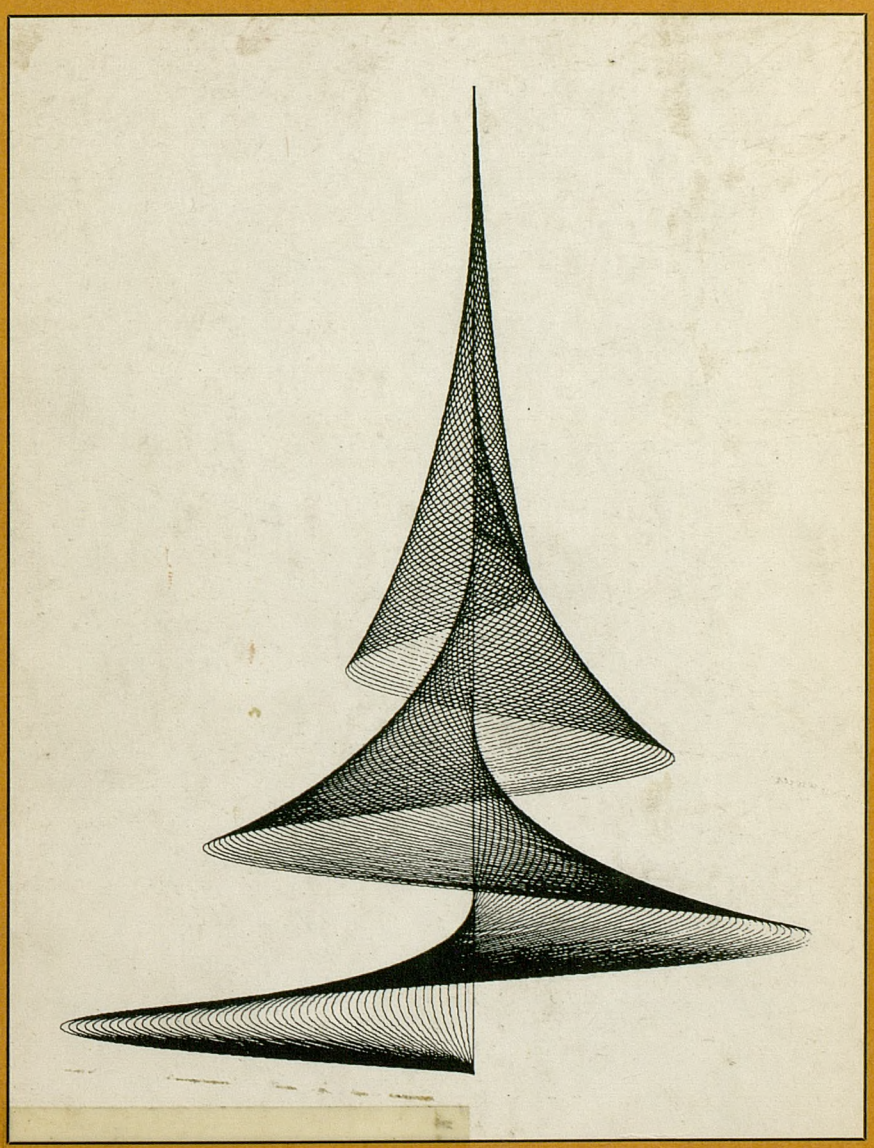
APUNTES DE METODOS MATEMATICOS DE APLICACION A LA INFORMATICA



SISTEMAS

APUNTES DE METODOS MATEMATICOS DE APLICACION A LA INFORMATICA

SISTEMAS

Tomados de las clases de:

L. CUENA BARTOLOME
C. DOMINGUEZ DELGADO
L. FERRER ARELLANO
J. MARTIN DE SAAVEDRA
A. REGIDOR ROPERO

Profesores del Instituto de Informática

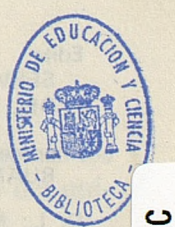
APUNTES DE METODOS MATEMATICOS DE APLICACION A LA INFORMATICA

SISTEMAS

Tomados de las clases de:

J. CUENA BARTOLOME
C. DOMINGUEZ DELGADO
I. FERRER ARELLANO
J. MARTIN DE SAAVEDRA
A. REGIDOR ROPERO

Profesores del Instituto de Informática



Edita:
SERVICIO DE PUBLICACIONES
DEL MINISTERIO DE EDUCACION Y CIENCIA

Imprime:
RUAN, S. A. - Alcobendas (Madrid)

D. L.: M. 2.077 - 1972

CAPITULO I

CONCEPTOS BASICOS DE ALGEBRA

1. *Definiciones.*

Los términos conjunto y elemento son indefinibles; puede darse una definición que en realidad es un circunloquio basado en conceptos análogos.

"Un conjunto es una colección bien determinada de objetos que por definición son sus elementos."

Los conjuntos se designan con letras mayúsculas y los elementos con minúsculas.

Símbolo $\in$

El símbolo $\in$ representa una relación entre un elemento y un conjunto; $m \in X$ significa "m es un elemento del conjunto X". Dado un elemento m y un conjunto X, siempre es posible determinar si se verifica $m \in X$.

Igualdad de conjuntos. Subconjuntos

Se dice que dos conjuntos X e Y son iguales y se escribe $X = Y$ únicamente si los dos conjuntos son idénticos, es decir, contienen exactamente los mismos elementos.

Si un conjunto X está compuesto íntegramente por elementos de otro conjunto Y, diremos que X es un *subconjunto* de Y, y se escribirá $X \subseteq Y$. Si, además, Y contiene uno o más elementos que no están en X, se dice que X es un *subconjunto propio* de Y.

Conjunto universal

Es el que incluye todos los elementos en discusión. Al conjunto universal se le asignan los símbolos u,1; de la definición anterior se sigue que todo conjunto es subconjunto del universal.

Conjunto vacío

Es el conjunto que no contiene ningún elemento.

Por definición, el conjunto vacío es un subconjunto de todos los conjuntos. La notación para conjuntos vacíos es el ϕ o el 0.

Conjunto unitario

Un *conjunto unitario* es aquel que contiene un solo elemento, y si ese elemento es, digamos, x, llamaremos al conjunto $\{x\}$.

En otros casos el conjunto se especifica por una lista de los elementos del conjunto y se usa el símbolo $\{\ \}$ para incluirlos. Por ejemplo, $\{a,b,c\}$ se entiende que es un conjunto que consta de los elementos a, b, c solamente.

Producto cartesiano de dos conjuntos es el conjunto formado por los pares ordenados de elementos de los dos conjuntos. Se indica con la notación x. Por tanto, si los dos conjuntos son E y F, el conjunto producto cartesiano es

$$ExF = \{(a,b)|a\in E\ \ b\in F\}$$

Conjuntos complementarios

Asociaremos a cada conjunto X otro conjunto X', llamado el *complementario* de X, o su complemento definido como el conjunto de los elementos del conjunto universal que no son elementos del conjunto X. Como caso especial, los conjuntos universal y vacío son complementarios uno de otro. El conjunto complementario también puede representarse por $\bar{X}$ y $\sim X$.

Ejemplo: Consideremos unos libros tales que algunos están forrados en rojo, otros en negro y el resto en amarillo. Supongamos que todos los libros rojos y alguno de los negros están escritos en inglés. El resto de los libros negros está escrito en alemán, y los amarillos en francés. El universo son todos los libros del estante.

R conjunto de los libros rojos.
Y conjunto de los libros amarillos.
B conjunto de los libros negros.
E conjunto de los libros escritos en inglés.
F conjunto de los libros escritos en francés.
G conjunto de los libros escritos en alemán.

En este ejemplo, $Y = F$ y $R \subseteq$ E. En efecto, R es un subconjunto propio de E. Si un libro rojo específico se le designa por m, podemos escribir $m\in R$, y también $m\in E$, o también $\{m\} \subseteq R$ y $\{m\} \subseteq E$. E' es el conjunto que consta de todos los libros amarillos y aquellos negros que están escritos en alemán.

2. *Operaciones con conjuntos*

Son éstas unas reglas por las cuales se pueden obtener nuevos conjuntos a partir de otros. Las principales son:

Unión.—Dados dos conjuntos arbitrarios X e Y, se define la unión de X e Y como el conjunto formado por elementos de X o de Y o de ambos X e Y. El nuevo conjunto lo representaremos por $X+Y$, y también puede representarse por $X \cup Y$ o $X \vee Y$. En el ejemplo anterior, $R+Y$ es el conjunto de todos los libros rojos y todos los libros amarillos, $Y+E+G$ es el conjunto universal de todos los libros del estante.

Intersección.—La intersección de X e Y, para dos conjuntos arbitrarios X e Y, es el conjunto formado por aquellos elementos que pertenecen a X y a Y, y se escribirá XY o $X.Y$. También se representa por $X \cap Y$ o $X \wedge Y$. Solamente se usarán los símbolos $+$ y $\cdot$ en la formación del nuevo conjunto. Refiriéndonos al ejemplo de la sección anterior EB es el conjunto de los libros rojos escritos en inglés, RY es el conjunto vacío y RE es R, conjunto de libros rojos.

Como consecuencia de las definiciones de las operaciones *unión*, *intersección* y *complementación* para un conjunto arbitrario X, se verificará que $X+X'=U$, y que $X \cap X' = \phi$.

3. *Relaciones binarias*

A veces una propiedad P puede concernir a dos elementos x e y de dos conjuntos dados A y B.

$$x \in A \quad \text{e} \quad y \in B$$

Si consideramos el producto cartesiano AxB, a las parejas (x,y) teniendo la propiedad P, diremos que están relacionadas, y escribiremos xRy. De esta forma diremos que está definida una relación binaria entre los conjuntos A y B.

Las parejas relacionadas entre sí forman un subconjunto del producto cartesiano de A y B.

$$F = \{(x,y) | xRy\} \subseteq AxB$$

este subconjunto F puede ser un subconjunto propio de AxB, ya que la relación binaria no tiene por qué estar definida para todas las parejas de elementos A y B.

En el caso de que $A=B$, es decir, se trata de un mismo conjunto, diremos que tenemos definida una relación binaria dentro del conjunto A.

Ejemplo: Sea: $A = \{\text{conjunto de habitantes de Madrid}\}$
$B = \{\text{conjunto de edificios de Madrid}\}$

Sea P la propiedad de que un determinado habitante viva en un determinado edificio.

Si consideramos el producto AxB, cuyos elementos serán parejas formadas por un habitante de Madrid y un edificio de Madrid, cuando en una de esas parejas, el habitante de Madrid viva en el edificio correspondiente, con el que forma pareja, diremos que ese habitante y ese edificio están relacionados; en caso contrario, diremos que no están relacionados.

De esta forma tendremos definida una relación binaria entre A y B.

Ejemplo: Sea: $A = \{$conjunto de todas las rectas del espacio$\}$
Sea la propiedad P de perpendicularidad.

Si consideramos el producto AxA, o sea todas las parejas posibles de rectas, si una pareja está formada por rectas perpendiculares diremos que esas dos rectas están relacionadas.
De esta forma tendremos definida una relación binaria en el conjunto A.
Las relaciones binarias definidas en un conjunto pueden tener las siguientes propiedades:

a) Reflexiva. Si aRa, es decir, cada elemento, cumple la relación consigo mismo. La relación "=" es reflexiva.
b) Simétrica. Si aRb implica que se verifica también bRa, es decir, si la relación es verificada por el par (a,b), se verifica por el par (b,a). Ejemplo de relación simétrica es "=". En efecto,

$$\text{si } a = b \qquad b = a$$

Otra relación simétrica es "es familiar de".
En efecto:

Si a es familiar de b
b es familiar de a

La relación "es hijo de" no es simétrica, ni la "<".
c) Antisimétrica. Son aquellas relaciones tales que

Si aRb sólo puede verificarse bRa si $a = b$.

Es el caso opuesto a b). La relación "mayor o igual que" es antisimétrica. En efecto, si a es mayor o igual que b,

b no "es mayor o igual que" a a menos que $a = b$.

d) Transitiva. Son aquellas que

Si aRb y bRc se verifica aRc.

Un caso de relación transitiva es "mayor que", en efecto:

si $a > b$ y $b > c$ $\qquad a > c$.

Los tipos de relación más usuales son los de equivalencia y de orden.

RELACIONES DE EQUIVALENCIA

Se dice que una relación binaria entre elementos de un conjunto es una equivalencia cuando es reflexiva, transitiva y simétrica.

Ejemplo de relaciones de equivalencia son: "es familia de", "ser paralela a".
En efecto, en todas ellas se verifica

aRa	reflexiva.
aRb y bRa	simétrica.
aRb, bRc implica que aRc	transitiva.

RELACIONES DE ORDEN

Se dice que una relación binaria es de orden cuando es a la vez reflexiva, transitiva y antisimétrica.

Ejemplo: "$\geqslant$" "es descendiente de"

En el caso de que no se cumpla la propiedad reflexiva se trataría de una relación de orden estricto (por ejemplo, "$<$").

Dado un conjunto C y una relación de orden R entre los elementos del mismo, se dice que el conjunto C está totalmente ordenado por R cuando dados dos elementos cualesquiera a y b de C, pueden compararse mediante R, es decir, puede escribirse aRb o bRa.

En caso contrario se dice que C está parcialmente ordenado por R.

En el primer caso puede decirse también que en el conjunto C la relación R determina un orden total y en el segundo un orden parcial.

4. *Clases de equivalencia*

Sea A un conjunto en el que está definida una relación R de equivalencia. Dado un elemento a de A, todos los elementos de A que estén relacionados con a forman un subconjunto de A que llamaremos *clase de equivalencia de representante a*, $C(a)$.

$C(a)$
$C(b)$
.
.
.
$C(d)$

C/A Clases de equivalencia, que formarán una serie de subconjuntos.

Ejemplo: En el conjunto de las rectas del espacio, el subconjunto de rectas paralelas a la recta r, el de las paralelas a r', ...

Teorema

Cualquier elemento del conjunto A, en el que está definida la relación de equivalencia, pertenece a una clase de equivalencia.

En efecto: Sea $a \in A$, este elemento pertenecerá al subconjunto de elementos de A que estén relacionados con a. En caso de que no existiera ninguno, este elemento a formaría por sí solo una clase de equivalencia, debido a la propiedad reflexiva aRa.

Teorema

Dos elementos cualquiera de una clase de equivalencia son equivalentes entre sí:

Sea $C(a)$ y sean $m,n \in C(a)$, por ser $m \in A$ se verifica que mRa, y por ser $n \in A$ se verifica que nRa.

Si nRa por la propiedad simétrica aRn, y si

$$\left.\begin{array}{l} mRa \\ \text{y} \\ aRn \end{array}\right\} \text{Transitiva} \rightarrow mRn$$

c.q.d.

Teorema

Dos clases de equivalencia no pueden tener un elemento común, ya que en caso de tener un elemento común se trataría de la misma clase.

Sean las clases $C(a)$ y $C(b)$ con un elemento x común a ambas clases

$$\left.\begin{array}{l} x \in C(a) \rightarrow xRa \\ x \in C(b) \rightarrow xRb \end{array}\right\} \rightarrow aRb$$

Veamos que ambas clases son la misma, es decir, que todo elemento de $C(a)$ está en $C(b)$ y recíprocamente.

