \sum_{k=n}^{\infty} \binom{k-1}{k-n} t^k = \sum_{k=n}^{\infty} \binom{k-1}{n-1} t^k.$$

Por consiguiente, el número de  $r$ -combinaciones buscadas es igual a 0 para  $r < n$ , y a  $\binom{r-1}{n-1}$ , para  $r \geq n$ .

**EJEMPLO 5.** Hállense el numerador y la función generatriz para las  $r$ -combinaciones de  $n$  elementos, donde se admite sólo un número par de apariciones para cada uno de los elementos.

Suponiendo en las condiciones del ejemplo 2,  $\Lambda_i = \{0, 2, 4, \dots\}$ ,  $i = 1, \dots, n$ , tenemos de (4) el numerador buscado:

$$\sum_{r=0}^{\infty} a_r t^r = \prod_{i=1}^n (1 + x_i^2 t^2 + x_i^4 t^4 + \dots) = \prod_{i=1}^n \frac{1}{1 - x_i^2 t^2}.$$

De aquí obtenemos la función generatriz

$$f(t) = (1 + t^2 + t^4 + \dots)^n = (1 - t^2)^{-n} = \sum_{r=0}^{\infty} \binom{n+r-1}{r} t^{2r}.$$

Ahora podemos obtener una identidad interesante: por cuanto  $(1 - t^2)^{-n} = (1 - t)^{-n}(1 + t)^{-n}$ , la comparación de los coeficientes de las potencias de  $t$  en los miembros primero y segundo nos da:

$$\sum_{k=0}^r (-1)^k \binom{n+r-k-1}{r-k} \binom{n+k-1}{k} = \begin{cases} 0, & \text{para } r \text{ impar,} \\ \binom{n+s-1}{s}, & \text{para } r = 2s. \end{cases}$$

**Ejercicio 4.** Hállense el numerador y la función generatriz para las  $r$ -combinaciones de  $n$  elementos, donde se admiten a lo sumo  $j$  repeticiones de cada elemento.

Pasemos ahora a la construcción de la teoría analítica para la enumeración de las  $r$ -muestras ordenadas o de las  $r$ -permutaciones.

En los márgenes del álgebra  $\mathbf{R}[x_1, x_2, \dots][[t]]$  de series de potencias formales con los coeficientes del álgebra de polinomios  $\mathbf{R}[x_1, x_2, \dots]$  sobre un campo  $\mathbf{R}$  de variables  $x_1, x_2, \dots$ , que no conmutan entre sí, examinemos la expresión

$$\frac{1}{n!} \sum_{\pi \in S_n} \prod_{i=1}^n (1 + x_{\pi(i)} t) = \sum_{r=0}^n a_r(x_1, x_2, \dots) \frac{t^r}{r!}, \quad (1)$$

en la que la suma en el primer miembro se toma por todas las sustituciones de grupo simétrico  $S_n$  de sustituciones de un  $n$ -conjunto. No es difícil ver que en el coeficiente de  $t^r$  del desarrollo en potencias de  $t$  de la expresión

$$\sum_{\pi \in S_n} \prod_{i=1}^n (1 + x_{\pi(i)} t)$$

el número de apariciones del monomio  $x_{i_1} \dots x_{i_r}$  es igual al número de sustituciones de  $\pi \in S_n$  tales, que  $\pi^{-1}(i_1) < \pi^{-1}(i_2) < \dots < \pi^{-1}(i_r)$ . Las sustituciones de esta índole pueden construirse del modo siguiente: elegimos  $r$  lugares para las preimágenes de los elementos  $i_1, \dots, i_r$  empleando  $\binom{n}{r}$  méto-

dos, y los demás  $n - r$  elementos pueden permutarse mediante  $(n - r)!$  métodos. Por eso, el monomio que se examina aparece sólo  $\binom{n}{r} (n - r)! = n!/r!$  veces. Por consiguiente, el polinomio  $a_n^*(x_1, x_2, \dots)$  en (6) se compone de monomios, correspondientes a todas las  $r$ -permutaciones de elementos  $x_1, \dots, x_n$ . La serie (6) se denominará numerador exponencial de las  $r$ -permutaciones de  $n$  elementos.

Ahora, suponiendo en (6)  $x_i = t, i = 1, \dots, n$  (aplicamos a los términos primero y segundo el operador multiplicativo  $T$  que convierte todos los  $x_i$  en  $t$ ), obtenemos

$$(1 + t)^n = \sum_{r=0}^n P(n, r) \frac{t^r}{r!}, \quad (7)$$

donde  $P(n, r)$  es el número de  $r$ -permutaciones de  $n$  elementos. La función  $f(t) = (1 + t)^n$  se llamará función generatriz exponencial para el número de  $r$ -permutaciones de  $n$  elementos. Observemos que la fórmula (7) podía ser deducida inmediatamente de la fórmula (2) § 2.1, puesto que  $P(n, r) = a_n(1, \dots, r)!$  Al desarrollar  $(1 + t)^n$  en potencias de  $t$ , obtenemos

$$\sum_{r=0}^n P(n, r) \frac{t^r}{r!} = \sum_{r=0}^n \frac{n!}{(n - r)!} \frac{t^r}{r!},$$

y de aquí hallamos otra vez el número de  $r$ -permutaciones de  $n$  elementos:  $P(n, r) = n!/(n - r)!$ .

Sea  $R$  un anillo con la unidad. El anillo  $S^*(R)$  de sucesiones exponenciales sobre  $R$  y el anillo  $R^*[[t]]$  (isomorfo a  $S^*(R)$ ) de series de potencias formales sobre  $R$  se construyen del modo siguiente. El anillo  $S^*(R)$ , siendo un grupo aditivo, coincide con el grupo aditivo del anillo  $S(R)$ . La operación de multiplicación en  $S^*(R)$  será la convolución binomial de las sucesiones:  $ab = d = (d_0, d_1, \dots)$ , donde  $a = (a_0, a_1, \dots)$ ,  $b = (b_0, b_1, \dots)$ ,

$$d_r = \sum_{i=0}^r \binom{r}{i} a_i b_{r-i}. \quad (8)$$

La unidad y el cero en  $S^*(R)$  son los mismos que en el anillo  $S(R)$ . El elemento inverso respecto de la multiplicación para la sucesión  $a = (a_0, a_1, \dots)$  existe sólo en el caso de invertibilidad del elemento  $a_0$ , y se calcula a partir del sistema de ecuaciones, análogo al sistema, ya analizado, de ecuaciones en el anillo  $S(R)$ .

**Ejercicio 5.** Demuéstrese que en  $S^*(R)$  están cumplidos todos los axiomas del anillo, y la aplicación  $\sigma = (a_0, a_1, \dots, a_n, \dots) \rightarrow a' = (a_0, a_1, \dots, a_n/n!, \dots)$  es un isomorfismo de los anillos  $S(R)$  y  $S^*(R)$ .

Como elementos del anillo  $R^*[[t]]$  intervienen las series de potencias exponenciales

$$[E_a(t)], E_a(t) = \sum_{r=0}^{\infty} a_r \frac{t^r}{r!},$$

correspondientes a las sucesiones  $a = (a_0, a_1, \dots)$ . Las operaciones de adición y multiplicación se determinan del modo siguiente:

$$E_a(t) + E_b(t) = E_c(t) = \sum_{r=0}^{\infty} c_r \frac{t^r}{r!},$$

$$b = (b_0, b_1, \dots), c_r = a_r + b_r;$$

$$E_a(t) \times E_b(t) = E_d(t) = \sum_{r=0}^{\infty} d_r \frac{t^r}{r!},$$

donde  $d_r$  se halla por la fórmula (8). El cero y la unidad en  $R^*[[t]]$  son los mismos que en el anillo  $R[[t]]$ ; el elemento inverso respecto de la adición se determina análogamente; el elemento inverso respecto de la multiplicación se calcula igual que en el anillo  $S^*(R)$ . Si  $R$  es el álgebra sobre el campo  $P$ , entonces (lo mismo que en el caso de  $S(R)$ ) el anillo  $S^*(R)$  se transforma en el álgebra sobre  $P$ . Una construcción análoga se realiza también para el anillo  $R^*[[t]]$  sobre el álgebra  $R$ .

Ejercicio 6. Realícense para el anillo  $R^*[[t]]$  las construcciones y demostraciones omitidas en el texto.

De la definición del anillo  $R^*[[t]]$  se ve que en el caso de las series convergentes el producto formal coincide con el ordinario. La serie  $E_a(t)$  recibe el nombre de *función generatriz exponencial* para la sucesión  $a \in S^*(\mathbf{R})$ , y la propia álgebra  $R^*[[t]]$  se denomina álgebra de funciones generatrices exponenciales.

Ejercicio 7. Muéstrese que las álgebras  $\bar{R}^*[[t]]$  y  $R^*[[t]]$  son isomorfas.

De nuevo con el fin de realizar la construcción algebraica de las  $r$ -muestras ordenadas, examinemos el álgebra  $\bar{R}^*(x; t) = (\mathbf{R}[x_1, x_2, \dots])^*[[t]]$  de series de potencias exponenciales sobre el álgebra  $\bar{\mathbf{R}}[x_1, x_2, \dots]$  de polinomios con variables no conmutables, la cual llamaremos álgebra numeradora exponencial, y el álgebra  $R^*(x; t) = (\mathbf{R}[x_1, x_2, \dots])^*[[t]]$  de series de potencias exponenciales sobre el álgebra  $\mathbf{R}[x_1, x_2, \dots]$  de polinomios habituales que llamaremos álgebra numeradora exponencial reducida. Denotemos con  $\bar{T}^*$  la aplicación de  $\bar{R}^*(x; t)$  en  $R^*[[t]]$  que reemplaza todos los  $x_i$  por 1.

Ejercicio 8. Demuéstrese que  $\bar{T}^*$  es un operador lineal multiplicativo.

Designemos con  $U$  la aplicación que traslada una serie de  $\bar{R}^*(x; t)$  en la misma serie de  $R^*(x; t)$ , es decir, que permite que las variables  $x_i$  conmuten entre sí.

Ejercicio 9. Demuéstrese que  $U$  es un operador multiplicativo lineal.

Designemos con  $T^*$  la aplicación  $R^*(x; t)$  en  $R^*[[t]]$  que reemplaza todos los  $x_i$  por 1.

Ejercicio 10. Demuéstrase que  $T^*$  es un operador multiplicativo lineal.

Veamos la aplicación  $V: R^*(x; t) \rightarrow R^*(x; t)$ , la cual todo monomio  $x_{i_1} x_{i_2} \dots x_{i_r}$  con la especificación  $(\lambda_1, \dots, \lambda_n)$  (esto quiere decir que  $x_1$  se encuentra  $\lambda_1$  veces,  $x_2$ ,  $\lambda_2$  veces, etc.) en el coeficiente de  $t^k/k!$  lo transforma en el polinomio

$$\frac{\lambda_1! \dots \lambda_n!}{r!} \sum x_{j_1} \dots x_{j_r}$$

donde la suma se toma respecto de todas las permutaciones  $(j_1, \dots, j_r)$  de los elementos  $i_1, \dots, i_r$ .

Ejercicio 11. Demuéstrase que  $V$  es un operador lineal, mas la propiedad de multiplicatividad para él no tiene lugar.

Ejercicio 12. Demuéstrase que  $UV$  es un operador idéatico sobre el álgebra  $R^*(x; t)$ .

A toda  $r$ -permutación  $i_1 i_2 \dots i_r$  de elementos  $1, \dots, n$  con repeticiones pongamos en correspondencia en el álgebra numeradora exponencial un monomio  $x_{i_1} \dots x_{i_r} t^r / r!$ . La serie correspondiente  $p(x_1, x_2, \dots; t)$  para la clase dada de permutaciones se llamará *numerador exponencial* de dicha clase. La imagen  $U_p(x_1, x_2, \dots; t)$ , al actuar el operador  $U$ , la llamaremos *numerador exponencial reducido* de la clase dada de permutaciones, y la serie  $T^* p(x_1, x_2, \dots; t)$ , *función generatriz exponencial*.

EJEMPLO 6. Hállense el numerador exponencial, el numerador exponencial reducido y la función generatriz exponencial para una  $r$ -permutación de  $n$  elementos.

El numerador exponencial ya lo hemos encontrado en la forma (6); el numerador exponencial reducido es el polinomio

$$\prod_{i=1}^n (1 + x_i t),$$

y la función generatriz exponencial para el número de  $r$ -permutaciones de  $n$  elementos la hemos hallado en la forma de (7).

EJEMPLO 7. Hállense el numerador exponencial, el numerador exponencial reducido y la función generatriz exponencial para las  $r$ -permutaciones con repeticiones del tipo  $(\lambda_1, \dots, \lambda_n)$  de  $n$  elementos.

Por  $(\lambda_1, \dots, \lambda_n)$ -permanente (véase [42]) de una  $(r \times n)$ -matriz

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{r1} & \dots & a_{rn} \end{pmatrix}$$

con los elementos del anillo  $R$  se entenderá un elemento

$$\text{Per}_{(\lambda_1, \dots, \lambda_n)} A = \sum a_{1i_1} a_{2i_2} \dots a_{ri_r}$$

donde la suma se toma respecto de todas las  $r$ -permutaciones  $(i_1, \dots, i_r)$  de elementos  $1, \dots, n$  con la repetición del tipo  $(\lambda_1, \dots, \lambda_n)$ , o bien, dicho de otro modo, en el producto pueden figurar  $\lambda$  elementos de la columna  $i$  sólo en el caso en que  $\lambda \in \Lambda_i$  si la suma tiene un conjunto vacío de sumandos,

entonces pongámosla igual a cero. Ahora podemos escribir el numerador exponencial buscado en la forma

$$p(x_1, x_2, \dots; t) = \sum_{r=0}^{\infty} \text{Per}(\Lambda_1, \dots, \Lambda_n) X_{r,n} \frac{t^r}{r!},$$

donde  $X_{r,n}$  es una  $(r \times n)$ -matriz con  $r$  filas iguales  $(x_1, \dots, x_n)$ . El numerador exponencial reducido  $Up(x_1, x_2, \dots; t)$  puede representarse ahora del modo siguiente:

$$Up(x_1, x_2, \dots; t) = \sum_{r=0}^{\infty} \sum_{\substack{r_1 + \dots + r_n = r \\ r_1 \in \Lambda_1, \dots, r_n \in \Lambda_n}} \frac{r!}{r_1! \dots r_n!} x_1^{r_1} \dots x_n^{r_n} \frac{t^r}{r!}, \quad (9)$$

de donde

$$Up(x_1, x_2, \dots; t) = \prod_{i=1}^n \left( \sum_{\lambda \in \Lambda_i} x_i^\lambda \frac{t^\lambda}{\lambda!} \right). \quad (10)$$

Por fin, la función generatriz exponencial tiene la forma

$$\tilde{T}_p^*(x_1, x_2, \dots; t) = T^* Up(x_1, x_2, \dots; t) = \prod_{i=1}^n \left( \sum_{\lambda \in \Lambda_i} \frac{t^\lambda}{\lambda!} \right),$$

por lo cual

$$p(1, 1, \dots; t) = \sum_{r=0}^{\infty} \sum_{\substack{r_1 + \dots + r_n = r \\ r_1 \in \Lambda_1, \dots, r_n \in \Lambda_n}} \frac{r!}{r_1! \dots r_n!} \frac{t^r}{r!}.$$

De aquí llegamos a que el número de  $r$ -permutaciones de  $n$  elementos con repeticiones del tipo  $(\Lambda_1, \dots, \Lambda_n)$  es igual a

$$\sum_{\substack{r_1 + \dots + r_n = r \\ r_1 \in \Lambda_1, \dots, r_n \in \Lambda_n}} \frac{r!}{r_1! \dots r_n!}.$$

Podemos hallar también el numerador exponencial partiendo del numerador exponencial reducido (10), al representarlo en la forma canónica (9) y al aplicar el operador lineal  $V$ .

**EJEMPLO 8.** Hállense el numerador exponencial, el numerador exponencial reducido y la función generatriz exponencial para las  $r$ -permutaciones con repeticiones ilimitadas de  $n$  elementos.

En este caso, en las condiciones del ejemplo antecedente  $\Lambda_i = N_0$  para  $i = 1, \dots, n$ , y

$$\text{Per}(N_0, \dots, N_0) X_{r,n} = (x_1 + \dots + x_n)^r.$$

Por eso el numerador exponencial tiene la forma de un exponente

$$p(x_1, x_2, \dots; t) = \sum_{r=0}^{\infty} (x_1 + \dots + x_n)^r \frac{t^r}{r!} = \exp((x_1 + \dots + x_n)t).$$

La misma forma tiene en este caso el numerador exponencial reducido, mientras que la función generatriz exponencial se obtiene en la siguiente forma

$$p(1, 1, \dots; t) = \exp(nt) = \sum_{r=0}^{\infty} n^r \frac{t^r}{r!}.$$

Así pues, el número de  $r$ -permutaciones con repeticiones ilimitadas de  $n$  elementos es igual a  $n^r$ , lo que concuerda con el resultado del § 1.3. La forma de la función generatriz de este ejemplo predetermina precisamente el término "exponencial" que se usa en la teoría analítica de enumeraciones de las  $r$ -permutaciones.

EMPLO 9. Hállense el numerador exponencial, el numerador exponencial reducido y la función generatriz exponencial para las  $r$ -permutaciones de  $n$  elementos con repeticiones, donde cada elemento ha de aparecer por lo menos una vez.

Para este caso, en las condiciones del ejemplo 7 tenemos  $\Lambda_i = \mathbf{N}$ ,  $i = 1, \dots, n$ , por consiguiente, el numerador exponencial reducido tendrá la forma

$$p^*(x_1, x_2, \dots; t) = \prod_{i=1}^n \left( \sum_{\lambda=1}^{\infty} \frac{(x_i t)^\lambda}{\lambda!} \right) = \prod_{i=1}^n (\exp(x_i t) - 1).$$

Ahora podemos escribir la función exponencial generatriz:

$$\begin{aligned} p^*(1, 1, \dots; t) &= (e^t - 1)^n = \sum_{k=0}^n (-1)^k \binom{n}{k} e^{t(n-k)} \\ &= \sum_{r=0}^n \frac{t^r}{r!} \sum_{k=0}^n (-1)^k \binom{n}{k} (n-k)^r, \end{aligned}$$

los números correspondientes, por lo tanto, son iguales a

$$p(n, r) = \sum_{k=0}^n (-1)^k \binom{n}{k} (n-k)^r. \quad (11)$$

Por fin, el numerador exponencial puede ser determinado con ayuda del operador lineal  $V$ :

$$p(x_1, x_2, \dots; t) = V p^*(x_1, x_2, \dots; t) = V \prod_{i=1}^n (e^{x_i t} - 1).$$

**Ejercicio 13.** Hállense el numerador exponencial, el numerador exponencial reducido y la función generatriz exponencial para las  $r$ -permutaciones con repeticiones de  $n$  elementos, donde cada elemento puede aparecer sólo un número par de veces.

La función generatriz de Dirichlet para una sucesión de números  $a = (a_1, a_2, \dots)$  es una serie formal

$$D_a(t) = \sum_{r=1}^{\infty} \frac{a_r}{r^r}.$$

Determinemos, igual que lo hicimos anteriormente, las operaciones de adición y multiplicación para estas series. Se llamará suma de  $D_a(t)$  con  $D_b(t)$  a la serie

$$D_a(t) + D_b(t) = D_c(t) = \sum_{r=1}^{\infty} \frac{c_r}{r^r}, \quad b = (b_1, b_2, \dots), \quad \dots$$

donde  $c_r = a_r + b_r$ , y producto de las series mencionadas, a la serie siguiente:

$$D_a(t) \times D_b(t) = D_d(t) = \sum_{r=1}^{\infty} \frac{d_r}{r^r},$$

donde

$$d_r = \sum_{ij=r} a_i b_j = \sum_{i|r} a_i b_{r/i}$$

(la adición se realiza según los divisores enteros  $r$ ). De aquí se ve con facilidad que  $O = (0, 0, \dots)$  define el cero con relación a la adición;  $e = (1, 0, 0, \dots)$  define la unidad con relación a la multiplicación;  $D_e(t) = 1$ ; el elemento inverso respecto de la multiplicación  $D_a^{-1}(t)$  se busca a partir de la igualdad

$$D_a(t) \times D_a^{-1}(t) = D_e(t) = 1,$$

o bien, que es lo mismo, del sistema de ecuaciones:

$$\begin{aligned} a_1 a_1' &= 1, \\ a_2 a_1' + a_1 a_2' &= 0, \\ a_3 a_1' + a_2 a_2' + a_1 a_3' &= 0, \\ a_4 a_1' + a_2 a_2' + a_3 a_3' + a_1 a_4' &= 0, \\ &\dots \end{aligned}$$

de donde tenemos, en particular:  $a_1' = \frac{1}{a_1}$ ,  $a_2' = -\frac{a_2}{a_1^2}$ ,  $a_3' = -\frac{a_3}{a_1^2}$ ,  $a_4' = \frac{a_2^2}{a_1^3} - \frac{a_4}{a_1^2}$ , etc., es decir, es necesaria y suficiente la invertibilidad del elemento  $a_1$ . No es difícil comprobar que la totalidad de funciones generatrices de Dirichlet es también un anillo. Si definimos la multiplicación natural de la serie  $D_a(t)$  por un número real, dicho anillo será el álgebra  $\mathbf{R}\{t\}$

sobre el campo  $\mathbf{R}$ . El álgebra de Dirichlet  $D(\mathbf{R})$  de sucesiones, isomorfa a la primera, se determina de un modo análogo.

La noción de función generatriz de Dirichlet surgió en la teoría de los números, donde es de amplio uso la zeta función de Riemann:

$$\xi(t) = \sum_{r=1}^{\infty} \frac{1}{r^t}.$$

Las tres formas de las funciones generatrices introducidas más arriba son fundamentales para el análisis combinatorio, pero están lejos de ser únicas. La diversidad de las formas que tienen funciones generatrices, se debe a los diversos planteamientos de los problemas. Veamos, como ejemplo, un problema sobre la construcción de las funciones generatrices para alojamientos y llenados, a saber, el problema del tipo  $(A_2)$  (véase § 1.4).

Se tienen un  $n$ -conjunto de diferentes elementos y un  $m$ -conjunto de diferentes células de especificación  $(n_1, n_2, \dots, n_m)$ . Se requiere construir la función generatriz para el número de alojamientos de  $n$  elementos en  $m$  células. Supongamos que el símbolo

$$x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$$

significa que en la  $i$ -ésima célula se alojan  $n_i$  elementos,  $i = 1, \dots, m$ .

Si  $n = 1$ , es decir, si se tiene sólo un elemento, entonces el correspondiente símbolo de alojamiento es  $x_i$ , siempre que el elemento está colocado en la  $i$ -ésima célula,  $i = 1, \dots, m$ . De conformidad con la regla de la suma, la posibilidad de alojar un elemento en cualquiera de  $m$  células se describe por el polinomio

$$x_1 + x_2 + \dots + x_m.$$

Si se tienen  $n$  elementos, de los cuales cada uno puede ser colocado en cualquiera de  $m$  células, entonces el polinomio correspondiente será

$$(x_1 + x_2 + \dots + x_m)^n,$$

mientras que la correspondiente función generatriz se representará por una función exponencial

$$\begin{aligned} E(t) &= \sum_{n=0}^{\infty} (x_1 + x_2 + \dots + x_m)^n \frac{t^n}{n!} = \exp\left(t \sum_{i=1}^m x_i\right) = \\ &= \exp\left(\sum_{i=1}^m t x_i\right) = \prod_{i=1}^m \exp(t x_i). \end{aligned}$$

Si se trata sólo del número de alojamientos posibles, suponemos  $x_i = 1$ ,  $i = 1, 2, \dots, m$ , y, en este caso, la función generatriz adopta la forma

$$E(t) = \exp(mt).$$

De acuerdo con el teorema polinomial tenemos:

$$\left(\sum_{i=1}^m x_i\right)^n = \sum \frac{n!}{n_1!n_2!\dots n_m!} x_1^{n_1} x_2^{n_2} \dots x_m^{n_m},$$

de donde obtenemos que el número de alojamientos de  $n$  diferentes elementos en  $m$  diferentes células con una  $(n_1, n_2, \dots, n_m)$ -especificación será igual a

$$\frac{n!}{n_1!n_2!\dots n_m!}.$$

### 2.3. APARATO OPERACIONAL DEL MÉTODO DE FUNCIONES GENERATRICES

El uso de las funciones generatrices, permite enfocar con un grado suficiente de generalidad problemas combinatorios del tipo enumerativo. Sin embargo, las funciones generatrices, construidas para diferentes tipos de muestras resultaron ser, en la mayor parte bastante engorrosas. Por esta razón, para una notación más cómoda de las funciones generatrices se emplean operadores especiales, cálculos simbólicos y números y funciones especiales.

Sea una sucesión  $a = (a_0, a_1, \dots)$ , la que se escribirá de otro modo:  $a = a(n)$ , es decir, como función de un argumento de número entero  $n(n = 0, 1, 2, \dots)$ . Para el conjunto de sucesiones  $\{a(n)\}$  se emplean con mayor frecuencia los siguientes operadores especiales:

a) el operador de desplazamiento  $E$ :

$$Ea(n) = a(n+1), \quad n = 0, 1, 2, \dots, \\ E^{-1}a(n) = a(n-1), \quad n = 1, 2, \dots, \quad E^{-1}a(0) = 0;$$

b) el operador de diferencia  $\Delta$ :

$$\Delta a(n) = a(n+1) - a(n);$$

c) el operador mediador  $\delta$ :

$$\delta a(n) = \frac{a(n-1) + a(n+1)}{2}, \quad n = 1, 2, \dots, \quad \delta a(0) = \frac{a(1)}{2}.$$

Estos operadores están unidos por medio de ciertas relaciones, por ejemplo:

$$\Delta a(n) = (E - I)a(n), \\ \delta a(n) = \frac{1}{2}(E + E^{-1})a(n),$$

donde  $I$  es un operador idéntico.

Las reiteradas aplicaciones de los operadores a los elementos de la sucesión pueden conducir a ciertas fórmulas útiles y cómodas. Por ejemplo, denotemos con  $n^r$  una sucesión con término general  $a(n) = n^r$ . La notación

$Ln^r$ , en la que  $L$  es un operador lineal en el conjunto de sucesiones se entenderá como  $(La)(n)$ , donde  $a(n) = n^r$ . Entonces,

$$E^n(0) = n; E^n(0^r) = n^r; \Delta 0^r = 1^r - 0^r = 1^r; \\ \Delta^2 0^r = 2^r - 2; \Delta^3 0^r = 3^r - 3 \cdot 2^r + 3,$$

etc. Los números  $\Delta^n 0^r$  llevan el nombre de *De Morgan*.

Como un ejemplo de empleo de los operadores en las fórmulas combinatorias aduzcamos el problema sobre el número de  $r$ -permutaciones con repeticiones de un  $n$ -conjunto a condición de que cada elemento aparezca no menos de una vez.

Reduzcamos el número  $p(n, r)$ , obtenido en el § 2.2, a la forma (11) del modo siguiente:

$$p(n, r) = \sum_{i=0}^n \binom{n}{i} (-1)^i (n-i)^r = \sum_{i=0}^n \binom{n}{i} (-1)^i E^{n-i} 0^r = (E-1)^n 0^r = \\ = \Delta^n 0^r.$$

Demostremos que

$$\Delta^n 0^{r+1} = n \Delta^n 0^r + n \Delta^{n-1} 0^r.$$

En efecto,

$$\Delta^n 0^{r+1} = \sum_{i=0}^n \binom{n}{i} (-1)^i (n-i)^{r+1} = n \sum_{i=0}^n \binom{n}{i} (-1)^i (n-i)^r - \\ - \sum_{i=0}^n \binom{n}{i} (-1)^i (n-i)^r i.$$

El primer sumando no es otra cosa que  $n \Delta^n 0^r$ , lo que se deduce con toda evidencia de lo expuesto anteriormente. En lo que se refiere al segundo sumando, está claro que al realizar la sustitución  $i = j + 1$ , obtenemos

$$\sum_{i=0}^n \binom{n}{i} (-1)^i (n-i)^r i = - \sum_{j=0}^{n-1} \binom{n}{j+1} (-1)^j (n-j-1)^r (j+1) \\ = - \sum_{j=0}^{n-1} \frac{n(n-1)! (j+1)}{(j+1)! (n-1-j)!} (-1)^j (n-j-1)^r = \\ = -n \sum_{j=0}^{n-1} \binom{n-1}{j} (-1)^j (n-1-j)^r = -n \Delta^{n-1} 0^r.$$

**Ejercicio 1.** Demuéstrese que el número de  $r$ -permutaciones de  $n$  elementos con repeticiones pares (incluido 0) ilimitadas es igual a  $\delta^n 0^r$ .

Las repeticiones frecuentes de las mismas expresiones condujeron a la aparición de números y funciones especiales. Los números especiales, por

ejemplo, se descubren y vuelven a descubrir en los diferentes apartados de las matemáticas: en el cálculo de las diferencias finitas, en la teoría de los números, en la teoría de las probabilidades y en la estadística matemática. He aquí algunos datos sobre dichos números.

Analicemos la factorial inferior  $(t)_n = t(t-1)\dots(t-n+1)$  como una función generatriz:

$$(t)_n = \sum_{k=0}^n s(n, k)t^k, \quad n > 0.$$

Los coeficientes  $s(n, k)$  en este desarrollo se denominan *números de Stirling de primer género*. Por cuanto  $(t)_k$  es un polinomio de grado  $k$ , entonces, podemos desarrollar  $t^n$  según el sistema de polinomios  $(t)_0, (t)_1, \dots, (t)_n$ :

$$t^n = \sum_{k=0}^n S(n, k)(t)_k, \quad n > 0. \quad (1)$$

Los coeficientes  $S(n, k)$  se denominan *números de Stirling de segundo género*. Realicemos una definición adicional para ambos géneros de números:

$$(t)_0 = t^0 = s(0, 0) = S(0, 0) = 1.$$

Los números de Stirling se encuentran en muchos problemas. Volvamos, por ejemplo, al problema examinado más arriba sobre el número de  $n$ -permutaciones con repeticiones de  $k$  elementos a condición de que cada elemento figure en las muestras mencionadas por lo menos una vez (véase el ejemplo 9 del § 2.2). Resulta que la función generatriz en este caso tiene la forma

$$\begin{aligned} (e^t - 1)^k &= \sum_{i=0}^k \binom{k}{i} (-1)^i e^{t(k-i)} = \sum_{n=0}^{\infty} \frac{t^n}{n!} \sum_{i=0}^k \binom{k}{i} (-1)^i (k-i)^n = \\ &= \sum_{n=0}^{\infty} \Delta^k 0^n \frac{t^n}{n!}. \end{aligned}$$

Recordemos que este problema admite su interpretación como un problema sobre el número de alojamientos de  $n$  diferentes elementos en  $k$  células distinguibles tales que no queden células vacías. Para cualesquiera  $t \geq n$  naturales tenemos

$$\begin{aligned} t^n &= E^t 0^n = (1 + \Delta)^t 0^n = \sum_{k=0}^t \binom{t}{k} \Delta^k 0^n = \sum_{k=0}^t (t)_k \frac{\Delta^k 0^n}{k!} = \\ &= \sum_{k=0}^n (t)_k \frac{\Delta^k 0^n}{k!}, \end{aligned}$$

puesto que  $\Delta^k 0^n = 0$  para  $k > n$  ( $\Delta^k 0^n$  es el número de  $n$ -permutaciones de  $k$  elementos con repeticiones, donde cada elemento figura no menos de 1 vez). Por cuanto el polinomio de grado  $n$  cuenta con  $n$  raíces, entonces la

igualdad

$$t^n = \sum_{k=0}^n (t)_k \frac{\Delta^k 0^n}{k!}$$

será válida para todos los valores reales de  $t$ . Al tener presente el desarrollo (1), obtenemos

$$\Delta^k 0^n = k! S(n, k).$$

Esto quiere decir que el número de alojamientos de  $n$  elementos diferentes en  $k$  células distinguibles, cuando ninguna célula queda vacía (problema del tipo (A)), es igual a  $k! S(n, k)$ , y el correspondiente número para las células indistinguibles (problema del tipo (C)) (o lo que es lo mismo, el número de particiones de un  $n$ -conjunto en  $k$  partes no vacías) es igual a  $S(n, k)$ .