1.º Si $\forall m \in C(a) \rightarrow mRa$
pero como $aRb \rightarrow mRb \rightarrow m \in C(b)$

2.º Si $\forall m \in C(b) \rightarrow mRb$
pero como $bRa \rightarrow mRa \rightarrow m \in C(a)$

por lo tanto:

$$C(a) = C(b)$$

Como consecuencia de estos teoremas se obtiene el siguiente:

Corolario

Dado un conjunto A, en el que está definida una relación de equivalencia R, todas las clases de equivalencia son tales que:

$$C(a) \cup C(a_2) \cup \ldots \cup C(a_n) = A$$
$$C(a_i) \cap C(a_j) = \phi \quad i \neq j$$

es decir, determinan una partición en el conjunto A.

Teorema

Supongamos que en un conjunto A está definida una partición $A\{A_1, A_2, \ldots A_n\}$ tal que:

$$\begin{cases} A_1 \cup A_2 \cup A_3 \cup \ldots A_n = A \\ A_i \cap A_j = \phi \quad i \neq j \end{cases}$$

Se puede definir una relación de equivalencia en el conjunto A, cuyas clases de equivalencia son precisamente los subconjuntos A_i.

Dos elementos están relacionados cuando los dos pertenezcan al mismo subconjunto. Es decir, definimos R tal que:

aRb cuando existe algún i tal que a y $b \in A_i$

Vamos a demostrar que esa relación es de equivalencia.

1. aRa
2. $aRb \Rightarrow bRa$
4. aRb ..... } pertenecen a A_i } Luego $a, c \in A_i$
   bRc ..... } pertenecen a A_i } Por tanto, aRc

Si $a \in A_i$, entonces $C(a) = A_i$.

Conjunto cociente

Es el conjunto que tiene como elementos las clases de equivalencia A_i, y se represente:

$$A/R \qquad \begin{matrix} A = \text{Conjunto inicial} \\ R = \text{Relación de equivalencia} \end{matrix}$$

Ejemplos

1. Supongamos S el conjunto de todos los números enteros, y que a y $b \in S$ y aRb cuando $a - b$ es múltiplo de n, lo que se indicará $a - b = \dot{n}$.
   Comprobar si R es una relación de equivalencia y hallar las clases de equivalencia cuando $n = 10$.

   1) aRa; $a - a = 0 = K\dot{n}$
   2) $aRb \Rightarrow bRa$
      $a - b = Kn = \dot{n}$ $\qquad$ $b - a = -Kn = \dot{n}$
   4) $\left.\begin{matrix} aRb \\ bRc \end{matrix}\right\} aRc \quad \begin{matrix} \longrightarrow a - b = Kn \\ \longrightarrow b - c = K'n \end{matrix}$ } sumando

      $a - c = (K + K')n = \dot{n} \rightarrow aRc$

   Luego es una relación de equivalencia.
   Clases de equivalencia:

$$\left.\begin{matrix} A_1 = 0, 10, 20 \ldots\ldots\ldots\ldots \\ A_2 = 1, 11, 21 \ldots\ldots\ldots\ldots \\ A_3 = 2, 12, 22 \ldots\ldots\ldots\ldots \\ \cdot \\ \cdot \\ \cdot \\ A_9 = 9, 19, 29 \ldots\ldots\ldots\ldots \end{matrix}\right\}$$

Conjunto cociente

$$S/R\{A_1, A_2, A_3, \ldots A_9\}$$

2. Supongamos el conjunto de todos los puntos del plano aRb si a y b equidistan del origen.
Todas las circunferencias concéntricas con centro en el origen formarían las clases de equivalencia.
$S\ R\{C_1, C_2, \ldots C_n \ldots\}$ el conjunto cociente tendría infinitas circunferencias.

5. APLICACIONES O FUNCIONES

Dados dos conjuntos S y T, una aplicación entre estos dos conjuntos es una correspondencia que asocia a cada elemento de S un elemento de T.

$$S \xrightarrow{f} T \qquad a \xrightarrow{f} x \text{ o } f(a) = x$$

Todo elemento de S tiene que tener un asociado en T y *sólo uno*.

S se llama conjunto de SALIDA o DOMINIO.
T se llama conjunto de LLEGADA o RANGO o CONDOMINIO.

Una aplicación está definida cuando para todo elemento del conjunto de SALIDA se conozca cuál es su asociado en el conjunto de LLEGADA.

5.1. APLICACIONES IGUALES

Dos aplicaciones f y g entre dos conjuntos S y T $\begin{matrix} S \xrightarrow{f} T \\ S \xrightarrow{g} T \end{matrix}$ son iguales cuando todo elemento de S se asocia con el mismo elemento de T a través de las aplicaciones f y g

$$f = g \qquad \forall s \in S \Rightarrow f(s) = g(s)$$

Cuando a todo elemento de un conjunto se le asocia otro elemento de ese mismo conjunto, se tiene una aplicación de ese conjunto en él mismo.
Por ejemplo, $a \to a^2$ en el conjunto de los números naturales $N \quad N \xrightarrow{f} N$.

5.2. APLICACION IDENTICA (I)

La aplicación que asocia cada elemento consigo mismo dentro de un conjunto.

5.3. COMPOSICION DE APLICACIONES O PRODUCTO

Sea la aplicación f de S en T y la g de T en R.

$$S \xrightarrow{f} T \quad \text{y} \quad T \xrightarrow{g} R \quad : \quad S \xrightarrow{g \cdot f} R$$

$$(gof)s = go(f(S) = g(t) = r$$

Sin embargo, $(fog)T = fo(g(T)) = f(R)$, que no existe, por no ser R dominio de f.

Propiedad asociativa del producto:

$$S \xrightarrow{f} T \qquad T \xrightarrow{g} R \qquad R \xrightarrow{h} P$$

$$(hog) \circ f = ho(gof)$$
$$[(hog)of]\ S = (hog)of(S) = (hog)T = hog(T) = h(R) = P$$
$$[ho(gof)]S = ho[(gof)(S)] = hogo(f(S)) = hog(T) = h(R) = P$$

Cualquier aplicación multiplicada por la aplicación identidad I_A reproduce la misma aplicación f.

Supongamos que tenemos:

$$\left.\begin{array}{l} A \xrightarrow{f} B \\ A \xrightarrow{I_A} A \end{array}\right\} \begin{array}{ll} foI_A = f & a \in A \quad f(a) = b \\ I_A\, of = f & (f.I_A)a = f\,(I_A(b)) = f(a) = b \end{array}$$

5.4. IMAGEN DE UNA APLICACION

Dada la aplicación $A \xrightarrow{f} B$, se llama imagen de A a través de f el conjunto de elementos b_i de B para los cuales existe al menos un a_i de A, tal que $f(a_i) = b_i$.

$$I_m(A) = \{b_i \in B \text{ para los cuales } \exists\ a_i \in A \Rightarrow f(a_i) = b_i\}$$

5.5. INYECCION

Una aplicación f de A en B se dice que es una aplicación inyectiva si dos elementos distintos de A se transforman en dos elementos distintos de B:

$$A \xrightarrow{f} B$$

Supongamos que $\left.\begin{array}{l} a_1 \to b_1 \\ a_2 \to b_2 \end{array}\right\}$ Si $a_1 \neq a_2$, entonces $b_1 \neq b_2$.

Forma de demostrar que una aplicación es inyectiva:
Suponemos que $b_1 = b_2$ y demostramos que, como consecuencia, $a_1 = a_2$. Es decir, en una inyección la igualdad de las imágenes implica la de los elementos de partida.

5.6. SOBREYECCION

Una aplicación f de A en B es sobreyectiva cuando la imagen de A coincide con el conjunto de llegada

$$A \xrightarrow{f} B; \quad I_m(A) = B$$

5.7. BIYECCION

Una aplicación f de A en B que sea inyectiva y sobreyectiva se la llama biyectiva (correspondencia biunívoca):

$$A \xrightarrow{f} B \qquad \begin{array}{ccc} S & x & T \\ & x & \\ & x & \end{array} \qquad \begin{array}{l} x \\ x \\ x \end{array}$$

5.8. RELACION DE EQUIVALENCIA ASOCIADA A UNA APLICACION

Sea f una aplicación de AaB.

$$A \xrightarrow{f} B$$

a través de esta aplicación veamos cómo se define en A una relación de equivalencia.

Dos elementos $a_1, a_2, \in A$ diremos que están relacionados cuando: $f(a_1) = f(a_2)$, esta relación cumple las propiedades:

Reflexiva: aRa, puesto que $f(a) = f(a)$.

Simétrica: si $a_1 R a_2 \Rightarrow f(a_1) = f(a_2)$, y por tanto $f(a_2) = f(a_1)$, luego $a_2 R a_1$.

Transitiva: Si $\left.\begin{array}{l} a_1 R a_2 \rightarrow f(a_1) = f(a_2 \\ a_2 R a_3 \rightarrow f(a_2) = f(a_3) \end{array}\right\} \Rightarrow f(a_1) = f(a_3)\ a_1 R a_3$

esta relación de equivalencia dará lugar a un conjunto cociente $A|f$, cuyos elementos son los subconjuntos de A que se representan en el mismo elemento de B.

5.9. DESCOMPOSICION CANONICA DE UNA APLICACION

Sea una aplicación f de AaB

$$A \xrightarrow{f} B$$

Consideramos el conjunto cociente $A|f$ y definimos la siguiente aplicación g de A en $A|f$.

$\forall a \in A \xrightarrow{g} C(a)$ esta aplicación es sobre.

Definimos la aplicación h de $A|f$ en $Im.\ (A)$,

$C(a) \xrightarrow{h} f(a)$ esta aplicación es inyectiva.

Por último, defino la aplicación I de $Im(A)$ a B, haciendo corresponder a cada elemento al mismo.

De esta forma pasamos de A a B a través de las tres aplicaciones definidas

$$A \xrightarrow{g} A | f \xrightarrow{h} Im(A) \xrightarrow{i} B$$

$$A \xrightarrow{iohog} B, \text{ o sea } f = iohog$$

5.10. INVERSA DE UNA APLICACION

Sea f una aplicación de S en T.

$$S \xrightarrow{f} T$$

si existe una aplicación g de T en S tal que gof produzca la identidad en S, es decir:

$$\forall s_i \in S \rightarrow t_i \in T \rightarrow s_i \in S, \quad \text{o sea, } gof = I_s$$

diremos que g es la inversa de f por la izquierda.

De forma análoga definimos la inversa de f por la derecha diciendo:

sea f una aplicación de S *a* T

$$S \xrightarrow{f} T$$

Si existe una aplicación g de T en S tal que fog produzca la identidad en T, es decir,

$$\forall t_i \in T \xrightarrow{f} s_i \in S \xrightarrow{g} t_i \in T, \text{ o sea } fog = I_t,$$

diremos que g es la inversa por la derecha de f.

Si dada una aplicación f existen las aplicaciones inversas por la izquierda y por la derecha y éstas son la misma a esta aplicación la llamaremos INVERSA o RECIPROCA, designándola por f^{-1}.

Teorema

Una aplicación f es inyectiva si y solamente si admite una inversa a la izquierda.

PRIMERA PARTE

Hipótesis

f admite una inversa a la izquierda

$$S \xrightarrow{f} T, \quad T \xrightarrow{g} S \Rightarrow gof = Is$$

Tesis

f es inyectiva.

Demostración

$$\left.\begin{array}{l} \text{Si } s_1 \xrightarrow{f} t_1 \\ s_2 \xrightarrow{f} t_2 \end{array}\right\} \text{ Si } t_1 = t_2 \text{ debe ser } s_1 = s_2$$

Supongamos que $t_1 = t_2$:

$$s_1 = (gof)s_1 = g[f(s_1)] = g(t_1)$$
$$s_2 = (gof)s_2 = g[f(s_2)] = g(t_2)$$

Como suponemos que $t_1 = t_2$, será: $g(t_1) = g(t_2)$.

Y por lo tanto, $s_1 = s_2$ c. q. d.

SEGUNDA PARTE

Hipótesis

f es inyectiva

$$S \xrightarrow{f} T$$

Tesis

f admite una inversa a la izquierda.

Demostración

Definimos una g de T en S, $T \xrightarrow{g} S$ de la forma:

$\forall t_i \in I_m(S) g(t_i) = s_i$ tal que $f(s_i) = t_i$
$\forall t_j \notin I_m(S) g(t_i) = s_o$, siendo s_o un elemento cualquiera de S

$$(gof)\, s_i = g(f(s_i)) = g(t_i) = s_i, \text{ luego } gof = I_s$$

Teorema

Una aplicación es sobreyectiva si y sólo si admite una inversa a la derecha.

PRIMERA PARTE

Hipótesis

f admite inversa a la derecha.

$$S \xrightarrow{f} T, \quad T \xrightarrow{g} S \Rightarrow fog = I_T$$

Tesis

f es sobreyectiva.

Demostración

$\forall t_i$, $t_i = (fog)t_i = f(g(t_i)) = f(s_i) = t_i$, para todo t_i existe, pues, un s_i tal que $f(s_i) = t_i$.

SEGUNDA PARTE

Hipótesis

f es sobreyectiva.

Tesis

f admite inversa a la derecha.

Demostración

Definiríamos una aplicación g de T en S de tal modo que a cada elemento de T le haga corresponder *uno* de los que proviene de S. Esta aplicación así definida es la inversa a la derecha de f, puesto que

$$\forall t_i \in T, (fog)t_i = fo[g(t_i)] = f(S_i) = t_i$$

$$fog = I_T$$

Teorema

Si g es biyectiva admite una inversa g^{-1}.

En efecto, como es una relación biunívoca, admite inversa por la izquierda, por ser inyectiva, e inversa por la derecha, por sobreyectiva, y como es biunívoca ambas inversas serán iguales (g^{-1}).

Inversa del producto

$$(fog)^{-1} = g^{-1} of^{-1}$$

Si demostramos que (gof) o $(f^{-1}$ o $g^{-1}) = \mathrm{I}$ (identidad), estará demostrado:

$$gof \text{ o } f^{-1}og^{-1} = goIog^{-1} = gog^{-1} = I$$

6. OPERACIONES BINARIAS

6.1. *Definición*

Una operación binaria o ley de composición interna, definida en un conjunto C es una regla que hace corresponder a cada par ordenado (a,b) de elementos de C otro elemento del mismo conjunto, denominado resultado de la operación. Esto se indica en la forma

$$a \square b = c$$

$\square$ es el símbolo de la operación.

Una operación binaria es, por tanto, una aplicación del producto cartesiano CxC en C.

La operación de substracción es una operación binaria sobre el conjunto de todos los números racionales (números de la forma p/q, donde p y q son enteros y $q \neq 0$), pero no es una operación binaria en el conjunto de todos los números enteros positivos. Para cualquier pareja de números racionales $A = p/q$ y $B = r/s$, la diferencia $A - B$ está únicamente definida por otro número racional $(ps - rq)/qs$; de aquí $(-)$ satisface las condiciones de la definición de una operación binaria en el conjunto de todos los números racionales. Sin embargo, la diferencia de dos números enteros positivos no es siempre un número entero positivo, y de aquí $(-)$ no representa una operación binaria en el conjunto de los números enteros positivos.