Los números de Stirling se encuentran a menudo en los razonamientos combinatorios, por lo cual daremos a conocer algunas observaciones más.

Se pueden obtener recurrencias útiles para dichos números, por ejemplo:

a) de  $(t)_{n+1} = (t-n)(t)_n$  se deduce

$$s(n+1, k) = s(n, k-1) - ns(n, k);$$

$$\begin{aligned} \text{b) } t^{n+1} &= \sum_{k=0}^{n+1} S(n+1, k)(t)_k = t \sum_{k=0}^n S(n, k)(t)_k = \\ &= \sum_{k=0}^n S(n, k)((t)_{k+1} + k(t)_k), \end{aligned}$$

de donde obtenemos

$$S(n+1, k) = S(n, k-1) + kS(n, k).$$

Con una de las dos expresiones

$$(t)_n = \sum_{k=0}^n s(n, k)t^k, \quad t^n = \sum_{k=0}^n S(n, k)(t)_k$$

sustituiremos la otra:

$$t^n = \sum_{k=0}^n S(n, k) \sum_{m=0}^k s(k, m)t^m = \sum_{k=0}^n \sum_{m=0}^k S(n, k)s(k, m)t^m.$$

Al igualar los coeficientes de las mismas potencias de  $t$ , obtenemos

$$\sum_{k=m}^n S(n, k)s(k, m) = \delta_{n,m} = \begin{cases} 1, & \text{si } n = m, \\ 0, & \text{si } n \neq m. \end{cases}$$

El número  $\delta_{n,m}$  se denomina *delta de Kronecker*.

He aquí una información acerca de los otros números especiales.

Se llaman de *Fibonacci* los números  $f(n)$ , donde

$$f(0) = f(1) = 1, f(n) = f(n-1) + f(n-2), n \geq 2.$$

Su función generatriz tiene la forma:

$$F(t) = 1 + t + 2t^2 + 3t^3 + 5t^4 + 8t^5 + 13t^6 + \dots$$

Si se toma en consideración la relación recurrente, llegamos a la siguiente expresión analítica para la función generatriz:

$$F(t) = 1 + t + (f(1) + f(0))t^2 + \dots + (f(n-1) + f(n-2))t^n + \dots = 1 + (t + t^2)F(t),$$

de donde

$$F(t) = (1 - t - t^2)^{-1}.$$

Esta función puede ser representada también en la forma

$$F(t) = ((1 - at)(1 - bt))^{-1}, \quad (2)$$

donde  $a$  y  $b$  se hallan de las correlaciones

$$a + b = 1, ab = -1,$$

de donde

$$a = \frac{1 + \sqrt{5}}{2}, b = \frac{1 - \sqrt{5}}{2}.$$

Al desarrollar (2) en fracciones simples, obtenemos

$$F(t) = \frac{\alpha}{1 - at} + \frac{\beta}{1 - bt}, \quad \alpha = \frac{1 + \sqrt{5}}{2\sqrt{5}}, \quad \beta = -\frac{1 - \sqrt{5}}{2\sqrt{5}}$$

( $\alpha$  y  $\beta$  se hallan por el método de coeficientes indeterminados). De aquí obtenemos la fórmula de Binet

$$f(n) = \alpha a^n + \beta b^n = \frac{\left(\frac{1 + \sqrt{5}}{2}\right)^{n+1} - \left(\frac{1 - \sqrt{5}}{2}\right)^{n+1}}{\sqrt{5}}$$

Los números de Fibonacci forman una sucesión específica que se encuentra a menudo en los problemas combinatorios. Por ejemplo, el número de Fibonacci  $f(n)$ ,  $n \geq 1$ , es el número de  $(n-1)$ -permutaciones de ceros y unidades que no contienen dos ceros seguidos.

De perfeccionamiento ulterior del aparato de funciones generatrices sirve el empleo del cálculo simbólico de Blissar. Demos a conocer la versión rígida del mismo que se basa en las ideas de Mullin y Rota [43] referentes a la utilización del aparato de operadores lineales con el objeto de fundamentar el cálculo de Blissar.

Recordemos que un operador lineal que actúa de un espacio vectorial en el campo sobre el cual está construido dicho espacio se denomina *funcional lineal*.

La idea fundamental del cálculo de Blissar consiste en la operación "de alzamiento de los subíndices": la función generatriz exponencial

$$E_a(t) = \sum_{n=0}^{\infty} a_n \frac{t^n}{n!}$$

de una sucesión  $a = (a_0, a_1, \dots)$  se sustituye por la serie

$$\exp(at) = \sum_{n=0}^{\infty} a^n \frac{t^n}{n!}$$

y después de realizar las transformaciones indispensables con la participación de esta serie, las potencias se sustituyen de nuevo por los subíndices (en lugar de  $a^n$  escribimos  $a_n$ ). Con el fin de fundamentar estas transformaciones introduzcamos el álgebra  $\mathbf{R}^*(a; t) = (\mathbf{R}[a])^*[[t]]$  de series exponenciales formales con los coeficientes en el álgebra de polinomios  $\mathbf{R}[a]$  de la variable  $a$ , y la funcional lineal  $L_a: \mathbf{R}[a] \rightarrow \mathbf{R}$  tal que  $L_a a^n = a_n$ , prolongada, naturalmente, hasta el operador lineal  $L_a: \mathbf{R}^*(a; t) \rightarrow \mathbf{R}^*[[t]]$ , de suerte que  $L_a \exp(at) = E_a(t)$ .

EjemPlo 1. Veamos una sucesión de los números de Bernoulli  $B = (B_0, B_1, \dots)$ , definida por su función exponencial

$$\sum_{n=0}^{\infty} B_n \frac{t^n}{n!} = \frac{t}{e^t - 1}.$$

Entonces, para la funcional lineal  $L_B: \mathbf{R}[B] \rightarrow \mathbf{R}$  tal que  $L_B B^n = B_n$ , tenemos

$$L_B \exp(Bt) = \frac{t}{e^t - 1}. \quad (3)$$

De aquí tenemos

$$\begin{aligned} t &= L_B(\exp((B+1)t) - \exp(Bt)) = L_B \left( \sum_{n=0}^{\infty} ((B+1)^n - B^n) \frac{t^n}{n!} \right) = \\ &= L_B \left( \sum_{n=0}^{\infty} \left( \sum_{r=0}^{n-1} \binom{n}{r} B^r \right) \frac{t^n}{n!} \right) = \sum_{n=0}^{\infty} \left( \sum_{r=0}^{n-1} \binom{n}{r} B_r \right) \frac{t^n}{n!}, \end{aligned}$$

y obtenemos, de este modo, la fórmula recurrente

$$\sum_{r=0}^{n-1} \binom{n}{r} B_r = \begin{cases} 1 & \text{para } n = 1 \\ 0 & \text{para } n = 0, 2, 3, 4, \dots \end{cases}$$

Sustituyendo en (3)  $t$  por  $-t$ , obtenemos

$$L_B \exp(-Bt) = \frac{-t}{e^{-t} - 1} = \frac{te^t}{e^t - 1} = L_B \exp((B+1)t).$$

Igualando los coeficientes de las potencias de  $x$ , tenemos

$$L_B(B + 1)^n = L_B(-B)^n,$$

es decir,

$$\sum_{r=0}^n \binom{n}{r} B_r = (-1)^n B_n. \quad (4)$$

De (3) y (4) obtenemos, ahora, que  $B_n = (-1)^n B_n$  para  $n \neq 1$ , y  $B_1 = -B_1 - 1$ . Por consiguiente,  $B_1 = -1/2$ ,  $B_3 = B_5 = B_7 = \dots = 0$ .

**Ejercicio 2.** Demuéstrase que en el álgebra  $\mathbb{R}^*(a; t)$  tienen lugar las propiedades de permutabilidad de los operadores lineales  $D$ ,  $\int$  y  $L_a$ :

1.  $D L_a = L_a D$ ;
2.  $\int L_a = L_a \int$ .

Analicemos ahora el caso cuando en las expresiones que se consideran participan dos sucesiones  $a = (a_0, a_1, \dots)$  y  $b = (b_0, b_1, \dots)$ . Entonces, para cada una de ellas construimos su funcional lineal:  $L_a: a^n \rightarrow a_n$ , y  $L_b: b^n \rightarrow b_n$  (trabajamos ya en el álgebra  $\mathbb{R}^*(a, b; t) = (\mathbb{R}[a, b])^*[[t]]$  con polinomios de dos variables que actúan en calidad de coeficientes). Veamos, por ejemplo, la sucesión  $c = (c_0, c_1, \dots)$  que representa su convolución binomial. Suponiendo que  $L_a(p(b)a^n) = p(b)L_a a^n$  para cualquier polinomio  $p(b)$  (y, análogamente, para  $L_b$ ), tenemos

$$c_n = \sum_{k=0}^n \binom{n}{k} a_k b_{n-k} = L_a L_b \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} = L_a L_b (a + b)^n.$$

Introduciendo la funcional lineal  $L_c: c^n \rightarrow c_n$ , obtenemos de aquí

$$L_c c^n = L_a L_b (a + b)^n.$$

Para el producto de funciones generatrices exponenciales correspondientes tenemos

$$\begin{aligned} L_c \exp(ct) &= E_a(t) \cdot E_b(t) = \\ &= L_a L_b \exp(at) \exp(bt) = L_a L_b \exp((a + b)t). \end{aligned}$$

La dificultad principal del cálculo clásico de Blissard consistía en que, al considerar la convolución

$$\sum_{k=0}^n \binom{n}{k} a_k a_{n-k}$$

después de alzar los subíndices:

$$\sum_{k=0}^n \binom{n}{k} a^k a^{n-k}$$

era necesario prohibir la multiplicación  $a^k a^{n-k} = a^n$ , puesto que dicha operación conduciría a un resultado absurdo:

$$\sum_{k=0}^n \binom{n}{k} a_k a_{n-k} = 2^n a_n.$$

Siguiendo las ideas de Guinand [44], esta posibilidad la eliminamos aquí exigiendo que, al alzar los subíndices de las convoluciones de las sucesiones iguales, se introduzcan para ellas diferentes variables. En el caso dado tomamos  $L_a : a^n \rightarrow a_n$  y  $L_{a'} : (a')^n \rightarrow a_n$ . Entonces

$$\sum_{k=0}^n \binom{n}{k} a_k a_{n-k} = L_a L_{a'} (a + a')^n.$$

**EJEMPLO 2.** Demostremos la identidad de Euler para la suma de los productos de los números de Bernoulli  $B_n$ :

$$\sum_{r=1}^{n-1} \binom{2n}{2r} B_{2r} B_{2n-2r} = -(2n+1) B_{2n}.$$

Esta identidad puede reescribirse en la forma

$$\sum_{s=0}^m (-1)^s \binom{m}{s} B_s B_{m-s} = (1-m) B_m \quad (5)$$

(cuando  $m$  es impar, los miembros primero y segundo son nulos). Introducimos las funcionales lineales  $L_B : B^n \rightarrow B_n$  y  $L_{B'} : (B')^n \rightarrow B_n$ , entonces (5) puede escribirse en la siguiente forma:

$$L_B L_{B'} (B - B')^m = (1-m) L_B B^m. \quad (6)$$

Analicemos la función generatriz exponencial para el primer miembro de (6):

$$\begin{aligned} L_B L_{B'} \sum_{m=0}^{\infty} (B - B')^m \frac{t^m}{m!} &= L_B L_{B'} \exp((B - B')t) = \\ &= L_B L_{B'} \exp(Bt) \exp(-B't) = \frac{t}{e^t - 1} \frac{-t}{e^{-t} - 1} = \frac{t^2 e^t}{(e^t - 1)^2} = \\ &= -t^2 \frac{d}{dt} \left( \frac{L_B \exp(Bt)}{t} \right) = L_B (1 - Bt) \exp(Bt) = \\ &= L_B \left( \sum_{m=0}^{\infty} B^m \frac{t^m}{m!} - \sum_{m=0}^{\infty} B^{m+1} \frac{t^{m+1}}{m!} \right) = L_B \left( \sum_{m=0}^{\infty} (1-m) B^m \frac{t^m}{m!} \right). \end{aligned}$$

De aquí obtenemos la identidad (6), lo que se trataba de demostrar.



Bell  $A_n = (1; y_1, y_2, \dots, y_n) = Y(y_1, y_2, \dots, y_n) = e^{-y} D_x^n e^y$ ,  $y = y(x)$ .

Dichos polinomios resultaron ser un medio operacional importante en la matemática estadística, y luego en la teoría combinatoria.

Hallemos una relación recurrente para los polinomios de Bell. Introduzcamos la designación abreviada

$$A_n(a) = A_n(a; g_1, \dots, g_n).$$

Entonces

$$A_{n+1}(a) = e^{-ag} D^n (d e^{ag}) = e^{-ag} a D^n (g_1 e^{ag}).$$

De aquí, con arreglo a la fórmula de Leibniz sobre la diferenciación de un producto, tenemos

$$A_{n+1}(a) = a \sum_{k=0}^n \binom{n}{k} (e^{-ag} D^{n-k} e^{ag}) D_k^k = a \sum_{k=0}^n \binom{n}{k} A_{n-k}(a) g_{k+1} =$$

$$= L_{A(a)} L_R a g [A(a) + g]^n, \quad (7)$$

$$L_{A(a)} [A(a)]^k = A_k(a), \quad L_R g^k = g_k, \quad k = 0, 1, 2, \dots$$

Veamos ahora la serie

$$G(x) = \sum_{n=1}^{\infty} g_n \frac{x^n}{n!}$$

y la función generatriz exponencial para los polinomios de

$$F(x) = \sum_{n=0}^{\infty} A_n(a) \frac{x^n}{n!}$$

De (7) obtenemos

$$DF(x) = aG(x)F(x),$$

de aquí, integrando esta ecuación, obtenemos

$$F(x) = \exp(aG(x)).$$

Ahora, según el teorema polinomial, tenemos

$$A_n(a) = \sum_{k_1 \dots k_n} \frac{a^k n!}{k_1! \dots k_n!} \left(\frac{g_1}{1!}\right)^{k_1} \dots \left(\frac{g_n}{n!}\right)^{k_n},$$

donde  $k = k_1 + \dots + k_n$ , y la suma se toma por todas las soluciones en números enteros de la ecuación  $k_1 + 2k_2 + \dots + nk_n = n$ . Y, por fin, obtenemos la expresión

$$A_n = A_n(f) = \sum_{k_1 \dots k_n} \frac{n! f_k}{k_1! \dots k_n!} \left(\frac{g_1}{1!}\right)^{k_1} \dots \left(\frac{g_n}{n!}\right)^{k_n},$$

que se conoce como fórmula de F. di Bruno

## 2.4. SOBRE LAS APLICACIONES DEL MÉTODO DE FUNCIONES GENERATRICES

Según lo dicho más arriba, el método de funciones generatrices se aplica para resolver problemas de carácter enumerativo, es decir, cuando se determina el número de objetos en cierta clase. Los razonamientos combinatorios inmediatos análogos a aquellos que ya se usaron en el cap. 1 jugaban y siguen jugando gran papel en calidad de métodos principales, mas las funciones generatrices introdujeron consigo una mayor generalidad de juicios y ampliaron el dominio de las aplicaciones posibles del análisis combinatorio.

Históricamente las circunstancias tomaron un cariz tal que los métodos combinatorios se aplicaron, ante todo, en la teoría de las probabilidades y en la estadística matemática. Y esto es bien explicable. En la moderna teoría axiomática de las probabilidades estas mismas se interpretan sólo en relación con los espacios de los sucesos elementales. Los últimos son conceptos originarios no definibles y se interpretan como conjuntos puntuales. Si un espacio de sucesos elementales se compone de un conjunto finito o numerable de puntos, dicho espacio se denomina discreto.

Todo el aparato de investigación de los espacios discretos de sucesos elementales es, en esencia, combinatorio. Más aún, podemos hablar sobre las interpretaciones teórico-probabilísticas de una parte determinada del análisis combinatorio.

Efectivamente, las  $r$ -muestras pueden ser interpretadas con ayuda de diferentes esquemas de urna. Los casos en que se admiten repeticiones de los elementos en las muestras, corresponden a los esquemas de urna con retorno. Las funciones generatrices de la forma

$$\sum_{i=1}^s p_i t^{x_i}$$

donde  $\sum_{i=1}^s p_i = 1$ ,  $p_i \geq 0$ , ( $i = 1, \dots, s$ ) intervienen en la teoría de las probabilidades, cuando una magnitud aleatoria  $X$  (una función sobre el conjunto de sucesos elementales) puede asumir los valores  $x_i$ ,  $i = 1, 2, \dots, s$ , con las probabilidades  $p_i$ ,  $i = 1, 2, \dots, s$ , respectivamente. Una de las funciones generatrices más simples en la teoría de las probabilidades está asociada con el lanzamiento de una moneda y con otros sucesos que pueden tener dos resultados:

$$P(t) = q + pt, \quad p + q = 1, \quad p, q \geq 0$$

(la magnitud aleatoria toma el valor 0 con la probabilidad  $q$ , y el valor 1 con la probabilidad  $p$ ). La función generatriz de lanzamiento de un dado hexaedro con las caídas equiprobables de puntos tiene la forma

$$\frac{1}{6} (t + t^2 + \dots + t^6) = \frac{t(1 - t^6)}{6(1 - t)}.$$

Sea  $X_1$  una magnitud aleatoria que toma los valores  $0, 1, 2, \dots, s$  con las probabilidades  $p_0, p_1, p_2, \dots, p_s$ , respectivamente; supongamos que  $X_2$  es otra magnitud aleatoria que toma los valores  $0, 1, 2, \dots, r$  con las probabilidades  $p'_0, p'_1, p'_2, \dots, p'_r$ , respectivamente. Sus funciones generatrices serán

$$\sum_{i=0}^s p_i t^i \quad \text{y} \quad \sum_{k=0}^r p'_k t'^k.$$

Si dos sucesos son independientes, entonces la probabilidad de su aparición simultánea es igual al producto de sus probabilidades. La correspondiente función generatriz de la magnitud aleatoria bidimensional  $(X_1, X_2)$  tiene por expresión:

$$\begin{aligned} p_0 p'_0 + (p_1 p'_0) t + (p_0 p'_1) t' + (p_1 p'_1) t t' + \dots + (p_s p'_r) t^s t'^r = \\ = \left( \sum_{i=0}^s p_i t^i \right) \left( \sum_{k=0}^r p'_k (t')^k \right). \end{aligned}$$

Si analizamos la distribución de la suma  $X_1 + X_2$ , entonces  $t = t'$ , y el producto tiene por expresión

$$\begin{aligned} \left( \sum_i p_i t^i \right) \left( \sum_k p'_k t^k \right) = p_0 p'_0 + (p_0 p'_1 + p_1 p'_0) t + \\ + (p_1 p'_1 + p_0 p'_2 + p_2 p'_0) t^2 + \dots \end{aligned}$$

Esta construcción se extiende con facilidad a las distribuciones de  $n$  magnitudes aleatorias independientes. En particular, para  $n$  pruebas independientes (con 2 resultados) la función generatriz del número de resultados de una forma determinada será

$$P(t) = (q + pt)^n, \quad p + q = 1, \quad p, q \geq 0.$$

En la teoría de las probabilidades pueden emplearse también funciones generatrices de tipo algo diferente. Por ejemplo, supongamos que cuatro partículas entran volando en una cámara, donde se encuentran centros de atracción con fuerzas proporcionales a 8:9:11:12. Diremos que la función generatriz de las probabilidades de distribución de una partícula por los centros es

$$\frac{8}{40} t_1 + \frac{9}{40} t_2 + \frac{11}{40} t_3 + \frac{12}{40} t_4.$$

En tal caso, si se asegura la independencia de las partículas, la función generatriz de las probabilidades de caída de las cuatro partículas tendrá por expresión:

$$\prod_{i=1}^4 \left( \frac{8}{40} t_1^{(i)} + \frac{9}{40} t_2^{(i)} + \frac{11}{40} t_3^{(i)} + \frac{12}{40} t_4^{(i)} \right).$$

Si nos interesa sólo cuántas partículas caen en los centros dados, la función



Es obvio que la expresión de los momentos factoriales a través de los ordinarios genera los números de Stirling de primer género, y la expresión inversa, los números de Stirling de segundo género;

d) momentos centrales:

$$M_k = L_m(m - m_1)^k, \quad L_m(m^i) = m_i, \quad i = 0, 1, 2, \dots,$$

o bien, de otro modo,

$$M_k = \sum_{j=0}^k \binom{k}{j} m_{k-j} (-m_1)^j, \quad k = 0, 1, 2, \dots$$

El más simple es el segundo momento central llamado de otro modo varianza:  $M_2 = m_2 - m_1^2$ . La idea principal que condujo al análisis de los momentos centrales consiste en que en lugar de la misma magnitud aleatoria se examinan sus desviaciones del valor medio.

He aquí algunos tipos de las funciones generatrices que se usan con mayor frecuencia en la teoría de las probabilidades:

a) para la distribución de las probabilidades:

$$P(t) = \sum_k p_k t^k;$$

b) para los momentos ordinarios;

$$m(t) = L_m \exp(mt) = \sum_k m_k \frac{t^k}{k!}; \quad L_m(m^k) = m_k, \quad k = 0, 1, \dots;$$

c) para los momentos factoriales:

$$(m)(t) = \sum_k (m)_k \frac{t^k}{k!};$$

d) para los momentos binomiales

$$B(t) = \sum_k B_k t^k$$

e) para los momentos centrales:

$$M(t) = L_M \exp(Mt) = \sum_k M_k \frac{t^k}{k!}, \quad L_M(M^k) = M_k, \quad k = 0, 1, \dots$$

Las operaciones de carácter formal sobre diferentes funciones generatrices conducen al descubrimiento de varias relaciones útiles, por ejemplo:

1)  $m(t) = P(e^t)$ . En efecto,

$$m(t) = \sum_k m_k \frac{t^k}{k!} = \sum_k \frac{t^k}{k!} \sum_j j^k p_j = \sum_j p_j \sum_k \frac{(tj)^k}{k!} = \sum_j p_j e^{tj} = P(e^t);$$

2)  $(m)(t) = P(1 + t)$ , lo que se ve de las siguientes igualdades:

$$\begin{aligned} (m)(t) &= \sum_k (m)_k \frac{t^k}{k!} = \sum_k \sum_j (j)_k p_j \frac{t^k}{k!} = \\ &= \sum_j p_j \sum_k \binom{j}{k} t^k = \sum_j p_j (1 + t)^j = P(1 + t). \end{aligned}$$

## 2.5. TEORÍA DE REDFIELD—POLYA

El tipo de funciones generatrices depende de las condiciones concretas en que se plantean los problemas y su construcción es, en cierto grado, un arte. Durante mucho tiempo no existía un enfoque regular respecto a la construcción de las funciones generatrices. En este sentido han hecho pasos considerables Redfield y Polya, que elaboraron el método de construcción de las funciones generatrices para objetos combinatorios no equivalentes de tipo bastante general. A los objetos enumerados se les atribuían pesos, mientras que la noción de equivalencia se introducía por medio de un grupo de sustituciones. Aclaremos esta cuestión detalladamente.

Veamos un grupo  $G$  de sustituciones de los elementos de un  $n$ -conjunto, es decir, un subgrupo de un grupo simétrico  $S_n$ . Cada sustitución engendra la partición del  $n$ -conjunto en ciclos, es decir, en subconjuntos cuyos elementos son cíclicamente permutables: la cantidad de elementos en un subconjunto se denomina longitud del ciclo. Supongamos, por ejemplo, que la sustitución  $g$  tiene  $k_1$  ciclos de longitud 1,  $k_2$  ciclos de longitud 2, etc. Entonces suele decirse que la sustitución posee estructura cíclica  $(k_1, k_2, \dots)$  y se le pone en correspondencia un monomio  $p(g) = t_1^{k_1} t_2^{k_2} \dots$ . Se llama *índice cíclico* del grupo  $G$  la media de tales monomios tomada de todas las  $g \in G$ :

$$P_G(t_1, t_2, \dots) = |G|^{-1} \sum_{g \in G} t_1^{k_1} t_2^{k_2} \dots$$

EJEMPLO. Basándonos en la fórmula (4) del § 1.3 para el número de sustituciones que poseen estructura cíclica dada, encontramos el índice cíclico del grupo simétrico  $S_n$  para todas las sustituciones del  $n$ -conjunto:

$$\begin{aligned} P_{S_n}(t_1, t_2, \dots, t_n) &= \frac{1}{n!} \sum \frac{n!}{1^{k_1} k_1! \dots n^{k_n} k_n!} t_1^{k_1} \dots t_n^{k_n} = \\ &= \sum \frac{1}{k_1! \dots k_n!} \left(\frac{t_1}{1}\right)^{k_1} \dots \left(\frac{t_n}{n}\right)^{k_n}, \end{aligned}$$

donde la sumación se realiza respecto de todas las soluciones en números enteros no negativos de la ecuación  $1 \cdot k_1 + 2 \cdot k_2 + \dots + n k_n = n$ , o bien, hablando de otro modo, respecto de todas las particiones del número  $n$ .

A todo grupo de sustituciones se le puede asignar su índice cíclico de

un modo único. Una afirmación contraria no será, sin embargo, cierta. En 1937 Polya construyó dos grupos no isomorfos de sustituciones de orden  $p^3$  ( $p > 2$ , primo) con iguales índices cíclicos.

Sean dados un conjunto finito  $D$  y un grupo finito  $G$  con su aplicación homomorfa  $\pi$  en un grupo simétrico de sustituciones del conjunto  $D$ , es decir, a todo  $g \in G$  le corresponde una sustitución  $\pi_g$  del conjunto  $D$ , y  $\pi_{gg'} = \pi_g \pi_{g'}$  (para cualesquiera  $g, g' \in G$ ). No se requiere que la aplicación  $\pi$  sea un encaje.

La equivalencia de los elementos del conjunto  $D$  se introduce por medio del grupo  $G$ :

$$d_1 \sim d_2 \quad (d_1, d_2 \in D),$$

si existe un elemento  $g \in G$  tal que  $\pi_g d_1 = d_2$ . Todos los requerimientos de equivalencia se cumplen en esta definición. En efecto:

a)  $d \sim d$  para todos los  $d \in D$ , puesto que  $\pi_e$ , donde  $e$  es un elemento unidad de  $G$ , es una sustitución idéntica;

b) de  $d_1 \sim d_2$  se deduce  $d_2 \sim d_1$ , por cuanto de la condición de homomorfismo se desprende que si  $g' = g^{-1}$ , entonces  $\pi_{g'} = (\pi_g)^{-1}$ ;

c) de  $d_1 \sim d_2$  y  $d_2 \sim d_3$  se deduce que  $d_1 \sim d_3$ , puesto que si  $\pi_g d_1 = d_2$  y  $\pi_{g'} d_2 = d_3$ , entonces  $\pi_{g'g} d_1 = \pi_{g'}(\pi_g d_1) = \pi_{g'} d_2 = d_3$ .

En virtud de la definición de equivalencia, el conjunto  $D$  resulta ser partido, con ayuda del grupo  $G$ , en clases de equivalencia (conjuntos transitivos). Los elementos son equivalentes, si y sólo si integran una misma clase de equivalencia.

**Lema de Bernsáid.** El número de clases de equivalencia definidas por el grupo finito  $G$  que actúa sobre el conjunto finito  $D$  es igual a

$$\frac{1}{|G|} \sum_{g \in G} \psi(g),$$

donde  $|G|$  es el número de elementos en  $G$ ;  $\psi(g)$ , el número de elementos en  $D$ , que son invariantes respecto de  $\pi_g$ , es decir, tales que  $\pi_g d = d$ , mientras que la sumación se hace de todos los elementos  $g \in G$ .

Esta afirmación se anunció por primera vez en las obras de Cauchy, Frobenius y Bernsáid.

*Demostración.* Veamos todos los pares  $(g, d)$ , para los cuales  $\pi_g d = d$  ( $g \in G, d \in D$ ) entonces:

- a) podemos fijar  $g$  y contar cuántos  $d$  existen, para los cuales  $\pi_g d = d$ ;  
 b) para cada  $d$  fijo calculemos todos los  $g$ , para los cuales  $\pi_g d = d$ ; designemos los números obtenidos con  $\eta(d)$ . Está claro que

$$\sum_{d \in D} \eta(d) = \sum_{g \in G} \psi(g).$$

Los elementos  $g \in G$  que fijan  $d$  forman un subgrupo  $G_d$  del grupo  $G$ :

$$|G_d| = \eta(d).$$

Si tomamos otro elemento de la misma clase de equivalencia  $d_1 \sim d$ , entonces el número de elementos  $g$ , para los cuales  $\pi_g d = d_1$ , será también igual a  $|G_d|$ . Efectivamente, se tiene un elemento  $h \in G$ , para el cual  $\pi_h d_1 = d$ , y, por tanto, de que  $\pi_g d = d_1$  se deduce que  $hg \in G_d$ . Así pues, el grupo  $G$  puede ser partido en subconjuntos disjuntos en cada uno de los cuales habrá  $|G_d|$  elementos (un subgrupo  $G_d$  en cada clase contigua izquierda del grupo  $G$ ): cada subconjunto corresponde exactamente a un solo elemento de la clase de equivalencia, en la que figura el elemento  $d$ . De aquí, para hallar  $\eta(d)$ , se debe dividir  $|G|$  por el número de elementos de la clase de equivalencia a la que pertenece  $d$ . Sumamos: a)  $\sum \eta(d) = |G|$ , si la suma se toma de todos los  $d$  que integran una misma clase de equivalencia; b) la suma  $\sum_{d \in D} \eta(d)$  es igual al producto de  $|G|$  por el número de clases de equivalencia, de donde se desprende el resultado que tratábamos de demostrar.

Hemos introducido, pues, el concepto de equivalencia para los elementos a través de un grupo de sustituciones y hemos deducido la fórmula para el número de clases de equivalencia.