6.2. PROPIEDADES

a) Una operación binaria $\square$ sobre un conjunto M es *asociativa* si y sólo si para toda a,b y c en M

$$a \square (b \square c) = (a \square b) \square c.$$

b) Una operación binaria $\square$ sobre un conjunto M es *conmutativa* si y sólo si para todo a y b en M

$$a \square b = b \square a.$$

c) Existencia de elemento neutro.

Un conjunto se dice que tiene elemento neutro respecto a una operación si existe algún elemento del conjunto tal que

$$u \square a = a \square u = a \qquad \text{(I)}$$

Cuando en un conjunto existe elemento neutro respecto a una operación, éste es único. En efecto, supongamos que hubiera dos elementos u y u' que verificase (I) para todo elemento del conjunto. Entonces

Si hubiera dos elementos unidad u y u', sería:

$$\left.\begin{array}{l} uu' = u \text{ por ser } u' \text{ unidad} \\ uu' = u' \text{ por ser } u \text{ unidad} \end{array}\right\} u = u'$$

En álgebra de números el cero es el neutro respecto a la suma y el 1 respecto a la multiplicación.

d) Si un conjunto C posee elemento neutro u respecto a una operación $\square$, puede definirse el elemento simétrico de uno dado $x \in C$ como aquél $y \in C$ que verifica

$$x \square y = y \square x = u$$

El elemento simétrico suele designarse por x^{-1}.

e) Propiedad distributiva.

Dado un conjunto S dotado de dos operaciones binarias $\square$ y *, se dice que la operación $\square$ es distributiva a la izquierda respecto a $(\square)^*$ si se verifica

$$a\square(b^*c)=(a\square b)^*(a\square c) \tag{1}$$

Cualquiera que sean $(a,b,c)\in S$; análogamente se dice que es distributiva a la derecha respecto a * si

$$(b^*c)\square a=(b\square a)^*(c\square a) \tag{2}$$

Cualquiera que sean $(a,b,c)\in S$.

Si se verifican (1) y (2), se dice simplemente que $\square$ es distributiva respecto a *.

Operación binaria estable para una relación binaria

Sea un conjunto A en el que está definida una operación 0 y una relación binaria R. Diremos que la operación 0 es estable para la relación R cuando

$$\left.\begin{matrix} a_1Ra_2 \\ a_3Ra_4 \end{matrix}\right\} \Rightarrow a_1 \text{ o } a_3 \; R \; a_2 \text{ o } a_4$$

Teorema

En un conjunto A en el que hay definida una operación o y una relación R de equivalencia, tal que la operación es estable para la relación, esta operación 0 induce una operación 0′ sobre el conjunto A/R.

$$A/R \left\{\begin{matrix} C(a_1) \\ C(a_2 \\ \cdot \\ \cdot \\ \cdot \\ C(a_n) \end{matrix}\right.$$

Definimos la operación 0′ entre dos clases, a aquella clase cuyo representante es el operado de los representantes

$$C(a_1)0'C(a_2)=C(a_1 \text{ o } a_2)$$

La clase resultante de operar dos clases es independiente de los representantes de las clases. En efecto:

$$b_1\in C(a_1)\rightarrow C(a_1)=C(b_1)$$
$$b_2\in C\,(a_2)\rightarrow C(a_2)=C(b_2)$$

$C(b_1)$ o $C(b_2)=C(b_1$ o $b_2)$, pero como

$\left.\begin{matrix} b_1Ra_1 \\ b_2Ra_2 \end{matrix}\right\}$ b_1 o b_2Ra_1 o a_2 por ser la operación estable para la relación.

Luego $C(b_1$ o $b_2)=C(a_1$ o $a_2)$.

7. MORFISMOS

Dados dos conjuntos A y A' en los cuales están definidas sendas operaciones o y o', un morfismo es una aplicación de A en A' que conserva las operaciones.

Tenemos definida una aplicación f de A en A':

$$A \xrightarrow{f} A'$$

Si se verifica que: $\left.\begin{matrix} a \xrightarrow{f} a' \\ b \xrightarrow{f} b' \end{matrix}\right\} \Rightarrow aob \xrightarrow{f} a'o'b'$

entonces f es un morfismo.

Según el tipo de f los morfismos pueden ser:

Aplicaciones f	*Morfismos*	*Conjunto sobre sí mismo*
Inyectiva ⟷	Monomorfismo	
Sobreyectiva ⟷	Epimorfismo	Endomorfismo
Biyectiva ⟷	Isomorfismo	Automorfismo

Teorema

La compuesta o producto de dos morfismos es otro morfismo.

Sean los tres conjuntos A, A' y A'', y tenemos:

$$A \xrightarrow{f_1} A' \qquad A' \xrightarrow{f_2} A''$$

f_3 es la compuesta de f_1 y f_2, o sea una aplicación de $A \to A''$; veamos qué es morfismo:

$$\left.\begin{matrix} a \xrightarrow{f_1} a' \\ b \xrightarrow{f_1} b' \end{matrix}\right\} a \circ b \xrightarrow{f_1} a' \circ b', \text{ por ser } f_1 \text{ un morfismo}$$

$$\left.\begin{matrix} a' \xrightarrow{f_2} a'' \\ b' \xrightarrow{f_2} b'' \end{matrix}\right\} a' \circ b' \xrightarrow{f_2} a'' \circ b'', \text{ por ser } f_2 \text{ un morfismo}$$

Luego $a \circ b \xrightarrow{f_3} a'' \circ b''$, por ser f_3 la compuesta de f_1 y f_2. Por lo tanto, f_3 conserva las operaciones, luego f_3 es un morfismo.

8. GRUPOS

8.1 *Semigrupos*

Un conjunto S con una operación binaria asociativa es un semigrupo.

El conjunto de los números naturales mayores que cero y con la operación + es un semigrupo $\{1,2,3,\ldots,+\}$.

8.2. *Monoides*

Un semigrupo con elemento neutro es un monoide $\{0,1,2,3,\ldots,+\}$.

8.3. *Grupos*

Un grupo es un monoide tal que cada elemento tiene un inverso. Ejemplo: $\{\ldots -2,-1,0,1,2,3,\ldots\}$. (números enteros positivos y negativos).

De donde se desprende que un conjunto A en el que está definida una operación tiene categoría de grupo cuando se verifican los tres axiomas siguientes:

1.º La operación es asociativa

$$(a \circ b) \circ c = a \circ (b \circ c)$$

2.º Existe un elemento u, que llamaremos neutro respecto a esa operación, tal que

$$\forall a \in A \rightarrow a \circ u = \circ a = a$$

3.º Para cada elemento del conjunto A existe otro elemento a' de ese conjunto, al que llamaremos simétrico, tal que

$$a \circ a' = a' \circ a = u.$$

Si el grupo goza además de la propiedad conmutativa diremos que es un grupo conmutativo o abeliano.

Las clases de resto de módulo n forman un grupo.

$$Ra \oplus Rb = R_{a+b}$$

1) Que es asociativa:

$$R_a + (R_b + R_c) = (R_a + R_b) + R_c$$
$$R_a + R_{b+c} = R_{a+bc} = R_{(a+b)+c} = R_a + b + R_c = (R_a + R_b) + R_c$$

2) Existe elemento neutro:

$$R_o + R_a = R_{a+o} = R_a$$

3) Existe elemento inverso.

El de R_a sería R_{n-a}; $R_a + R_{n-a} = R_{a+n-a} = R_n = R_o$

8.4. *Propiedades de los grupos*

Teorema

En todo grupo se verifica que si $aob = aoc$, entonces $b = c$; $a'oaob = a'oaoc$; $uob = uoc$. Luego $b = c$.

Teorema

En un grupo G una ecuación del tipo $ax = b$ tiene una solución y sólo una.
Multiplicando por a^{-1} por la izquierda,

$$a^{-1} \cdot a \cdot x = a^{-1}b;\ u \cdot x = a^{-1}b;\ x = a^{-1}b$$

Veamos que es única:
Supongamos que hubiese dos x_1 y x_2; ambas verificarán la ecuación

$$\left.\begin{array}{l} ax_1 = b \\ ax_2 = b \end{array}\right\} ax_1 = ax_2;\ x_1 = x_2 \text{ por el teorema anterior.}$$

Corolario

El simétrico de un elemento es único, por ser éste por definición solución de la ecuación

$$aox = xoa = u$$

Teorema

El inverso de un producto es el producto de las inversas cambiados de orden

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$$

En efecto, para ver que el inverso de $a \circ b$ es $b^{-1} \circ a^{-1}$ basta multiplicar los dos elementos y ver si el producto es el elemento neutro,

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ b \circ b^{-1} \circ a^{-1} = a \circ u \circ a^{-1} = a \circ a^{-1} = u$$

Teorema

Dado un morfismo f entre dos grupos g y g'.
Veamos que el neutro de g se transforma en el neutro de g'
Sea u el elemento neutro de g.

$$u \to b'$$

Veamos que b' es el neutro de g'.

En efecto:

$$\begin{array}{l} a \to a' \\ u \to b' \\ \hline a \circ u = a \to a' \circ b' = a'. \end{array}$$

Por lo tanto, b' será el neutro de g'.

Teorema

Dado un morfismo f entre dos grupos g y g', si $a \to a'$, el inverso de a se transforma en el inverso de a'.

En efecto:

$$\begin{array}{c} a \to a' \\ a^{-1} \to b' \\ \hline a \circ a^{-1} = u \to a' \circ b' = u' \end{array}$$

Luego b' es el inverso de a'.

Definición

Utilizaremos la notación a^m para indicar la aplicación sucesiva de la operación o m veces con el elemento a. Es decir,

$$a^m = \underbrace{a \circ a \circ \ldots \circ a}_{m \text{ factores}}$$

Definimos análogamente

$$a^o = u \text{ y } a^{-m} = (a^{-1})^m = a^{-1}{}_o a^{-1}{}_o \ldots a^{-1}$$

Teorema

Para todo $a \in G$, $a^m{}_o a^n = a^{m+n}$, siendo m y n números enteros positivos o negativos.

Demostración

En el caso en que m y n sean ambos positivos, por definición se verifica:

$$a^m \circ a^n = \underbrace{(aoao \ldots oa)}_{m \text{ factores}} \circ \underbrace{(aoao \ldots oa)}_{n \text{ factores}} = a^{m+n}$$

De forma análoga puede verse el caso en que sean negativos los exponentes:

1.º Si uno de ellos es negativo:

$$a^n a^{-m} = a^n . (a^{-1})^m = \underbrace{(ao,ao \ldots a)}_{n \text{ factores}} \circ \underbrace{(a^{-1} \circ a^{-1} \circ \ldots oa^{-1})}_{m \text{ factores}}$$

eliminando cada a con su inmediata a^{-1} se obtendrán:

1.º Si $|n| > |m|$, se obtendrán $m - n$ veces el factor a^{-1}, quedando

$$a^{n-m}$$

2.º Si $|n| > |m|$, se obtendrán $m - n$ veces el factor a^{-1}, quedando

$$(a^{-1})^{m-n} = a^{n-m}$$

2.º Si los dos son negativos:

$$a^{-n} \circ a^{-m} = (a^{-1})^n \circ (a^{-1})^m =$$

$$= (a^{-1} \circ a^{-1} \circ \ldots a^{-1}) \, 0 \, (a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1}) = (a^{-1})^{m+n} = a^{-m-n}$$

(n factores; m factores)

Ejercicio

Sea el conjunto formado por los elementos x_1, x_2 y x_3, y consideremos todas las aplicaciones biyectivas de este conjunto en sí mismo. Demostrar que el conjunto de todas estas aplicaciones forman un grupo

$$S = \{x_1, x_2, x_3\} \qquad S \to S$$

El número de aplicaciones biyectivas que puedo formar sería:

$$P_3 = 6, \text{ es decir, } \{f_1, f_2, f_3, f_4, f_5 \text{ y } f_6\} = A$$

f_1	f_2	f_3	f_4	f_5	f_6
$x_1 \to x_1$	x_1	x_2	x_2	x_3	x_3
$x_2 \to x_2$	x_3	x_1	x_3	x_1	x_2
$x_3 \to x_3$	x_2	x_3	x_1	x_2	x_1

Veamos si forma grupo:

$f_1 \cdot f_2 = f_2$;

$x_1 \to x_1 \to x_1$
$x_2 \to x_2 \to x_3$
$x_3 \to x_3 \to x_2$
. . . . .
$f_2 \cdot f_3 = f_3$

$x_1 \to x_1 \to x_2$
$x_2 \to x_3 \to x_1$
$x_3 \to x_2 \to x_3$

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_3			
f_3	f_3					
f_4	f_4					
f_5	f_5					
f_6	f_6					

En la tabla se observará si existe elemento neutro f_1, y si cada elemento tiene su inverso; en este caso formarán grupo.

8.5. *Subgrupos*

Subgrupo

Un subconjunto S de un grupo G se dice que es un subgrupo de G si:

1.º S es cerrado respecto de la operación de G.

2.º Si el elemento neutro de G está en S

$$u \in S$$

3.º Si cada elemento de S tiene su simétrico también en S

$$\forall a \in S \rightarrow a^{-1} \in S$$

es decir, si S por sí solo tiene categoría de grupo.

Como caso particular de subgrupos de un grupo G se puede considerar al mismo grupo G y al grupo $\{U\}$ formado por el elemento neutro; a estos dos subgrupos se les llama subgrupos impropios.

Teorema

La condición necesaria y suficiente para que un subconjunto S cerrado de un grupo G sea un subgrupo es que si:

$$a \text{ y } b \in S \Rightarrow a \text{ o } b^{-1} \in S.$$

1.º La condición necesaria:

Hipótesis) S es un subgrupo de G.
Tesis) Si a y $b \in S \Rightarrow a$ o $b^{-1} \in S$.

En efecto:

Si $a \in S$ y $b \in S$, por ser S subgrupo $b^{-1} \in S$.

Si $a \in S$ por ser S subgrupo
$b^{-1} \in S$

---

a o $b^{-1} \in S$ c. q. d.

2.º La condición es suficiente:

Hipótesis) Si a y $b \in S \Rightarrow a$ o $b^{-1} \in S$
Tesis) S es un subgrupo.

En efecto:

1.º Si $a, a \in S$ a o $a^{-1} \in S \rightarrow u \in S$, luego S contiene el elemento neutro.
2.º Si $ua \in S \rightarrow u$ o $a^{-1} = a^{-1} \in S$, luego si está un elemento está su inverso.
3.º S es cerrado, es decir, si a y $b \in S \rightarrow a$ o $b \in S$.

En efecto:

$$a, b \in S$$

Si $b \in S \rightarrow b^{-1} \in S \rightarrow b^{-1}$ y $a \in S$, por hipótesis se verifica que b^{-1} o $a^{-1} \in S$, y por lo tanto,

$$(b^{-1} \text{ o } a^{-1})^{-1} \in S \rightarrow a \text{ o } b \in S \quad \text{c. q. d.}$$

Corolario

Dado un grupo G, el subconjunto de G formado por todas las potencias de un elemento de G es subgrupo de G.

En efecto, sea G' el conjunto formado por todas las potencias de $a \in G$.
Sean x e y dos elementos de G', se verificará $x = a^m$, $y = a^n$,

$$x \circ y^{-1} = a^m \circ a^{-n} = a^{m-n} \in G'$$

Teorema

Si A y B son dos subgrupos de G, se verifica que $A \cap B$ es también un subgrupo de G.