Introduzcamos la relación de equivalencia para las aplicaciones. Sean dados los conjuntos finitos  $D$  y  $R$ . Designemos el conjunto de todas las aplicaciones de  $D$  en  $R$  con  $R^D$ . El número de estas aplicaciones es igual a  $|R|^{|D|}$ , puesto que para cada  $d \in D$  existe  $|R|$  posibilidades independientes para la imagen. Supongamos que se dispone de un grupo  $G$  de sustituciones del conjunto  $D$ . Las aplicaciones  $f_1$  y  $f_2$  son equivalentes ( $f_1 \sim f_2$ ), si existe una sustitución  $g \in G$  tal que  $f_1(gd) = f_2(d)$  para todos los  $d \in D$ , o bien  $f_1 g = f_2$ . Las condiciones de equivalencia son: a)  $f \sim f$ ; b) si  $f_1 \sim f_2$ , entonces  $f_2 \sim f_1$ ; c) si  $f_1 \sim f_2$  y  $f_2 \sim f_3$ , entonces  $f_1 \sim f_3$  se cumplen todas. La primera condición se deduce de la existencia en  $G$  de una sustitución idéntica; la segunda, de que junto con  $g$  figura en  $G$  también  $g^{-1}$ ; la tercera, de que si  $g_1 \in G$  y  $g_2 \in G$ , entonces  $g_1 g_2 \in G$ .

La equivalencia de las aplicaciones introducida de este modo parte el conjunto  $R^D$  en clases de equivalencia (*modelos*).

Introduzcamos ahora los pesos. Estos darán la posibilidad de enumerar las clases especiales de los objetos combinatorios. Al principio, a todo elemento  $r \in R$  se le asigna un peso  $\omega(r)$ , donde  $\omega(r)$  es un elemento de anillo conmutativo sobre el campo de números racionales. El peso de la aplicación  $W(f)$ , donde  $f \in R^D$ , se define como un producto

$$W(f) = \prod_{d \in D} \omega(f(d)),$$

donde  $f(d)$  es la imagen del elemento  $d \in D$  al realizarse la aplicación  $f$ , y  $\omega(f(d))$ , su peso. Las aplicaciones equivalentes tienen pesos iguales. En efecto, si  $f_1 g = f_2 (g \in G)$ , entonces

$$\prod_{d \in D} \omega(f_1(d)) = \prod_{d \in D} \omega(f_1(gd)) = \prod_{d \in D} \omega(f_2(d)).$$

La igualdad es obvia, puesto que tanto el primer producto, como el segundo, difieren sólo en el orden de los factores. Por cuanto todas las aplicaciones  $f$  de la clase de equivalencia  $F$  poseen un mismo peso, asignemos este peso a toda la clase  $F$ , designándolo con  $W(F)$ . La suma de pesos

$$\sum_{r \in R} \omega(r)$$

de los elementos del conjunto  $R$  se llamará (siguiendo a de Buijn) *inventario* (inventory) del conjunto  $R$  y se denotará con  $\text{inv } D$ .

Ahora podemos calcular el inventario del conjunto  $R^D$  de aplicaciones

$$\text{Inv } R^D = \sum_f W(f) = \left( \sum_{r \in R} \omega(r) \right)^{|D|} = (\text{inv } R)^{|D|}.$$

Mostremos que esta afirmación es cierta. En el segundo miembro tenemos  $|R|^{|D|}$  términos. Se puede establecer una correspondencia entre  $|D|$  factores y los elementos del conjunto  $D$ . La elección de un término de cada factor y la formación de un término del desarrollo se interpretan como la aplicación  $f: D \rightarrow R$ . Pero, para cada  $f$  tenemos  $W(f) = \prod_{d \in D} \omega(f(d))$ . Todo el producto es igual a la suma de todos los  $W(f)$ , lo que se requería demostrar.

Si consideramos el conjunto  $S$  de aplicaciones, constantes sobre los subconjuntos  $D_1, \dots, D_k$ , que forman la partición del conjunto  $D$ , entonces

$$\text{inv } S = \prod_{i=1}^k \sum_{r \in R} (\omega(r))^{|D_i|}, \quad (1)$$

lo que se demuestra mediante un razonamiento análogo al aducido más arriba.

Ahora, introducidos todos los conceptos indispensables, podemos enunciar el teorema básico. Se trata en él sobre el paso de los pesos de las funciones a los de los modelos (de las clases de equivalencia).

**Teorema de Polya.** Sean  $D$  y  $R$  los conjuntos finitos dados, y  $G$ , un grupo de sustituciones de los elementos de  $D$ : supongamos, además, que a los elementos  $r \in R$  están asignados los pesos  $\omega(r)$ ; a las aplicaciones  $f \in R^D$  y a los modelos (clases)  $F$ , se les asignan los pesos  $W(f)$  y  $W(F)$ , respectivamente. Entonces

$$\sum_F W(F) = P_G \left( \sum_{r \in R} \omega(r), \sum_{r \in R} (\omega(r))^2, \sum_{r \in R} (\omega(r))^3, \dots \right),$$

donde  $P_G$  es el índice cíclico del grupo  $G$ . En un caso particular, cuando todos los pesos son iguales a uno, el número de clases de equivalencia será

$$P_G(|R|, |R|, \dots).$$

**Demostración.** Elijamos de  $R^D$ , es decir, del conjunto de todas las aplicaciones  $f: D \rightarrow R$ , un conjunto  $S$  de aquellas aplicaciones, cuyos pesos son iguales, digamos, a  $\omega$ . Para  $f \in S$  tenemos:  $W(f) = \omega$ , y el número de clases

de equivalencia para el conjunto  $S$  es igual a

$$\frac{1}{|G|} \sum_{g \in G} \psi_{\omega}(g),$$

donde  $\psi_{\omega}(g)$  denota el número de aplicaciones  $f$ , para las cuales

$$W(f) = \omega, \quad f = fg \text{ (o bien } fg^{-1} = f).$$

En efecto, se ha demostrado que si  $g \in G$  y  $f_1 = f_2g$ , entonces  $f_1$  y  $f_2$  son de peso igual. Quiere decir, que si  $f_1 \in S$ , también  $f_1g^{-1} \in S$ . De este modo, a cada  $g \in G$  corresponde una aplicación  $\pi_g$  del conjunto  $S$  sobre sí mismo que se determina por la correlación

$$\pi_g f = fg^{-1}.$$

Si dos elementos  $f_1$  y  $f_2$  del conjunto  $S$  son equivalentes, esta afirmación es equivalente a la siguiente: la existencia del elemento  $g \in G$ , para el cual  $\pi_g f_2 = f_1$ , es equivalente a la existencia del elemento  $g \in G$ , para el cual  $f_2 = f_1g$ . Ahora resta por alegar el lema de Bernsaid para convencerse de que el número de clases de equivalencia está determinado correctamente.

Todas las clases de equivalencia que integran  $S$  tienen un peso igual a  $\omega$ . Por consiguiente, si multiplicamos

$$\frac{1}{|G|} \sum_{g \in G} \psi_{\omega}(g)$$

por  $\omega$  y sumamos respecto de todos los  $\omega$ , obtendremos

$$\sum_t W(F) = \frac{1}{|G|} \sum_{\omega} \sum_{g \in G} \psi_{\omega}(g) \omega.$$

Pero, es evidente que

$$\sum_{\omega} \psi_{\omega}(g) \omega = \sum_f^{(g)} W(f),$$

donde la sumación se realiza por todas las  $f \in R^D$  que satisfacen la igualdad  $f = fg$ ; quiere decir

$$\sum_F W(F) = \frac{1}{|G|} \sum_{g \in G} \sum_f^{(g)} W(f). \quad (2)$$

Calculemos ahora  $\sum_f^{(g)} W(f)$ . La sustitución  $g$  divide  $D$  en ciclos. La condición  $f = fg$  significa que

$$f(d) = f(gd) = f(g^2d) = \dots,$$

es decir,  $f = \text{const}$  para cada ciclo. Es cierta también la afirmación contra-

ria: toda aplicación  $f$ , constante en cada ciclo, satisface la igualdad  $fg = f$ , puesto que  $g(d)$  y  $d$  pertenecen siempre a un mismo ciclo. De modo que si  $D_1, D_2, \dots, D_k$  son los ciclos de  $g$ , entonces, según (1), tenemos

$$\sum_f^{(g)} W(f) = \prod_{i=1}^k \sum_{r \in R} (\omega(r))^{i D_i}.$$

Supongamos que la sustitución  $g$  es de estructura cíclica  $(b_1, b_2, \dots)$ , entonces

$$\sum_f^{(g)} W(f) = \left( \sum_{r \in R} \omega(r) \right)^{b_1} \left( \sum_{r \in R} (\omega(r))^2 \right)^{b_2} \dots$$

Al sustituir esta expresión en (2), obtenemos

$$\sum_F W(F) = \frac{1}{|G|} \sum_{g \in G} \left( \sum_{r \in R} \omega(r) \right)^{b_1} \left( \sum_{r \in R} (\omega(r))^2 \right)^{b_2} \dots$$

lo que se trataba de demostrar.

Este teorema fue enunciado por Polya en 1937. Más tarde se notó que el mismo teorema, pero en una forma algo diferente, fue publicado en 1927 por J. Redfield (véase en [12]). Sin embargo, debido a una costumbre ya arraigada el teorema conserva el nombre de Polya.

Posteriormente dicho teorema fue demostrado basándose en suposiciones generales. Según lo observado anteriormente, para las aplicaciones  $f: D \rightarrow R$  la equivalencia se introducía por intermedio del grupo  $G$  de sustituciones de los elementos  $d \in D$ . Si añadimos el segundo grupo  $H$  de sustituciones de los elementos  $r \in R$ , la introducción de la equivalencia con ayuda de ambos grupos  $G$  y  $H$  se realiza del modo siguiente: dos funciones (dos aplicaciones)  $f_1 \in R^D$  y  $f_2 \in R^D$  son equivalentes:  $f_1 \sim f_2$ , si existen elementos  $g \in G$  y  $h \in H$  tales que  $f_1 g = h f_2$ , es decir,

$$f_1(gd) = h f_2(d) \text{ para todos } d \in D.$$

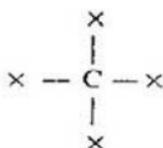
Entre otras generalizaciones del teorema de Polya indiquemos aquella que está ligada con el enlace de los grupos. Sean los grupos de sustituciones  $G$  y  $H$  para los conjuntos  $S$  y  $T$ , respectivamente. En el producto directo de los conjuntos  $S \times T$  formemos las sustituciones de un tipo especial. A saber, elegimos  $g \in G$ ; para cada  $s \in S$  elegimos un elemento  $h_s \in H$ . Estos elementos definen la sustitución:

$$(s, t) \rightarrow (gs, h_s t), \quad s \in S, \quad t \in T.$$

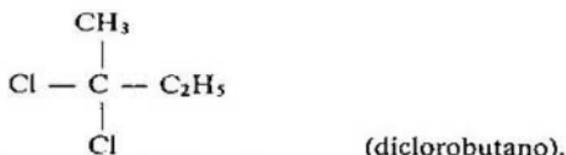
En total hay  $|G| \cdot |H|^{|\mathcal{S}|}$  de tales sustituciones; ellas forman precisamente un grupo denominado por Polya como enlace de los grupos (Gruppenkranz).

La explicación acertada de los teoremas de Polya provista de ejemplos se da en [10]. El desarrollo ulterior ha enriquecido poco la teoría de Redfield — Polya y no la cambió en principio.

Como conclusión, aduzcamos un ejemplo no complejo que explica la aplicación del teorema de Polya. Se trata de la enumeración de los isómeros de las moléculas orgánicas de una estructura dada. Se consideran las moléculas del tipo:



donde C es un átomo de carbono, y en los lugares marcados con cruces pueden encontrarse: CH<sub>3</sub> (metilo), C<sub>2</sub>H<sub>5</sub> (etilo), H (hidrógeno) y Cl (cloro). Por ejemplo,



De modelo matemático de estas moléculas sirve un tetraedro en cuyo centro se dispone el átomo de carbono. El problema de enumeración de las moléculas se interpretará como problema sobre el número de clases de equivalencia *D* (para cuatro vértices):

$$f : D \rightarrow R = \{\text{CH}_3, \text{C}_2\text{H}_5, \text{H}, \text{Cl}\}.$$

El grupo *G* será un grupo de rotaciones del tetraedro compuesto por: una permutación idéntica de los vértices; ocho rotaciones en 120° alrededor de los vértices; tres rotaciones en 180° alrededor de los ejes que pasan por los centros de las aristas que no se intersecan. Entonces

$$P_G(x_1, x_2, x_3) = \frac{1}{12} (x_1^4 + 8x_1x_3 + 3x_2^2).$$

Supongamos que todos los pesos son iguales a la unidad y obtendremos el número total de moléculas:

$$P_G(4, 4, 4) = 36.$$

Sustituyamos los tipos particulares de las moléculas de la estructura dada: supongamos, por ejemplo, que se debe calcular el número de tales moléculas, en las que no interviene el átomo de hidrógeno. En este caso para CH<sub>3</sub>, C<sub>2</sub>H<sub>5</sub> y Cl los pesos serán iguales a la unidad, y para H, a cero:

$$P_G(3, 3, 3) = \frac{1}{12} (3^4 + 8 \cdot 3 \cdot 3 + 3 \cdot 3^2) = 15 \text{ moléculas buscadas.}$$

Para poder clasificar las demás 21 moléculas atribuyamos, como lo hicimos antes, los pesos unidad a CH<sub>3</sub>, C<sub>2</sub>H<sub>5</sub> y Cl, y el peso H al átomo de hidrógeno:

$$P_G(H + 3, H^2 + 3, H^3 + 3) = \frac{1}{12} ((H + 3)^4 + 8(H + 3)(H^3 + 3) + 3(H^2 + 3)^2) = H^4 + 3H^3 + 6H^2 + 11H + 15.$$

Por consiguiente, existen: 1 molécula de  $\text{CH}_4$  (metano); 3 moléculas con 3 átomos de H; 6 moléculas con 2 átomos de H; 11 moléculas con 1 átomo de H; 15 moléculas que no tienen átomos de H.

La teoría de las funciones generatrices es la parte del análisis combinatorio que mayor avance tiene en los aspectos teórico y práctico para la resolución de los problemas prácticos. La composición y las posibilidades de esta teoría ya están bien determinadas.

En este capítulo describiremos procedimientos lógicos característicos que constituyen la base de muchas demostraciones combinatorias.

### 3.1. MÉTODO DE INCLUSIONES Y EXCLUSIONES<sup>1)</sup>

Sean dados un  $n$ -conjunto  $S$  de ciertos elementos y un  $N$ -conjunto de propiedades  $p_1, p_2, \dots, p_N$ , con la particularidad de que los elementos del conjunto pueden poseer dichas propiedades y pueden no tenerlas. Se requiere hallar el número de elementos que no poseen ninguna de las propiedades mencionadas.

Elijamos una  $r$ -muestra de propiedades  $(p_{i_1}, p_{i_2}, \dots, p_{i_r})$ . Designemos con  $n(p_{i_1}, p_{i_2}, \dots, p_{i_r})$  el número de elementos del conjunto  $S$ , cada uno de los cuales posee todas las propiedades elegidas. Denotemos con  $\bar{p}_i$  la ausencia en los elementos de la propiedad  $p_i$ . Así pues, el número de elementos que, digamos, poseen las propiedades  $p_1, p_3, p_5$ , y no poseen las propiedades  $p_2, p_4, p_6$  se escribirá en la forma  $n(p_1, \bar{p}_2, p_3, \bar{p}_4, p_5, \bar{p}_6)$ .

Examinemos al principio dos casos sencillos:

a) se tiene sólo una propiedad  $p$ ; entonces, evidentemente,

$$n(\bar{p}) = n - n(p);$$

b) se tiene un número finito de propiedades  $p_1, p_2, \dots, p_N$  que no son compatibles; tenemos, evidentemente

$$n(\bar{p}_1, \bar{p}_2, \dots, \bar{p}_N) = n - \sum_{i=1}^N n(p_i).$$

Pasemos a un planteamiento más general del problema, cuando los elementos del conjunto pueden poseer combinaciones de las propiedades compatibles. En este caso tiene lugar el

**Teorema 1.** Si están dados un  $n$ -conjunto de elementos y un  $N$ -conjunto de propiedades  $p_i$ ;  $i = 1, 2, \dots, N$ , entonces

$$\begin{aligned} n(\bar{p}_1, \bar{p}_2, \dots, \bar{p}_N) = & n - \sum_{i=1}^N n(p_i) + \sum_{1 \leq i < j \leq N} n(p_i, p_j) - \\ & - \sum_{1 \leq i < j < k \leq N} n(p_i, p_j, p_k) + \dots + (-1)^N n(p_1, p_2, \dots, p_N). \end{aligned} \quad (1)$$

<sup>1)</sup> Se conoce también bajo la denominación de método de criba, método lógico, método simbólico y principio de clasificación cruzada.

*Demostración.* Con el fin de obtener elementos que no posean ninguna de las propiedades mencionadas, hace falta excluir del  $n$ -conjunto los elementos que tienen la propiedad  $p_1$ , luego, los elementos poseedores de la propiedad  $p_2$ , etc., es decir,  $\sum_i n(p_i)$  elementos. En este caso, sin embargo,

los elementos que poseen dos propiedades, digamos  $p_1$  y  $p_2$  resultaron excluidos dos veces (al principio, como poseedores de la propiedad  $p_1$ , y a continuación, como poseedores de la propiedad  $p_2$ ). Quiere decir, que es necesario devolver todos los conjuntos, cuyos elementos poseen dos propiedades, o sea hay que añadir  $\sum_{1 \leq i < j \leq N} n(p_i, p_j)$  elementos. Mas, en tal caso los

elementos que poseen tres propiedades, digamos  $p_1$ ,  $p_2$  y  $p_3$  quedan incluidos, por lo cual se debe sustraer  $\sum_{1 \leq i < j < k \leq N} n(p_i, p_j, p_k)$ , elementos.

Siguiendo razonando de un modo análogo, obtendremos un algoritmo para calcular  $n(\bar{p}_1, \bar{p}_2, \dots, \bar{p}_N)$  el cual consiste en rechazar y devolver alternativamente los subconjuntos. A esto se debe precisamente una de las denominaciones del método: el de inclusiones y exclusiones. Vamos a seguir este método en adelante.

A parte de los razonamientos sencillos aducidos más arriba, podemos realizar la demostración por inducción respecto de  $N$ . El teorema es válido para  $N = 1$ ;

$$n(p) = n - n(p).$$

De acuerdo con la formulación del teorema, podemos escribir también:

$$n(p_1, p_2, \dots, p_N) = n(\bar{p}_1, p_2, \dots, \bar{p}_{N-1}) - n(\bar{p}_1, \bar{p}_2, \dots, \bar{p}_{N-1}, p_N).$$

Supongamos que el teorema es válido para  $N - 1$  propiedades, es decir,

$$\begin{aligned} n(p_1, \bar{p}_2, \dots, \bar{p}_{N-1}) &= n - \sum_i n(p_i) + \sum_{i < j} n(p_i, p_j) - \dots \\ &\dots + (-1)^{N-1} n(p_1, p_2, \dots, p_{N-1}). \end{aligned}$$

Pasemos al caso en que se tienen  $N$  propiedades. Apliquemos la correlación obtenida para el número  $n(\bar{p}_1, \bar{p}_2, \dots, \bar{p}_{N-1}, \bar{p}_N)$ :

$$\begin{aligned} n(\bar{p}_1, \bar{p}_2, \dots, \bar{p}_{N-1}, p_N) &= n(p_N) - \sum_i n(p_i, p_N) + \dots \\ &\dots + (-1)^{N-1} n(p_1, p_2, \dots, p_N). \end{aligned}$$

Al sustraer esta igualdad de la anterior, llegamos a la afirmación del teorema.

El carácter de la demostración es tal que puede ser utilizada para cualquier combinación de las propiedades. En el primer miembro de la igualdad demostrada puede figurar no sólo  $n(\bar{p}_1, \bar{p}_2, \dots, \bar{p}_N)$ , sino también, por ejemplo,  $n(p_1, \bar{p}_2, p_3, \bar{p}_4)$ . En este caso el teorema se enuncia respecto a una totalidad de las propiedades  $p_2$  y  $p_4$ , con el cumplimiento obligatorio de las

propiedades  $p_1$  y  $p_3$ , del modo siguiente:

$$n(p_1, p_3, \bar{p}_2, \bar{p}_4) = n(p_1, p_3) - n(p_1, p_3, p_2) - \\ - n(p_1, p_3, p_4) + n(p_1, p_3, p_2, p_4).$$

El método se hace más complicado cuando se introducen los pesos de los elementos. Al igual que en el cap. 2, no habrá limitaciones o precisiones algunas para el concepto de peso. Para nosotros los pesos son características numéricas de los elementos de los conjuntos definidas por las condiciones del problema.

Así pues, sea dado un  $n$ -conjunto  $S$  y supongamos que a cada elemento  $s_i \in S$ ,  $i = 1, 2, \dots, n$ , se le atribuye el peso  $V(s_i)$ . Del  $N$ -conjunto de propiedades  $p_1, p_2, \dots, p_N$  elijamos una  $r$ -muestra  $p_{i_1}, \dots, p_{i_r}$  y designemos con  $V(p_{i_1}, p_{i_2}, \dots, p_{i_r})$  la suma de pesos de los elementos que poseen todas las  $r$  propiedades elegidas. La suma de los pesos extendida a todas las  $r$ -muestras posibles de propiedades la denotaremos con

$$\sum V(p_{i_1}, p_{i_2}, \dots, p_{i_r}) = V(r).$$

Para el caso de  $r = 0$  el símbolo correspondiente  $V(0)$  designará la suma de pesos de todos los elementos del conjunto  $S$ .

El teorema antecedente se enuncia en este caso del modo siguiente.

**Teorema 2.** Si están dados el  $n$ -conjunto  $S$ , cada elemento del cual tiene un peso, y el  $N$ -conjunto de propiedades, entonces la suma  $V_N(0)$  de pesos de los elementos que no poseen ninguna de las propiedades dadas se determina por la fórmula

$$V_N(0) = V(0) - V(1) + V(2) - \dots + (-1)^N V(N).$$

Ha de notarse que el teorema 2 generaliza el teorema 1. Si todos los elementos  $s_i \in S$  son de peso unitario, entonces la suma de los pesos será igual a la suma de los sumandos en la suma. En este caso  $V(0) = N$  y  $V_N(0)$  es igual al número de elementos del conjunto  $S$  que no tienen ninguna de las  $N$  propiedades; la fórmula que se obtiene en tal caso es precisamente la fórmula (1).

El teorema 2 puede ser, a su vez, generalizado.

**Teorema 3.** La suma de pesos de los elementos que poseen exactamente  $r$  propiedades de las  $p_1, p_2, \dots, p_N$  se determina por la fórmula

$$V_N(r) = V(r) - \binom{r+1}{1} V(r+1) + \binom{r+2}{2} V(r+2) - \dots \\ \dots + (-1)^{N-r} \binom{N}{N-r} V(N),$$

o bien, lo que es lo mismo,

$$V_N(r) = V(r) - \binom{r+1}{r} V(r+1) + \binom{r+2}{r} V(r+2) - \dots$$

$$\dots + (-1)^{N-r} \binom{N}{r} V(N).$$

Los teoremas 2 y 3 se demuestran igual que el teorema 1. Se propone que el lector mismo realice estas demostraciones o se dirija al § 8.3, donde se aducen generalizaciones ulteriores del método de inclusiones y exclusiones.

Estudiemos, a título de ejemplo, un problema sobre desórdenes, llamado también problema de encuentros. Sea un conjunto ordenado finito de números  $1, 2, 3, \dots, n$ . Para estos números pueden formarse las permutaciones  $a_1, a_2, \dots, a_n$ . El número de todas las permutaciones es  $s = n!$  Entre las permutaciones citadas hay tales, donde ninguno de los elementos conserva su lugar original:  $a_i \neq i, i = 1, 2, \dots, n$ . Las permutaciones de esta índole se llaman desórdenes. ¿Cuántos desórdenes existen?

Un conjunto de  $n$  elementos se examina con relación al conjunto de propiedades de los elementos de quedarse en su lugar:  $p_i \sim \{a_i = i \mid i = 1, 2, \dots, n\}$ . Es evidente que si  $s$  elementos quedan fijados en sus lugares, el número  $N(s)$  de las respectivas permutaciones es igual a  $(n-s)!$ . El número de desórdenes en tal caso se determina con ayuda del método de inclusiones y exclusiones:

$$N(0) = n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \dots + (-1)^s \times \\ \times \binom{n}{s}(n-s)! + \dots = n! \left( 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!} \right),$$

lo que representa un número entero, el más próximo a  $n!e^{-1}$ .

Si se trata no de los desórdenes, sino de un número de permutaciones, en las que quedan en sus lugares  $s$  elementos, entonces

$$N(s) = \frac{n!}{s!} \left( 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^{n-s} \frac{1}{(n-s)!} \right).$$

Es fácil observar el desarrollo de los razonamientos durante la resolución: entre  $n$  elementos se eligen  $s$  elementos inmóviles, sirviéndose para ello de  $\binom{n}{s}$  métodos; a continuación, se realiza la multiplicación (según la regla del producto) por el número de desórdenes que se encuentran entre los  $(n-s)$  elementos restantes.

Demos a conocer la interpretación teórico-probabilística del método de inclusiones y exclusiones. El conjunto de elementos se interpreta en estas circunstancias como un espacio discreto de sucesos elementales, simultáneos o incompatibles (excluyentes),  $a_1, a_2, \dots, a_n$ , y los pesos de los elementos, como probabilidades. La probabilidad de la aparición simultánea de los sucesos  $a_{i_1}, a_{i_2}, \dots, a_{i_k}$  se designará con  $P(a_{i_1}, \dots, a_{i_k})$ . Para el caso en que los sucesos no aparecen se emplea la llamada ecuación de Poincaré:

$$P(\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n) = [1 - P(a_1)][1 - P(a_2)] \dots [1 - P(a_n)],$$

en la cual podemos abrir paréntesis, rigiéndonos por la regla:  $P(a_i)P(a_j) = P(a_i, a_j)$ . Esta ecuación es una generalización de la fórmula para las probabilidades de los sucesos independientes aplicada al caso de los sucesos dependientes y simultáneos. La fórmula general para el método de inclusiones y exclusiones tiene por expresión:

$$n(p_1, p_2, \dots, p_n) = n - \sum_i n(p_i) + \sum_{i,j} n(p_i, p_j) - \dots \\ \dots + (-1)^n n(p_1, p_2, \dots, p_n),$$

con la particularidad de que la fórmula se modifica: ambos miembros se dividen por  $n$ , para obtener magnitudes no absolutas, sino relativas, es decir, probabilidades

$$n^{-1}n(p_1, p_2, \dots, p_n) = 1 - n^{-1}\sum_i n(p_i) + n^{-1}\sum_{i,j} n(p_i, p_j) - \dots \\ \dots + (-1)^n n^{-1}n(p_1, p_2, \dots, p_n).$$

Más abajo señalaremos como se aplica el método de inclusiones y exclusiones al cálculo de los permanentes (§ 4.4) y al cálculo de los valores de las funciones especiales que figuran en la teoría de los números (§ 8.3).

### 3.2. SISTEMAS DE REPRESENTANTES DE LOS CONJUNTOS

Se examina aquí uno de los accesos combinatorios a la característica de la estructura de los conjuntos finitos. Ya por denominación se puede concebir que la idea principal consiste en sustituir el sistema de conjuntos por la reunión de sus representantes.

El planteamiento de los problemas de este tipo y los métodos de su resolución dependen de los requerimientos que dichos representantes deben satisfacer.

**Sistemas de representantes distintos (s.r.d.).** Sean un  $n$ -conjunto  $S$  y el conjunto  $P(S)$  de todos los subconjuntos suyos. Supongamos que  $M = (S_1, S_2, \dots, S_m)$  es una  $m$ -muestra de  $P(S)$ , y  $a = (a_1, a_2, \dots, a_m)$ , cierta  $m$ -muestra de  $S$ . Si a la muestra  $M$  se le puede poner en correspondencia (no forzosamente de una manera unívoca) una muestra  $a$  tal que los elementos  $a_i, i = 1, 2, \dots, m$ , sean distintos dos a dos y, además,  $a_i \in S_i, i = 1, 2, \dots, m$ , suele decirse que el elemento  $a_i$  representa el conjunto  $S_i$ , y toda la muestra  $(a_1, a_2, \dots, a_m)$  se denomina sistema de representantes distintos (en forma abreviada, s.r.d.) para  $M$ . Observemos a la vez que si  $i \neq j$ , entonces  $a_i \neq a_j$ , incluso si  $S_i = S_j$ . Si un conjunto aparece varias veces, debe tener cada vez un representante que sea distinto de los demás.

Resulta seguidamente que el s.r.d. puede existir no para todas las colecciones de conjuntos. Si en un sistema finito los conjuntos no son vacíos y no se intersecan, el s.r.d., obviamente, existe. Tomemos un caso más complejo. Por ejemplo, si  $S = (a, b, c, d, e)$ , y  $M$  es una colección de cuatro conjun-

tos  $S_1 = (a, b, c, d)$ ,  $S_2 = (a, b, e)$ ,  $S_3 = S_4 = (b, e)$ , entonces existen dos s.r.d.:  $(c, a, b, e)$  y  $(b, a, e, d)$ . Pero, apenas cambiamos uno de los subconjuntos, por ejemplo, tomamos  $S_2' = (b, e)$  en lugar de  $S_2$  y ya no podremos obtener ningún s.r.d. La respuesta a la pregunta de si existe o no un s.r.d. para una familia dada de conjuntos la da el teorema de P. Hall enunciado por éste no más tarde de 1935. El teorema formula las condiciones necesarias y suficientes para la existencia del s.r.d.

**Teorema de P. Hall.** Los subconjuntos  $S_1, S_2, \dots, S_m$  tienen un s.r.d., cuando y sólo cuando la reunión de cualesquiera  $k$  de estos conjuntos contiene no menos de  $k$  elementos. Dicho de otro modo, el s.r.d. para  $S_1, S_2, \dots, S_m$  existe, si y sólo si  $S_{i_1} \cup S_{i_2} \cup \dots \cup S_{i_k}$  consta por lo menos de  $k$  elementos, siendo en este caso  $k = 1, 2, \dots, m$ , y  $(i_1, i_2, \dots, i_m)$ , cualquier  $k$ -muestra de  $1, 2, \dots, m$ .

*Demostración.* La necesidad es casi evidente, puesto que la existencia del s.r.d. asegura la presencia de un número necesario de elementos en calidad de representantes distintos. En lo que se refiere a la suficiencia, aduzcamos una formulación perfeccionada que nos da, además, la cota inferior para el número de los propios s.r.d.

**Teorema.** Supongamos que una familia  $M = (S_1, S_2, \dots, S_m)$  satisface la condición necesaria para la existencia de un s.r.d. y que cada uno de los conjuntos  $S_1, S_2, \dots, S_m$  consta por lo menos de  $t$  elementos. Entonces; a) si  $t \leq m$ ,  $M$  tiene no menos de  $t!$  s.r.d.; b) si  $t > m$ , la familia  $M$  tiene no menos de  $t!/(t-m)!$  s.r.d.

La *demostración* la realizaremos por inducción respecto de  $m$ . Para  $m = 1$  (e, incluso, para  $m = 2$ ) el teorema es evidente. Demostremos que es lícito para cualquier  $m$  finito, partiendo de su validez para  $m' < m$ .

Veamos una (reunión) de cierta  $k$ -muestra de los conjuntos:

$$S_{i_1} \cup S_{i_2} \cup \dots \cup S_{i_k};$$

se deben examinar dos casos: uno cuando el número de elementos en la unión es igual a  $k$ , y otro cuando el número de elementos es superior a  $k$ . Empecemos por el segundo caso, cuando la unión en consideración posee no menos de  $k+1$  elementos, cualesquiera que sean  $k: k = 1, 2, \dots, m$ , y el juego  $i_1, i_2, \dots, i_k$  de números  $1, 2, \dots, m$ . Elijamos algún elemento  $a_1 \in S_{i_1}$  y eliminémoslo en  $S_2, S_3, \dots, S_m$ , si él se encuentra en dichos conjuntos. Llegamos de este modo a  $M^* = (S_2^*, S_3^*, \dots, S_m^*)$ . Esta  $(m-1)$ -muestra satisface la condición necesaria para la existencia de un s.r.d., puesto que  $S_{i_1}^* \cup S_{i_2}^* \cup \dots \cup S_{i_k}^*$  contiene no menos de  $k$  elementos y, además,  $M^*$  tiene o bien no menos de  $(t-1)$  s.r.d., si  $t \leq m$  (y, por tanto,  $t-1 \leq m-1$ ), o bien  $(t-1)!/(t-m)!$  s.r.d., si  $t > m$  (y, por tanto  $t-1 > m-1$ ). El resultado buscado se logra, si tomamos en consideración que en  $S_1$  hay por lo menos  $t$  posibilidades de fijar el elemento  $a_1$  y que este elemento constituye, junto con el s.r.d. para  $M^*$ , el s.r.d. para  $M$ .

Volvamos al primer caso en que la demostración realizada no puede

considerarse válida, pues existe una  $k$ -muestra  $S_{i_1}, S_{i_2}, \dots, S_{i_k}$  tal que  $S_{i_1} \cup S_{i_2} \cup \dots \cup S_{i_k}$  contiene exactamente  $k$  elementos ( $1 \leq k \leq m-1$ ). Reenumeremos los conjuntos  $S_1, S_2, \dots, S_m$  de un modo tal que  $S_{i_1}$  se haga  $S_1, S_{i_2}$  se haga  $S_2, \dots$ , y  $S_{i_k}$  se haga  $S_k$ ; escribamos estos conjuntos en el siguiente orden nuevo:

$$S_1, S_2, \dots, S_k, S_{k+1}, \dots, S_m.$$

Por cuanto  $S_1 \cup S_2 \cup \dots \cup S_k$  contiene exactamente  $k$  elementos, entonces  $t \leq k$ . Por consiguiente, por hipótesis de inducción,  $(S_1, S_2, \dots, S_k)$  tiene no menos de  $t!$  s.r.d. Tomemos uno de estos s.r.d.:  $(a_1, a_2, \dots, a_k)$ , donde  $a_i \in S_i, i = 1, 2, \dots, k$ . Eliminemos los elementos  $a_1, a_2, \dots, a_k$  de  $S_{k+1}, \dots, S_m$ , siempre que se encuentren allí. La  $(m-k)$ -muestra obtenida  $M^* = (S_{k+1}^*, \dots, S_m^*)$  satisface la condición necesaria para que existe un s.r.d. Efectivamente, si esto no es así y si la unión de cierta  $k^*$ -muestra  $S_{k+1}^* \cup \dots \cup S_{k+k^*}^*$  tiene menos de  $k^*$  elementos, entonces la unión

$$S_1 \cup S_2 \cup \dots \cup S_k \cup \dots \cup S_{k+k^*}$$

tendría menos de  $k+k^*$  elementos, lo que contradice la hipótesis del teorema. Así pues,  $M^*$  tiene por lo menos un s.r.d., y, por consiguiente,  $M$  tiene no menos de  $t!$  s.r.d.

**Algoritmo de elección de un s.r.d.** Prácticamente es muy difícil comprobar si en este caso concreto se cumple o no la hipótesis del teorema de P. Hall. La demostración que acabamos de ofrecer, basada en la inducción matemática completa, no proporciona ninguna indicación que ayude a hallar el s.r.d. Esto no es sorprendente. Los teoremas de existencia aparecen, las más de las veces, cuando resulta difícil o imposible hallar un algoritmo que conduzca a la determinación de la solución. El algoritmo que permite elegir un s.r.d. para un número finito de conjuntos, o mostrar que para el juego dado de conjuntos tal sistema no existe, lo dió M. Hall como demostración del teorema de P. Hall sobre los distintos representantes.

Sean dados  $n$  conjuntos  $S_1, S_2, \dots, S_n$ . Se requiere hallar para ellos el s.r.d., o mostrar que tal sistema no existe. Elijamos al azar un elemento del primer conjunto  $a_1 \in S_1$  en calidad de representante de este último. Elegiremos por turno los representantes de otros conjuntos:  $a_2 \in S_2; a_3 \in S_3; \dots$ , preocupándonos sólo de que todos estos representantes sean distintos. Si llevamos este proceso hasta  $a_n \in S_n$  inclusive, obtendremos el s.r.d. buscado.

Puede ocurrir que en un  $r$ -ésimo paso llegaremos a conseguir cierto  $t$ -conjunto  $S_r$ , todos los elementos del cual  $b_1, b_2, \dots, b_t$  ya habían sido elegidos en calidad de representantes de otros conjuntos. Esto, sin embargo, no significa todavía que el s.r.d. no existe. Vamos a tomar, uno tras otro, todos aquellos conjuntos, cuyos representantes son los elementos  $b_i (i = 1, 2, \dots)$ , y eliminar de ellos todos los elementos de la sucesión  $b_1, b_2, \dots, b_t$ , agregando los elementos restantes al final de la sucesión citada. Procedamos de este modo hasta que ocurra una cosa de dos: o bien 1) llegaremos al elemen-

to  $b_i$ , el cual no puede servir de representante, o bien 2) la sucesión se agotará con los elementos  $b_1, b_2, \dots, b_s$  como representantes de los conjuntos.

En el caso 2) podemos estar convencidos de que el s.r.d. no existe. En efecto, los elementos  $b_1, b_2, \dots, b_s$  son representantes de  $s$  conjuntos y, por construcción, cada elemento de estos  $s$  conjuntos se contiene en la sucesión dada. Pero, en tal caso, los  $s$  conjuntos mencionados, y también el conjunto  $S_r$ , forman  $s + 1$  conjuntos que sólo contienen  $s$  elementos distintos, lo que contradice la hipótesis del teorema.

En cambio, si tiene lugar el caso 1), entonces encontramos, en cierta etapa, el elemento  $b_i = b_{i_1} \in S_{j_1}$  ( $i_1 > t$ ) que no ha sido hasta ahora un representante. Esto es testimonio de que como representante de  $S_{j_1}$  ya fue elegido otro elemento  $b_{i_2}$  ( $i_2 < i_1$ ). Si  $i_2 > t$ , entonces el elemento  $b_{i_2}$  pertenece al conjunto  $S_{j_2}$  cuyo representante es  $b_{i_3}$  ( $i_3 < i_2$ ), etc. Surge, pues, una sucesión  $b_{i_1}, b_{i_2}, \dots, b_{i_m}$ , cuyos índices decrecen ( $i_m \leq t$ ), con la particularidad de que cada elemento de esta sucesión integra un conjunto, cuyo representante es el término sucesivo. Sustituyamos los representantes, eligiendo los elementos del modo siguiente:  $b_{i_1}$  para  $S_{j_2}$ ,  $b_{i_2}$  para  $S_{j_3}$ ,  $\dots$ ,  $b_{i_{m-1}}$  para  $S_{j_{m-1}}$ . Como resultado de esta sustitución, el elemento  $b_{i_m}$  se libera para poder ser elegido en calidad de representante de  $S_r$ . Así pues,  $S_1, \dots, S_r$  tienen representantes distintos y podemos seguir la misma senda, teniendo en cuenta o bien la posibilidad de llegar a  $S_n$  y obtener el s.r.d. completo, o bien encontrarse con el caso 2) y establecer que el s.r.d. no existe.

La conclusión sobre el número de s.r.d. se obtiene del algoritmo mencionado como una consecuencia. Efectivamente, si el s.r.d. existe, esto significa que existe también un conjunto, cada elemento del cual puede ser elegido en calidad de su representante en el s.r.d. Esto quiere decir, que si los conjuntos de una familia dada de  $n$  elementos tienen  $t$  o más elementos, entonces existen por lo menos  $t!$  s.r.d., si  $t < n$ , o bien  $t(t-1) \dots (t-n+1)$  elementos, si  $t \geq n$  (por cuanto la elección del primer representante puede realizarse empleando por lo menos  $t$  métodos; al tachar este representante elegido por nosotros en todos los demás conjuntos, llegaremos al sistema de conjuntos  $S_2^*, \dots, S_n^*$ , donde el conjunto menor tiene no menos de  $t-1$  elementos. Continuando así, paso a paso, obtendremos el resultado mencionado).

La condición de que el sistema sea finito es aquí de mucha importancia. Si retiramos esta condición, entonces, para, por ejemplo, un sistema infinito de conjuntos

$$S_0 = \{1, 2, 3, \dots, k, \dots\};$$

$$S_1 = \{1\};$$

$$\dots$$

$$S_k = \{k\};$$

$$\dots$$

no existe un s.r.d., aunque sí existe para cualquier parte de él.

**Otros sistemas de representantes de los conjuntos.** Los problemas de partición de los conjuntos condujeron al concepto de sistemas de representantes comunes. Sean dadas dos particiones diferentes de un mismo conjunto  $S$  en  $k$  componentes no vacías:

$$S = A_1 \cup A_2 \cup \dots \cup A_k; \quad S = B_1 \cup B_2 \cup \dots \cup B_k.$$

Si existe un subconjunto  $O$  del conjunto  $S$ , compuesto de  $k$  elementos, y si, además, dicho subconjunto es tal que su intersección con cualquiera de las componentes no es vacía:

$$O \cap A_i \neq \emptyset; \quad O \cap B_i \neq \emptyset; \quad i = 1, 2, \dots, k,$$

éste se denominará *sistema de representantes comunes* (s.r.c.) de las particiones dadas. En este caso cada una de las intersecciones resulta estar compuesta por un solo elemento. Los conjuntos de las particiones primera y segunda, tomados dos a dos y elegidos, si es necesario, de un modo correspondiente, tienen uno y sólo un elemento común, el cual es precisamente su representante común.

No es forzosamente obligatorio, por supuesto, que se cumpla el requerimiento de existencia de un solo elemento común. Pueden plantearse y tomarse en consideración condiciones diferentes: existencia de un número dado de elementos comunes, de un conjunto dado, etc. Por ejemplo, si exigimos que cada elemento  $s_i \in S$  figure no menos de  $k_{1i}$  y no más de  $k_{2i}$  veces ( $k_{2i} \geq k_{1i} \geq 1$ ) en el sistema de representantes comunes, este último se llamará sistema de un número limitado de representantes [28]. Está claro que el problema de s.r.d es un caso particular de tal problema para  $k_{1i} = 0$ ,  $k_{2i} = 1$ .

El otro caso particular en que

$$k_{1i} = \begin{cases} 1 & \text{para } i = 1, 2, \dots, l; \\ 0 & \text{para } i = l + 1, l + 2, \dots, m; \end{cases}$$

$$k_{2i} = 1 \text{ para } i = 1, 2, \dots, m,$$

lleva el nombre de problema sobre la existencia del s.r.d. que contiene el conjunto dado de elementos marginales  $s_1, s_2, \dots, s_l$ .

El criterio de existencia o no existencia del s.r.c. es próximo al criterio que se aplica al s.r.d.

**Teorema.** Dos particiones de un conjunto

$$S = A_1 \cup A_2 \cup \dots \cup A_k = B_1 \cup B_2 \cup \dots \cup B_k$$

tienen un s.r.d., cuando y sólo cuando la unión de cualesquiera  $m$  del conjunto  $A_i$  se intersecan no menos que con  $m$  del conjunto  $B_j$ , donde  $m = 1, \dots, k$ .

*Demostración.* La necesidad es obvia, igual que en el caso del s.r.d. La suficiencia se demuestra por reducción a los teoremas sobre el s.r.d.

En efecto, elijamos para cada  $B_i$ ,  $i = 1, 2, \dots, k$ , un conjunto  $S_i$  de todos los índices  $j \in K = \{1, \dots, k\}$  tales que  $A_j \cap B_i \neq \emptyset$ . Obtendremos una  $m$ -muestra  $M = (S_1, S_2, \dots, S_k)$  de subconjuntos del conjunto  $K$ . Para  $M$

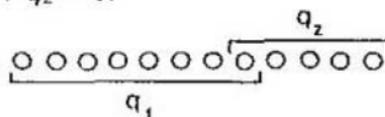
existe el s.r.d. (el criterio enunciado de existencia de un s.r.d. es el criterio de existencia del s.r.d. para  $M$ ). La elección de los distintos representantes da para cada  $B_i$  su  $A_j$ , con la particularidad de que su intersección es no vacía. En esta intersección puede elegirse por lo menos un elemento que sea común para  $A_j$  y  $B_i$ , es decir, su representante común.

El concepto de representantes de los conjuntos y de sistemas de representantes tiene en las matemáticas numerosas y variadas aplicaciones, como son, por ejemplo, los representantes de las clases de equivalencia. El método de sistemas de representantes se usa también en la teoría de las redes, al investigar la admisibilidad de los flujos, y en la teoría de ampliación de los cuadrados latinos.

### 3.3. PRINCIPIOS DE LA TEORÍA DE RAMSEY

La operación de partición de los conjuntos es el fundamento de una cantidad infinita de problemas prácticos. En este párrafo se describe el procedimiento que permite obtener los datos sobre el carácter de las propias particiones y sobre la posibilidad de realizar una partición del tipo prefijado de antemano.

Sea un  $n$ -conjunto  $S$ , cuyos elementos han de distribuirse en dos cajones. ¿Cuál debe ser el número  $n$ , para asegurar que  $q_1$  elementos caigan en el primer cajón, o que  $q_2$  elementos caigan en el segundo? La respuesta es casi evidente:  $n \geq q_1 + q_2 - 1$ .



Así pues, el número mínimo de elementos que aseguran la resolución del problema es igual a

$$N(q_1, q_2; 1) = q_1 + q_2 - 1.$$

Si se plantea un problema de distribución no entre dos, sino entre el mayor número (digamos,  $t$ ) de cajones, siendo  $q_1, q_2, \dots, q_t$  los números correspondientes que caracterizan el llenado requerido de los cajones, entonces

$$N(q_1, q_2, \dots, q_t; 1) = \sum_{i=1}^t q_i - (t - 1).$$

Ramsey [45] demostró en 1930 un teorema en el que generalizó estos resultados particulares. En lugar de la distribución de los elementos unidad del  $n$ -conjunto el teorema analiza la distribución de los  $r$ -subconjuntos del conjunto citado. Designemos con  $S_n$  el conjunto de  $n$  elementos y con  $P_r(S_n)$ , la colección de sus  $r$ -subconjuntos.

**Teorema de Ramsey.** Supongamos que  $r \geq 1$ ,  $q_i \geq r$  ( $i = 1, \dots, t$ ). Existe un número natural mínimo  $N = N(q_1, \dots, q_t; r)$  tal que para cualquier

$n \geq N$  y para toda  $t$ -partición ordenada  $P_r(S_n) = A_1 \cup \dots \cup A_t$ , se encontrará (para cierto  $i \in \{1, \dots, t\}$ ) un  $(q_i, A_i)$ -subconjunto, es decir, un  $q_i$ -subconjunto del conjunto  $S_n$ , cuyos  $r$ -subconjuntos están contenidos todos en  $A_i$ .

Hagamos previamente tres observaciones con el fin de facilitar la comprensión del teorema en su planteamiento y demostración.

1. Los ejemplos aducidos más arriba y referentes a las particiones de los conjuntos representan casos particulares del teorema de Ramsey para  $r = 1$ ,  $P_r(S) = S$ , y el  $(q_i, A_i)$ -conjunto es simplemente un  $q_i$ -subconjunto del conjunto  $A_i$ .

2. Para un caso particular en que  $t = 1$ , tenemos  $N(q_1, r) = q_1$ , lo que es trivial.

3. Si demostramos el teorema de Ramsey para  $t = 2$ , quedará válido también para  $t = 3$ . En efecto, sea

$$P_r(S) = A_1 \cup A_2 \cup A_3 = A_1 \cup (A_2 \cup A_3).$$

Denotemos  $A_2 \cup A_3 = A_2^*$ . Pongamos  $q_2^* = N(q_2, q_3; r)$ . Si  $n \geq N(q_1, q_2^*; r)$ , entonces, o bien  $S$  contiene el  $(q_1, A_1)$ -subconjunto, o bien  $S$  contiene el  $(q_2^*; A_2 \cup A_3)$ -subconjunto. El primer caso corresponde a la afirmación del teorema. En cambio, si tiene lugar el segundo caso, entonces el  $q_2^*$ -subconjunto del conjunto  $S$  contendrá, por hipótesis, o bien el  $(q_2, A_2)$ -conjunto o bien el  $(q_3, A_3)$ -subconjunto. Por lo tanto, nuestra afirmación es lícita. De aquí se deduce que resulta suficiente demostrar el teorema de Ramsey para  $t = 2$ , y, a continuación concluir por inducción, que es válido también para todo  $t > 2$  entero.

La demostración del teorema para el caso de  $t = 2$  empieza escribiendo las siguientes igualdades, considerándolas como iniciales:

$$N(q_1, q_2; 1) = q_1 + q_2 - 1; \quad N(q_1, r; r) = q_1; \quad N(r, q_2; r) = q_2. \quad (1)$$

La primera de estas igualdades ya la conocemos. En la segunda cualquier partición  $A_1 \cup A_2$  lleva o bien al  $(r, A_2)$ -subconjunto, si  $A_2$  es no vacío, o bien al  $(q_1; P_r(S))$ -subconjunto. En este caso  $q_1$  no es inferior a  $r$ . Cualquiera de estos casos corresponde exactamente a la formulación del teorema. Unos razonamientos no complejos mostrarán la validez también de la tercera igualdad. Además,

$$r > 1; \quad q_1 \geq r; \quad q_2 \geq r. \quad (2)$$

Así pues, ya podemos afirmar que existen los números  $N(2, 2, 2)$ ,  $N(3, 2, 2)$ ,  $N(4, 2, 2)$  etc., como también  $N(2, 3, 2)$ ,  $N(2, 4, 2)$ , etc. Las igualdades (1) y las desigualdades (2) sirven de datos iniciales para la demostración del teorema de Ramsey por inducción. El primer paso, pues, lo hicimos. El segundo paso, que da por terminada la demostración, consiste en demostrar la existencia de  $N(q_1, q_2; r)$  a condición de que existen

$$p_1 = N(q_1 - 1, q_2; r); \quad p_2 = N(q_1, q_2 - 1; r); \quad N(p_1, p_2; r - 1).$$

Por cuanto hasta el momento no se logra calcular exactamente  $N(q_1, q_2; r)$ , el sentido de la demostración consiste en estimar este número superiormente, demostrando la desigualdad

$$N(q_1, q_2; r) \leq N(p_1, p_2; r - 1) + 1.$$

En efecto, tomemos un conjunto  $S_n$ , donde  $n \geq N(p_1, p_2; r - 1) + 1$ , y fijemos en él un elemento  $a_0$ ; entonces,  $S_n \setminus \{a_0\} = S_{n-1}$ . Pasemos de la partición  $P_r(S_n) = A_1 \cup A_2$  a la  $P_{r-1}(S_{n-1}) = B_1 \cup B_2$  del modo siguiente: en el conjunto  $S_{n-1}$  tomamos por turno los  $(r - 1)$ -subconjuntos; si la unión de tal subconjunto, digamos, de  $B'$ , y del elemento fijo  $a_0$  integra  $A_1$ , entonces este  $(r - 1)$ -subconjunto  $B'$  lo atribuiremos a la clase  $B_1$ , y si la unión está contenida en  $A_2$ , entonces  $B'$  lo atribuiremos a la clase  $B_2$ .

El conjunto  $S_{n-1}$  tiene no menos de  $N(p_1, p_2; r - 1)$  elementos y para este conjunto el teorema es válido por hipótesis de inducción. Por consiguiente, en él se contiene o bien a) el  $(p_1, B_1)$ -subconjunto, o bien b) el  $(p_2, B_2)$ -subconjunto. Supongamos que tiene lugar el caso a). Esto significa que en  $S_{n-1}$  se contiene el  $p_1$ -conjunto  $T$ , cuyos  $(r - 1)$ -subconjuntos están contenidos todos en  $B_1$ . Pero,  $p_1 = N(q_1 - 1, q_2; r)$ ;  $T \subseteq S_n$ , y en este conjunto  $T$  existe o bien un  $(q_1 - 1)$ -subconjunto, cuyos  $r$ -subconjuntos integran todos  $A_1$ , o bien un  $q_2$ -subconjunto, cuyos  $r$ -subconjuntos integran todos  $A_2$ . Si tiene lugar el último caso, entonces obtendremos el  $q_2$ -conjunto que satisface las condiciones del teorema. Si en cambio, tiene lugar el primer caso, es decir, existe el  $(q_1 - 1)$ -subconjunto, cuyos  $r$ -subconjuntos integran todos  $A_1$ , entonces reunámoslo con el elemento fijo  $a_0$ . Obtendremos el  $q_1$ -conjunto integrado en  $S$ . Veamos sus  $r$ -subconjuntos. Si alguno de ellos no contiene  $a_0$ , será el  $r$ -conjunto que está contenido en  $A_1$ . Si él contiene  $a_0$ , entonces está compuesto por este elemento y el  $(r - 1)$ -subconjunto que integra  $B_1$ . Esto quiere decir que está integrado en  $A_1$ . Hemos obtenido el  $q_1$ -subconjunto del conjunto  $S_n$ , todos los  $r$ -subconjuntos del cual están contenidos en  $A_1$ .

Se ha examinado el caso en que el  $(p_1, B_1)$ -conjunto está contenido en  $S_{n-1}$ . El caso b) se demuestra de una manera análoga. El teorema de Ramsey queda demostrado.

A lo que parece para toda  $t$ -partición y para cualesquiera  $(q_1, q_2, \dots, q_t; r)$  convenientes, se puede determinar mín  $n = N(q_1, q_2, \dots, q_t; r)$ , cuya existencia está asegurada en virtud del teorema de Ramsey. Mas, este trabajo resultó ser extremadamente difícil, pues por ahora no se conoce ningún método para calcular estos números. Para  $t = r = 2$ , todos los números conocidos  $N(q_1, q_2; 2)$  se aducen en la Tabla 3.1 (si no se conocen los valores exactos, se dan las fronteras dentro de las cuales éstos están encerrados):

Los casos en que  $t > 2$  están poco estudiados por ahora. Se sabe, por ejemplo, que

$$\begin{array}{ll} N(3, 3, 3; 2) = 17; & N(5, 5, 5; 2) \geq 257; \\ N(4, 4, 4; 2) \geq 128 & N(6, 6, 6; 2) \geq 906. \end{array}$$

	3	4	5	6	7	8	9
3	6	9	14	18	23	28 ... 29	36
4	9	18	25 ... 28	34 ... 44			
5	14	25 ... 28	42 ... 55	57 ... 94			
6	18	34 ... 44	57 ... 94	102 ... 169			
7	23						
8	28 ... 29						
9	36						

Aún menos sabemos sobre los valores de los números de Ramsey para  $r > 2$ . Merece la atención el siguiente resultado importante:

$$13 \leq N(4, 4; 3) \leq 15.$$

Pese a las excepcionales dificultades y al avance lento, no cesan los esfuerzos que tienen por objeto determinar los números de Ramsey o de sus estimaciones (superiores e inferiores). Esto se explica por la peculiaridad del problema que admite numerosas interpretaciones y aplicaciones diversas. En la teoría de los grafos, por ejemplo, este problema se interpreta como un problema de coloración de las aristas de los grafos. El propio problema de buscar los números de Ramsey se considera, a menudo, para las clases aisladas de grafos.

Otra dirección, en la que se desarrolla la teoría de Ramsey, representa el estudio de las condiciones de existencia, es decir, de tales restricciones, bajo las cuales los planteamientos generalizados del problema resulten fundamentados, y las demostraciones, factibles.

Los problemas de la teoría de Ramsey se estudian ahora con un elevado grado de generalidad. Supongamos que el símbolo  $\binom{n}{k} \tau(l_1, \dots, l_r)$  significa lo siguiente: si los  $k$ -conjuntos de un  $n$ -conjunto  $S_n$  están partidos en  $r$  clases, entonces para cierto  $i$  existe un  $l_i$ -subconjunto  $L_i \subseteq S_n$  tal que todos los  $k$ -subconjuntos de  $L_i$  integran la  $i$ -ésima clase. En este caso el teorema de Ramsey se enuncia del modo siguiente:

**Teorema.** Para cualesquiera  $k, r, l_1, \dots, l_r$  naturales existe un  $N = N(k, r, l_1, l_r)$  tal que si  $n \geq N$ , entonces  $\binom{n}{k} \tau(l_1, \dots, l_r)$ .

En general, los teoremas de tipo Ramsey tienen la forma de las afirmaciones  $\binom{n}{k} \tau(C_1, \dots, C_r)$ , donde los símbolos  $A, B, C_1, \dots, C_r$  designan objetos (del conjunto) de estructura determinada. Los últimos pueden ser conjuntos con relaciones de orden sobre ellos, grafos e hipergrafos, espacios vectoriales finitos, conjuntos de soluciones de los sistemas de ecuaciones lineales, álgebras de Bool y particiones de los conjuntos finitos. Las generalizaciones relacionadas con el caso de los conjuntos finitos conducen al análisis de las operaciones con números cardinales. Los resultados conseguidos en este camino por ahora no son grandes.

## CAPÍTULO 4 APARATO TABULAR DE MATRIZ DEL ANÁLISIS COMBINATORIO

En este capítulo se analizan los conceptos y métodos combinatorios que están relacionados con la representación de los sistemas de conjuntos finitos en forma de tablas. Sirve de base para tales representaciones tabulares el concepto general de sistemas de incidencia.

### 4.1. SISTEMAS DE INCIDENCIA Y MATRICES ESPECIALES

Se denomina *sistema de incidencia* una terna ordenada  $(M, S, \varphi)$ , donde  $\varphi$  es una correspondencia binaria entre los conjuntos  $M$  y  $S$  (véase § 1.2). Por ejemplo, un plano puede ser representado como sistema de incidencia, si tomamos en calidad de  $S$  el conjunto de puntos del plano, en calidad de  $M$ , el conjunto de rectas y en calidad de  $\varphi$ , el conjunto de pares  $(a, b) \in M \times S$  que satisfacen la condición "el punto  $b$  se dispone en la recta  $a$ ". La correspondencia binaria  $\varphi$  en el sistema de incidencia recibe el nombre de *relación de incidencia*. En la mayoría de los casos los elementos del conjunto  $M$  se interpretan como ciertos subconjuntos del conjunto  $S$ , mientras que  $\varphi$  es simplemente una relación que caracteriza la pertenencia de los elementos del conjunto  $S$  a los subconjuntos de la familia  $M$ . Si  $M = \{S_1, \dots, S_m\}$ ,  $S = \{s_1, \dots, s_n\}$ , entonces a la relación  $\varphi$  le corresponderá biunívocamente la matriz  $A = [a_{ij}]$  de orden  $m \times n$ , donde  $a_{ij}$  (elemento de la  $i$ -ésima fila y de la  $j$ -ésima columna) es igual a la unidad, siempre que  $(S_i, s_j) \in \varphi$ , y a cero, en el caso contrario. En particular, cuando  $M = \{S_1, \dots, S_m\}$  se interpreta como un sistema de subconjuntos del conjunto  $S$ , entonces

$$a_{ij} = \begin{cases} 1, & \text{si } s_j \in S_i; \\ 0, & \text{si } s_j \notin S_i. \end{cases}$$

Esta matriz se llama *matriz de incidencia* para la familia de subconjuntos  $M = \{S_1, \dots, S_m\}$  respecto del conjunto  $S$ . Las unidades dispuestas en la  $i$ -ésima fila expresan elementos del subconjunto  $S_i$ , y las unidades dispuestas en la  $j$ -ésima columna señalan los subconjuntos que contienen  $s_j$ . La matriz  $A$  da una descripción completa del sistema de incidencia  $(M, S, \varphi)$ . Es *binaria*, esto es, se compone de símbolos de los tipos. Para que los cálculos sean más cómodos, se ha elegido aquí, a título de elementos de la matriz, 0 y 1 (en adelante las matrices de esta índole se llamarán  $(0, 1)$ -matrices), aunque se eligen, a veces, otros pares de magnitudes, por ejemplo,  $+1$  y  $-1$ .

El dominio de aplicación de las matrices de incidencia es muy amplio. Kirchhoff, por ejemplo, las introdujo para investigar los circuitos eléctricos; A. Poincaré, en la topología, etc.

Los teoremas del análisis combinatorio se interpretan frecuentemente e, incluso, se demuestran con ayuda de las matrices de incidencia. Por ejemplo, en el § 3.2 se ha enunciado el teorema de P. Hall sobre el sistema de representantes distintos. De su análogo matricial sirve el

**Teorema de König [46].** En una matriz rectangular el número mínimo  $m$  de líneas (de filas y de columnas) que contienen todos los elementos no nulos, es igual al número máximo  $M$  de dichos elementos elegidos de un modo tal que de ellos cualesquiera dos no están dispuestos en una línea.

*Demostración.* Basta estudiar el caso en que viene dada una  $(0,1)$ -matriz rectangular  $A = [a_{ij}]$ ,  $i = 1, 2, \dots, n$ ;  $j = 1, 2, \dots, t$ . La demostración de que  $m = M$  consta de dos etapas; al principio se demuestra que  $m \geq M$ , luego que  $M \geq m$ . La primera desigualdad es obvia, pues ninguna línea contiene más de un elemento de los  $M$  elegidos. Demostremos la segunda desigualdad.

Supongamos que  $m$  líneas están compuestas por  $r$  filas y  $s$  columnas:  $m = r + s$ . Permutemos estas filas y columnas de un modo tal que ellas ocupen los primeros lugares. A cada  $j$ -ésima fila ( $i = 1, \dots, r$ ) pongámosle en correspondencia un conjunto de números de las columnas  $j$ , para las cuales  $a_{ij} = 1$ ,  $j > s$ . Los conjuntos obtenidos satisfacen las condiciones del teorema de P. Hall. Efectivamente, si esto no fuera así, es decir, si  $k$  de los conjuntos citados contienen  $v < k$  elementos, dichas  $k$  filas pueden ser sustituidas por  $v$  columnas y todas las unidades figurarán en el número menor de líneas, lo que contradice la condición de que  $m$  es el número mínimo. Por cuanto la condición del teorema de P. Hall se cumple, se pueden elegir  $r$  representantes distintos de  $r$  filas, es decir,  $r$  unidades de manera tal que haya dos unidades en una fila y ninguna, en las primeras  $s$  columnas. Razonando análogamente, se pueden obtener  $s$  representantes de  $s$  primeras columnas de un modo tal que estén ausentes en las primeras  $r$  filas. Este conjunto de  $r + s = m$  unidades está elegido de una manera tal que no hay dos de ellas que se dispongan en una línea. Esto quiere decir, que  $m \leq M$ , lo que se trataba de demostrar.