En efecto:

Si $a,b \in A \cap B \rightarrow \begin{cases} a,b \in A \\ a,b \in B \end{cases}$

Si $a,b \in A \begin{cases} ab^{-1} \in A \\ a,b \in B \end{cases} ab^{-1} \in B$ por ser A y B subgrupos.

Luego $ab^{-1} \in A \cap B$ *c.q.d.*

8.6. *Nucleo*

Dado un morfismo f entre los grupos g y g', se llama núcleo del morfismo al conjunto de elementos de g que se transforman por medio del morfismo en el elemento neutro de g'.

$$N = (x \in g / x \xrightarrow{f} u')$$

Teorema

Dado un morfirmo f entre dos grupos g y g', el núcleo es un subgrupo de g.

En efecto:

$a,b \in N$ (núcleo de f), por pertenecer al núcleo

$$\begin{array}{l} a \xrightarrow{f} u' \\ b \xrightarrow{f} u' \end{array} \Bigg\} \begin{array}{l} a \rightarrow u' \\ b^{-1} \rightarrow u' \end{array}$$

$a \circ b^{-1} \rightarrow u' \circ u' = u'$, luego
$a \circ b^{-1} \in N$, por lo tanto, el núcleo es un subgrupo de g.

Teorema

La condición necesaria y suficiente para que un morfismo sobre f, entre dos grupos g y g' sea un isomorfismo, es que el núcleo contenga únicamente el elemento neutro u.

Condición necesaria

Hipótesis) f es isomorfismo.
Tesis) N contiene únicamente el neutro.

En efecto, Como el emento u, neutro de g, siempre está en N, ya que para todo morfismo $u \rightarrow u'$, si existiera otro elemento a en N,

$$a \xrightarrow{f} u'$$

Resultando que por medio de f, dos elementos distintos u y a se transforman en el mismo u' de g', contradicción, pues f es un isomorfismo.

Condición suficiente

Hipótesis) $N = \{u\}$
Tesis) f es un isomorfismo.

En efecto, veamos que dos elementos distintos de g, no pueden transformarse en un mismo elemento de g'.

$$\text{Si} \quad \left.\begin{array}{l} a_1 \to a' \\ a_2 \to a' \end{array}\right\} \quad \begin{array}{l} a_1 \to a' \\ a_2^{-1} \to a'^{-1} \end{array}$$

$$a_1 \circ a_2^{-1} \to a' \circ a'^{-1} = u'$$

Si $a_1 \circ a_2^{-1} \to u'$ es que $a_1 \circ a_2^{-1}$ pertenece al núcleo, y como éste sólo contiene al elemento neutro u, deberá ser:

$$a_1 \circ a_2^{-1} = u, \text{ o sea } a_1 = a_2$$

Teorema

Dado un morfismo f entre dos grupos g y g', la imagen de g es un subgrupo de g'.
En efecto.

$$g \xrightarrow{f} g' \text{ veamos que } Im(g) \subseteq g' \text{ es un subgrupo.}$$

Si $a', b' \in Im(g)$, habrá dos elementos a y b tales que

$$\left.\begin{array}{l} a \xrightarrow{f} a' \\ b \xrightarrow{f} b' \end{array}\right\} \quad \begin{array}{l} a \to a' \\ b^{-1} \to b'^{-1} \end{array}$$

$$ab^{-1} \to a'b'^{-1} \in Im(f)$$

Luego $Im(g)$ es un subgrupo g'.

8.7. *Automorfismo interno*

Dado un grupo g, se define la siguiente aplicación f de g en g.
Fijado un elemento $a \in g$,

$$V\, x \in g \xrightarrow{f} axa^{-1}$$

Veamos que esta aplicación así definida es un automorfismo, y le llamaremos *automorfismo interno* engendrado por el elemento a.

1.º Veamos que es un morfismo; es decir, veamos que conserva las operaciones:

$$\begin{array}{l} x \to axa^{-1} \\ y \to aya^{-1} \end{array}$$

$$xy \to axa^{-1}aya^{-1} = axya^{-1}$$

2.º Veamos que es un morfismo sobre, es decir, que para cualquier elemento $x \in g$, existe al menos un elemento de g, que al aplicarlo el automorfismo interno engendrado por a, da el elemento x.

$$a^{-1}xa \xrightarrow{f} aa^{-1}xaa^{-1} = x.$$

Por lo tanto, todo elemento x proviene de $a^{-1}xa$.

3.º Veamos que es un isomorfismo, es decir, que el núcleo contiene únicamente el elemento neutro.

Si $x \in N$,

$$x \to axa^{-1} = u \text{ por ser } x \text{ del núcleo.}$$
$$axa^{-1} = u \quad x = ana^{-1} = u$$

8.8. *Conjunto de automorfismos internos*

Dado un grupo g, cada elemento da lugar a un automorfismo interno.

Sea A un grupo y sea $B = (A_0, A_1, \ldots A_n \ldots)$ el conjunto de todos los automorfismos internos. Es decir, A_i es el automorfismo interno engendrado por a_i.

Veamos primero que la compuesta de dos automorfismos es otro automorfismo:

A_i y A_j son los automorfismos interno engendrados por a_i y a_j.

$$a \xrightarrow{A_i} a_i a a_i^{-1} \xrightarrow{A_j} a y a_i a a_i^{-1} a_j^{-1} = (a_j a_i) a (a_j a_i)^{-1}$$

La compuesta de dos automorfismos internos engendrados por a_i y a_j es otro automorfismo interno engendrado por $a_i a_j$.

Tenemos, pues, el conjunto de los automorfismos internos, definida una operación cerrada, y veamos si esta operación cumple los axiomas de grupo.

1.º Es asociativa puesto que la compuesta de aplicaciones es asociativa.

2.º El elemento neutro es el automorfismo engendrado por u (elemento neutro de g).

$$A(a_i) \bar{o}\, A(u) = A(a_i \,.\, u) = A(a_i).$$

3.º Para todo automorfismo interno engendrado por a_i definimos el elemento inverso al automorfismo interno engendrado por a_i^{-1}.

$$A(a_i) \bar{o}\, A(a_1^{-1}) = A(a_i a_i^{-1}) = A(u).$$

Resultando, pues, que el conjunto de automorfismos internos de un grupo g tiene categoría de grupo.

9. SUBGRUPO NORMAL

Dado un grupo g, y sea H un subgrupo de g, definimos para un elemento $a \in g$ tal que $A \in H$, el conjunto

$$aH = \{ah_i \quad h_i \in H\} \text{ y llamaremos clase a la izquierda de } H.$$

De igual forma definimos la clase por la derecha de H.

$$Ha = \{h_i a \quad h_i \in H\}$$

De igual forma definiríamos, tomando un elemento $b \in g$ tal que $b \in H$ y $b \in aH$, la clase bH.

Teorema

Cada clase tiene el mismo número de elementos que el subgrupo H. Para ello basta definir la aplicación f.

$$H \xrightarrow{f} aH \;/\; h_i \xrightarrow{f} ah_i$$

que se trata de una correspondencia biunívoca.

Teorema

Doa clases distintas de H no pueden tener ningún elemento común.

Sean aH y bH dos clases y supongamos que tuvieran un elemento común c.:

$$\left.\begin{array}{l} c \in aH \to c = ah_i \\ c \in bH \to c = bh_j \end{array}\right\} (1)\ ah_i = bh_j \to a = bh_j h_i^{-1} = bh_q$$

Cualquier $x \in aH$,

$$x = ah_i = bh_q h_i = bh_r \in bH.$$

De igual forma, si de (1) despejamos $b, b = ah_i h_j^{-1} = ah_s$, cualquier $y \in bH$

$$y = bh_j = ah_s h_j = ah_t \in aH.$$

Luego $aH = bH$.

9.1. *Subgrupo normal*

Si H es un subgrupo de g y formamos las clases por la derecha y por la izquierda:

$$a_1 H, a_2 H, \ldots a_n H, \ldots$$
$$Ha_1, Ha_2, \ldots Ha_n, \ldots$$

Si $a_i H = Ha_i$, o sea $a_i h_j = h_q a_i$, diremos que H es un *subgrupo normal*.

Teorema

La condición necesaria y suficiente para que un subgrupo H de un grupo g sea normal, es que sea invariante frente a todos los automorfismos internos.

H diremos que es invariante frente a los automorfismos internos cuando;

$$\forall a \in g, H \xrightarrow{A(a)_i} aHa^{-1} = H.$$

Condición necesaria

Hipótesis) H es normal.
Tesis) H es invariante frente a todos los automorfismos internos.

En efecto, sea el automorfismo interno engendrado por a; apliquemos este automorfismo interno al subgrupo H.

$$h_i \in H \rightarrow a h_i a^{-1}$$

Pero como H es normal, $aH = Ha \rightarrow ah_i = h_j a$, o sea $ah_i a^{-1} = h_j \in H$. Luego cualquier elemento de H se transforma en otro de H. Por tanto, H es invariante.

Condición suficiente

Hipótesis) H es invariante frente a todos los automorfismos internos.
Tesis) H es normal.

En efecto: $\forall a \in g H \xrightarrow{A(a)} aHa^{-1} = H$, o sea $aH = Ha$. Por lo tanto, H es normal.

10. GRUPOS FINITOS

Un grupo con un número finito de elementos se llama grupo finito.

Ejemplo de grupos finitos

1.º $A(1, i, -1, -i)$

2.º Las siguientes aplicaciones:

$$f_1(z) = z \quad f_2(z) = \frac{1}{1-z} \quad f_3(z) = \frac{z-1}{z}$$

$$f_4(z) = \frac{1}{z} \quad f_5(z) = 1 - z \quad f_3(z) = \frac{z}{z-1}$$

3.º Clases de resto módulo m.

Se llama orden de un grupo finito al número de elementos del grupo.

Teorema de Lagrange

El orden de un subgrupo de un grupo finito es un divisor del orden del grupo.

Sea g un grupo finito de orden n, y sea H un subgrupo de orden p.

Formando las clases por la izquierda de H.

$a_1 H, a_2 H, \ldots a_r H$, cada una de estas clases contienen p elementos, como todos los elementos del grupo están en alguna de las clases y como dos clases no tienen ningún elemento común,

$$r + r + \overset{p}{\ldots} + {}^{v} = n$$

$$pr = n \qquad p = \frac{n}{r} = \text{entero}$$

11. GRUPO CICLICO

Un grupo en el que cualquier elemento se puede poner como potencia de un elemento g del grupo se dice que es un grupo cíclico; al elemento g se le llama generador del grupo; es decir:

$$\forall a \rightarrow a = g^n \quad \begin{cases} g = \text{generador} \\ n = \text{núm. entero} \end{cases}$$

Teorema

En todo grupo finito cada elemento tiene una potencia que reproduce la unidad.
Sea un grupo finito g de orden g

$$g = \{a_1, a_2, \ldots a_g\}$$

Sea $a_i \in g$, formamos las potencias de este elemento $a_i^1, a_i^2, \ldots a_i^m \ldots$, como cada potencia da lugar a un elemento de g, sólo habrá g potencias distintas; es decir, al calcular todas las potencias las habrá repetidas:

$$a_i^m = a_i^n \rightarrow a_i^{m-n} = u$$

cada elemento tiene una potencia que reproduce la unidad.
Al menor entero positivo h tal que $a_i^h = u$ se llama orden del elemento a_i.

Teorema

Si a es de orden h, entonces $a^m = u$ si y sólo si m es un múltiplo de h.

Condición necesaria

Hipótesis) a es de orden $h, a^m = u$
Tesis) m es un múltiplo de h.

En efecto, $a^m = u^m$ ya que m no puede ser menor que h, pues h es el orden de a.

$$m = qh + r$$
$$u = a^m = a^{qh+r} = (a^h)^q a^r = u^q \,.\, a^r = a^r$$

pero como $r < h$ para que $a^r = u$ debe ser $r = o$, luego $m = qh$, es decir, un múltiplo de h.

Condición suficiente

Hipótesis) a es de orden $h, m = \hbar$
Tesis) $a^m = u$

En efecto, $m = qh$

$$a^m = a^{qh} = (a^h)^q = u^q = u$$

Teorema

Si en un grupo finito de orden n existe un elemento de orden n, este grupo es cíclico engendrado por ese elemento.

Sea: $A=\{a_1,a_2,\ldots a_n\}$ grupo finito de orden n, donde a_p es de orden n, $a_p^n=u$.

Formamos todas las potencias de a_p.

$$a_p,a_p^2,a_p^3,\ldots,a_p^n=u$$

Tenemos n elementos que todos pertenecen a A y veremos que no puede haber dos iguales, pues si

$$a_p^r=a_p^s \quad r,s<n$$
$$a_p^{r-s}=u \text{ y } r-s<n$$

Contradicción, pues entonces $r-s$ sería el orden de a_p. Por lo tanto, cualquier elemento de A se puede poner como una potencia de a_p.

Teorema

Todo grupo cíclico es abliano.

Sea g cíclico engendrado por g, como todo elemento se puede poner como una potencia de g.

$$\left.\begin{array}{l} a=g^n \\ b=g^m \end{array}\right\} ab=g^n.g^m=g^{n+m}=g^{m+n}=g^m.g^n=b\,.\,a$$

Teorema

Todo grupo cíclico de orden infinito es isomorfo del conjunto Z de los números enteros, con la operación suma.

La regla f del isomorfismo es $n|\rightarrow g^n$.

Demostración

1.º La aplicación es un morfismo

$$\begin{array}{lll} m,n\in Z & m|\rightarrow g^m \\ & n|\rightarrow g^n \\ & m+n|\rightarrow g^{m+n}=g^m \text{ o } g^n \end{array}$$

2.º La aplicación es sobreyectiva.

En efecto, todo elemento del grupo G es imagen de un elemento de Z, ya que por ser G un grupo cíclico, por definición del mismo todo elemento puede ponerse en la forma g^n: luego existe un entero, que verifica la regla f, del que es imagen.

3.º La aplicación es inyectiva.

En efecto. Supongamos que no lo fuera: habría dos elementos r y $s\in Z$ con imágenes iguales: $r|\rightarrow g^r$, $s|\rightarrow g^s$, $g^r=g^s$.

Supongamos $r < s$, realizando la operación del grupo o, a la derecha, con g^{-s}, g^r o $g^{-s} = g^r$ o g^{-s}, $g^{r-s} = u$, luego existe un entero $r - s$ tal que $g^{r-s} = u$, y por tanto el grupo sería de orden $r - s$, lo que no puede ser por hipótesis de orden infinito. Por tanto, la aplicación f es inyectiva.

Por tanto, si f es un morfismo y f es inyectiva y sobreyectiva, f es un isomorfismo.

Teorema

Todo grupo cíclico de orden n finito, es isomorfo de Z/n, conjunto de las clases residuales módulo n con la operación $\oplus$ definida en la forma $a \oplus b =$ resto $(a + b)$ (módulo n).

La regla es $r \mid \rightarrow g^r \quad (r > n)$.

Demostración

1.º La aplicación es un morfismo.

$$\begin{array}{ll} k,s \in Z/n & r \mid \rightarrow g^r \\ & s \mid \rightarrow g^s \\ & r \oplus s \mid \rightarrow g^{r+s} \end{array} \qquad \text{(a)}$$

Por otro lado, g^r o $g^s = g^{r+s}$.

$$\begin{array}{lll} \text{si } r + s > n & r + s = r \oplus s & \text{Luego } g^{r+s} = g^{r+s} \\ \text{si } r + s < n & r + s = (r \oplus s) + k.n & \\ & \text{Luego } g^{r+s} = g^{r+s+k.n} = g^{r+s} \text{ o } g^{kn}; & \end{array} \qquad \text{(b)}$$

pero por ser el grupo de orden n $g^{kn} = u^k = u$

luego $g^{r+s} = g^{r+s}$ (c)

Por tanto, sustituyendo en (a) los resultados (b) y (c),

$$r \oplus s \mid \rightarrow g^r \text{ o } g^s;$$

por tanto, f es un morfismo.

2.º La aplicación es sobreyectiva.

En efecto, por definición de grupo cíclico todo elemento puede ponerse en la forma g^m, siendo m un entero. Por ser el grupo de orden n, si $m < n$, $m = q.n + r$, siendo $r > n$.

$g^m = g^{q.n+r} = g^{qn}$ o $g^r = g^r$; por tanto, todo elemento del grupo puede ponerse en la forma g^r, siendo r un número entero menor que n; luego $r \in Z/n$. Por tanto, todo elemento del grupo es imagen de algún elemento de Z/n, luego la aplicación es sobreyectiva.

3.º La aplicación es inyectiva.

En efecto, supongamos que no lo fuera; en ese caso habría dos elementos r y s de Z/n cuyas imágenes por f serían iguales:

$$r \mid \rightarrow g^r \qquad s \mid \rightarrow g^s \qquad g^r = g^s \ (1)$$

por ser $r,s \in Z/n$, $r < n$, $s < n$, supongamos $r < s$

Si en (1) posmultiplicamos por g^{-s},

$$g^r \circ g^{-s} = g^{s-s} = u \qquad g^{r-s} = u$$

Al ser $r - s < n$, el grupo sería entonces de orden $r - s$, contra lo supuesto, por tanto, no puede ocurrir $g^r = g^s$, siendo $r \neq s$; luego la aplicación es inyectiva.

Como consecuencia de lo anterior, al ser f un morfismo y f sobreyectiva e inyectiva, f es un isomorfismo.

Teorema

Todo subgrupo de un grupo cíclico es cíclico.

Demostración

Sea un grupo G cuyo generador es g; sea $S \subseteq G$ un subgrupo de G; sea m el menor exponente de los elementos de S, es decir:

$$\forall a \in S \qquad a = g^p \qquad p \geqslant m$$

Cualquier elemento de S será de la forma g^p, siendo $p = q.m + > m$
$g^p = g^{qm+r}$ $\quad g^p = g^{qm}$ o gr premultiplicando por g^{-qm}
$g^{-qm} \circ g^p = g^{-qm} \circ g^{qm} \circ g^r$, simplificando,

$$g^r = g^{-qm} \circ g^p$$

Esta expresión puede ponerse en la forma:

$$g^r = \underbrace{g^{-m} o g^{-m} o g^{-m} o \ldots g^{-m} o g^p}_{q \text{ factores.}}$$

Por ser la operación asociativa podemos obtener g^r calculando primero $z_1 = g^{-m} \circ g^p$; a continuación, $z_2 = g^{-m} \circ z_1$, $z_3 = g^{-m} \circ z_2$, ... y $z_q = g^{-m} \circ Z_{q-1}$ $\quad g^r = z_q$ $\quad g^{-m} = (g^m)^{-1}$; luego $z_1 = (g^m)^{-1} \circ g^p$, por ser g^m y g^p elementos de S por hipótesis, y ser S subgrupo de G, $z_1 = (g^m)^{-1} \circ g^p$ será también elemento de S (teorema tercero del apartado 9). Análogamente, $z_2 = (g^m)^{-1} \circ z_1$ es también elemento de S (por ser g^m, $z_1 \in S$ y S subgrupo de G), y, por tanto, aplicando reiteradamente este razonamiento, debe ser $z_q = g^r \in S$. Sin embargo, por ser m el menor entero positivo de los exponentes de los elementos de S y ser r por definición menor que m, la única forma en que puede verificarse $g^r \in S$ es $r = 0$, pero si $r = 0$, ello quiere decir que cualquier elemento de S, g^p es de la forma $g^{qm+r} = g^{qm} = (g^m)^q$; luego S es cíclico con generador g^m. Por tanto, todo subgrupo de un grupo cíclico es cíclico.

12. GRUPOS SIMETRICOS Y ALTERNADOS

Como se dijo anteriormente, al poner ejemplos de grupos, una permutación σ de un conjunto $n = \{1, \ldots n\}$ es una biyección $\sigma : n \to n$ y el *grupo simétrico*. S_u de grado n es el con-

junto de las permutaciones de n dotado de la operación de composición, tal y como se definió al hablar de aplicaciones.

Por ejemplo, si $n=5$,

$$\sigma:\begin{array}{ccccc}1&2&3&4&5\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 2&3&4&5&1\end{array}\qquad \tau:\begin{array}{ccccc}1&2&3&4&5\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 3&4&1&5&2\end{array}$$

σ y τ son dos permutaciones que normalmente se escribirán con la notación:

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}\ ;\quad \tau=\begin{pmatrix}1&2&3&4&5\\3&4&1&5&2\end{pmatrix}$$

La permutación idéntica I será:

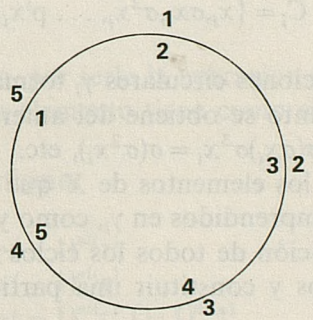
$$I=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$$

En el caso presente: $\sigma \circ \tau = 1\to3\to4,\ 2\to4\to5,\ldots$ mientras que
$\tau \circ \sigma = 1\to2\to4,\ 2\to3\to1,\ldots$, que con la notación de dos líneas

$$\sigma\circ\tau=\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix}\ ;\quad \tau\circ\sigma=\begin{pmatrix}1&2&3&4&5\\4&1&5&2&3\end{pmatrix}$$

Por tanto, $\sigma \circ \tau \neq \tau \circ \sigma$.

Permutaciones tales como σ equivalen a un desplazamiento circular de los símbolos permutados, como se indica en la figura. Una permutación así se llama *permutación circular o ciclo.*



Para permutaciones circulares hay una notación sobre una línea: se comienza por escribir una cifra cualquiera y su imagen; así se continúa hasta que se cierre el ciclo.

Con esta notación la permutación tomará una cualquiera de estas formas: (12345), (23451), (34512), (45123) o (51234). σ es de orden 5, ya que $\sigma^5 = 1_5$, siendo 1_5 la permutación idéntica.

Toda permutación circular de K letras es de orden K. El número de letras de un ciclo llama su *longitud*; un ciclo de longitud 2 se llama una transposición.

Adaptando esta notación por ciclos para las permutaciones en general, por ejemplo τ, se puede escribir $\tau = (13)$ o $(245) = (245)$ o (13). Se puede descomponer cualquier permutación de esta manera en forma única en producto de ciclos disjuntos; se entiende por ciclos dis-

juntos aquellos que no tienen elementos comunes. Al aplicar ciclos de menos número de elementos que el conjunto sobre el que se aplica se entenderá que a los elementos no comprendidos en el cilo les aplica la identidad.

Así, el ciclo (13), aplicado al conjunto $X_5 = \{1,2,3,4,5\}$, equivale a $\{^{12345}_{32145}\}$. Por ello la composición de ciclos disjuntos es conmutativa.

Teorema

Toda permutación σ puede descomponerse en forma única en producto de ciclos disjuntos.

Demostración

Sea $X = \{1,2,3, \ldots n)$, un conjunto de elementos y σ una permutación de los mismos.

Se define una relación R en X de forma que dos elementos x,y verifican R si existe algún m entero tal que $x = \sigma^m y$.

La relación R definida de esta forma es de equivalencia. En efecto:

Es reflexiva $x = \rho^o y$

Es simétrica si $x = \sigma^m y$, por formar grupo las permutaciones se verificará $y = \sigma^{-m} x$

Es transitiva si $x = \sigma^m y$ e $y = \sigma^n z$ $\quad x = {}^{m+n} z$.

Luego xRz.

Por tanto, esta relación R define en x una partición en clases de equivalencia según R, constituida por los subconjuntos $C_1, C_2, \ldots C_k$, tales que son dsijuntos, y la unión de todos es x. Los elementos de cada conjunto C_4 pueden ponerse en la forma siguiente, en función de uno de ellos, ya que cada dos verifican $a = \sigma^m b$:

$$C_i = \{x_i, \sigma x_i, \sigma^2 x_i, \ldots \mathrm{p}^i x_i\}$$

Si consideramos las permutaciones circulares γ_i formadas por $\gamma_i = (x_i, \sigma x_i, \sigma^2 x_i, \ldots \sigma^{pi} x_i)$, en cada una de ellas cada elemento se obtiene del anterior por aplicación de la permutación σ, ya que $\sigma x_i = \sigma . x_i \;\; \sigma^2 x_i = \sigma(\sigma x_i) \sigma^3 x_i = \sigma(\sigma^2 x_i)$, etc.

Es decir, un ciclo γ actúa sobre los elementos de X que comprende, como la permutación ción σ sobre X, y para los no comprendidos en γ_i, como ya se indicó, actúa como la función identidad; por tanto, la composición de todos los ciclos $\gamma_1, \gamma_2, \ldots \gamma_k$ reproducirá la permutación σ, por ser las C_i disjuntos y constituir una partición de X (es decir, $C_1 \cup C_2 \cup \ldots \ldots \cup C_k = X$).

Recíprocamente, caso de que exista una descomposición de σ en producto de ciclos $\beta_1, \beta_2, \beta_3, \beta_4, \ldots \beta_h$, los elementos de los mismos constjtuyen una partición correspondiente a la relación de equivalencia $x = \sigma^m y$ (ya que en todo ciclo se verifica tal relación); luego los elementos de los ciclos $\beta_1, \beta_2, \ldots \beta_k$ deben ser los mismos que los de $\gamma_1, \gamma_2, \ldots \gamma_k$, y si bien cabe que la escritura de los ciclos sea en otro orden; por ejemplo, los ciclos (2351) y (5123) son iguales.

Corolario

Toda permutación puede descomponerse en producto de transposiciones no necesariamente disjuntas.

Basta demostrar que un ciclo puede descomponerse en producto de transposiciones. En efecto, cualquier ciclo $(a,b,c,\ldots m)$ es igual a la composición de (am) o $\ldots$ (ac) o (ab).

Definiciones

Dada una permutación σ, diremos que una pareja (i,j) de elementos de X forma inversión en σ cuando se verifica $i>j$ y $\sigma i<\sigma j$ (σ_i imagen de i por la permutación σ).

Si designamos por $ni(\sigma)$ el número de inversiones de σ; si $n_i(\sigma)$ es por la permutación σ es de clase par, y de clase impar en caso contrario.

La transposición (h,k) si $h>k$ tiene por cada elemento l, intermedio, $h>l>k$ dos inversiones, ya que las parejas (h,l) y (l,k) se convierten al aplicar la transposición en (l,h) y (k,l); por tanto, si el número de elementos intermedios entre h y k es m, el número de inversiones debidas a ellos es $2m$, y a este número hay que a adir la inversión provocada por la transposición; luego el número de inversiones de una transposición es un par.

Teorema

Si llamamos S_n al conjunto de permutaciones de n elementos del conjunto $X=\{1,2,\ldots n\}$, la aplicación f de S_n sobre el conjunto $\{-1,1\}$ con la regla $\sigma\rightarrow(-1)^{ni}(\sigma)$ es un morfismo de grupos para las operaciones de composición en S_n y producto en $\{-1,1,\}$.

1.º El conjunto $\{-1,1\}$ con la operación de multiplicación definida en la misma forma que en el conjunto de los números enteros forma grupo.

	-1	1
-1	1	-1
1	-1	1

En efecto, la operación es asociativa, por serlo la operación en Z.

El elemento neutro es 1 y cada elemento tiene como simétrico el mismo; por tanto, la estructura es un grupo.

2.º La aplicación f es un morfismo.

Es decir,
$$\sigma|\rightarrow(-1)^{ni(\tau)}$$
$$\tau|\rightarrow(-1)^{ni(\tau)}$$
$$\sigma\ o\ \tau|\rightarrow(-1)^{ni(\tau)}.(-1)^{ni(\tau)}$$

Para demostrarlo vamos a definir inicialmente un conjunto L del producto cartesiano XxX tal que está formado por parejas (i,j) de elementos de X que cumplen las siguientes condiciones:

a) No existe ninguna pareja con dos elementos iguales (i,j) por ejemplo.
b) Se contiene la pareja (i,j) no contiene la pareja (j,i). Es decir, dos parejas se diferencian al menos en un elemento.

Se define como par propio aquel (i,j) tal que $i>j$, siendo par impropio, por tanto, aquel en que $i<j$.

Asimismo se atribuye a L un número $e(L)$ constituido por el número de pares propios de L, y asimismo se define un número atribuido a L:

$$|L| = (-1)^{e(\ )}$$

Si se aplica al conjunto L la permutación σ, llamaremos al conjunto resultante σL, estará formado por las parejas $(\sigma i, \sigma j)$ resultantes de aplicar a cada elemento de las parejas (i,j) de L la permutación σ. El conjunto σL, por tanto, verifica los mismos axiomas a) y b) que el conjunto L.

Lema

$$|\sigma L| = (-1)^{ni(\ )}.|L|$$

Demostración

Si llamamos NA al número de pares propios de L no afectados por σ, es decir, tales que σ no cambia el orden de los elementos y NP el número de pares propios afectados por σ:

$$e(L) = NA + NP.$$

Por otro lado, el número de pares propios e impropios afectados por σ es $ni(\sigma)$; asimismo, todo par propio de L afectado por σ se convierte en impropio, y análogamente, todo impropio se convierte en propio. Por tanto, el número de pares propios afectados por σ en σL será $ni(\sigma) - NP$ (= al número de impropios afectados por σ en L).

Por otro lado, a este número de pares propios habrá que añadir el nñmero de pares propios no afectados por σ, es decir,

$$e(\sigma L) = NA + ni(\sigma) - NP$$

Por tanto,

$$e(\sigma L) - e(L) = ni(\sigma) - 2.NP \qquad (1)$$

$$|\sigma L| = (-1)^{e(\sigma L)} = (-1)^{e(\sigma L) - e(L)}.(-1)^{e(L)} = (-1)^{e(\sigma L) - e(L)}.|L|.$$

Pero por la fórmula (1), $e(\sigma L) - e(L)$ tiene la misma paridad que $ni(\sigma)$, ya que su diferencia es el número par $2.NP$, por tanto,

$$(-1)^{e(\sigma L) - e(L)} = (-1)^{ni(\sigma)}$$

Es decir,

$$|\sigma L| = (-1)^{ni(\sigma)}.|L| \qquad (2) \qquad \text{c.q.d.}$$

$$|(\sigma o \tau)L| = (-1)^{ni(\sigma o \tau)}|L|$$

$$(\sigma o \tau)L = (\tau L)$$

según (2):

$$|(\sigma o \tau)L| = |\sigma(\tau L)| = (-1)^{ni(\sigma)}|\tau L| = (-1)^{ni(\sigma)}.(-1)^{ni(\tau)}|L|$$

luego $(-1)^{ni(\sigma o \tau)} = (-1)^{ni(\sigma)}.(-1)^{ni(\tau)}$ (3)

Por tanto, si la aplicación f atribuye

$$\sigma o \tau \to (-1)^{ni(\sigma o \tau)}$$

de acuerdo con (3),

$$\sigma o \tau \to (-1)^{ni(\sigma)}.(-1)^{ni(\tau)} \quad (4)$$

Por tanto, la aplicación es un morfismo, ya que $(-1)^{ni(\sigma)}$ es la imagen de σ por f y $(-1)^{ni(\tau)}$ es la imagen de τ por f y la composición de σ y τ con la operación o tiene como imagen, de acuerdo con (4), la composición de las imágenes con la operación.