La demostración aludida aquí se apoya en el teorema de P. Hall. Este último puede demostrarse también apoyándose en el teorema de König. Sean un conjunto  $S$  y un sistema de sus  $n$  subconjuntos. Construyamos la  $(0, 1)$ -matriz de incidencia. Supongamos que todas las unidades de ésta se disponen en  $r$  filas y  $s$  columnas. Si  $r + s = n$ , entonces, según el teorema de König, existen  $n$  unidades, de las cuales cualesquiera dos no están en una misma línea, y ellas forman el s.r.d para  $n$  conjuntos. Si, en cambio,  $r + s < n$ , entonces la validez del teorema de P. Hall se perturba, puesto que para  $k = n - r$  filas las unidades figurarán sólo en  $s < n - r = k$  columnas.

Las matrices binarias se utilizan en el análisis combinatorio al investigar las estructuras de los conjuntos discretos. La teoría de las matrices binarias experimentó en los últimos años un desarrollo considerable precisamente merced al papel creciente (práctico y teórico) del análisis combinatorio.

Según sea el tipo de problemas combinatorios, en el proceso de su resolución aparecen diferentes tipos de matrices. Las operaciones sobre ellas se realizan, por supuesto, de acuerdo con las reglas generales de la teoría de matrices. Así, por ejemplo, a la par con las sumas y los productos ordinarios, están determinadas para ellas las sumas y los productos directos (de Kronecker). Recordemos que la *suma directa* de la matriz  $A = [a_{ij}]$  de  $n$ -ésimo orden con la matriz  $B$  de orden  $m$  se representa por una matriz de orden  $n + m$  que tiene la forma

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

y el *producto directo* de estas matrices es una matriz de orden  $nm$  que tiene la forma

$$\begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \dots & \dots & \dots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}.$$

Más abajo estudiaremos ciertos tipos especiales de las matrices que con mayor frecuencia se usan en el análisis combinatorio.

**Matrices conmutables.** Son matrices de incidencia para el caso en que  $S = M = \{1, \dots, n\}$ , y la relación de incidencia  $i\varphi j$  significa que el elemento  $i$  se dispone en el  $j$ -ésimo lugar de cierta permutación fija de números  $1, \dots, n$ . Sea, por ejemplo, una permutación  $(5, 3, 4, 1, 2)$ . La matriz correspondiente será

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Sus filas corresponden a los números de los elementos de la permutación, y las columnas, a los números ordinales de los lugares.

Así pues, una matriz conmutable es la  $(0, 1)$ -matriz cuadrada, en la cual cada línea (fila o columna) contiene exactamente una unidad. La matriz conmutable posee la propiedad de que

$$PP^T = I,$$

donde  $P^T$  es una matriz transpuesta, e  $I$ , una matriz unidad. Esta propiedad se emplea con frecuencia a título de definición de la matriz conmutable.

Las matrices conmutables, siendo las más simples, son de interés en primer lugar por el hecho de que a través de ellas pueden expresarse otras matrices más complejas (véase más abajo el teorema de Birkhoff).

**Matrices de congruencia de dos en dos.** Estas son matrices de incidencia para el caso en que  $M = S$ , y la relación de incidencia  $\varphi$  es antisimétrica y satisface las condiciones:

a) para cualquier  $s \in S$ :  $(s, s) \notin \varphi$  (irreflexividad);

b) para cualesquiera diferentes  $s_i, s_j \in S$  ( $i \neq j$ ): o bien  $(s_i, s_j) \in \varphi$ , o bien  $(s_j, s_i) \in \varphi$ .

Tal relación puede interpretarse como resultado de un torneo circular con participación de  $|S|$  jugadores. La matriz de incidencia es la tabla de este torneo, en la que la diagonal está ocupada por ceros ( $a_{ii} = 0$ ). El premio del  $i$ -ésimo jugador y del  $j$ -ésimo se nota como  $a_{ij} = 1$ ,  $a_{ji} = 0$ .

Así pues, las matrices de congruencia de dos en dos son binarias, cuadradas, con ceros en la diagonal principal. Ellas satisfacen la ecuación matricial

$$A + A^T = J - I,$$

donde  $A$  es una matriz de congruencia de dos en dos,  $A^T$  es la matriz transpuesta  $A$ ,  $I$  es una matriz unidad y  $J$ , una matriz compuesta por ceros.

**Matrices de Hadamard.** Así se llaman las matrices cuadradas binarias  $H$  (abreviadamente de Hadamard), compuestas de unidades positivas y negativas, que satisfacen la ecuación matricial

$$H \cdot H^T = nI,$$

donde  $n$  es el orden de la matriz  $H$ ;  $I$  es la matriz unidad de  $n$ -ésimo orden;  $H^T$ , la matriz  $H$  transpuesta. De la definición proviene que cada dos filas de la matriz  $H$  son ortogonales, y, además, que  $|\det H| = n^{n/2}$  y  $H^{-1} = n^{-1}H^T$ , de donde

$$H \cdot H^T = H^T \cdot H = nI.$$

Si en una matriz de Hadamard multiplicamos cualquier línea (sea fila o columna) por  $-1$ , la matriz conserva sus cualidades de Hadamard. Las matrices obtenidas del modo citado se consideran equivalentes. Si  $H_1$  y  $H_2$  son equivalentes, entonces

$$H_2 = PH_1Q,$$

donde  $P$  y  $Q$  son matrices conmutables, en las cuales, sin embargo, el único elemento no nulo de la línea es igual a  $+1$ , o bien a  $-1$ . Multiplicando las filas o columnas por  $-1$ , podemos normalizar las matrices de Hadamard, es decir, reducirlas a una forma en que la primera fila y la primera columna están compuestas sólo por las unidades positivas. Las matrices de Hadamard normalizadas de órdenes 1 y 2 son

$$(1) \quad \text{y} \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

En lo que atañe a las matrices de orden  $n \geq 3$ , resulta que si existen, entonces  $n \equiv 0 \pmod{4}$ . Efectivamente, conmutemos en la matriz de

Hadamard las columnas de un modo tal que en la segunda fila la primera mitad de términos conste sólo de unidades positivas, y la segunda mitad, de unidades negativas. Examinemos la tercera fila. Supongamos que en los primeros  $n/2$  lugares encontramos  $t$  unidades positivas y en los segundos  $t'$  unidades positivas. Entonces, por definición,

$$2t + 2t' = n;$$

$$2t - 2t' = 0,$$

de donde  $n = 4t$ . No obstante, la demostración de la existencia de las matrices en el sentido de su construcción eficaz es un proceso que avanza con lentitud, pese a la diversidad de los métodos inventados.

Observemos que los productos directos de las matrices de Hadamard son también matrices de Hadamard. Se sabe que estas matrices de orden  $n$  existen, en particular, en los siguientes casos (véase [47]):

1.  $n = 2^r$ ;
2.  $n = p^r + 1 \equiv 0 \pmod{4}$ , donde  $p$  es un número primo;
3.  $n = (h - 1)^2 + 1$ , donde  $h$  es un producto de los números del tipo 1 y 2;
4.  $n = h(h + 3)$ , donde  $h$  y  $h + 4$  son productos de los números del tipo 1 y 2;
5.  $n = h(h - 1)$ , donde  $h$  es un producto de los números del tipo 1 y 2;
6.  $n = 92, 116, 156, 172$ ;
7.  $n = q(q + 2) + 1$ , donde  $q$  y  $q + 2$  son potencias de los números primos;
8.  $n$  es igual al producto de cualesquiera números mencionados más arriba.

Para el caso incierto mínimo de existencia de las matrices de Hadamard tenemos:  $n = 268$ .

**Matrices estocásticas.** Este tipo de matrices surgió para ser aplicado en el aparato combinatorio de la teoría de probabilidades. Una matriz se llama estocástica por filas (columnas), si sus elementos son no negativos y la suma de ellos en cada fila (columna) es igual a 1. Una matriz se llama dos veces estocástica, si es estocástica tanto por filas, como por columnas. No es difícil mostrar que una matriz dos veces estocástica es cuadrada. Un producto de las matrices dos veces estocásticas de igual orden será matriz dos veces estocástica. Efectivamente, si  $C = [c_{ij}]^n$ ,  $A = [a_{ij}]^n$ ,  $B = [b_{ij}]^n$ ,  $C = A \cdot B$ , entonces

$$c_{ij} = \sum_{l=1}^n a_{il} b_{lj} \geq 0, \quad \sum_{j=1}^n c_{ij} = \sum_{l=1}^n a_{il} \sum_{j=1}^n b_{lj} = 1,$$

y, por analogía,  $\sum_{i=1}^n c_{ij} = 1$ .

En una matriz cuadrada de  $n$ -ésimo orden, se llamará *transversal* a un juego de  $n$  elementos, en el que ningún par de ellos está dispuesto en una misma línea (fila o columna).

**Lema.** Una matriz dos veces estocástica tiene la transversal compuesta de los elementos no nulos.

*Demostración.* Sea  $A = [a_{ij}]$  una matriz dos veces estocástica. Incluyamos todos los elementos no nulos de la matriz en  $p$  columnas y  $q$  filas de un modo tal que la suma  $p + q$  asuma el valor mínimo posible. Con arreglo al teorema de König, el número máximo de elementos no nulos de  $A$ , de los cuales ningún par se dispone en una misma línea, es igual a  $p + q$ . Por cuanto todos los elementos no nulos de  $A$  pueden encerrarse dentro de  $n$  filas, entonces  $p + q \leq n$ . Por otra parte,

$$n = \sum_{i,j=1}^n a_{ij} \leq p + q.$$

Por consiguiente,  $p + q = n$ , y en la matriz se encontrará una transversal compuesta por elementos no nulos.

**Teorema de Birkhoff.** Para toda matriz dos veces estocástica de orden  $n$  es válido el desarrollo:  $A = \sum_{i=1}^k \lambda_i P_i$ , donde  $P_i$  son matrices conmutables,  $\lambda_i > 0$ ,  $\sum_{i=1}^k \lambda_i = 1$ ,  $k \leq n^2 - n + 1$ .

*Demostración.* De acuerdo con el lema, en la matriz  $A$  existe una transversal compuesta por elementos no nulos. Supongamos que el mínimo de dichos elementos es igual a  $\lambda_1 > 0$  ( $\lambda_1 \neq 1$ , pues, de lo contrario, la matriz  $A$  será conmutable y la afirmación del teorema se hará trivial):  $P_1$  es una matriz conmutable correspondiente a la transversal. Por cuanto la matriz  $(1 - \lambda_1)^{-1}(A - \lambda_1 P_1)$  es dos veces estocástica, entonces en la matriz  $A - \lambda_1 P_1$  existe una transversal compuesta de los elementos no nulos. Designemos con  $\lambda_2$  el mínimo de ellos, etc. La matriz  $A - \sum_{i=1}^j \lambda_i P_i$  contiene no menos de  $j$  elementos nulos, razón por la cual el proceso citado es finito y se dará por terminado no más tarde que el  $(n^2 - n + 1)$ -ésimo paso. Esto se debe a que después de realizarse el  $(n^2 - n + 1)$ -ésimo paso, la matriz  $A - \sum_{i=1}^{n^2-n+1} \lambda_i P_i$ , en la que las sumas de elementos en las filas y en las columnas son iguales, contendría no más de  $(n - 1)$  elementos no nulos, por lo cual todos los elementos de esta matriz serían nulos.

Observemos que la estimación del número  $k$  en el teorema de Birkhoff puede ser precisada:  $k \leq n^2 - 2n + 2$ , con la particularidad de que existen matrices de orden  $n$ , dos veces estocásticas, las cuales no son representables en forma de una combinación lineal de menos que  $n^2 - 2n + 2$  matrices conmutables.

Al resolver problemas de carácter combinatorio surge la necesidad de emplear, además, otros tipos de matrices especiales. No será nuestra aspiración enumerarlas y describirlas. Nos limitaremos sólo al análisis de algunos accesos generales que pueden ser aplicados a la investigación de tales matrices.

Ya hace tiempo que en las matemáticas se acostumbra a comenzar el

estudio de las propiedades de las clases de objetos por la búsqueda de las invariantes y el análisis de los mismos. Una de las invariantes más importantes de cualquier matriz es el permanente de ésta. Al permanente le dedicamos un párrafo especial de este capítulo (4.4).

Estudiemos otras direcciones notables en este sentido. Ultimamente en las investigaciones teóricas de las matrices binarias se pasa, con una frecuencia cada vez mayor, del análisis de los tipos particulares de las matrices al estudio de sus clases. Se utilizan en dicho estudio las nociones de rango de frontera, de  $\alpha$ -anchura y otras. Se denomina *traza* de una matriz a la suma de los elementos que constituyen su diagonal principal; el valor máximo para la traza, obtenido para toda clase de permutaciones de las filas y columnas de una matriz, recibe precisamente el nombre de *rango de frontera* (rango límite). Se llama  $\alpha$ -anchura de la matriz a un número mínimo de columnas que pueden elegirse en ella de una manera tal que la suma de sus valores en cada fila sea no inferior a  $\alpha$ .

He aquí uno de los procedimientos que se usa para elegir las clases de las matrices. Sea  $A$  una  $(0, 1)$ -matriz de dimensión  $m \times n$ . Las sumas de sus elementos por filas la denotamos con  $r_i$ ;  $i = 1, 2, \dots, m$  y por columnas, con  $s_j$ ;  $j = 1, 2, \dots, n$ . Es evidente que

$$\sum_{i=1}^m r_i = \sum_{j=1}^n s_j = \tau.$$

Haciendo uso de las totalidades de las sumas de las filas y de las sumas de las columnas de la matriz  $A$ , formamos los vectores correspondientes:

$$R = (r_1, r_2, \dots, r_m); \quad S = (s_1, s_2, \dots, s_n).$$

Al contrario, fijando los vectores  $R$  y  $S$ , cuyas componentes están representadas por los números no negativos, hallamos que ellos definen la clase de  $(m \times n)$ -matrices  $A$ , la cual se denotará con  $\mathcal{A}(R, S)$ . Para las clases  $\mathcal{A}(R, S)$  están determinadas las condiciones necesarias y suficientes del estado no vacío. Sin embargo, en esta parte del análisis combinatorio las investigaciones sólo acaban de iniciarse. Ni siquiera existe un método regular para calcular los números de todas las matrices de esta clase o, por lo menos, de las matrices normalizadas, es decir, tales en las que las líneas que constan solamente de ceros están tachadas y las líneas restantes están permutadas de un modo tal que

$$r_1 \geq r_2 \geq \dots \geq r_m > 0; \quad s_1 \geq s_2 \geq \dots \geq s_n > 0.$$

Para las clases de matrices se estudian los valores máximos y mínimos de los permanentes, de los rangos de frontera, de la  $\alpha$ -anchura, etc.

## 4.2. RECTÁNGULOS Y CUADRADOS LATINOS

Así se denominan las disposiciones de los elementos por filas y por columnas, cuando los elementos en las líneas (tanto en las filas, como en columnas) no se repiten. La denominación "latinos" se debe, pro-

bablemente, a Euler quien usó, al estudiar la disposición de este tipo, las letras del alfabeto latino a título de sus elementos.

Sea dado un  $n$ -conjunto  $S$ . El problema de construcción sobre él (a base de sus elementos) de un  $(r \times s)$ -rectángulo latino se reduce a la construcción de una tabla  $(r \times s)$ -rectangular en la cual las líneas serán representadas, respectivamente, por las  $r$ - y  $s$ -permutaciones sin repetición de los elementos del conjunto  $S$  (evidentemente,  $r, s \leq n$ ). Por ejemplo, la disposición

2	1	5	7	3
1	3	2	4	5
7	4	1	8	2
5	2	3	1	6

representará un  $(4 \times 5)$ -rectángulo latino para  $S = \{1, 2, \dots, 8\}$ . En los  $(r \times n)$ -rectángulos latinos las filas son permutaciones, elegidas de un modo tal que los elementos en las columnas no se repitan. Por ejemplo,

1	2	3	4	5	6
3	1	2	6	4	5
2	4	6	5	3	1
5	3	4	1	6	2

es un  $(4 \times 6)$ -rectángulo latino para  $S = \{1, 2, \dots, 6\}$ . Si la primera fila de un rectángulo latino es tal que sus elementos quedan dispuestos en un orden fijado de antemano (con mayor frecuencia como  $1, 2, \dots, n$ ), entonces el rectángulo se llama *normalizado*. El ejemplo que acabamos de aducir puede considerarse como ejemplo de rectángulo latino normalizado. Se analizan, a veces, rectángulos latinos que están normalizados no sólo por la primera fila, sino también por la primera columna.

Los rectángulos latinos que pueden obtenerse uno del otro mediante las permutaciones de las líneas y la reenumeración de los elementos se denominan *equivalentes*. Es fácil ver que para cada rectángulo latino existe un rectángulo equivalente normalizado por la primera fila y por la primera columna.

Resulta natural preguntar ¿cuántos rectángulos latinos del tipo dado pueden existir? Sea  $L(r, n)$  el número de todos los  $(r \times n)$ -rectángulos latinos y  $N(r, n)$ , el número de  $(r \times n)$ -rectángulos latinos normalizados. Es obvio que

$$L(r, n) = n!N(r, n);$$

con la particularidad de que

$$L(1, n) = n!; \quad N(1, n) = 1.$$

Por cuanto los rectángulos latinos normalizados de dos filas son, en ausencia, desórdenes, su número será igual al número de desórdenes:

$$N(2, n) = n! \left( \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \dots + \frac{(-1)^n}{n!} \right) = D_n,$$

y, respectivamente,

$$L(2, n) = n! N(2, n) = n! D_n.$$

Sin embargo, ya para el cálculo del número de rectángulos latinos de tres filas se necesitó superar dificultades mucho más grandes. Examinemos primeramente un tipo particular de tales rectángulos:

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & \dots & n-1 & n \\ 2 & 3 & 4 & & \dots & n & 1 \\ a_1 & a_2 & a_3 & & \dots & & a_n \end{array}$$

y tratemos de determinar su número. El problema planteado de este modo es equivalente, en particular, al problema sobre el número de conmutadores, cuyos  $2n$  jacks se disponen por un círculo, están unidos dos a dos y, además, ninguno de dos jacks vecinos están unidos entre sí. Este problema se conoce en otra interpretación, a saber, como problema sobre el número de colocaciones de  $n$  cónyuges en una mesa redonda bajo la condición de que ningún par conyugal se sienta juntos. La preocupación inicial es, naturalmente, sobre las damas; ellas se acomodan de  $2n!$  maneras, quedándose vacantes las sillas a la derecha y a la izquierda de cada dama. Las sillas desocupadas se numeran  $1, 2, \dots, n$ . Ahora está claro que el primer conyuge no puede sentarse en las sillas primera y segunda; el segundo, en las sillas  $2^a$  y  $3^a$ , etc. hasta el  $n$ -ésimo conyuge, para el cual están "prohibidas" las sillas  $1^a$  y  $n$ -ésima. El problema se resuelve por la fórmula del método de inclusiones y exclusiones con las propiedades  $p_i: a_i = i$ , o bien  $i + 1$  ( $i = 1, 2, \dots, n - 1$ ),  $a_n = n$  ó  $a_1 = 1$ . El número buscado es:

$$U_n = n! - 2n(n-1)! + \dots + (-1)^r \frac{2n}{2n-r} \binom{2n-r}{r} (n-r)! + \dots \\ \dots + (-1)^n \cdot 2.$$

En el caso general, el número de todos los rectángulos latinos de tres filas compuestos de  $n$  elementos se determina por la fórmula (véase [48]):

$$N(3, n) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{k} D_{n-k} D_k U_{n-2k}.$$

Los números de  $(3 \times n)$ -rectángulos latinos resultaron ser muy grandes. Los rectángulos latinos están por ahora débilmente estudiados, lo que se debe, probablemente, a la complejidad de las demostraciones y los enormes valores de sus números. En lo que se refiere a los rectángulos latinos con un número mayor de filas, podemos decir que en este dominio, en general, es poco lo que se conoce (véase [49]). En relación con esto no disminuye la importancia de las fórmulas asintóticas. Partiendo de los resultados conocidos:

$$L(2, n) = n! D_n \sim (n!)^2 e^{-1}; \quad L(3, n) \sim (n!)^3 e^{-3};$$

se ha supuesto que

$$L(k, n) \sim (n!)^k e^{-\binom{k}{2}}.$$

Esta hipótesis para  $k < n^{1/3}$  fue demostrada por Yamamoto [50].

A pesar de que las tentativas de estimar superiormente el número de  $(k \times n)$ -rectángulos latinos posibles no han llevado todavía a resultados exactos, ya podemos ver que este número es muy grande y crece rápidamente con el aumento de  $k$ . Esto se confirma con el hecho de que puede obtenerse la estimación inferior empleando la idea de ampliación de los rectángulos latinos.

Ampliar el rectángulo latino significa agregarle filas y columnas de tal modo que el rectángulo siga siendo latino. Esto sólo será posible, si el número de filas y columnas no sobrepasa el número de elementos  $n$ . La demostración de la posibilidad de ampliar un rectángulo se realiza por una simple repetición de los razonamientos que conducen a la adición de una fila por debajo y una columna, a la derecha. Como límite de ampliación interviene el cuadrado latino de orden  $n$ .

Sea dado un rectángulo latino  $\mathcal{L}(r, n)$  de  $n$  elementos, los cuales se designarán con  $1, 2, \dots, n$ . Planteemos el problema de ampliar  $\mathcal{L}(r, n)$  hasta que se obtenga  $\mathcal{L}(r+1, n)$ . Veamos las columnas  $j = 1, 2, \dots, n$ , y a cada  $j$ -ésima columna pongámosle en correspondencia un conjunto  $S_j$  compuesto de  $n-r$  elementos que no han integrado la columna dada. Obtendremos una colección  $M = (S_1, S_2, \dots, S_n)$ , donde cada conjunto  $S_i$  consta de  $n-r$  elementos.

El problema de ampliación de  $\mathcal{L}(r, n)$  hasta  $\mathcal{L}(r+1, n)$  se reduce ahora a la construcción de un s.r.d. para la colección  $M$ . Demostremos que tal s.r.d. existe. Efectivamente, tomemos  $\mathcal{L}(r, n)$ . Todo elemento  $i$  de  $n$  elementos se encuentra en él  $r$  veces. En los conjuntos  $S_1, S_2, \dots, S_n$  el citado elemento se encuentra  $(n-r)$  veces. Elijamos cualesquiera  $k$  conjuntos de  $S_1, S_2, \dots, S_n$ . En ellos habrá  $k(n-r)$  elementos, contando también los que se repiten. Pero, cada elemento se encuentra no más de  $n-r$  veces. Esto quiere decir que  $k$  conjuntos elegidos tienen no menos de  $k$  elementos distintos. La condición de existencia del s.r.d. está cumplida, lo que demuestra precisamente la posibilidad de la ampliación requerida.

La resolución del problema de ampliación de los rectángulos latinos permite dar una estimación inferior para el número de ellos. A saber, existen  $n!$  rectangulares latinos  $\mathcal{L}(1, n)$ , cada uno de los cuales puede ser ampliado por lo menos hasta  $(n-1)$  rectángulos latinos  $\mathcal{L}(2, n)$ . Por consiguiente, existen al menos  $n!(n-1)!$  rectángulos  $\mathcal{L}(2, n)$ . Razonando de esta manera, llegaremos a la conclusión de que existe por lo menos

$$n!(n-1)! \dots (n-r+1)!$$

rectángulos latinos  $\mathcal{L}(r, n)$ .

Los cuadrados latinos en los que ahora concentraremos nuestra aten

ción representan un caso particular de los rectángulos latinos  $\mathcal{L}(r, s)$  para  $r = s = n$ . En otras palabras, los cuadrados latinos son nada más que  $(n \times n)$ -arreglos de  $n$  elementos, donde las filas y columnas son permutaciones de dichos elementos. Por ejemplo, todos los 4 cuadrados latinos posibles dos veces normalizados de cuarto orden son:

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
2	3	4	1	2	1	4	3	2	1	4	3	2	4	1	3
3	4	1	2	3	4	1	2	3	4	2	1	3	1	4	2
4	1	2	3	4	3	2	1	4	3	1	2	4	3	2	1

La existencia de los cuadrados latinos de cualquier orden se asegura no sólo por los razonamientos combinatorios generales, sino también por el hecho de que todo cuadrado latino puede interpretarse como la tabla de Cayley, es decir, la tabla de multiplicación en cierto casi grupo finito. Con el fin de calcular el número de cuadrados latinos y estimar este número superiormente hemos de superar, prácticamente, las mismas dificultades que tuvimos en el caso de los rectángulos latinos, en particular, las estimaciones inferiores tienen por expresión  $(r - n)$ :

$$n!(n - 1)! \dots 2!!!.$$

Los cálculos del número de cuadrados latinos han mostrado que esta estimación es muy aproximada. Designemos con  $L(n)$  el número de cuadrados latinos dos veces normalizados y con  $L(n)$ , el número de cuadrados latinos no equivalentes de orden  $n$ . Entonces, el número de todos los cuadrados latinos de  $n$ -ésimo orden es igual a  $n!(n - 1)!L(n)$ . Todos los números conocidos  $I(n)$  y  $\tilde{L}(n)$  se exponen en la siguiente tabla (véase [20]):

Tabla 4.1

$n$	$I(n)$				$\tilde{L}(n)$		
1				1	1		
2				1	1		
3				1	1		
4				4	2		
5				56	2		
6			9	408	22		
7			16	942	080	563	
8		535	281	401	856	1 676	257
9	377	597	570	964	258	816	

En la teoría de los cuadrados latinos los problemas que mayor interés provocan son los relacionados con el concepto de ortogonalidad. Dos cuadrados latinos se llaman *ortogonales*, si al superponer uno de ellos sobre el otro se obtienen todos los pares de elementos ordenados sin repetición.

Dicho de otro modo, dos cuadrados latinos de orden  $n$ :

$$A_1 = [a_{ij}^{(1)}]; \quad A_2 = [a_{ij}^{(2)}]; \quad i, j = 1, 2, \dots, n,$$

se llaman ortogonales, si todos los  $n^2$  pares  $(a_{ij}^{(1)}, a_{ij}^{(2)})$  son distintos.

El estudio de la ortogonalidad de los cuadrados latinos tiene por origen el problema ampliamente conocido de Euler sobre 36 oficiales que llegaron de 6 regimientos. Cada regimiento asignaba 6 oficiales de rangos militares distintos. Se necesitaba incluir dichos oficiales en una formación de cuadro de un modo tal, que en ninguna línea hubiera repeticiones ni de rangos ni de nombres de regimientos. Dicho de otro modo, se planteaba el problema de construir dos cuadrados latinos ortogonales de sexto orden.

El problema sobre la construcción de un par de cuadrados latinos ortogonales de sexto orden no admitía resolución y Euler llegó a la conclusión de que tal par no existía. En una obra relacionada con este tema y publicada en 1782 Euler emitió la hipótesis de que la imposibilidad de hallar la solución se extendía también a los casos de  $n = 10$ ,  $n = 14$ , y, en general, de  $n \equiv 2 \pmod{4}$ , es decir,  $n = 2, 6, 10, 14, 18, \dots$ .

Solamente pasados 118 años se dio la primera respuesta a la hipótesis de Euler. G. Tarry [51] confirmó la hipótesis a principios del siglo XX para  $n = 6$ , construyendo y arreglando una y otra vez todos los cuadrados latinos de sexto orden. La comprobación ulterior de la hipótesis se demoró de nuevo. Sólo para el año 1960 se demostró que los pares de cuadrados latinos ortogonales existían para cualquier orden, a excepción de  $n = 2$  y  $n = 6$ , que resultaron ser la única excepción (véase [53]).

Como generalización natural del concepto de par de cuadrados latinos ortogonales interviene el conjunto compuesto por más de dos cuadrados latinos ortogonales dos a dos. Tal conjunto también se llama ortogonal. Reenumeremos los elementos de los cuadrados de una manera tal que quede normalizada la primera fila de cada cuadrado (al reenumerar los elementos de un cuadrado, la propiedad de ortogonalidad queda intacta). Entonces, los primeros elementos de las segundas filas deben ser diferentes y no iguales a 1. Por consiguiente, el número de cuadrados latinos ortogonales dos a dos de orden  $n$  no puede ser superior a  $n - 1$ . Un conjunto ortogonal se denomina *completo*, si en él están contenidos exactamente  $n - 1$  cuadrados.

En la teoría de los cuadrados latinos ortogonales se distinguen dos grandes problemas: el problema de existencia de los pares y de las familias de cuadrados latinos ortogonales y el de su construcción. Estos dos problemas están estrechamente ligados, puesto que la demostración de la existencia con frecuencia también resulta ser construcción. El problema de existencia de los conjuntos de cuadrados latinos ortogonales resultó ser bastante difícil, y las demostraciones de los teoremas correspondientes, complejas y engorrosas. Damos a conocer aquí sólo algunos resultados.

1. No para todo cuadrado latino existe otro cuadrado latino que sea ortogonal al primero.

Este hecho, al igual que las condiciones de existencia, fue establecido en [52].

2. Si  $n = p^\alpha$ , donde  $p$  es un número primo y  $\alpha$ , un número natural, entonces para  $n \geq 3$  existe un conjunto completo de  $n - 1$  cuadrados latinos ortogonales.

*Demostración.* Para cualquier  $n = p^\alpha$  existe el campo de Galois. Supongamos que  $a_0 = 0$  y  $a_1 = 1, a_2, a_3, \dots, a_{n-1}$  son elementos del campo de Galois. Construyamos  $n - 1$  matrices de orden  $n$  del modo siguiente:

$$A = [a_{ij}^{(l)}]; \quad i, j = 1, 2, \dots, n - 1; \quad l = 1, 2, \dots, n - 1$$

donde

$$a_{ij}^{(l)} = a_l a_i + a_j.$$

Esta familia de matrices  $A_l$  será precisamente el conjunto completo de cuadrados latinos ortogonales. En efecto:

a) cada una de las matrices construidas es un cuadrado latino, pues si cualquiera de ellas, digamos  $A_l$ , tiene dos elementos iguales en una misma fila, existen  $j$  y  $j'$  tales que

$$a_l a_i + a_j = a_l a_i + a_{j'}.$$

de donde

$$a_j = a_{j'}.$$

En cambio, si admitimos que dos elementos iguales figuran en una misma columna, entonces han de existir distintos  $i$  e  $i'$  tales que

$$a_l a_i + a_j = a_l a_{i'} + a_j;$$

y, por cuanto  $a_l \neq 0$ , tenemos  $a_i = a_{i'}$ , y, por lo tanto  $i = i'$ .

b) cada par de dichas matrices es ortogonal. Sea  $1 \leq l < f \leq n - 1$ , y supongamos que  $A_l$  no es ortogonal respecto de  $A_f$ , entonces existen  $i, i', j, j'$  tales que

$$(a_{ij}^{(l)}, a_{ij}^{(f)}) = (a_{i'j'}^{(l)}, a_{i'j'}^{(f)}),$$

es decir,

$$\begin{aligned} a_l a_i + a_j &= a_l a_{i'} + a_{j'}; \\ a_f a_i + a_j &= a_f a_{i'} + a_{j'}. \end{aligned}$$

De aquí

$$a_i(a_l - a_f) = a_{i'}(a_l - a_f),$$

y, por cuanto  $a_l \neq a_f$ , tenemos  $a_i = a_{i'}$ , de donde  $i = i'$ , y por lo tanto  $j = j'$ . El conjunto buscado está, de este modo, construido.