Corolario 1

Una permutación, compuesta con otra de igual paridad, da una permutación par y compuesta con otra de distinta paridad da un par.

En efecto, si σ y τ con pares se verifica

$$\rho \to 1$$
$$\tau \to 1$$

y por ser f un morfismo

$$\sigma o \tau \to 1.1 = 1$$

o es par.

Si son ambas impares,

$$\sigma \to -1$$
$$\tau \to -1$$
$$\sigma o \tau \to (-1).(-1) = 1. \quad \text{Luego } o \text{ es par.}$$

Si una es par y otra impar,

$$\sigma \to 1$$
$$\tau \to -1$$
$$\sigma o \tau \to (1).(-1) = -1$$

luego $\sigma o \tau$ es impar.

El producto de K transposiciones es par o impar según sea K par o impar.

Puede verse inmediatamente a partir del corolario 1 y de que toda transposición es impar.

Corolario 3

La paridad de un ciclo de orden m es $(-1)^{m-1}$.

Es consecuencia del corolario anterior y de que, como se vio anteriormente, todo ciclo de orden m puede descomponerse en producto de $m-1$ transposiciones.

Teorema

El conjunto de las permutaciones pares, A_n, es un subgrupo de S_n y contiene $ni/2$ elementos.

Demostración

Sean σ y τ dos permutaciones pares.

Por el teorema anterior, al ser $\sigma \to (-1)^{ni(\sigma)}$ un morfismo de grupos, se verificará

$$\sigma \to 1 \qquad \tau \to 1$$

Por otro lado, deberá ser $\sigma^{-1} \to 1^{-1}$, pero en el grupo $\{-1,1\}$ el simétrico de $1'$ es el mismo elemento, luego $\sigma^{-1} \to 1$. Por tanto,

$$\forall \sigma\tau \in A_n \quad \sigma^{-1} o \tau \to 1.$$

Luego,

$$\sigma^{-1} o \tau \in A_n$$

Por el teorema segundo del apartdo 9 esta condición es necesaria y suficiente para que A_n sea subgrupo de S_n; por tanto, se verifica la primera parte del teorema.

Para demostrar que el número de elementos de A_n es $^n i/2$, se hace el siguiente razonamiento:

n_1 al número de permutaciones pares.
n_2 al número de permutaciones impares.

Si a cada permutación par le aplicamos una transposición (12) por ejemplo, obtendremos (por el corolario 1 del teorema anterior) una permutación impar, distinta para cada permutación par.

En efecto, caso de que se obtuviera la misma permutación impar a partir de dos pares distintos σ y τ, se verificaría:

$$(12) o \sigma = (12) o \tau$$

lo que conduciría, simplificando (por formar grupo las permutaciones), a $\sigma = \tau$.

Por tanto, si cada permutación par, al componerla con la (12), genera una impar, se verificará:

$$n_2 \geqslant n_1 \tag{5}$$

Análogamente, cada permutación impar, al componerse con (12), dará una par distinta; luego

$$n_1 \geqslant n_2 \tag{6}$$

Por tanto, para que se verifiquen (5) y (6), es necesario que $n_1 = n_2$. Como el número total de permutaciones es ni, el número de los pares será $ni/2$.

13. ANILLOS Y CUERPOS

13.1 *Definición*

Dado un grupo abeliano A, que denotaremos aditivamente, definimos sobre A una estructura de anillo, dotando a este conjunto de una segunda ley interna, llamada multiplicación, asociativa y doblemente distributiva con relación a la adición.

Los axiomas de la estructura de anillo son los siguientes:

I. *Grupo abeliano aditivo*

Sean x,y,z elementos cualesquiera de A.

1.º Existencia de una ley $+ \forall x,y \in A \,|\, (x+y) \in A$.
2.º Propiedad conmutativa $x+y = y+x \forall x,y \in A$.
3.º Propiedad asociativa $x+(y+z) = (x+y)+z$; $\forall x.y.z \in A$.
4.º Existencia del elemento neutro $x+u = u+x = x$.
5.º Existencia de simétrico $\forall x \in A \exists -x \in A \,|\, x+(-x) = u$.

II. *Segunda ley interna. Multiplicación.*

1.º Cerrada $\forall x.y \in A$; $(xy) \in A$.
2.º Propiedad asociativa $x.(yz) = (xy)z \forall x.y.z \in A$.

III. *Axiomas que ligan las dos leyes.*

1.º Propiedad distributiva $\forall x,y, \in A \Rightarrow x(y+z) = xy + xz$.
2.º Propiedad distributiva $(y+z)x = yx + yz$.

Cuando la multiplicación es conmutativa, el anillo se llama conmutativo. Existen anillos no conmutativos, por ejemplo el de las matrices cuadradas.

Ejemplos

(a) El conjunto $S = \{a,b\}$ con adición y multiplicación definidas por las tablas

$+$	a	b
a	a	b
b	b	a

y

$.$	a	b
a	a	a
b	a	b

es un anillo.

(b) El conjunto $T = \{a,b,c,d\}$ con adición y multiplicación definidas por

$-$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

y

$.$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

es un anillo.

Para estos anillos es elemento cero es a y cada elemento es su propio simétrico aditivo.

Como los elementos tienen estructura de grupo abeliano para la adición, se verifican las propiedades de los grupos con notación aditiva:

(i) Existe un elemento neutro aditivo único, z (el cero del anillo).
(ii) Cada elemento tiene un simétrico aditivo único (el opuesto de dicho elemento).
(iii) Se cumple la ley de simplificación para la adición.
(iv) El opuesto del opuesto de un elemento es igual a dicho elemento.
(v) El opuesto de la suma es la suma de los opuestos de cada sumando.
(vi) Ley de simplificación para la adición.
(vii) Solución única para las ecuaciones de la forma $x + b = a$.

13.2 *Anillo de integridad*

Sobre un anillo la ley de simplificación es siempre válida para la adición, pero no necesariamente para la multiplicación. La igualdad

$$ac = bc$$

no implica, pues, $a = b$, incluso para $c \neq 0$. En particular, así es en el anillo de las matrices cuadradas. Indiquemos una condición equivalente a la ley de simplificación.

Teorema

La ley de simplificación para la multiplicación es válida sobre un anillo, para todo elemento no nulo si, y sólo si, el producto de dos elementos diferentes de cero es distinto de cero.

Partiendo de $ac = bc$, con $c \neq 0$, se deduce que $ac - bc = 0$, de donde $(a - b)c = 0$.

Si suponemos que el producto de elementos distintos de cero es diferente de cero, necesariamente tendremos que $a - b = 0$, o sea $a = b$, ya que $c \neq 0$. Es, por tanto, válida la ley de simplificación.

Recíprocamente, demostraremos que si puede satisfacerse la igualdad $a'b' = 0$, con $a' \neq 0$ y $b' \neq 0$, no es válida la ley de simplificación. Si a es un elemento cualquiera, tendremos:

$$ab' = ab' + a'b' = (a + a')b'$$

Si la ley de simplificación fuera válida para $b' \neq 0$, se tendría $a = a + a'$, de donde $a' = 0$, contra la hipótesis.

Un *anillo conmutativo* en el que es válida la ley de simplificación se denomina *anillo de integridad.* Para un anillo que no sea de integridad existen ciertos elementos no nulos cuyo producto es nulo: los llamados *divisores de cero.*

Existen muchos casos de *anillos de integridad en los que la multiplicación admite elemento neutro e.* Diremos que se trata de *dominios de integridad.*

13.3 *Subanillos*

En todo anillo A, cualquier subconjunto que sea un subgrupo del grupo aditivo, cerrado con relación a la ley de multiplicación, posee una estructura de anillo y constituye un *subanillo* de A.

13.4 *Cuerpos*

Un anillo en el que los elementos distintos de cero forman grupo con relación a la multiplicació, del anillo se llama cuerpo. Si el grupo multiplicativo es abeliano el cuerpo se llama conmutativo.

Teorema

En un cuerpo cualquiera la ecuación $bx = a$ admite solución única si $b \neq 0$.

Esta es una propiedad del grupo multiplicativo. La solución es $x = ab^{-1}$, que también se escribe $x = a/b$; se dice que x es el cociente o razón de los dos elementos a y b.

CAPITULO II

ALGEBRA DE BOOLE

1. *Definición axiomática del álgebra de Boole*

Las operaciones y las relaciones permiten clasificar distintas estructuras de conjuntos que se tratarán en otra parte del curso con más amplitud.

Para que una estructura algebraica se llame élgebra hay que haber definido *al menos dos operaciones* sobre el conjunto base.

Para definir el álgebra de Boole [sistema algebraico de tratamiento de la lógica desarrollado por George Boole (1815-1864)] elegimos el grupo de axiomas dado por Huntington en 1904, si bien existen otros juegos de axiomas para definición de este sistema.

La condición necesaria y suficiente para que un conjunto de elementos B, junto con dos operaciones binarias $(+)$ y $(.)$ sea un álgebra de Boole, es que se verifiquen los siguientes postulados:

A_1 Las operaciones $(+)$ y $(.)$ son conmutativas.

A_2 Existen en B los elementos neutros para las operaciones $(+)$ y $(.)$ y son 0 y 1, respectivamente.

A_3 Cada operación es distributiva respecto de la otra.

A_4 Para cada a de B existe el elemento a' en B tal que

$$a + a' = 1 \qquad aa' = 0$$

No hay razón para simbolizar las dos operaciones definidas como $(+)$ y $(.)$. Cualquier otro símbolo servirá igual. Si un conjunto con operaciones $\cup$ y $\cap$, satisface análogos postulados, será un álgebra de Boole. Se han elegido por uniformidad con los otros capítulos los símbolos $(+)$ y $(.)$.

El álgebra de conjuntos satisface los postulados definidos anteriormente; por tanto, es un álgebra de Boole. A continuación vamos a probar que todo álgebra de Boole definida de la forma anterior satisface las leyes del álgebra de conjuntos, obteniéndolas como teoremas a partir de los axiomas. De hecho, *todo álgebra de Boole puede interpretarse como un álgebra de conjuntos seleccionando debidamente el conjunto universal.*

T. 1. *Dualidad en un álgebra de Boole.*

Las propiedades que *axiomáticamente* definen un álgebra de Boole pueden escribirse de la siguiente forma:

1.	$a+b=b+a$	$a\,.\,b=b\,.\,a$ ——————— A_1
2.	$a+0=a$	$a\,.\,1=a$ ——————— A_2
3.	$a+b\,.\,c=(a+b)\,.\,(a+c)$	$a\,.\,(b+c)=(a\,.\,b)+(a\,.\,c)$ —— A_3
4.	$a+\bar{a}=1$	$a\,.\,\bar{a}=0$ ——————— A_4

(En lo sucesivo $a\,.\,b$ se escribirá ab.

Como puede verse, las propiedades descritas a la derecha pueden deducirse de las de la izquierda sustituyendo

En lugar de $+$	. y viceversa	(I)
En lugar de 0	1 y viceversa	

Por tanto, si una propiedad se ha deducido mediante una sucesión de aplicaciones de axiomas, puede darse por demostrado la propiedad dual de ella obtenida mediante las sustituciones (I), ya que esta última podrá obtenerse mediante la aplicación de la secuencia de axiomas duales de los que sirvieron para demostrar la primera.

Cada uno de los siguientes teoremas contiene dos expresiones duales. Para demostrar ambos se siguen pasos que son duales uno del otro, y la justificación para cada paso es el mismo postulado o teorema, tanto en un caso como en otro.

T. 2. Para todo elemento a en un álgebra de Boole:

$$\boxed{a+a=a \quad \text{y} \quad aa=a} \qquad \text{(Ley de idempotencia)}$$

Demostración:

$a=a+0$	por A_2
$=a+aa'$	por A_4
$=(a+a)(a+a')$	por A_3
$=(a+a)(1)$	por A_4
$=a+a$	por A_2

y análogamente:

$a=a\,.\,(1)$	por A_2
$=a(a+a')$	por A_4
$=aa+aa'$	por A_3
$=aa+0$	por A_4
$=aa$	por A_2

T. 3. Para cada elemento a en un álgebra de Boole:

$$\boxed{a+1=1 \text{ y } a0=0}$$

Demostración:

$$\begin{aligned} 1 &= a+a' && A_4 \\ &= (a+a')(a+1) && A_3 \\ &= 1\,(a+1) && A_4 \\ &= a+1 && A_2 \end{aligned}$$

T. 4. Para cada pareja de elementos a y b en un álgebra de Boole:

$$\boxed{a+ab=a \text{ y } a(a+b)=a}$$

Demostración:

$$\begin{aligned} a &= 1\,.\,a && A_2 \\ &= (1+b)a && \text{Teorema 3} \\ &= 1a+ba && A_3 \text{ y } A_1 \\ &= a+ba && A_2 \\ &= a+ab && A_1 \end{aligned}$$

T. 5. En todo álgebra de Boole, cada operación binaria $(+)$ y $(.)$ es asociativa. Esto es, para todo a,b y c en B:

$$\boxed{a+(b+c)=(a+b)+c \text{ y } a(bc)=(ab)\,c.}$$

Demostración:

Primero veamos que $a+a(ab)=a+(ab)c$ (I).

$$\begin{aligned} a+a(ab) &= a && \text{Teorema 4} \\ &= a(a+c) && \text{Teorema 4} \\ &= (a+ab)(a+c) && \text{Teorema 4} \\ &= a+(ab)c && A_3 \end{aligned}$$

Veamos que $a'+a(bc)=a'+(ab)c$ (II).

$$\begin{aligned} a'+a(bc) &= (a'+a)(a'+bc) && A_3 \\ &= 1(a'+bc) && A_4 \end{aligned}$$

$$
\begin{aligned}
&= a' + bc && A_2\\
&= (a' + b)(a' + c) && A_3\\
&= [1(a' + b)](a' + c) && A_2\\
&= [(a' + a)(a' + b)](a' + c) && A_4\\
&= (a' + ab)(a' + c) && A_3\\
&= a' + (ab)c && A_3
\end{aligned}
$$

Multiplicando (I) y (II) se verificará:

$$[a + a(bc)]\ [a' + a(bc)] = [a + (ab)c]\ [a' + (ab)c] \quad \text{(III)}$$

ya que una operación binaria tal y como ha sido definida atribuye el mismo elemento a las parejas (x,y) y (u,v) si se verifica $x = u \quad y = v$.

El lado izquierdo de la ecuación (III) puede reducirse como sigue:

$$
\begin{aligned}
[a + a(bc)][a' + a(bc)] &= [a(bc) + a]\ [a(bc) + a'] && A_1\\
&= a(bc) + aa' && A_3\\
&= a(bc) + 0 && A_4\\
&= a(bc) && A_2
\end{aligned}
$$

Análogamente, el lado derecho de la ecuación se reduce así:

$$
\begin{aligned}
[a + (ab)c]\ [a' + (ab)c] &= [(ab)c + a]\ [(ab)c + a'] && A_1\\
&= (ab)c + aa' && A_3\\
&= (ab)c + 0 && A_4\\
&= (ab)c && A_2
\end{aligned}
$$

Por tanto, la ecuación (III) queda reducida a

$$a(bc) = (ab)c$$

que es la ley asociativa que deseábamos probar.

Por tanto, ahora escribiremos $a(ab)$ y $(ab)c$ como abc, y análogamente, $(a + b) + c$ y $a + (b + c)$ como $a + b + c$.

T. 6. El elemento a' asociado con el elemento a en un álgebra de Boole es único (esto equivale a decir que solamente un elemento a' satisface las condiciones de A_4).

Demostración

Supongamos que $a + x = 1$ y $ax = 0$, y también que $a + y = 1$ y que $ay = 0$. Entonces:

$$
\begin{aligned}
x &= 1x && \text{por } A_2\\
&= (a + y)x && \text{tal como se ha supuesto}\\
&= ax + ay && A_3 \text{ y } A_1
\end{aligned}
$$

$$
\begin{aligned}
&= 0 + yx && A_3 \text{ y } A_1 \\
&= yx && \text{por } A_2 \\
&= xy && A_1 \\
&= xy + ay && A_1 \\
&= (x + a)y && \text{por } A_3 \text{ y } A_1 \\
&= 1y && \text{por } A_3 \text{ y } A_1 \\
&= y && \text{por } A_2.
\end{aligned}
$$

Luego los dos elementos asociados con a, tal como se especifica en A_4, son iguales. En otras palabras, a' está determinado únicamente por a.

Nos referiremos a a' como el complementario de a, tal como se hizo en el capítulo I.

T. 7. Para todo a en un álgebra de Boole,

$$(a')' = a$$

Demostración:

Por A_4, $a + a' = 1$ y $aa' = 0$, que son las condiciones necesarias para que $(a')'$ es igual a a. Por el teorema 6 no hay otro elemento con la misma propiedad.

T. 8. En cualquier álgebra de Boole, $0' = 1$ y $1' = 0$.

Demostración:

Por el teorema 3, $1 + 0 = 1$ y $(1)(0) = 0$. Puesto que por el teorema 6 cada elemento sólo tiene un complemento a', esta ecuación implica que $0' = 1$ y que $1' = 0$.

T. 9. Para cada pareja a y b en un álgebra de Boole:

$$\boxed{(ab)' = a' + b' \text{ y } (a + b)' = a'b'}$$

(Leyes de De Morgan)

Demostración:

$$
\begin{aligned}
(ab)(a' + b') &= aba' + abb' && A_3 \\
&= 0b + a0 = 0 + 0 = 0 && A_1, A_2, A_4 \text{ Teorema 3} \\
ab + a' + b' &= a' + b' + ab && A_1 \\
&= (a' + b' + a)(a' + b' + b) && A_3 \\
&= (1 + b')(1 + a') && {}_4 \text{ y } A_1 \\
&= 1 && \text{Teorema 3 y } A_2
\end{aligned}
$$

A partir del teorema 6 y A_4 estas condiciones implican que $(ab)' = a' + b'$. El dual se sigue del teorema 1.

2. *Relación de orden en un álgebra de Boole*

Definiremos una relación de orden en un álgebra de Boole mediante la condición

$$a \subseteq b \text{ o } a \leqslant b \text{ (se lee } a \text{ anterior a b) si se verifica } ab' = 0.$$

Vamos a demostrar que esta condición crea una relación de orden.

1. $a \subseteq a$, ya que $aa' = 0$, luego la relación es reflexiva.
2. Si $a \subseteq b$ y $b \subseteq c$, se verifica $a \subseteq c$.
   En efecto, por las dos primeras hipótesis se verifica $ab' = 0$ y $bc' = 0$.
   Teniendo en cuenta esto:
   $$ac' = ac'(b + b') = abc' + ab'c' = a \,.\, 0 + 0 \,.\, c' = 0.$$

   Luego $a \subseteq c$.
   Por tanto, la relación es transitiva.

3. Si $a \subseteq b$ y $b \subseteq a$ (1), se verifica $a = b$.
   Si $a \neq b$ no pueden verificarse (1)

   1.º) Si $ab' = 0 \Rightarrow a + b = b$
   En efecto:
   $a + b = (a + b)(b + b') = b + ab' = b.$

   2.º) Si $a \subseteq b$ $\qquad a + b = b$
   Si $b \subseteq a$ $\qquad b + a = a$

   Luego $a = b$.

Por tanto, la relación definida es reflexiva, transitiva y antisimétrica; es, por tanto, una relación de orden. El orden es parcial, ya que pueden existir elementos no comparables; ejemplo a y a'.
Otras propiedades de la relación de orden son:

4. Si $x \subseteq y$ $\qquad x \subseteq y + z$

Demostración:

Si $x \subseteq y$ $\qquad xy' = 0$
$x(y + z)' = xy'z' = 0 \,.\, z' = 0$, cualquiera que sea z; luego $x \subseteq y + z$.

5. Si $x \subseteq y$ e $x \subseteq z$, se verifica $x \subseteq yz$.

En efecto, si $x \subseteq y$ $\quad xy' = 0$
si $x \subseteq z$ $\quad xz' = 0$
$x(yz)' = xy' + xz' = 0.$
Luego $x \subseteq yz$.

6. Si $x \subseteq y$ se verifica $y' \subseteq x'$, y viceversa:

1.º) Si $x \subseteq y$ $\quad y' \subseteq x'$
En efecto. Si $x \subseteq y$ $\quad xy' = 0,$
que también puede escribirse

$$y'(x')' = 0, \text{ lo que implica:}$$
$$y' \subseteq x'.$$

2.º) Si $y' \subseteq x'$ $\quad x \subseteq y.$
Si se verifica $y' \subseteq x'$, se verificará por 1.º): $(x')' \subseteq (y')'$, lo que, aplicando la propiedad involutiva del complemento, es: $x \subseteq y$.

7. En un álgebra de Boole la relación $\subseteq$ crea un orden parcial, como ya hemos indicado antes, ya que pueden encontrarse elementos no comparables. Sin embargo, dados dos elementos cualesquiera, siempre se puede encontrar uno que les preceda y otro que les siga.
En efecto, sean x e y dos elementos cualesquiera, se verifica siempre:

$$x \subseteq x + y \qquad \text{(T. 4)}$$
$$y \subseteq x + y$$

por tanto, $x + y$ es posterior o mayorante a x y a y.

Asimismo: $\quad xy \subseteq x$
$xy \subseteq y$

En efecto: $\quad xy \,.\, x' = 0$ y $xy \,.\, y' = 0.$

Por tanto, xy es anterior (o minorante) a x y a y.

Una estructura sobre la que se define un orden parcial de forma que dados dos elementos cualquiera puede encontrarse siempre uno que les antecede y otro que les sigue en dicho orden, se llama retículo (en francés *treillis*, en inglés *lattice*). Por tanto, el álgebra de Boole con la relación de orden definida anteriormente es un retículo.
Los elementos 0,1 del álgebra de Boole son minorantes y mayorantes absolutos, respectivamente.
En efecto, cualquiera que sea x,

$$0 \,.\, x' = 0; \text{ luego } 0 \subseteq x$$
$$x \,.\, 1' = x \,.\, 0 = 0; \text{ luego } x \subseteq 1.$$

3. *Formas normales o canónicas*

3.1. DEFINICIONES

Constante es un símbolo que representa un elemento específico del álgebra de Boole.

Variable es un símbolo que representa un elemento cualquiera de un álgebra de Boole.

Monomio es una expresión formada por constantes y variables separadas por el signo de la operación (.).

Polinomio es una expresión formada por monomios separados por el signo de la operación (+).

Una regla que aplique un elemento del conjunto sobre el que se ha definido el álgebra de Boole a un grupo de variables o constantes definidas en ese conjunto diremos que es una función booleana si dicha regla puede definirse mediante una expresión formada por las constantes y variables y los signos de operación (.), (+) y (′).

Así, $f(a,b,x,z)$ es una función booleana si la regla que atribuye a las constantes a,b, y los valores cualquiera de las variables x,z un elemento del mismo álgebra es una expresión del tipo:

$$a + bx'z + a'b(x + z')$$

o análoga.

Interesa subrayar que a efectos de contabilización de número de variables se considerará como una misma variable la aparición de un símbolo con o sin el signo de complementación. Por ejemplo,

$ax + bx'$ es una función de a,b y x

Entre las funciones de n variables $x_1, x_2, \ldots x_n$ que pueden escribirse, es de especial interés *una clase particular de funciones*: aquellas escritas como una suma de términos en los que cada término es un producto que relaciona todas las n variables, bien con o sin apóstrofo.

Ejemplos de tales funciones son $x + x'$, xy', $xyz' + x'yz + xy'z$ con una, dos o tres variables, respectivamente.

Una función booleana se dice que está en una forma normal (o canónica) disyuntiva en n variables $x_1, x_2, \ldots x_n$, para $n < 0$, si la función es una *suma* de términos del tipo $f_1(x_1)$, $f_2(x_2) \ldots f_n(x_n)$, donde $f_i(x_i)$ es x_i o x_i' para cada $i = 1,2, \ldots n$, y no son idénticos dos términos.

3.2. PROPIEDADES DE LA FORMA NORMAL DISYUNTIVA

T. 1. *Toda función en un álgebra de Boole que no contenga constantes es igual a una función en forma normal (o canónica) disyuntiva.*

Para ello se aplica el siguiente proceso:

1.º Se suprimen los signos de complementación aplicados a expresiones mediante aplicación reiterada de las leyes de De Morgan. Así, por ejemplo, expresiones del tipo $(A + B)'$, siendo A y B a su vez expresiones, se reducen a $A'B'$, si $A = x + yz$. A' se sustituye por $x'(y + z)$, etcétera.

Como consecuencia de esta etapa sólo aparecerán apóstrofos en las variables simples.

2.º Se aplica la ley distributiva de (.) sobre (+), con lo que la función se reduce a un polinomio.

3.º En el caso general no aparecerán en todos los términos del polinomio todas las variables. Sin embargo, a partir de éste puede obtenerse otro polinomio tal que en cada término aparezcan todas las variables.

Para ello, si en un término no aparece la variable x_i bastará multiplicarlo por $x_i + x_i'$, con lo que la función no se altera, y se obtendrán dos términos que sí contienen dicha variable.

4.º Como consecuencia del paso tercero se habrá obtenido la función como polinomio constituido por monomios en que aparezcan todas las variables, para que esta forma sea la normal disyuntiva se precisa que todos los términos sean distintos. Para ello si, como consecuencia de 3.º en el polinomio, aparecieran términos iguales, podrían suprimirse uno de ellos por la ley de idempotencia.

De esta forma cualquier función puede ponerse en esta forma normal.

Ejemplo

Escribir la función $f = (xy' + xz)' + x'$ en forma normal disyuntiva.

Solución

$$\begin{aligned}(xy' + xz)' + x' &= (xy')'(xz)' + x' \\ &= (x' + y)(x' + z') + x' \\ &= x' + x'y + yz' + x' \\ &= x'(y + y')(z + z') + z'y(x + x') \\ &= x'yz + x'yz' + x'y'z + x'y'z' + xyz' + x'yz' \\ &= x'yz + xyz' + x'yz' + x'y'z + x'y'z'\end{aligned}$$

La utilidad de la forma normal estriba principalmente en el hecho de que cada función determina únicamente una forma normal en un número dado de variables, como veremos en posteriores teoremas. Sin embargo, cualquier función puede ponerse en forma normal por más de un camino cambiando el número de variables. Por ejemplo, $f = xy$ es una forma normal en x y en y. Pero si se multiplica por $z + z'$, entonces $f = xyz + xyz'$, que también es una forma normal en las variables x,y,z. Análogamente, $g = x'yz + xyz + x'yz' + xyz$, es una forma normal en x,y,z, pero se reduce sacando factores a $g = x'y + xy$, que es una forma normal en x e y.

Consideraremos forma normal disyuntiva aquella de todas las que pueden formarse que contenga el menor número posible de variables. Con esta definición existe una correspondencia entre la función y la forma normal, única.

El número máximo de términos posibles de una función de n variables en forma normal disyuntiva es 2^n.

En efecto, cada variable x_i puede aparecer de dos formas posibles, x_i y x'_i. Por tanto, si hay n variables, el número de términos distintos que pueden formarse será $2 \cdot 2 \ldots 2 = 2^n$.

La función de n variables que contiene los n términos posibles en forma normal disyuntiva se llama *forma normal disyuntiva completa.*

La forma normal disyuntiva completa es idénticamente 1.

Sea f_n la forma completa en n variables; elegimos una variable cualquiera de las n, supongamos que es x_n. Los términos pueden clasificarse en dos tipos: los que contienen x_n y los que contienen n'_n; sacando factor común f_n puede ponerse en la forma

$$f_n = x_n \phi_1 + x'_n \phi_2$$

ϕ_1 y ϕ_2 son dos funciones en forma normal disyuntiva en $n-1$ variables. Contienen los mismos términos, ya que si un término T, de ϕ_1, no estuviera en ϕ_2, la forma f_n no sería completa, por faltarle el término $x'_n T$.

Además, $\phi_1 = \phi_2$ es la forma completa en $n-1$ variables, ya que si no lo fueran y les faltara un término B, a la forma f_n le faltarían Bx_n y Bx'_n. Por tanto,

$$f_n = (x_n + x'_n) f_{n-1} = f_{n-1}$$

Para $n = 1$,

$$f_1 = x_1 + x'_1 = 1. \text{ Luego } f_n = f_{n-1} = f_{n-2} = f_2 = f_1 = 1$$

T. 2.—Si se asigna a una forma arbitraria el valor 0 ó 1 a cada una de las n variables, de una función prefijada, entonces un término de la forma normal disyuntiva completa en los n variables tendrá el valor 1, y el resto de los términos, el valor 0.

Demostración.—Tomemos a_1, $a_2 \ldots a_n$ como representantes de los valores asignados a $x_1, x_2 \ldots x_n$, en este orden, donde cada a_j es 0 ó 1. Seleccionaremos un término de la forma normal completa de la siguiente forma.

Para cada x_i usaremos x_i si $a_i = 1$ y x'_i si $a_i = 0$, para $i = 1,2, \ldots n$. El término así seleccionado es un producto de n elementos iguales a 1 y, por tanto, igual a 1. Todos los términos en la forma normal completa contendrán como mínimo un factor 0 y, por tanto, serán 0.

La condición necesaria suficiente para que dos funciones sean iguales es que sus formas normales disyuntivas contengan los mismos términos.

Diremos que dos funciones son iguales cuando establecen la misma correspondencia, es decir, cuando sus valores son los mismos para cualquier combinación de valores de las variables; por tanto, si tienen los mismos términos, dos funciones son iguales.