3. Enunciemos ahora una afirmación más general. Sean dados un número natural arbitrario  $n$  y su desarrollo en potencias naturales de los

distintos números primos:  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ . Sea

$$t = \min(p_i^{\alpha_i} - 1); \quad t = 1, 2, \dots, N.$$

Si  $t \geq 2$ , existe una familia de  $t$  cuadrados latinos ortogonales de orden  $n$ .

Efectivamente, se ha demostrado anteriormente que para cada  $n_i = p_i^{\alpha_i}$ ,  $i = 1, 2, \dots, N$  existe una familia  $n_i - 1$  (y por tanto, también de  $t$ ) de cuadrados buscados. Para pasar al producto de las magnitudes se debe demostrar un teorema intermedio (la validez de la afirmación general se demuestra por la aplicación sucesiva de este teorema).

**Teorema.** Si se tienen dos familias, cada una de las cuales está compuesta por  $t$  cuadrados latinos ortogonales de órdenes  $n$  y  $n'$  respectivamente, existe una familia de  $t$  cuadrados latinos ortogonales de orden  $nn'$ .

*Demostración.* A toda familia de  $t$  cuadrados latinos ortogonales de orden  $n$  ( $t \geq 2$ ,  $n \geq 3$ ) se le puede poner en correspondencia una  $[n^2 \times (t + 2)]$  — tabla construida de los mismos  $n$  elementos (designados  $1, 2, \dots, n$ ) de un modo tal que cualquier par de columnas contenga todas las  $n^2$  2-muestras de elementos (tal tabla se llamará tabla de potencia 2). Permutemos en esta tabla sus filas de tal modo que en las primeras dos columnas (leyendo desde arriba) los pares se contengan en el siguiente orden:  $(1, 1), (1, 2), \dots, (1, n), \dots, (n, 1), (n, 2), \dots, (n, n)$ . En este caso, las siguientes  $t$  columnas reescritas por turno desde arriba ( $n$  columnas en una fila) forman  $t$  cuadrados latinos de orden  $n$ . De hecho, la primera columna de la tabla está construida de una manera tal que en ninguno de los  $t$  cuadrados latinos figuren en una fila dos elementos iguales. La segunda columna de la tabla está construida de tal manera que tampoco figuren dos elementos iguales en las columnas de los cuadrados. Por ejemplo, la  $(9 \times 4)$ -tabla tiene la forma

1	1	1	1
1	2	2	2
1	3	3	3
2	1	2	3
2	2	3	1
2	3	1	2
3	1	3	2
3	2	1	3
3	3	2	1

corresponde a dos cuadrados latinos ortogonales:

1	2	3
2	3	1
3	1	2

y

1	2	3
3	1	2
2	3	1

Construyamos dos tablas correspondientes a dos  $t$ -familias de cuadrados latinos ortogonales de órdenes  $n$  y  $n'$ . Las dimensiones de estas tablas serán  $n^2 \times (t + 2)$  y  $(n')^2 \times (t + 2)$ , respectivamente. Elijamos en estas tablas la  $i$ -ésima y  $j$ -ésima filas:

$$\begin{array}{cccc} a_{i,1} & a_{i,2} & \dots & a_{i,t+2} \\ a_{j,1} & a_{j,2} & \dots & a_{j,t+2} \end{array}$$

y construyamos, usando dichas filas, una fila compuesta por los pares de elementos:

$$a_{i,1}a'_{j,1}, a'_{i,2}a'_{j,2}, \dots; a_{i,t+2}a'_{j,t+2}.$$

De este modo, se obtienen en total  $(nm')^2$  filas que forman una  $[(nm')^2 \times (t+2)]$ -tabla en la que cada dos columnas forman todos los pares de los siguientes  $nm'$  elementos:

$$(1, 1), (1, 2), \dots, (1, n'), \dots, (n, 1), (n, 2), \dots, (n, n').$$

A esta tabla le corresponden  $t$  cuadrados latinos ortogonales de orden  $nm'$ .

La monografía [20] contiene una información abundante sobre las cuestiones examinadas en este párrafo.

### 4.3. BLOQUE-ESQUEMAS

El tipo de construcciones combinatorias del cual se trata en este párrafo, surgió en la literatura matemática aproximadamente a mediados del siglo pasado. J. Steiner publicó en 1853 un pequeño artículo [54] en el que se trataba sobre el problema siguiente: ¿qué número de símbolos pueden dividirse en ternas de un modo tal que cualquier par resulte ubicado en una y sólo una terna?

Se ha hallado sin dificultad alguna que sólo los números  $n = 6k + 1$  y  $n = 6k + 3$ , es decir,  $n \equiv 1, 3 \pmod{6}$  son la solución de este problema. En efecto, por cuanto cada elemento integra la terna junto con los otros dos,  $n - 1$  debe ser un número par, y, por consiguiente,  $n$ , un número impar, es decir,  $n \equiv 1 \pmod{2}$ . Además, en cada terna hay tres pares. Cada par aparece una sola vez. En total hay  $\binom{n-1}{2}$  pares. Este número ha de ser múltiplo de tres. De aquí,  $n \equiv 1, 3 \pmod{6}$ , es decir,  $n = 3, 7, 9, 13, 15, 19, \dots$ . Estas condiciones son necesarias. Steiner planteó una cuestión: ¿son ellas también suficientes? Reiss [55] dio en 1859 una respuesta afirmativa.

Ni Steiner ni Reiss sabían que un problema combinatorio análogo fue planteado y resuelto un poco antes, en 1847, por Kirkman [56]. Pasados tres años, Kirkman propuso otro problema combinatorio [57]: una profesora saca cada día a pasear a un grupo de 15 niñas; las forma en 5 filas de a 3 niñas en cada una; se requiere organizar las ternas de un modo tal que en el transcurso de 7 días cada alumna se encuentre con todas las demás una sola vez.

El sistema de ternas descrito en este problema lleva el nombre de Kirkman. En comparación con el sistema de ternas de Steiner, en éste está presente una condición adicional (la llamada condición de solubilidad): el conjunto de ternas ha de ser partido en  $\frac{n-1}{2}$  componentes (en el problema de Kirkman hay 7 componentes y cada una corresponde a un día

de la semana) de tal modo que cada uno de  $n$  elementos aparece exactamente una vez en las ternas de cada componente.

Surge la pregunta: ¿cuántos sistemas del tipo dado existen? Para las ternas de Steiner se sabe lo siguiente. Si  $n = 3, 7, 9$ , entonces existe solamente un tipo de tal sistema, a saber:

a) para  $n = 3$ , solamente el sistema de una terna

1 2 3

b) para  $n = 7$ , solamente de siete ternas

1	2	3		2	4	6		3	4	7
1	4	5		2	4	6		3	4	7
1	6	7		2	5	7		3	5	6

c) para  $n = 9$ , solamente el sistema de 12 ternas

1	2	3		2	4	9		3	4	8		4	6	7
1	4	5		2	4	9		3	4	8		4	6	7
1	6	8		2	5	6		3	5	7		4	6	7
1	7	9		2	7	8		3	6	9		5	8	9

Resultó que para  $n = 13$  existen dos sistemas de soluciones no isomorfas, es decir tales que no pueden ser obtenidos uno del otro por sustitución de los elementos o por permutación de las ternas. Estos sistemas constan de 22 ternas iguales

1	2	3		2	4	6		4	3	8		7	3	11		8	5	11
1	4	5		2	4	6		4	3	8		7	3	11		8	5	11
1	6	7		2	5	7		4	3	8		7	3	11		8	5	11
1	8	9		2	8	10		4	7	9		7	8	13		8	6	12
1	10	11		2	9	12		4	10	13		7	10	12		6	9	11
1	12	13		2	11	13		4	11	12		7	10	12		6	9	11
1	12	13		2	11	13		4	11	12		7	10	12		3	5	12

y cuatro no equivalentes: para el primer sistema

3	6	10		5	6	13
3	9	13		5	9	10

y para el segundo,

3	6	13		5	6	10
3	9	10		5	9	13

Para el año 1925 fueron terminados los cálculos de los sistemas de ternas de Steiner para  $n = 15$ ; tales sistemas diferentes resultaron ser 80. Por lo que sabe, no se volvieron a calcular las ternas de Steiner para  $n > 15$ . En lo que atañe al número de sistemas no isomorfos de ternas de Steiner, éste crece indefinidamente con el aumento de  $n$  (véase [58]).

La solución del problema de Kirkman (conocida desde el año 1921) es



2. Pongamos los elementos del par de conjuntos  $M_0$  y  $M_i$ ,  $i = 1, 2, \dots, v_1$  en una correspondencia biunívoca con el sistema  $S_2$  de un modo tal que  $M_0$  corresponda a su subsistema  $S_3$ . Las ternas compuestas por los elementos de  $M_0$  ya se han encontrado según la regla antecedente. Las demás ternas han de contener no más de un elemento de  $M_0$ , y, por consiguiente, tienen la forma:  $(a_m, b_{ij}, b_{ik})$  ó  $(b_{ij}, b_{ik}, b_{ir})$ . Por supuesto, ellas deben corresponder a las ternas restantes del sistema  $S_2$ .

3. Definamos el sistema  $S_1$  sobre los números  $1, 2, \dots, v_1$ . Si  $(j, i, r)$  es una terna de este sistema, formemos todas las ternas de la forma  $(b_{jx}, b_{ky}, b_{rz})$ , donde  $x + y + z \equiv 0 \pmod{v_2 - v_3}$ .

Las reglas citadas dan todas las ternas del sistema  $S$  de orden  $v = v_3 + v_1(v_2 - v_3)$ .

En lo que se refiere a las ternas de Kirkman, podemos decir que se han encontrado métodos, con ayuda de los cuales ellas se construyen para los órdenes (véase [60])

$$v = 15, 15 \cdot 3^n, 3^n, 2^{2n} - 1.$$

Pueden considerarse también ternas de otros tipos, diferentes de las de Steiner y Kirkman. Así, por ejemplo, un cuadrado latino genera el conjunto de  $n^2$  ternas ordenadas, donde cada terna  $(i, j, k)$  corresponde a que en la  $i$ -ésima fila y la  $j$ -ésima columna se dispone un elemento  $k$ ;  $i, j, k = 1, 2, \dots, n$ . La condición de que una totalidad de ternas  $(i, j, k)$  ( $i, j, k = 1, 2, \dots, n$ ) forma un cuadrado latino consiste en que cualquier par de componentes de la terna ha de encontrarse una y sólo una vez.

Introducidos los sistemas de ternas de Steiner y Kirkman, los problemas en el dominio de las muestras combinatorias, a lo que parece, deberían concentrarse en las siguientes direcciones:

a) en la elaboración de los métodos de construcción eficaz de los diversos sistemas, en primer lugar, de las ternas de Steiner y Kirkman;

b) en las generalizaciones de los problemas de ternas para los sistemas de 4-, 5-, 6-, etc. conjuntos. Aunque dichos problemas siguen siendo actuales hoy día (véase [61]), tal camino de desarrollo paulatino fue perturbado. Tuvo lugar un salto lógico, cosa no tan rara en las matemáticas. La superación de las dificultades se empezó a buscar en la vía de construcción de una teoría más general.

Actualmente entre los sistemas de incidencia los que mayor interés presentan son los bloque-esquemas (esquemas en bloque). El estudio de estos se efectúa con gran actividad, lo que se explica tanto por las necesidades de la práctica, como por los intereses científicos puros.

En forma simplificada el origen de los bloque-esquemas puede ser descrito del modo siguiente. Los resultados del experimento realizado a un mismo tiempo en condiciones determinadas se escriben en forma de columna (bloque). Los resultados reiterativos, obtenidos en otras condiciones (cambiadas), proporcionan bloques nuevos. La colección de los bloques da

una tabla bidimensional llamada bloque-esquema (en forma abreviada BD, que proviene de la expresión inglesa "block-design").

De la elaboración estática de los resultados nace un enfoque al problema de planificación del experimento, es decir, de formación de su esquema (plan) con el fin de obtener resultados óptimos con un número mínimo de pruebas.

Para el análisis combinatorio, entre un gran número de problemas concernientes a los bloque-esquemas los que mayor interés representan son los problemas de existencia y clasificación, los que estudian las propiedades de los diferentes tipos de bloque-esquemas, los métodos de construcción de los mismos, la correlación, la elaboración de las cuestiones contiguas de la matemática discreta, de las geometrías finitas, de los grupos finitos, etc. Estos problemas teóricos se analizan intensamente desde el fin de los años 30 y el principio de los 40.

Sea un  $v$ -conjunto de elementos  $m_1, m_2, \dots, m_v$ . Los elementos de dicho conjunto están distribuidos entre  $b$  bloque-subconjuntos  $M_1, M_2, \dots, M_b$ , la intersección de los cuales no es obligatoriamente un vacío. El número de elementos en el bloque  $M_j$  lleva el nombre de volumen del bloque y se denota con  $k_j$ . Los elementos pueden aparecer en varios bloques. Sea  $r_i$  el número de apariciones del elemento  $m_i$  (es decir, el número de bloques que contienen  $m_i$ ),  $i = 1, 2, \dots, v$ ; por fin, introduzcamos el número de repeticiones (pares no ordenados) de los elementos:  $\lambda_p$  ( $p = 1, 2, \dots, (v/2)$ ). En tal caso suele decirse que el conjunto de bloques  $M_1, \dots, M_b$  forma un *bloque-esquema* con los parámetros  $v, b, r_i, k_j, \lambda_p$  (si en lugar de los pares se analizan las ternas o  $t$ -muestras de elementos, entonces la disposición correspondiente se denomina *configuración táctica*). Así pues, un bloque-esquema se caracteriza por los parámetros  $v, b, r_i, k_j, \lambda_p$ .

Pueden haber varios tipos diferentes de bloque-esquemas. Por eso introduzcamos el principio de la clasificación de los bloque-esquemas tal como se formó hasta el presente. Ante todo, un bloque-esquema se llama *completo*, si en cada bloque están contenidos todos los elementos del conjunto, es decir,  $k_j = v, j = 1, 2, \dots, b$ , e *incompleto*, si  $k_j < v, j = 1, 2, \dots, b$ . Los cuadrados latinos pueden servir de ejemplo de los bloque-esquemas completos.

Los bloque-esquemas incompletos se dividen, a su vez, en dos grandes clases: la clase de bloque-esquemas incompletos equilibrados (en la forma abreviada BIB-esquemas, lo que viene del inglés "balanced incomplete block design") y la clase de bloque-esquemas incompletos parcialmente equilibrados (PBIB, del inglés "partially balanced incomplete block design").

Un bloque-esquema se llama BIB-esquema, si  $k_1 = k_2 = \dots = k_b = k < v$ ;  $r_1 = \dots = r_v = r$ , y  $\lambda_p = \lambda$  para cualquier  $p$ ; dicho de otro modo, en un BIB-esquema todos los elementos tienen un mismo número de repeticiones, todos los bloques son de igual volumen y cada

par de elementos aparece en un mismo número  $\lambda = \text{const}$  de bloques. Los PBIB-esquemas se diferencian en que en ellos  $\lambda \neq \text{const}$ . Debido a esta circunstancia se genera un gran número de diferentes tipos de PBIB-esquemas, lo que crea dificultades considerables en la investigación de ellos.

Se denomina bloque-esquema incompleto parcialmente equilibrado con  $m$  clases, o, en forma más breve, PBIB( $m$ )-esquema a un bloque-esquema, en el que el conjunto de todos los  $\binom{v}{2}$  pares de sus elementos puede ser partido en  $m$  clases disjuntas (un par de elementos referente a la  $i$ -ésima clase se denominará  $i$ -conexo), de un modo tal que

a) cualquier par de elementos  $i$ -conexos esté contenido exactamente en  $\lambda_i$  bloques ( $i = 1, 2, \dots, m$ );

b) para cualquier elemento exista exactamente  $n_i$  elementos que sean  $i$ -conexos con el primero ( $i = 1, 2, \dots, m$ );

c) para todo par de elementos  $i$ -conexos,  $\lambda$  y  $\beta$ , el número de elementos,  $j$ -conexos con  $\alpha$ , y, al mismo tiempo,  $l$ -conexos con  $\beta$ , es igual a  $p_{jl}^i$ , con la particularidad de que  $p_{jl}^i = p_{lj}^i$  ( $i, j, l = 1, 2, \dots, m$ ).

Por consiguiente, los parámetros de un PBIB( $m$ )-esquema son los números

$$v, b, k, r, \lambda_i, n_i, p_{jl}^i \quad (i, j, l = 1, 2, \dots, m).$$

Con el objeto de contribuir a concebir un gran número de construcciones combinatorias nuevas y, a veces, complejas, proponemos al lector el esquema de la clasificación primaria de los bloque-esquemas señalando las continuaciones posibles (fig. 4.1).

La teoría moderna de los bloque-esquemas es enorme en cuanto al número y volumen de las investigaciones reales, a menudo dispersadas y débilmente organizadas. Más abajo se expondrán los fundamentos de esta teoría sin pretender interpretar los hechos plenamente.

Al principio de este capítulo ya se ha considerado en forma general el método de representación matricial de la estructura de un conjunto. Apliquémoslo a los bloque-esquemas. Sea un bloque-esquema con los parámetros  $v, b, k, r^{1)}$ . Pongamos

$$n_{ij} = \begin{cases} 1, & \text{si el } i\text{-ésimo elemento se encuentra en el } j\text{-ésimo bloque} \\ 0, & \text{en el caso contrario,} \end{cases}$$

$$i = 1, 2, \dots, v; \quad j = 1, 2, \dots, b.$$

La  $(v \times b)$ -matriz  $N = \|n_{ij}\|$  se llama matriz de incidencia del bloque-esquema dado; en este caso cada fila de la matriz  $N$  contiene  $r$  unidades y cada columna contiene  $k$  unidades ( $\lambda_p$  es igual al producto escalar de

<sup>1)</sup> No vamos a escribir el parámetro  $\lambda$ , si no se indica de qué, precisamente, bloque-esquema (equilibrado o parcialmente equilibrado) se trata en el caso a considerar.

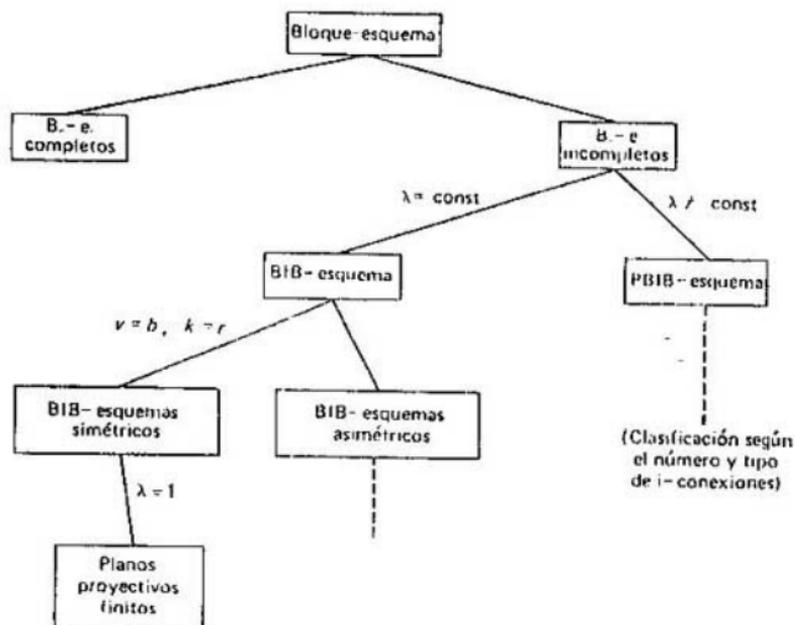


Fig.4.1.

(dos filas). Por ejemplo, un BIB-esquema con los parámetros  $v = 6$ ,  $b = 10$ ,  $k = 3$ ,  $r = 5$ ,  $\lambda = 2$  tiene la siguiente representación matricial (matriz de incidencia):

Bloque-esquema

1	1	1	1	1	2	3	2	3	2
2	3	4	5	2	3	4	4	5	4
3	4	5	6	6	5	6	5	6	6

Matriz

1	1	1	1	1	0	0	0	0	0
1	0	0	0	1	1	0	1	0	1
1	1	0	0	0	1	1	0	1	0
0	1	1	0	0	0	1	1	0	1
0	0	1	1	0	1	0	1	1	0
0	0	0	1	1	0	1	0	1	1

He aquí un ejemplo más: supongamos que para un 9-conjunto se examina el siguiente sistema de subconjuntos:

$$\begin{aligned}
 B_1 &= (1, 2, 3); & B_2 &= (4, 5, 6); & B_3 &= (7, 8, 9) & B_4 &= (1, 4, 7); \\
 B_5 &= (2, 5, 8); & B_6 &= (3, 6, 9); & B_7 &= (1, 5, 9); & B_8 &= (2, 6, 7); \\
 B_9 &= (3, 4, 8); & B_{10} &= (1, 6, 8); & B_{11} &= (2, 4, 9) & B_{12} &= (3, 5, 7).
 \end{aligned}$$

No es difícil ver que este sistema es un BIB-esquema con los parámetros  $v = 9$ ,  $b = 12$ ,  $k = 3$ ,  $r = 4$ ,  $\lambda = 1$ . Escribamos el bloque-esquema, como antes, en forma de una  $(k \times b)$ -tabla rectangular:

1	4	7	1	2	3	1	2	3	1	2	3
2	5	8	4	5	6	5	6	4	6	4	5
3	6	9	7	8	9	9	7	8	8	9	7

La matriz de incidencia de este bloque-esquema es

1	0	0	1	0	0	1	0	0	1	0	0
1	0	0	0	1	0	0	1	0	0	1	0
1	0	0	0	0	1	0	0	1	0	0	1
0	1	0	1	0	0	0	0	1	0	1	0
0	1	0	0	1	0	1	0	0	0	0	1
0	1	0	0	0	1	0	1	0	1	0	0
0	0	1	1	0	0	0	1	0	0	0	1
0	0	1	0	1	0	0	0	1	1	0	0
0	0	1	0	0	1	1	0	0	0	1	0

Pese a que la matriz parece ser engorrosa, las matrices binarias de incidencia son en la práctica muy simples para las operaciones. Del análisis de sus estructuras, podemos obtener directamente una serie de propiedades, incluidas las relaciones entre los parámetros. Por ejemplo, para los bloque-esquemas tenemos en general

$$\sum_{i=1}^n r_i = \sum_{j=1}^h k_j.$$

lo que es obvio. En particular, para los BIB-esquemas tenemos

$$bk = vr; \quad (1)$$

$$r(k-1) = \lambda(v-1). \quad (2)$$

La primera de las relaciones expresa un simple cálculo del número de elementos en el bloque-esquema (es decir, el número de todas las unidades en la matriz de incidencia). En la segunda relación los razonamientos son los siguientes: cada elemento se encuentra  $r$  veces y está siempre contiguo de  $k-1$  elementos. Este mismo elemento se encuentra  $\lambda$  veces haciendo un par con cada uno de las  $v-1$  elementos.

Veamos las relaciones entre los parámetros del PBIB( $m$ )-esquema. Es evidente que subsiste, como antes, la igualdad (1). Establezcamos algunas otras igualdades:

$$\sum_{i=1}^m n_i = v-1; \quad \sum_{i=1}^m \lambda_i n_i = r(k-1);$$

$$\sum_{l=1}^m p_{jl}^i = \begin{cases} n_j, & \text{si } i \neq j; \\ n_j - 1, & \text{si } i = j; i, j = 1, 2, \dots, m; \end{cases} \quad (3)$$

$$n_i p_{jl}^i = n_j p_{li}^j = n_l p_{ij}^l; \quad i, j, l = 1, 2, \dots, m.$$

La primera de las relaciones es obvia. La segunda es una modificación de (2) y se demuestra por razonamientos análogos. En la siguiente igualdad

$\sum_{l=1}^m p_{jl}^i$  significa el número de elementos  $j$ -conexos con cualquiera de los dos elementos  $i$ -conexos. Es igual, por consiguiente, a  $n_j$  (si  $i \neq j$ ), o bien a  $n_j - 1$ , (si  $i = j$ ). En lo que se refiere a la última relación, esta se

demuestra del modo siguiente: tomemos un elemento fijo  $\alpha$ . Por definición, existen  $n_i$  elementos  $\beta_1, \beta_2, \dots, \beta_{n_i}$ ,  $i$ -conexos con  $\alpha$ , y, además,  $n_j$  elementos  $\gamma_1, \gamma_2, \dots, \gamma_{n_j}$ ,  $j$ -conexos con  $\alpha$ . Construyamos una tabla binaria

$$\begin{pmatrix} b_{\gamma_1, \beta_1}^{\beta_1} & \dots & b_{\gamma_1, \beta_{n_i}}^{\beta_{n_i}} \\ \dots & \dots & \dots \\ b_{\gamma_{n_j}, \beta_1}^{\beta_1} & \dots & b_{\gamma_{n_j}, \beta_{n_i}}^{\beta_{n_i}} \end{pmatrix}$$

en la cual

$$b_{\gamma_j, \beta_i}^{\beta_i} = \begin{cases} 1, & \text{si } \beta_i \text{ y } \gamma_j \text{ son } i\text{-conexos;} \\ 0, & \text{en el caso contrario.} \end{cases}$$

Calculemos el número de unidades en cada columna de la matriz:

$$\sum_{j=1}^{n_j} b_{\gamma_j, \beta_i}^{\beta_i} = p_{j,i}^i;$$

y en cada columna:

$$\sum_{i=1}^{n_i} b_{\gamma_j, \beta_i}^{\beta_i} = p_{j,i}^i;$$

De los dos métodos de cálculo de todas las unidades en la matriz obtenemos

$$n_i p_{j,i}^i = n_j p_{j,i}^i.$$

Las relaciones (1), (2) y (1), (3) son condiciones necesarias para que exista los BIB- y PBIB(m)-esquemas, respectivamente.

Sea  $N = [n_{ij}]$  una  $(v \times b)$  matriz de incidencia de un bloque-esquema incompleto equilibrado con los parámetros  $v, b, r, k, \lambda$ . En este caso  $N$  satisface la siguiente ecuación matricial

$$NN^T = (r - \lambda)I + \lambda J,$$

donde  $N^T$  es la matriz transpuesta de  $N$ ;  $I$  es la matriz unidad de orden  $v$ ;  $J$  es una matriz integrada plenamente por unidades, también de orden  $v$ .

Efectivamente, calculemos el producto

$$N \cdot N^T = B = [b_{ij}]; \quad i, j = 1, 2, \dots, v.$$

El elemento  $b_{ij}$  es igual al producto escalar de la  $i$ -ésima fila de  $N$  por la  $j$ -ésima columna de  $N^T$ , por consiguiente,

$$b_{ij} = \sum_{l=1}^b n_{il} n_{jl} = \begin{cases} r, & \text{si } i = j \\ \lambda, & \text{si } i \neq j; \end{cases}$$

$$i, j = 1, 2, \dots, v.$$

De aquí

$$B = \begin{pmatrix} r & & \\ & r & \lambda \\ & \lambda & \dots & r \end{pmatrix} = rJ + \lambda(J - I) = (r - \lambda)I + \lambda J.$$

Para la matriz  $B$  puede hallarse el valor de su determinante:

$$\det B = (r - \lambda)^{v-1}(v\lambda - \lambda + r).$$

Para obtener este resultado basta sustraer la primera columna de todas las demás columnas, y a continuación, agregar la suma de todas las filas, partiendo de la segunda, hacia la primera fila. En este caso, por arriba de la diagonal principal se dispondrán sólo los ceros:  $a'_{11} = r + (v - 1)\lambda$ ;  $a'_{22} = \dots = a'_{vv} = r - \lambda$ , lo que nos da el resultado buscado. Por cuanto de que  $k < v$  se deduce que  $\lambda = r \frac{k-1}{v-1} < r$ , entonces  $\det B \neq 0$ . Haciendo uso de (2), tenemos

$$\det B = (r - \lambda)^{v-1}rk \neq 0.$$

De este modo, el rango de la matriz  $B$  es igual a  $v$ . Por otra parte, el rango de  $N$  (y el de  $N^T$ ) no sobrepasa  $b$ . Según se sabe por la teoría de las matrices, el rango de un producto no es superior a los rangos de los factores. De aquí se deduce una desigualdad importante

$$b \geq v,$$

llamada desigualdad de Fisher, la cual sirve también de condición necesaria para la existencia de un BIB-esquema.

Del análisis de la matriz de incidencia  $N$  y de la matriz  $B = N \cdot N^T$  pueden deducirse una serie de teoremas referentes a los tipos particulares de los bloque-esquemas (véase [62]).

Las matrices de incidencia no son el único método de describir los bloque-esquemas; otro método análogo es el de aplicación de las formas cuadráticas. Este último método es singularmente interesante, porque la teoría de las formas cuadráticas está suficientemente elaborada. En efecto, la correlación  $N \cdot N^T = (r - \lambda)I + \lambda J$  se reencuadra en las formas cuadráticas. Introduzcamos las variables indeterminadas:  $x_1, x_2, \dots, x_v$ , correspondientes a los elementos de los bloque-esquemas, y asignamos a cada bloque  $b_j$  la forma

$$L_j = \sum_{i=1}^v n_{ij}x_i, \quad j = 1, 2, \dots, v,$$

donde  $n_{ij}$  es la multiplicidad del elemento  $i$  en el bloque  $b_j$ . Entonces, a la ecuación matricial  $N \cdot N^T = (r - \lambda)I + \lambda J$  se le pondrá en correspondencia la forma cuadrática:

$$\sum_{i=1}^b L_i^2 = (r - \lambda) \sum_{i=1}^v x_i^2 + \lambda \left( \sum_{i=1}^v x_i \right)^2.$$

En la teoría del análisis combinatorio y en las aplicaciones del mismo los bloque-esquemas desempeñan un papel de importancia. Varias de las estructuras combinatorias conocidas representan tipos particulares de los

bloque-esquemas o son equivalentes a los últimos. Aclaremos esto con un ejemplo.

Según lo dicho con anterioridad, los cuadrados latinos resultan ser bloque-esquemas completos. Las ternas de Steiner son, en esencia, BIB-esquemas, para los cuales  $k = 3$ ,  $\lambda = 1$ . Para ellos las correlaciones (1) y (2) entre parámetros adquieren la forma

$$3b = vr; \quad 2r = v - 1;$$

de donde

$$v = 2r + 1; \quad b = \frac{r(2r + 1)}{3}$$

y, por consiguiente,

$$r \equiv 0, 1 \pmod{3}; \quad v \equiv 1, 3 \pmod{6}.$$

Las matrices de Hadamard  $H$  son equivalentes a los tipos particulares de los bloque-esquemas. Efectivamente, tomemos la matriz  $H$  de orden  $n \geq 3$ . Se conoce (véase § 4.1) que  $n \equiv 0 \pmod{4}$ . Normalicemos  $H$ , es decir, multiplicando las filas y las columnas correspondientes por  $-1$ , reduzcámosla a una forma, en la cual la primera fila y la primera columna estarán compuestas de unidades positivas. Tal matriz  $H$  de orden  $n = 4t \geq 8$  resulta ser equivalente al BIB-esquema simétrico con los parámetros

$$v = b = 4t - 1; \quad k = r = 2t - 1; \quad \lambda = t - 1.$$

En efecto, a toda matriz normalizada  $H$  se le puede poner en correspondencia una  $(0, 1)$ -matriz  $A$  de orden  $v = 4t - 1$ , en cada línea de la cual se tienen  $k = 2t - 1$  unidades. El método de esta operación consiste en que en la matriz normalizada  $H$  se tachan la primera fila y la primera columna, y en la matriz restante todos los menos uno se sustituyen por ceros. La matriz  $A$  satisface la relación

$$A \cdot A^T = tI + (t - 1)J$$

y representa, pues, una matriz de incidencia de un bloque-esquema incompleto equilibrado en el que  $r - \lambda = t$ , y  $\lambda = t - 1$ . Los razonamientos son fácilmente invertidos, lo que precisamente demostrará nuestra afirmación.

En el § 4.2, al demostrar el teorema de existencia de la familia de cuadrados latinos ortogonales, se ha mostrado que la construcción de tal familia es equivalente a la conformación de una tabla ortogonal de fuerzas. Resulta, no obstante, que la existencia de la última origina la existencia de un bloque-esquema de determinado tipo. Expliquemos este hecho más detalladamente, pero, antes demos a conocer la definición general de la tabla ortogonal.

Sea dada una  $(m \times N)$ -matriz  $A$  con elementos del conjunto  $S = \{0,$

1, 2, ..., s - 1}. Existen en total  $s^t$  diferentes columnas de longitud  $t$  con los elementos del conjunto mencionado. Si en cada submatriz de  $t$  filas de la matriz  $A$  la columna  $(x_1, x_2, \dots, x_t)^T$  aparece  $\lambda(x_1, x_2, \dots, x_t)$  veces, donde el número  $\lambda$  es positivo y no varía al realizarse las permutaciones de  $x_1, x_2, \dots, x_t$ , entonces la matriz  $A$  se llama *tabla parcialmente equilibrada de fuerza  $t$*  con  $N$  columnas,  $m$  filas,  $s$  símbolos y los parámetros  $\lambda(x_1, x_2, \dots, x_t)$ , o, en una forma más breve, tabla  $(N, m, s, t)$  con los parámetros  $\lambda(x_1, x_2, \dots, x_t)$ . Si  $\lambda = \text{const}$  para todas las columnas  $(x_1, x_2, \dots, x_t)$ , entonces la tabla  $(N, m, s, t)$  se denomina *tabla ortogonal de índice  $\lambda$* .

Aduzcamos, a título de ejemplo, una tabla ortogonal  $(18, 7, 3, 2)$  de índice  $\lambda = 2$  con los símbolos 0, 1, 2:

Tabla 4.2

Números de las filas	Números de las columnas																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
2	0	1	2	0	1	2	1	2	0	2	0	1	1	2	0	2	0	1
3	0	1	2	1	2	0	0	1	2	2	0	1	2	0	1	1	2	0
4	0	1	2	2	0	1	2	0	1	0	1	2	1	2	0	1	2	0
5	0	1	2	1	2	0	2	0	1	1	2	0	0	1	2	2	0	1
6	0	1	2	2	0	1	1	2	0	1	2	0	2	0	1	0	1	2
7	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2

Si separamos de esta tabla las tres primeras columnas y la última fila obtendremos una tabla parcialmente equilibrada  $(15, 6, 3, 2)$  con los parámetros

$$\lambda(x_1, x_2) = \begin{cases} 2, & \text{si } x_1 \neq x_2; \\ 1, & \text{si } x_1 = x_2. \end{cases}$$

La existencia de  $k$  cuadrados latinos biunívocamente ortogonales de orden  $s$  es equivalente a la existencia de una tabla ortogonal  $(s^2, k + 2, s, 2)$  de índice  $\lambda = 1$ .

Efectivamente, sea que tenemos una tabla ortogonal  $(s^2, k + 2, s, 2)$  y supongamos que los elementos en esta tabla están designados con los números 1, 2, ...,  $s$ . Permutemos las columnas en la tabla de una manera tal que los elementos de las columnas en las primeras dos filas se encuentren en orden

$$(1, 1), (1, 2), \dots, (1, s), \dots, (s, 1), (s, 2), \dots, (s, s).$$

Para cada  $l = 3, 4, \dots, k + 2$  construyamos la tabla  $A_l = (s^2, s, s, 2)$  del

modo siguiente: la primera columna  $A_l$  consta de los primeros  $s$  elementos de la fila  $l$  de la tabla inicial; la segunda columna, de los siguientes  $s$  elementos, etc. hasta la última compuesta por los últimos  $s$  elementos de la misma fila. Las tablas  $A_1, A_2, \dots, A_{k+2}$ , conformadas del modo indicado, forman un conjunto compuesto por  $k$  cuadrados latinos biunívocamente ortogonales de orden  $s$ . El hecho de que la tabla  $A_l$  no contiene dos elementos iguales en la columna lo muestra el examen de la primera fila de la tabla inicial. Una propiedad análoga de las filas se ve del examen de la segunda fila. Si  $l \neq j$ , entonces,  $A_l$  y  $A_j$  son ortogonales, lo que se desprende del método de construcción de las filas correspondientes. La demostración como es fácil comprobar es convertible.

Las investigaciones científicas en el dominio de los bloque-esquemas se agrupan actualmente alrededor del problema de existencia (o no existencia) de los tipos aislados de los bloque-esquemas, del estudio de sus propiedades y de la búsqueda de los métodos de su construcción. La teoría combinatoria se encuentra en este respecto sólo al principio de su desarrollo. Para el estudio ulterior de este tema podemos recomendar al lector las capítulos 10—16 del libro [4].

Las investigaciones modernas en el dominio de las disposiciones combinatorias y de los bloque-esquemas requieren, en particular, la utilización de la teoría de los números, la teoría de las matrices, la teoría de los cuerpos convexos, etc.

#### 4.4. PERMANENTES

Este concepto ha adquirido en el análisis combinatorio moderno una importancia teórica y práctica tan grande que consideramos necesario dedicarle un párrafo especial aparte.

Sean dados un conjunto  $S = \{s_1, \dots, s_n\}$  y cierta familia de sus subconjuntos  $M = \{S_1, S_2, \dots, S_m\}$ . El teorema de P. Hall da las condiciones necesarias y suficientes para que la familia  $M$  posea sistemas de representantes distintos y una frontera inferior para el número de tales sistemas. Sin embargo, en muchos problemas del análisis combinatorio surge la necesidad de obtener estimaciones más exactas de este número. Este objetivo se consigue por introducción de una nueva noción, permanente de la matriz, y estudiando las propiedades del mismo.

Sea una matriz  $A = [a_{ij}]$ ,  $i = 1, 2, \dots, m$ ;  $j = 1, 2, \dots, n$ , cuyos elementos están representados por números reales. Se denomina *permanente* de la matriz citada la expresión (el número)

$$\text{per } A = \sum_{\sigma} \prod_{i=1}^m a_{i\sigma(i)},$$

en la que la sumación se realiza respecto de todos los encajes  $\sigma$  de  $\{1, 2, \dots, m\}$  en  $\{1, 2, \dots, n\}$ . En este caso se supone, naturalmente, que  $m \leq n$ .

Sea  $A$  una matriz de incidencia para  $M$  respecto de  $S$ , entonces  $\text{per } A$  será el número de sistemas de representantes distintos, de los cuales dispone la familia de subconjuntos  $M$ .

Los permanentes fueron introducidos en 1812, casi simultáneamente, en las memorias de Binet [63] y Cauchy [64] en relación con el desarrollo de la teoría de determinantes como tipo especial de las funciones simétricas de signo variable. El término "permanente" apareció por primera vez en la obra de Muir [65], donde están enunciadas algunas propiedades del permanente.

Es evidente que el permanente es invariante respecto a las permutaciones de las filas y columnas en la matriz  $A$ ; la multiplicación de los elementos de cualquier fila de la matriz  $A$  por un escalar  $a$  sustituye  $\text{per } A$  por  $a \text{ per } A$ ; el desarrollo de Laplace en menores respecto a las filas es válido también para los permanentes.

Una lista  $(a_{1\sigma(1)}, a_{2\sigma(2)}, \dots, a_{m\sigma(m)})$  de elementos de la matriz  $A$ , en la cual ningún par se encuentra en una línea (fila o columna) se denominará *transversal*. El permanente de la matriz  $A$  representa, de este modo, una suma de todas las  $n!(n - m)$  transversales de los productos de los elementos de la matriz  $A$ , dispuestos en una misma transversal.

La determinación de permanente y de sus propiedades señalan que la noción de permanente es próxima a la de determinante. Sin embargo, si la técnica de cálculo de los determinantes está actualmente bien elaborada, el cálculo de los permanentes es un problema técnicamente difícil, cuya resolución requiere nuevos avances. Hoy día sabemos sólo un método que consiste en la aplicación de la fórmula de inclusiones y exclusiones.

Denotemos con  $A_r$  una matriz que se obtiene de la matriz  $A$  reemplazando  $r$  de sus columnas por columnas compuestas de ceros. Sea  $S(A_r)$  el producto de las sumas de las filas  $A_r$ , y  $\sum S(A_r)$ , las sumas  $S(A_r)$  respecto de todas las selecciones para  $A_r$ . En este caso es válida la siguiente fórmula de Ryser:

$$\text{per } A = \sum_{i=0}^{m-1} (-1)^i \binom{n-m+i}{i} \sum S(A_{n-m+i}).$$

En efecto, designemos con  $M$  el conjunto de todas las  $m$ -permutaciones  $(j_1, \dots, j_m)$  con repeticiones de los números naturales  $1, 2, \dots, n$ . Supongamos que el peso de tal permutación es igual a  $\prod_{i=1}^m a_{ij_i}$ , y la propiedad  $p_i$  significa que dicha permutación no contiene el número entero  $i$  ( $i = 1, 2, \dots, n$ ). Supongamos ahora que  $A_r$  se obtuvo de  $A$  por sustitución de las columnas con los números  $i_1, i_2, \dots, i_r$  por las compuestas de ceros. Entonces, la suma de los pesos de las permutaciones de  $M$  que poseen cada una de las propiedades  $p_{i_1}, p_{i_2}, \dots, p_{i_r}$  es igual a

$$V(p_{i_1}, p_{i_2}, \dots, p_{i_r}) = S(A_r).$$

Por consiguiente,

$$V(r) = \sum_{\substack{1 \leq i_1 < i_2 < \dots < i_r \leq n}} V(p_{i_1}, p_{i_2}, \dots, p_{i_r}) = \sum S(A_r).$$

La función per  $A$  es igual a la suma de los pesos de los elementos de  $M$  que satisfacen las  $n - m$  propiedades  $p_i$  ( $i = 1, \dots, n$ ). Al hacer uso de la fórmula del método de inclusiones y exclusiones, llegamos a la fórmula de Ryser aducida más arriba. Para una matriz cuadrada  $A$  de orden  $n$  esta fórmula adopta la forma

$$\text{per } A = \sum_{i=0}^{n-1} (-1)^i \sum S(A_i).$$

Si  $J$  es una matriz de orden  $n$ , compuesta íntegramente por unidades, entonces per  $J = n!$ , y a título de corolario, obtenemos la identidad

$$n! = \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} (n-i)^n.$$

Si consideramos la matriz  $J - I$ , donde  $I$  es la matriz unidad, tenemos

$$\text{per}(J - I) = n! \sum_{i=0}^n (-1)^i \frac{1}{i!} = D_n,$$

donde  $D_n$  es el número de desórdenes. Valiéndonos de la fórmula de Ryser, podemos obtener otra fórmula para el número de desórdenes:

$$D_n = \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} (n-i)^i (n-i-1)^{n-1}.$$

Existe una conexión interesante entre el permanente de una matriz cuadrada  $A = [a_{ij}]$  ( $i, j = 1, 2, \dots, n$ ) de orden  $n$  y los permanentes y determinantes de sus submatrices principales. Designemos con  $Q_{k,n}$  el conjunto de todas las sucesiones crecientes  $\vec{j} = (j_1, \dots, j_k)$  de longitud  $k$  de los números naturales  $1, 2, \dots, n$ :  $1 \leq j_1 < j_2 < \dots < j_k \leq n$ . Sea  $\vec{j} \in Q_{k,n}$ ; con  $A[\vec{j}]$  denotemos una submatriz  $[a_{j_s j_t}]$  ( $r, s = 1, 2, \dots, k$ ) de la matriz  $A$ , y con  $A(\vec{j})$ , una submatriz de la matriz  $A$  de orden  $(n - k)$ , complementaria a  $A[\vec{j}]$ .

Resulta válida la siguiente relación (véase [66]):

$$\text{per } A = \sum_{k=1}^n (-1)^{k-1} \sum_{\vec{j} \in Q_{k,n}} \text{per } A(\vec{j}) \det A[\vec{j}]. \quad (1)$$

Efectivamente, no es difícil notar que la expresión en el segundo miembro de esta fórmula representa una suma de los productos de los elementos de la matriz  $A$  dispuestos en una misma transversal con ciertos coeficientes enteros. Por consiguiente,

$$\sum_{k=1}^n (-1)^{k-1} \sum_{\vec{j} \in Q_{k,n}} \text{per } A(\vec{j}) \det A[\vec{j}] = \sum_{\sigma \in \sigma_n} d_\sigma \prod_{i=1}^n a_{i\sigma(i)},$$

donde la sumación se realiza respecto de todas las sustituciones  $\sigma$  del grupo simétrico  $\mathfrak{S}_n$  de grado  $n$ . Demostremos que  $d_\sigma = 1$  para cualquier sustitución  $\sigma \in \mathfrak{S}_n$ . Con ello quedará demostrada la fórmula (1). Desarrollemos  $\sigma$  en producto de ciclos:  $\sigma = (c_1) \dots (c_m)$ , y notemos que la expresión  $a_{1\sigma(1)} \dots a_{n\sigma(n)}$  figura en aquellos y sólo aquellos productos per  $A(j)$  det  $A[j]$  del segundo miembro de la fórmula (1), para los cuales existen los números naturales  $l_1, \dots, l_i$  ( $1 \leq l_1 \leq \dots < l_i \leq m, 1 \leq i \leq m$ ) tales que  $\{j_1, \dots, j_k\} = \bigcup_{p=1}^m \tilde{c}_p$ , donde  $\tilde{c}_p$  es el conjunto de números naturales que forman la notación del  $l_p$ -ésimo ciclo. Por consiguiente

$$\begin{aligned} d_\sigma &= \sum_{i=1}^m \sum_{j \in Q_{i,m}} (-1)^{|l_1, \dots, l_i|} \dots (-1)^{|l_1, \dots, l_i|} \dots \\ &= \sum_{i=1}^m \sum_{j \in Q_{i,m}} (-1)^{i+1} = \sum_{i=1}^m \binom{m}{i} (-1)^{i+1} = 1, \end{aligned}$$

donde  $|l_1, \dots, l_i|$  es la longitud sumaria de los ciclos  $c_{l_1}, \dots, c_{l_i}$ . La afirmación está demostrada.

Observemos que la identidad (1) puede ser escrita en la siguiente forma

$$\det A = \sum_{k=1}^n (-1)^{k-1} \sum_{j \in Q_{k,n}} \det A[j] \text{ per } A[j].$$

He aquí dos identidades de MacMahon [72] que pueden obtenerse como simples consecuencias de la fórmula (1):

$$\text{per } A = \sum_{k=1}^n (-1)^{n-k} k! \sum_{N/N_1, \dots, N_k} \prod_{i=1}^k \det A[N_i], \quad (3)$$

$$\det A = \sum_{k=1}^n (-1)^{n-k} k! \sum_{N/N_1, \dots, N_k} \prod_{i=1}^k \text{per } A[N_i]. \quad (4)$$

La suma se toma aquí respecto de todas las particiones del conjunto  $N = \{1, 2, \dots, n\}$  en  $k$  partes  $N_1, \dots, N_k$ . En efecto, sustituyendo per  $A(j)$  en el segundo miembro de la fórmula (1) por la expresión correspondiente según la misma fórmula y haciendo así un número finito de veces, llegamos, tras algunas transformaciones sencillas, a (3). La identidad (4) se demuestra de un modo análogo empleando la fórmula (2). Las dificultades que existen con los cálculos de los permanentes condujeron a la aparición de desigualdades, las cuales desempeñaron un papel fundamental en la investigación de toda una serie de problemas del análisis combinatorio: problemas de Van der Waerden sobre el mínimo del permanente de una matriz dos veces estocástica, problemas de estimación del número de ternas de Steiner no isomorfas y de rectángulos latinos, problemas sobre el número de recubrimientos de un grafo dimensional reticular por dímeros, etc.

Cronológicamente la primera desigualdad no trivial para los permanentes fue obtenida en 1961 por Marcus y Newman [18]. Sea  $A$  una  $(m \times n)$ -matriz, y sea  $B$  una  $(n \times m)$ -matriz. Entonces

$$|\text{per}(A \cdot B)|^2 \leq \text{per}(A \cdot A^T) \cdot \text{per}(B \cdot B^T),$$

con la particularidad de que la igualdad se consigue, si y sólo si existe una fila nula en  $A$ , o bien una columna nula en  $B$ , o bien  $A = DPB^T$  para cierta matriz diagonal  $D$  y la matriz conmutadora  $P$ . El signo  $T$  denota la operación de transposición de la matriz. Para una matriz cuadrada de orden  $n$  de aquí se deduce (si ponemos  $B = I$ ):

$$|\text{per} A|^2 \leq \text{per}(A \cdot A^T).$$

La igualdad se verifica, si y sólo si  $A$  tiene una fila nula o bien  $A = DP$ .

En 1980 Egórychev [67], haciendo uso de la representación del permanente en forma de un discriminante mixto, introdujo en la teoría de permanentes las desigualdades clásicas de Alexándrov y Brunn-Minkowski que se emplean en la geometría. Debido a ello él tuvo éxito en demostrar la validez de la conocida hipótesis de Van der Waerden<sup>1)</sup>.

Aducimos estas desigualdades para los permanentes, dejando al lado su fuente originaria, es decir, la teoría geométrica de los discriminantes mixtos de A. D. Alexándrov, desarrollada por él en los años 30 y utilizada para estudiar los volúmenes de los cuerpos convexos en el espacio euclidiano.

Nos harán falta algunos hechos del álgebra lineal. Sea  $L$  un espacio lineal de dimensión finita sobre  $\mathbb{R}$ , y sea  $\varphi$  una forma bilineal simétrica en  $L$ . Suele decirse que  $(L, \varphi)$  es un *espacio con métrica*. Se denomina *signatura* de  $\varphi$  a la terna  $(k_1, k_2, k_3)$ , donde  $k_1$  es el número de valores propios positivos de una matriz de la forma  $\varphi$  en cierta base,  $k_2$ , el número de valores propios negativos, y  $k_3$ , el número de valores propios nulos de la matriz mencionada. El teorema de Sylvester (la ley de inercia) afirma que dicha terna no depende de la base. Se dice que el espacio con métrica  $(L, \varphi)$  es el *espacio de Minkowski*, si la signatura de  $\varphi$  es igual a  $(1, n-1, 0)$ .

**Lema 1.** Un espacio con métrica  $(L, \varphi)$  es el de Minkowski, si y sólo si se cumple la condición  $\Phi$ : existe un vector  $a \in L$  tal que  $\varphi(a, a) > 0$ , y para cualquier  $b \in L$  de  $\varphi(a, b) = 0$ ,  $b \neq 0$ , se deduce que  $\varphi(b, b) < 0$ .

*Demostración.* Recordemos que el vector  $a \in L$  se denomina regular, si existe tal  $b \in L$  que  $\varphi(a, b) \neq 0$ . Un subespacio  $M \subseteq L$  es regular, si lo es cualquier vector no nulo suyo. Supongamos ahora que  $(L, \varphi)$  es un espacio con métrica, para el cual se cumple la condición  $\Phi$ . Por cuanto el vector  $a$  es regular, podemos descomponer  $L = \{a\} \oplus L_a$ , donde  $\{a\}$  es la cápsula lineal de  $a$ , y  $L_a$  el complemento ortogonal de  $a$  (véase [69]). Cons-

<sup>1)</sup> D. I. Falikman [68] obtuvo independientemente la solución del problema de Van der Waerden (sin demostrar la unicidad de la matriz minimizadora).

truyamos en  $L_a$  una base ortogonal  $b_2, \dots, b_n$ . Entonces  $a, b_2, \dots, b_n$  será la base ortogonal en  $L$ , donde  $\varphi(a, a) > 0$ , y  $\varphi(b_i, b_i) < 0$ , cualquiera que sea  $i \in \{2, \dots, n\}$ , es decir,  $(L, \varphi)$  es el espacio de Minkowski. Lo recíproco, evidentemente, también tiene lugar (partimos del hecho de que en un espacio con métrica existe una base ortogonal). El lema está demostrado.

Sea  $(L, \varphi)$  un espacio con métrica. Un vector  $a \in L$  se llama *positivo* (*negativo*), si  $\varphi(a, a) > 0$  ( $\varphi(a, a) < 0$ ), e *isótropo*, si  $\varphi(a, a) = 0$ .

**Teorema.** (Desigualdad de Cauchy—Buniakovski para el espacio de Minkowski). Sea  $(L, \varphi)$  un espacio de Minkowski;  $a$ , un vector positivo y  $b$ , un vector arbitrario. Entonces

$$\varphi^2(a, b) \geq \varphi(a, a) \cdot \varphi(b, b) \quad (5)$$

y la igualdad tiene lugar, cuando y sólo cuando  $b = \lambda a$  para cierto  $\lambda \in \mathbb{R}$ .

*Demostración.* Si  $b = \lambda a$  para cierto  $\lambda \in \mathbb{R}$ , entonces en (5) tiene lugar la igualdad. Si  $\varphi(b, b) \leq 0$ , entonces, evidentemente, (5) se verifica. Supongamos que  $b \notin \{a\}$ ,  $\varphi(b, b) > 0$ ; en este caso examinemos un plano  $P = [a, b]$ . Demostraremos que en  $P$  hay un vector negativo. Si para cierto  $y \in P$ ,  $y \neq 0$ , se verifica  $\varphi(y, y) = 0$ , entonces, según el lema 1, tenemos  $\varphi(a, y) \neq 0$ . De aquí resulta que la expresión  $\varphi(a + \lambda y, a + \lambda y) = \varphi(a, a) + 2\lambda\varphi(a, y)$  será inferior a cero con  $\lambda$  correspondiente, es decir, se ha encontrado un vector negativo en  $P$ . Supongamos ahora que para todo  $x \in P$ ,  $x \neq 0$ , tiene lugar  $\varphi(x, x) > 0$ . En este caso  $P$  es un subespacio regular. Por eso se construye una descomposición en la suma directa:  $L = P \oplus P_1$ , donde  $P_1$  es un complemento ortogonal de  $P$ . Tomemos las bases ortogonales;  $\{e_1, e_2\}$  en  $P$  y  $\{e_3, \dots, e_n\}$  en  $P_1$ . La unión de ellas es una base ortogonal para  $L$ . En esta base  $\varphi(e_1, e_1) > 0$ ,  $\varphi(e_2, e_2) > 0$ , por consiguiente, la signatura de  $L$  es  $(k_1, k_2, k_3)$  con  $k_1 \geq 2$ , lo que contradice la afirmación de que  $(L, \varphi)$  es un espacio de Minkowski. Así pues, la suposición de partida no es cierta y en  $P$  siempre existe un vector negativo. Examinemos ahora la expresión  $\varphi(a + \lambda b, a + \lambda b) = \varphi(a, a) + 2\lambda\varphi(a, b) + \lambda^2\varphi(b, b)$ ; para cierto  $\lambda$  ella es negativa, por lo cual el trinomio cuadrado de  $\lambda$  cuenta con raíces reales. Por consiguiente, su discriminante no es negativo:

$$\varphi^2(a, b) - \varphi(a, a) \cdot \varphi(b, b) \geq 0,$$

lo que demuestra (5). El caso de igualdad se analiza con ayuda de los razonamientos análogos y se sugiere que el lector lo haga como un ejercicio. El teorema queda demostrado.

**Teorema** (desigualdad de Alexándrov-Egórychev para permanentes). Sea  $a_{ij} \geq 0$  para  $i, j = 1, \dots, n$ . Entonces se verifica la desigualdad

$$\text{per}^2 \begin{bmatrix} a_{1,1} & \dots & a_{1,n-2} a_{1,n-1} a_{1,n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n,1} & \dots & a_{n,n-2} a_{n,n-1} a_{n,n} \end{bmatrix} \geq$$

$$\geq \begin{bmatrix} a_{1,1} & \dots & a_{1,n-2} & a_{1,n-1} & a_{1,n-1} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n,1} & \dots & a_{n,n-2} & a_{n,n-1} & a_{n,n-1} \end{bmatrix} \cdot \text{per} \begin{bmatrix} a_{1,1} & \dots & a_{1,n-2} & a_{1,n} & a_{1,n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n,1} & \dots & a_{n,n-2} & a_{n,n} & a_{n,n} \end{bmatrix}. \quad (6)$$

Las matrices que están en el segundo miembro difieren sólo por las dos últimas columnas: en una matriz la última columna repite la penúltima, en la otra, viceversa. Si  $a_{ij} > 0$  para  $i = 1, \dots, n; j = 1, \dots, n-2$ , entonces la igualdad se consigue, cuando y sólo cuando para todo  $i = 1, 2, \dots, n$  tiene lugar  $a_{i,n-1} = \lambda a_{i,n}$ , donde  $\lambda \in \mathbf{R}$ . Para demostrar el teorema se requieren dos lemas de D. I. Falikman [68].

**Lema 2.** Sea  $\varphi(x, y)$  una función bilineal simétrica en el espacio vectorial  $V$  tal, que existe un vector no nulo  $a \in V$ , el cual posee la propiedad de que  $\varphi(a, a) = 0$ , y para todo  $x \in V, x \neq \lambda a$  ( $\lambda \in \mathbf{R}$ ) se afirma que de la igualdad  $\varphi(x, a) = 0$  se deduce que  $\varphi(x, x) < 0$ . Entonces, si  $b, c \in V, B, c \neq 0$ , y  $\varphi(b, c) = 0, \varphi(b, b) > 0$ , entonces  $\varphi(c, c) < 0$ .

*Demostración.* Si para cierto  $x \in V$  se cumple la condición  $\varphi(x, a) = 0$ , entonces  $\varphi(x, x) \leq 0$ . De la desigualdad  $\varphi(b, b) > 0$  se deduce  $\varphi(b, a) \neq 0$ . Pongamos  $\eta = -\varphi^{-1}(b, a) \cdot \varphi(c, a)$ . Entonces  $\varphi(c + \eta b, a) = 0$ , y, por consiguiente,

$$0 \geq \varphi(c + \eta b, c + \eta b) = \varphi(c, c) + \eta^2 \varphi(b, b).$$

Si  $\eta \neq 0$ , entonces  $\varphi(c, c) \leq -\eta^2 \cdot \varphi(b, b) < 0$ . En cambio, si  $\eta = 0$ , tenemos  $\varphi(c, a) = 0$ . Los vectores  $c$  y  $a$  no son colineales, puesto que de lo contrario de la condición  $\varphi(b, c) = 0$  se desprendería que  $\varphi(b, a) = 0$ , lo que no es cierto. Por eso,  $\varphi(c, c) < 0$  también en este caso.

**Lema 3.** Sea  $\varphi(x, y) = \text{per} \begin{bmatrix} a_{1,1} & \dots & a_{1,n-2} & x_1 y_1 \\ \dots & \dots & \dots & \dots \\ a_{n,1} & \dots & a_{n,n-2} & x_n y_n \end{bmatrix}$ , donde  $a_{ij} > 0$  para  $i, j$  tales que  $1 \leq i \leq n, 1 \leq j \leq n-2, n \geq 2$ .

Entonces, si  $b, c \in \mathbf{R}^n, b, c \neq 0, \varphi(b, c) = 0, \varphi(b, b) > 0$ , se tiene que  $\varphi(c, c) < 0$ .

La demostración del lema la realizaremos por inducción respecto de  $n \geq 2$ . Cuando  $n = 2, \varphi(x, y) = \text{per} \begin{bmatrix} x_1 y_1 \\ x_2 y_2 \end{bmatrix} = x_1 y_2 + x_2 y_1$ . Tenemos:  $0 = \varphi(b, c) = b_1 c_2 + b_2 c_1, \varphi(b, b) = 2b_1 b_2 > 0$ . Por consiguiente,  $b_1 \neq 0, b_2 \neq 0$  y  $c_1 \neq 0, c_2 \neq 0$ . Al multiplicar ambos miembros de la igualdad  $-b_1 c_2 = b_2 c_1$  por  $b_1 c_2$ , obtenemos  $-b_1^2 c_2^2 = b_1 b_2 c_1 c_2$ . Por consiguiente,  $c_1 c_2 < 0$ , y  $\varphi(c, c) = 2c_1 c_2 < 0$ .

Supongamos ahora que  $n > 2$ , y que para todos los  $k$  naturales:  $2 \leq k \leq n-1$  y la afirmación del lema es válida. Pongamos  $a = (0, \dots, 0, 1)$ . Entonces

$$\varphi(a, a) = \text{per} \begin{bmatrix} a_{1,1} & \dots & a_{1,n-2} & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n-1,1} & \dots & a_{n-1,n-2} & 0 & 0 \\ a_{n,1} & \dots & a_{n,n-2} & 1 & 1 \end{bmatrix} = 0.$$

Elijamos un vector arbitrario  $x = (x_1, \dots, x_n) \in \mathbb{R}^n$  tal que  $\varphi(x, a) = 0$ , y los vectores  $x$  y  $a$  no son colineales, es decir,  $x' = (x_1, \dots, x_{n-1}) \neq 0$ . Entonces  $\varphi(x, x) < 0$ . En efecto,

$$\begin{aligned} \varphi(x, a) &= \text{per} \begin{bmatrix} a_{1,1} & \dots & a_{1,n-2} & x_1 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n,1} & \dots & a_{n,n-2} & x_n & 1 \end{bmatrix} = \\ &= \text{per} \begin{bmatrix} a_{1,1} & \dots & a_{1,n-2} & x_1 & \\ \dots & \dots & \dots & \dots & \\ a_{n-1,1} & \dots & a_{n-1,n-2} & x_{n-1} & \end{bmatrix} = 0 \end{aligned}$$

Por consiguiente

$$\varphi(x, x) = \text{per} \begin{bmatrix} a_{1,1} & \dots & a_{1,n-2} & x_1 & x_1 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n,1} & \dots & a_{n,n-2} & x_n & x_n \end{bmatrix} = \sum_{i=1}^{n-2} a_{ni} \varphi_i(x', x'),$$

donde

$$\begin{aligned} \varphi_i(x', x') &= \\ &= \text{per} \begin{bmatrix} a_{1,1} & \dots & a_{1,i-1} & a_{1,i+1} & \dots & a_{1,n-2} & x_1 & x_1 \\ \dots & \dots \\ a_{n-1,1} & \dots & a_{n-1,i-1} & a_{n-1,i+1} & \dots & a_{n-1,n-2} & x_{n-1} & x'_{n-1} \end{bmatrix} \end{aligned}$$

Está claro que  $\varphi_i(x', a'_i) = \varphi(x, a) = 0$ , y, además,  $\varphi_i(a'_i, a'_i) > 0$  (puesto que  $a_{ij} > 0$  para  $i = 1, \dots, n, j = 1, \dots, n-2$ ), donde  $a'_i = (a_{1,i}, \dots, a_{n-1,i})$ . Por consiguiente, de acuerdo con la hipótesis de inducción,  $\varphi_i(x', x') < 0$ , de donde  $\varphi(x, x) < 0$ . La aplicación del lema anterior finaliza la demostración del lema 3.

Demostremos ahora (6). Supongamos al principio que todos los elementos de la matriz  $A = [a_{ij}]$  son positivos. Para la función  $\varphi$ , construida en el lema 3, existe un vector positivo  $a = (1, \dots, 1)$ . De acuerdo con el lema 3, de que  $\varphi(a, b) = 0, b \neq 0$ , se desprende  $\varphi(b, b) < 0$ . Por eso, según el lema 1, el par  $(\mathbb{R}^n, \varphi)$  es un espacio de Minkowski, y la desigualdad (6) es la desigualdad de Cauchy—Buniakovski (5) para dicho espacio.

El caso en que entre los elementos  $a_{ij}$  pueden encontrarse elementos nulos se desprende del examinado más arriba con ayuda de un paso límite. Sin embargo, en estas circunstancias no es obligatorio que el signo de igualdad tenga lugar sólo cuando los vectores  $b$  y  $c$  son colineales. El caso general en que (6) se convierte en una igualdad ha sido analizado por A. A. Panov [70].

En 1926 Van der Waerden [71] planteó una cuestión; ¿cuál será el valor mínimo de la función del permanente sobre el conjunto  $\Omega_n$  de todas las matrices dos veces estocásticas de orden  $n$ ? La respuesta positiva a esta pregunta era conocida como hipótesis de Van der Waerden. Se suponía que si  $A$  era una matriz dos veces estocástica de orden  $n$ , entonces per

$A \geq n^{-n} \cdot n!$ , con la particularidad de que la igualdad se consigue, cuando y sólo cuando  $A$  es la matriz  $J_n$ , todos los elementos de la cual son iguales a  $n^{-1}$ . La demostración de la validez de la hipótesis ha sido obtenida en 1980. Comencemos su exposición por una serie de lemas auxiliares (véase [18]). Introduzcamos algunas nociones preliminares.

Una matriz no negativa de orden  $n$  la llamaremos *parcialmente descomponible* si contiene una submatriz nula de dimensión  $k \times (n - k)$ . En otras palabras, la matriz  $A$  es parcialmente descomponible, si existen matrices conmutables  $P$  y  $Q$  de tal índole que

$$PAQ = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix},$$

donde  $B$  y  $D$  son matrices cuadradas. Si la matriz no contiene submatriz nula de dimensión  $k \times (n - k)$  para ningún  $k = 1, \dots, n - 1$ , se denominará *bien indescomponible*.

Observemos que si  $A$  es una matriz dos veces estocástica parcialmente descomponible, se encontrarán matrices conmutables  $P$  y  $Q$  tales que  $PAQ$  se descomponga en una suma directa de las matrices dos veces estocástica.

En efecto, supongamos que

$$PAQ = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix},$$

donde  $B$  y  $D$  son matrices cuadradas, y el orden  $D$  es igual a  $k$ . Denotemos con  $s(X)$  la suma de los elementos en la matriz  $X$ . Puesto que  $PAQ$  es una matriz dos veces estocástica, la suma de los elementos dispuestos en sus primeras  $n - k$  columnas, es igual a  $n - k$ , es decir,  $s(B) = n - k$ . Análogamente,  $s(D) = k$ . Por consiguiente,  $s(C) = s(PAQ) - s(B) - s(D) = n - (n - k) - k = 0$ . Por cuanto  $C$  es no negativa, tenemos  $C = 0$ . Es obvio que las matrices  $B$  y  $D$  son dos veces estocásticas.

**Lema 4.** Sea  $A$  una matriz de orden  $n$ . Para que cada transversal suya contenga cero, es necesario y suficiente que en  $A$  exista una submatriz nula de dimensión  $r \times t$ , donde  $r + t = n + 1$ .

La validez de la afirmación se deduce del teorema de König (véase § 4.1).

Denotemos con  $A_{ij}$  una submatriz de la matriz  $A$  obtenida por supresión de la  $i$ -ésima fila y de la  $j$ -ésima columna.

**Lema 5.** Una matriz no negativa  $A$  de orden  $n \geq 2$  es bien indescomponible, cuando y sólo cuando para todos los  $i, j = 1, \dots, n$  se verifica la desigualdad: per  $A_{ij} > 0$ .

*Demostración.* Según el lema 4 per  $A_{ij} = 0$ , cuando y solo cuando la submatriz  $A_{ij}$ , y, por tanto, la matriz  $A$  contienen una submatriz nula de dimensión  $r \times t$ , donde  $r + t = (n - 1) + 1$ . Dicho de otro modo, per  $A_{ij} = 0$ , si y sólo si  $A$  es parcialmente descomponible.

La matriz dos veces estocástica  $A$  de orden  $n$  se llamará *minimizadora*, siempre que per  $A = \min_{B \in \Omega} B$ .

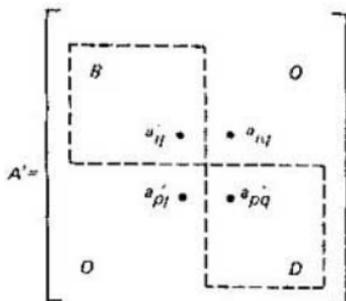


Fig. 4.2.

**Lema 6.** La matriz minimizadora es bien indescomponible.

*Demostración.* Sea  $A \in \Omega_n$  una matriz minimizadora y supongamos que  $A$  es parcialmente descomponible. En este caso existirán matrices conmutables  $P$  y  $Q$  tales que  $PAQ$  será una suma directa de las matrices  $B \in \Omega_{n-k}$  y  $D \in \Omega_k$ . Denotemos  $A' = PAQ$ . Está claro que  $A' \in \Omega_n$ ,  $A'$  es una matriz minimizadora. Elijamos en la transversal de la matriz  $A'$ , compuesta por los elementos no nulos, los elementos  $a'_{ij}$  y  $a'_{pq}$  que pertenecen a las matrices  $B$  y  $D$ , respectivamente. Tenemos:  $a'_{ij} \neq 0$ ,  $a'_{pq} \neq 0$ ,  $a'_{iq} = a'_{pj} = 0$ , per  $A'_{ij} > 0$  y per  $A'_{pq} > 0$ . Del lema 4 se deduce que per  $A'_{iq} = \text{per } A'_{pj} = 0$ . Veamos la matriz  $A'(\varepsilon)$ :  $a'_{ij}(\varepsilon) = a'_{ij} - \varepsilon$ ,  $a'_{pq}(\varepsilon) = a'_{pq} - \varepsilon$ ,  $a'_{iq}(\varepsilon)a'_{pj}(\varepsilon) = \varepsilon$ ,  $a'_{ri}(\varepsilon) = a'_{ri}$ , si  $r \neq i, p$ , o bien  $t \neq j, q$ . Está claro que  $A'(\varepsilon) \in \Omega_n$ , cuando los valores de  $\varepsilon > 0$  son suficientemente pequeños. Nos convencemos inmediatamente de que  $\frac{d}{d\varepsilon} \text{per } A'(\varepsilon)|_{\varepsilon=0} = -\text{per } A'_{ij} + \text{per } A'_{iq} - \text{per } A'_{pq} + \text{per } A'_{ij} = -\text{per } A'_{ij} - \text{per } A'_{pq} < 0$ . Por consiguiente, per  $A'(\varepsilon) < \text{per } A'$ , cuando los valores de  $\varepsilon > 0$  son suficientemente pequeños. Esto contradice el hecho de que la matriz  $A'$  es minimizadora.

**Lema 7.** Si una matriz  $A \in \Omega_n$  es minimizadora y si  $a_{pq} > 0$ , entonces per  $A_{pq} = \text{per } A$ .

*Demostración.* Estudiemos el siguiente conjunto de las matrices de dimensión  $n \times n$ :  $C(A) = \{X = [x_{ij}] | x_{ij} \geq 0 \text{ para cualesquiera } i, j = 1, \dots, n; x_{ij} = 0 \text{ para } (i, j) \in Z\}$ , donde  $Z = \{(i, j) | a_{ij} = 0\}$ . Consideramos  $C(A)$  como un conjunto de puntos en un espacio euclidiano de dimensión  $n^2 - |Z|$ ; en este caso  $A$  será un punto interior de dicho conjunto. En  $C(A)$  tenemos un problema suave (véase [11]):

$$\text{per } X \rightarrow \inf$$

con restricciones

$$\sum_{j=1}^n x_{ij} = 1, \quad i = 1, \dots, n; \quad (7)$$

$$\sum_{i=1}^n x_{ij} = 1, \quad j = 1, \dots, n-1$$



por construcción. Esta submatriz tiene las dimensiones  $(n - k) \times (n - l - 1)$ . De aquí y de la desigualdad (10):  $n - k + n - l - 1 = n + (n - k - l - 1) \geq n$ , puesto que  $n - k - l - 1 \geq 0$ . Lo último contradice la plena descomponibilidad de la matriz  $A$ . Esto quiere decir que la igualdad  $\lambda_0 = 0$  es imposible. Al dividir las relaciones (8) por  $\lambda_0$ , obtenemos

$$\text{per } A_{ij} = \bar{\lambda}_i + \bar{\mu}_i \text{ para cualesquiera } (i, j) \notin Z \\ i, j \in \{1, \dots, n\}$$

(aquí tomamos  $\bar{\mu}_n = 0$ ).

Permutando, si es necesario, las filas y columnas de la matriz  $A$ , logremos que se cumplan las desigualdades:  $\bar{\lambda}_1 \leq \bar{\lambda}_2 \leq \dots \leq \bar{\lambda}_n$ ,  $\bar{\mu}_1 \leq \bar{\mu}_2 \leq \dots \leq \bar{\mu}_n$ . Descomponiendo per  $A$  respecto de la primera fila y la última columna, y empleando el hecho de que la suma de los elementos en cualquier fila (columna) de la matriz  $A$  es igual a la unidad, obtendremos

$$\lambda_1 + \bar{\mu}_n \geq \sum_{\substack{j=1 \\ (1, j) \notin Z}}^n a_{1j} \text{ per } A_{1j} = \sum_{j=1}^n a_{1j} \text{ per } A_{1j} \text{ per } A_{1j} = \text{per } A = \\ = \sum_{i=1}^n a_{in} \text{ per } A_{in} = \sum_{\substack{i=1 \\ (i, n) \notin Z}}^n a_{in} \text{ per } A_{in} \geq \bar{\lambda}_1 + \bar{\mu}_n.$$

Por consiguiente,  $\bar{\lambda}_1 + \bar{\mu}_n = \text{per } A = \text{Per } A_{1j} = \text{per } A_{in}$  para todos los  $i, j$  tales que  $(1, j) \notin Z$ ,  $(i, n) \notin Z$ .

Supongamos que para todos los  $i, j$  tales que  $j \geq j_1$ ,  $i \leq i_1$ ,  $(i, j) \notin Z$  ya se ha demostrado que  $\text{per } A_{ij} = \text{per } A$ . Veamos la  $(i_1 + 1)$ -ésima fila de la matriz  $A$ . Si existe  $\bar{j} \geq j_1$  tal que  $(i_1 + 1, \bar{j}) \notin Z$ , entonces para todo  $j \geq \bar{j}$  tal que  $(i_1 + 1, j) \notin Z$ , tenemos:  $\text{per } A_{i_1+1, j} = \text{per } A$  (por suposición) y para todo  $j < \bar{j}$  tal que  $(i_1 + 1, j) \notin Z$  tenemos:  $\text{per } A_{i_1+1, j} = \bar{\lambda}_{i_1+1} + \bar{\mu}_j \leq \bar{\lambda}_{i_1+1} + \bar{\mu}_{\bar{j}} = \text{per } A_{i_1+1, \bar{j}} = \text{per } A$ . Por consiguiente,  $\text{per } A = \sum_{j=1}^n a_{i_1+1, j} \text{ per } A_{i_1+1, j} \leq \text{per } A$ , y para todos los  $j$  tales que  $(i_1 + 1,$

$j) \notin Z$ , se verifica la igualdad

$$\text{per } A_{i_1+1, j} = \text{per } A.$$

Los razonamientos análogos son lícitos también para la  $(j_1 - 1)$ -ésima columna de la matriz  $A$ . En cambio, si para cualesquiera  $j \geq j_1$  y  $i \leq i_1$  se verifica:

$$(i_1 + 1, j) \in Z \text{ y } (i, j_1 - 1) \in Z, \text{ es decir, } a_{i_1+1, j} = 0 \text{ y } a_{i, j_1-1} = 0,$$

entonces

$$\bar{\lambda}_{i_1+1} + \bar{\mu}_{j_1-1} \geq \sum_{j=1}^{j_1-1} a_{i_1+1, j} \text{ per } A_{i_1+1, j} = \text{per } A = \\ = \sum_{i=i_1+1}^n a_{i, j_1-1} \text{ per } A_{i, j_1-1} \geq \bar{\lambda}_{i_1+1} + \bar{\mu}_{j_1-1},$$

y, por consiguiente, para cualesquiera  $i, j$  tales que  $(i, j_1 - 1) \notin Z, (i_1 + 1, j) \notin Z$ , tenemos:  $\text{per } A_{i, j_1 - 1} = \text{per } A_{i_1 + 1, j} = \text{per } A$ .

Así pues, si  $(i, j) \notin Z$ , entonces  $\text{per } A_{ij} = \text{per } A$ , lo que se trataba de demostrar.

**Lema 8** (desigualdad de London). Si  $A$  es una matriz minimizadora en  $\Omega_n$ , para cualesquiera  $i, j = 1, \dots, n$  se verifica la desigualdad  $\text{per } A_{ij} \geq \text{per } A$ .

*Demostración.* Para toda matriz conmutadora  $P = [p_{ij}]$  y el número  $\theta \in [0, 1]$  pongamos  $f_p(\theta) = \text{per}((1 - \theta)A + \theta P)$ . Por cuanto  $A$  es la matriz minimizadora, entonces  $f'_p(0) \geq 0$  para cualquier matriz conmutadora  $P$ . Sea  $\sigma$  una permutación correspondiente a  $P$ . Tenemos

$$\begin{aligned} f'_p(0) &= \sum_{r,t=1}^n (-a_{rt} + p_{rt}) \text{per } A_{rt} = \sum_{r,t=1}^n p_{rt} \text{per } A_{rt} - n \text{per } A = \\ &= \sum_{j=1}^n \text{per } A_{r\sigma(r)} - n \text{per } A \geq 0. \end{aligned}$$

Por consiguiente,

$$\sum_{r=1}^n \text{per } A_{r\sigma(r)} \geq n \text{per } A \quad (11)$$

para toda permutación  $\sigma$ . Según el lema 6, la matriz  $A$  es bien indescomponible, por lo cual, de conformidad con el lema 5, cualquier elemento de  $A$  se dispone en cierta transversal, cuyos elementos restantes son todos positivos. Dicho de otro modo, para cualquier par  $(i, j)$  existe tal permutación  $\sigma$  que  $j = \sigma(i)$ , y  $a_{r\sigma(r)} > 0$ , cuando  $r = 1, \dots, i - 1, i + 1, \dots, n$ . Pero, en virtud del lema 7, esto significa que  $\text{per } A_{r\sigma(r)} = \text{per } A$  para  $r = 1, \dots, i - 1, i + 1, \dots, n$ . Por cuanto  $j = \sigma(i)$ , obtenemos de (11):  $\text{per } A_{ij} \geq \text{per } A$ , lo que se trataba de demostrar.

Ahora, siguiendo los razonamientos de Egórychev, señalemos cómo se puede demostrar, al hacer uso de la desigualdad (6), la validez de la suposición de Van der Waerden.

Sea  $A$  una matriz minimizadora. Probemos que  $\text{per } A_{ij} = \text{per } A$  para cualesquiera  $i, j = 1, \dots, n$ . Supongamos lo contrario: existe al menos un solo par  $r, s \in \{1, \dots, n\}$  tal que  $\text{per } A_{rs} > \text{per } A$ . Por cuanto la matriz  $A$  es dos veces estocástica, existe  $t \in \{1, \dots, n\}$  tal que  $a_{rt} > 0$ . Entonces, en virtud de la desigualdad (6) y del lema 8, tenemos

$$\begin{aligned} \text{per}^2 A &\geq \left( \sum_{k=1}^n a_{ks} \text{per } A_{kt} \right) \left( \sum_{k=1}^n a_{kt} \text{per } A_{ks} \right) > \\ &> \left( \sum_{k=1}^s a_{ks} \text{per } A \right) \left( \sum_{k=1}^n a_{kt} \text{per } A \right) = \text{per}^2 A \end{aligned}$$

(el carácter estricto de la desigualdad en este caso se desprende de que  $a_{rt} > 0$  y  $\text{per } A_{rs} > \text{per } A > 0$ ).

Demostremos ahora que si  $A$  es una matriz minimizadora, entonces  $a_{ij} = n^{-1}$  ( $i, j = 1, \dots, n$ ). Supongamos que la columna de la matriz  $A$

de número  $n$  se diferencia de  $(n^{-1}, \dots, n^{-1})^T$ . Por cuanto  $A$  no se descompone en una suma directa de matrices no nulas, cada elemento de la  $n$ -ésima columna de  $A$  es inferior a la unidad. Por consiguiente, entre los primeros  $n - 1$  elementos de cada fila de la matriz  $A$  hay por lo menos un elemento no nulo. Pasando de  $A$  a una matriz que se obtiene a partir de  $A$  sustituyendo la  $i$ -ésima y  $j$ -ésima columnas de su semisuma ( $i \neq j$ ,  $i, j = 1, \dots, n - 1$ ), obtendremos, al hacer un número finito de pasos, la matriz  $A'$  en la que todos los elementos de las primeras  $n - 1$  columnas son positivos, mientras que la  $n$ -ésima columna coincide con la  $n$ -ésima columna de la matriz  $A$ , con la particularidad de que  $\text{per } A' = \text{per } A$ , puesto que, hecho cualquier paso, el permanente no varía (lo que se desprende de la fórmula de descomposición del permanente de una matriz respecto de las columnas y de la igualdad de todos los permanentes de las submatrices de  $(n - 1)$ -ésimo orden).

Designemos con  $A_j(b)$  una matriz obtenida de  $A'$  como resultado de la sustitución de la  $j$ -ésima columna por la columna  $b$ . Ya hemos aclarado que en la desigualdad

$$\text{per}^2 A' \geq \text{per } A'_n(a'_n) \text{ per } A'_n(a_n)$$

se realiza la igualdad. El carácter positivo de las componentes  $a'_1, \dots, a'_{n-1}$  da el derecho de afirmar que  $a_n = \lambda_i a'_i$  ( $i = 1, \dots, n - 1$ ). Por cuanto las sumas de componentes de los vectores son todas iguales a 1, entonces  $a_n = a'_i$  ( $i = 1, \dots, n - 1$ ). Como la matriz  $A'$  es dos veces estocástica llegamos a que  $a'_1 = \dots = a'_{n-1} = a_n = (n^{-1}, \dots, n^{-1})^T$ , lo que es una contradicción. Por consiguiente, todas las columnas de la matriz  $A$  son iguales a  $(n^{-1}, \dots, n^{-1})^T$  y esto demuestra nuestra afirmación.

Veamos el problema sobre las estimaciones superiores para los permanentes. En 1960 Ryser supuso que en la clase de  $(0, 1)$ -matrices de orden  $mk$ , cada línea de las cuales contiene  $k$  unidades, el valor máximo del permanente se logra en la suma directa de matrices de orden  $k$ , compuestas por unidades. J. Minc enunció en 1963 una suposición más general de que si  $A$  era una  $(0, 1)$ -matriz de orden  $n$  que tiene  $r_1, \dots, r_n$  sumas respecto de las filas, entonces  $\text{per } A \leq \prod_{i=1}^n (r_i!)^{\frac{1}{r_i}}$ . De esta desigualdad se deduce

inmediatamente la hipótesis de Ryser.

La desigualdad de Minc la demostró por primera vez (en 1973) Bregman [73]. Más abajo aducimos una demostración más sencilla de esta desigualdad que se debe a Schrijver [74].

**Lema 9.** Para los números reales no negativos  $x_1, \dots, x_r$  es válida la desigualdad

$$\left( r^{-1} \sum_{i=1}^r x_i \right)^{\sum_{i=1}^r x_i} \leq \prod_{i=1}^r x_i^{x_i}$$

(en esta fórmula se supone que  $0^0 = 1$ ).

*Demostración.* Al hacer uso de la convexidad de la función  $y = x \log_2 x$ , obtenemos

$$r^{-1} \sum_{i=1}^r x_i \log_2 \left( r^{-1} \sum_{i=1}^r x_i \right) \leq r^{-1} \sum_{i=1}^r x_i \log_2 x_i,$$

de donde se deduce inmediatamente el resultado del lema.

Sea  $A = [a_{ij}]$  una  $(0, 1)$ -matriz cuadrada de orden  $n$ , y sea  $S$  un conjunto de todas las permutaciones  $\pi$  de los números  $1, \dots, n$  tales que  $\prod_{i=1}^n a_{i\pi(i)} = 1$  entonces

$$\prod_{\substack{i,j \\ a_{ij}=1}} \text{per}(A_{ij})^{\text{per}A} = \prod_{\pi \in S} \prod_{i=1}^n \text{per} A_{i\pi(i)}, \quad \prod_{i=1}^n r_i^{\text{per}A} = \prod_{\pi \in S} \prod_{i=1}^n r_i.$$

La validez de estas identidades se confirma con facilidad mediante una comprobación directa. Aprovechémoslas para demostrar la desigualdad de Minc. Apliquemos el método de inducción matemática completa respecto de  $n$ . Del lema 9 tenemos

$$\begin{aligned} (\text{per} A)^{n \text{per}A} &= \prod_{i=1}^n (\text{per} A)^{\text{per}A} = \prod_{i=1}^n \left( \prod_{j=1}^n a_{ij} \text{per} A_{ij} \right)^{\sum_{j=1}^n a_{ij} \text{per}A_{ij}} \leq \\ &\leq \prod_{i=1}^n \left( r_i^{\text{per}A} \prod_{j: a_{ij}=1} (\text{per} A_{ij})^{\text{per}A_{ij}} \right) = \prod_{\pi \in S} \left[ \left( \prod_{i=1}^n r_i \right) \left( \prod_{i=1}^n \text{per} A_{i\pi(i)} \right) \right]. \end{aligned}$$

Apliquemos ahora la hipótesis de inducción a cada una de las matrices  $A_{i\pi(i)}$ :

$$\begin{aligned} \prod_{i=1}^n \text{per} A_{i\pi(i)} &\leq \prod_{i=1}^n \left( \prod_{\substack{j \neq i \\ a_{j\pi(i)}=0}} (r_j!)^{\frac{1}{r_j}} \right) \left( \prod_{\substack{j \neq i \\ a_{j\pi(i)}=1}} (r_j - 1)!^{\frac{1}{(r_j-1)}} \right) = \\ &= \prod_{j=1}^n \left( \prod_{\substack{i \neq j \\ a_{j\pi(i)}=0}} (r_j!)^{\frac{1}{r_j}} \right) \left( \prod_{\substack{i \neq j \\ a_{j\pi(i)}=1}} (r_j - 1)!^{\frac{1}{(r_j-1)}} \right) = \prod_{j=1}^n \left[ r_j!^{\frac{n-r_j}{r_j}} (r_j - 1)! \right]. \end{aligned}$$

La última igualdad se ha obtenido por cálculo de los factores  $(r_j!)^{1/r_j}$  y  $(r_j - 1)!^{1/(r_j-1)}$ . Siendo fijos  $\pi$  y  $j$ , el número de índices  $i$ , para los cuales  $i \neq j$ , es igual a  $n - r_j$  si  $a_{j\pi(i)} = 0$ , y a  $r_j - 1$ , si  $a_{j\pi(i)} = 1$ . Así pues,

$$\begin{aligned} (\text{per} A)^{n \text{per}A} &\leq \prod_{\pi \in S} \left[ \left( \prod_{i=1}^n r_i \right) \left( \prod_{j=1}^n r_j!^{\frac{n-r_j}{r_j}} (r_j - 1)! \right) \right] = \\ &= \prod_{\pi \in S} \left( \prod_{i=1}^n r_i^{\frac{n}{r_i}} \right) = \left( \prod_{i=1}^n r_i! \frac{1}{r_i} \right)^{n \text{per}A}, \end{aligned}$$

lo que se trataba de demostrar.

Volvamos a las aplicaciones de las desigualdades a los permanentes.

Denotemos con  $L(r, n)$  el número de  $(r \times n)$ -rectángulos latinos compuestos por los elementos de un conjunto  $S = \{1, 2, \dots, n\}$ . Analicemos algún rectángulo latino de dimensión  $t \times n$ ,  $1 \leq t < r$ . De cuántas maneras puede ser extendido hasta que se obtenga un  $(t+1) \times n$ -rectángulo latino? Está claro que el número de tales métodos es igual a  $\text{per } A$ , donde  $A$  es la matriz de incidencia del sistema de subconjuntos  $(S_1, \dots, S_n)$ , donde  $S_i$  es un subconjunto de aquellos elementos de  $S$  que no se encuentran en la  $i$ -ésima columna del rectángulo a extender ( $i = 1, \dots, n$ ).

En cada fila de la matriz  $A$  están contenidas  $n-t$  unidades; la matriz  $(n-t)^{-1}A$  será dos veces estocástica. Aplicando las desigualdades de Minc y de Van der Waerden, obtendremos

$$\frac{n!}{n^n} (n-t)^n \leq \text{per } A \leq (n-t)!^{n-t}.$$

Cuando  $t=1$ ,  $\text{per } A = n! \sum_{i=0}^n (-1)^i \frac{1}{i!} = D_n$ , lo que constituye el número de desórdenes sobre  $n$  elementos. Por consiguiente,

$$\frac{(n!)^{r-1}}{n^{n(r-2)}} D_n \prod_{i=2}^{r-1} (n-t)^n \leq L(r, n) \leq n! D_n \prod_{i=2}^{r-1} (n-t)!^{n-t}.$$

Si ponemos  $r=n$ , obtendremos  $L(n, n) \geq (n!)^{2n} n^{-n^2} > (e^{-2}n)^{n^2}$ . Se ha aprovechado aquí la conocida desigualdad:  $n! > e^{-n}n^n$ . Wilson [58] utilizó la desigualdad reducida  $L(n, n) > (e^{-2}n)^{n^2}$  para determinar la frontera inferior del número  $N(v)$  de ternas no isomorfas de Steiner de orden  $v$  y obtuvo la siguiente estimación:

$$N(v) \geq (e^{-5}v)^{v^2/6}.$$

Examinemos en conclusión las aplicaciones de los permanentes a los problemas de dímeros que surgieron en la física y química. Llamemos  $n$ -ladrillo a un paralelepípedo  $k$ -dimensional ( $k \geq 2$ ) de volumen  $n$ , en el cual las longitudes de las aristas son de números enteros:  $a_1, \dots, a_k$ . Sea  $n$  par. Se plantea una cuestión: ¿cuántos son los métodos para componer un  $n$ -ladrillo, sirviéndose de 2-ladrillos (dímeros)? Denotemos este número con  $N$ . Dividamos el  $n$ -ladrillo en cubos unitarios y numeremos los:  $1, 2, \dots, n$ . Supongamos que  $A = [a_{ij}]$  es una matriz de incidencia que caracteriza la disposición mutua de los cubos:  $a_{ij} = 1$  ó  $0$ , lo que depende de si tienen o no aristas comunes los cubos marcados con los números  $i$  y  $j$  ( $a_{11} = a_{22} = \dots = a_{nn} = 0$ ).

Se afirma que  $N^2 = \text{per } A$ . Efectivamente, a todo par ordenado de particiones del  $n$ -ladrillo en dímeros le corresponde una transversal biunívoca de la matriz  $A$  compuesta por unidades. Por ejemplo, sea  $n=6$ ,  $k=2$ ,  $a_1=2$ ,  $a_2=3$ . La matriz de incidencia tendrá la forma siguiente:

1	2	3
4	5	6

Fig. 4.3.

	1	2	3	4	5	6
1	0	1	0	1	0	0
2	1	0	1	0	1	0
3	0	1	0	0	0	1
4	1	0	0	0	1	0
5	0	1	0	1	0	1
6	0	0	1	0	1	0

Fig. 4.4.

1	2	3
4	5	6

1	2	3
4	5	6

Al par ordenado de particiones del ladrillo en la fig. 4.4, le corresponde unívocamente la permutación

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 5 & 2 & 3 \end{pmatrix}$$

y la transversal de la matriz  $A$  compuesta por unidades contorneadas en la fig. 4.3.

Observemos que todas las sumas respecto de las filas y columnas de la matriz de incidencia  $A$  son iguales a  $2k$ , a excepción de aquellas que corresponden a los cubos en la superficie. Veamos, en lugar del  $n$ -ladrillo un ladrillo toroidal correspondiente, el cual se obtiene por pegadura de las aristas opuestas del ladrillo original. La matriz de incidencia  $A'$  del ladrillo toroidal tiene  $2k$  unidades en cada fila y en cada columna. Valiéndonos de la desigualdad de Mine, obtendremos:  $\text{per } A' \leq (2k)!^{n/2k}$ , y, por consiguiente,  $N \leq (2k)!^{n/4k}$ .

Hammersley [75] mostró que si  $a_i \rightarrow \infty$  para todo  $i = 1, \dots, k$ , la magnitud  $n^{-1} \ln N$  tiende a cierto límite  $\lambda_k$ . De este modo,

$$\lambda_k \leq \frac{1}{2} \ln [(2k)!]^{1/2k} < \frac{1}{2} \ln k.$$

La aplicación de la desigualdad de Van der Waerden a la matriz  $A'$  nos conduce a la estimación por debajo:  $\lambda_k \geq \frac{1}{2} \ln \frac{2k}{e}$  (véase [75]). Por consiguiente,

$$\lambda_k \sim \frac{1}{2} \ln \frac{2k}{e} (1 + o(1)) \quad \text{para } k \rightarrow \infty.$$