Recíprocamente, si dos funciones son iguales tienen los mismos términos.

En efecto, si dos funciones son iguales, de acuerdo con la definición anterior, tendrán igual valor para cualquier juego de valores de las variables independientes, y en particular tendrán iguales valores para cualquier juego de valores 0,1. Sin embargo, a cada combinación de valores 0,1 de las variables que dé valor 1 a ambas funciones corresponde un único término posible de los 2^n existentes; por tanto, ambas tendrán tantos términos como valores 1 correspondientes a combinaciones 0,1 resulten, y esos términos por el T. 2. son los mismos.

Por tanto, para establecer cualquier identidad en un álgebra de Boole, es suficiente comprobar el valor de cada función para todas las combinaciones de 0 y 1 que se puedan asignar a las variables.

De acuerdo con los teoremas precedentes, una función queda completamente determinada por los valores que toma para cada asignación posible de 0 y 1 a las variables.

Por tanto, una forma de *representar las funciones* es *mediante una tabla* que represente tales propiedades.

Si se da una tabla de valores de función para valores 0,1 de las variables, se puede construir la forma canónica disyuntiva de dicha función aplicando el procedimiento descrito en el Teorema 2, es decir, para cada conjunto de condiciones para las cuales la función es 1, se incluye el término correspondiente en la forma normal completa. La suma de estos términos da la función, no en su forma más simplificada. El ejemplo siguiente indica este método. Las simplificaciones se realizan una vez obtenida la función en forma canónica disyuntiva.

Ejemplo.

Encontrar y simplificar la función $f(x, y, z)$ especificada por la tabla siguiente (tener en cuenta que la tabla da el valor de f para cada uno de los $2^3 = 8$ asignaciones posibles de 0 y 1 a x, y, z)

TABLA 2-1

Fila	x	y	z	$f(x,y,z)$
1	1	1	1	0
2	1	1	0	1
3	1	0	1	1
4	1	0	0	0
5	0	1	1	0
6	0	1	0	0
7	0	0	1	1
8	0	0	0	0

Solución

Observamos que para las combinaciones representadas por las filas 2, 3 y 7 de la tabla la función tiene valor 1. Por tanto, la forma canónica disyuntiva de f tendrá tres términos. Seleccionando estos términos como se describe en la demostración del teorema 2 obtendre-

mos $f(x,y,z) = xyz' + xy'z + x'y'z = xyz' = y'z$. Comprobando esta función para cada combinación propuesta en la tabla verifica las propiedades requeridas.

Una aplicación inmediata de los resultados de esta sección es *encontrar*, por inspección, *el complemento de cualquier función* en forma normal disyuntiva. El complemento contendrá exactamente aquellos términos de la forma normal completa que no aparezcan en la función dada.

La justificación de esto es la siguiente:

Si f es la función dada y g la formada por los términos de la forma completa no incluidos en f, evidentemente:

$$f + g = \text{forma completa} = 1$$

Por otro lado, la función $h = f.g$ es idénticamente nula. En efecto, para cualquier combinación de valores 0,1 de las variables habrá un único término que valdrá 1 y el resto 0; por tanto, una de las funciones valdrá 1 y la otra 0, por lo que h valdrá siempre 0.

Por tanto, al verificarse

$$f + g = 1 \qquad f.g = 0$$

para cualquier valor de las variables, las funciones f y g son complementarias. Por ejemplo, el complemento de $a'b + ab'$ es $ab + a'b'$, y el complemento de $abc + ab'c' + a'b'c'$ es

$$a'bc + abc' + a'b'c + a'bc'.$$

3.3. FORMA CANONICA (NORMAL) CONJUNTIVA

Aparte de la forma normal disyuntiva hay otra forma normal de representación de funciones de Boole, igualmente útil. La primera representaba a la función con suma de productos de las variables; ésta la representará como producto de sumas. Si cada sentencia de la sección precedente se reemplaza por su dual, el resultado será la forma canónica conjuntiva. Para presentar de una forma clara este nuevo tipo de representación se repetirán los teoremas y definiciones en la forma dual. Las demostraciones, naturalmente, se omiten.

Definición.—Una función boolena está en forma normal conjuntiva en n variables $x_1, x_2, \ldots x_n$ para $n < 0$, si la función es un producto de factores del tipo $f_1(x_1) + f_2(x_2) + \ldots + f_n(x_n)$, donde $f_i(x_i)$ es x_i o x_i' para cada $i = 1,2, \ldots n$, y no hay dos factores idénticos.

T. 1. Toda función en un álgebra de Boole que no contenga constantes es igual a una función en forma normal conjuntiva.

El proceso a aplicar será análogo o dual del seguido para la forma normal disyuntiva:

1.º Se suprimen los signos de complementación aplicados a expresiones mediante aplicación reiterada de las leyes de De Morgan. Así, por ejemplo, expresiones del tipo $(A + B)'$, siendo A y B, a su vez, expresiones, se reducen a $A'B'$, si $A = x + yz$ A' se sustituye por $x'(y + z)$, etcétera.

Como consecuencia de esta etapa sólo aparecerán apóstrofos en las variables simples.

2.º Se aplica la ley distributiva de (+) sobre (.), con lo que la función se reduce a un producto de factores formados por suma de variables.

3.º En el caso general no aparecerán en todos los términos del producto todas las variables. Si en un término no aparece la variable x_i bastará sumarle $x_i \,.\, x_i'$, con lo que el término no se altera. Una vez añadido este último término, el término antiguo se descompone en producto de dos que contienen x_i, aplicando la propiedad distributiva de (+) sobre (.).

4.º Como consecuencia del paso tercero se habrá obtenido la función como producto constituido por factores en los que aparecen sumadas todas las variables, para que esta forma sea la normal conjuntiva se precisa que todos los factores sean distintos; para ello si, como consecuencia de tercero, aparecieran términos iguales, podría reducirse a uno de ellos por la ley de idempotencia.

Ejemplo

Escribir la función $(xy' + xz)' + x'$ en forma normal conjuntiva.

$$\begin{aligned}(xy' + xz)' + x' &= (x' + y)(x' + z') + x' \\ &= (x' + x' + y)(x' + x' + z') \\ &= (x' + y)(x' + z') \\ &= (x' + y + zz')(x' + z' + yy') \\ &= (x' + y + z)(x' + y + z')(x' + y + z')(x' + y' + z') \\ &= (x' + y + z)(x' + y + z')(x' + y' + z')\end{aligned}$$

La forma normal conjuntiva en n variables que contiene 2^n factores se llama *forma normal conjuntiva completa* en n variables.

T. 2. Si se asigna a cada una de las n variables el valor 0 ó 1 de una manera arbitraria, pero fija, entonces exactamente un factor de la forma normal completa en n variables tendrá el valor 0, y los otros factores tendrán el valor 1.

Para seleccionar el factor que será 0 cuando se asigna un conjunto de valores $a_1, a_2, \ldots a_n$ a $x_1, x_2, \ldots x_n$, en este orden, donde a_i es 0 ó 1, analizamos el método de 4.2.: x_i es seleccionado si $a_i = 0$, y x_i' si $a_i = 1$ para cada $i = 1,2, \ldots n$. El factor apropiado es la suma de aquellas letras, cada una de las cuales tiene valor 0. Los otros factores tienen valor 1.

Corolario

Dos funciones que están expresadas en forma normal conjuntiva en n variables, son iguales si y sólo si contienen idénticos factores.

Ejemplo

Encontrar y simplificar la función $f(x,y,z)$ especificada en la tabla.

TABLA 2-3

Fila	x	y	z	$f(x,y,z)$
1	1	1	1	1
2	1	1	0	1
3	1	0	1	0
4	1	0	0	1
5	0	1	1	1
6	0	1	0	1
7	0	0	1	0
8	0	0	0	1

Solución

Usando el método dual del ejemplo 2, sección 2.4, sólo dos filas de la tabla dan a f un valor 0. Seleccionando los factores para que se cumplan las filas 3 y 7, tenemos:

$$f(x.y.z) = (x' + y + z')(x + y + z') = y + z'.$$

En problemas de este tipo se elige para representar la función la forma a que corresponde al menor número de 0 ó 1 en columna de $f(x, y, z)$. Forma normal disyuntiva si el número de 1 es menor que el de 0, ó forma normal conjuntiva si sucede lo contrario.

Tal como se explicó en 3.2., se puede usar la forma normal conjuntiva para encontrar *complementos de funciones* por la simple inspección de la misma. El complemento de cualquier función escrita en forma normal conjuntiva es aquella función cuyos factores son exactamente aquellos de la forma completa que no aparecen en la función dada.

La justificación de esto puede hacerse de una manera análoga a 4.2., sea f la función dada en forma normal conjuntiva, sea g la función constituida por los términos de la forma completa que no aparecen en f. De acuerdo con ello:

$$f.g = 0.$$

por otro lado, $f + g = 1$, ya que cualquier juego de valores 0,1 de las variables hará 0 un único factor (que podrá estar en el factor f o en g, pero no en ambos), y todos los demás 1. Por tanto, para cualquier juego de valores 0,1 de las variables habrá siempre una función f o g que valga 1 y, por tanto, también $f + g$.

Como consecuencia de estas dos propiedades (producto 0 y suma 1), las funciones f y g son complementarias.

Por ejemplo, el complemento de $(x+y')(x'+y)$ es $(x+y)(x'+y')$.

Para *cambiar una función de una a otra forma normal* puede aplicarse esta última propiedad teniendo en cuenta la propiedad involutiva del complemento $f=(f')'$, obteniendo el primer complemento por la ley de De Morgan y el segundo por la última propiedad, tal como se indica en el ejemplo siguiente:

Encontrar la forma normal conjuntiva para la función

$$f=xyz+x'yz+xy'z'+x'yz'.$$

Solución

$$\begin{aligned} f &= xyz+x'yz+xy'z'+x'yz' \\ &= [(xyz+x'yz+xy'z'+x'yz')']' \\ &= [(x'+y'+z')(x+y'+z')(x'+y+z)(x+y'+z)]' \\ &\quad \text{(Tomando el complemento a la forma normal completa)} = \\ &= (x+y+z)(x'+y+z')(x+y+z')(x'+y'+z). \end{aligned}$$

CAPITULO III

ALGEBRA DE CONJUNTOS

1. *Definición*

Si se considera el conjunto $P(u)$ de todos los subconjuntos de un universal dado u con las operaciones entre dichos subconjuntos unión, intersección y complementación tal y como se han definido en el capítulo I, la estructura algebraica así constituida:

$$> P(u), \cup, \cap', < \text{ es un álgebra de Boole.}$$

En efecto:

1.º Las operaciones unión e intersección son operaciones binarias cerradas en $P(u)$, ya que la unión o intersección de dos subconjuntos de u es otro subconjunto de u y, por tanto, elemento de $P(u)$.

2.º Ambas operaciones son conmutativas por definición, luego se verifica el primero de los axiomas de Huntington.

3.º Existen elementos neutros para cada operación.

En efecto:

La unión de todo subconjunto de u con el conjunto vacío es el mismo subconjunto, es decir, $A \cup \phi = A = \phi \cup A$, luego el conjunto vacío es el elemento neutro respecto de la operación unión.

La intersección de todo subconjunto X de u con u está formada por definición po raquellos elementos que pertenecen a u y a X, como todo elemento de X pertenece a u la intersección buscada es X. Por tanto,

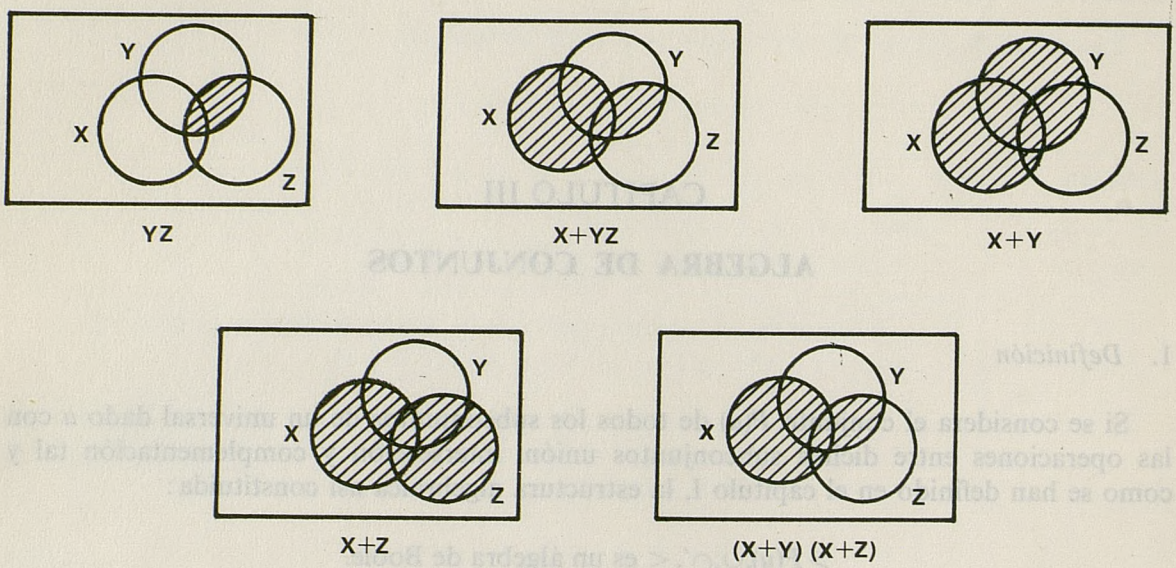
$$X \cup u = u \cup X = X$$

Por tanto, el conjunto universal u es elemento neutro respecto de la operación intersección.

Por lo mismo se verifica el segundo axioma de Huntington.

4.º Cada operación es distributiva respecto de la otra.

Para visualizar esta propiedad a partir de la definición de cada operación mediante los conceptos intuitivos de conjunto y elemento se emplean los diagramas de Venn, en los que el conjunto universal se representa por un rectángulo y cada subconjunto del mismo por un círculo interior a él; de esta forma pueden representarse, dados distintos conjuntos, mediante áreas rayadas los resultados de las distintas operaciones. En la figura 3.1 se representa la comprobación de la propiedad distributiva de la unión (+) respecto a la intersección (·).



Análogamente puede verse la recíproca.

Por tanto, se verifica el tercer axioma de Huntington.

5.º Para cada elemento X de $P(u)$ existe otro X' tal que

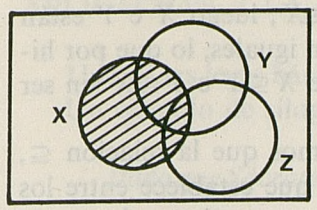
$$X \cup X' = u \quad \text{y} \quad X \cap X' = \phi$$

Este elemento es el conjunto complementario tal y como se definió en el capítulo I; por tanto, también se verifica el cuarto axioma de Huntington.

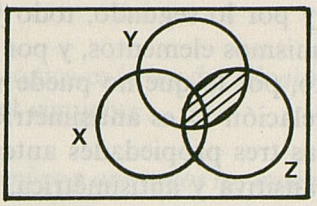
Luego el álgebra de los subconjuntos de uno universal dado, con las operaciones unión e intersección es un álgebra de Boole y, por tanto, se verificarán los teoremas demostrados en el capítulo II de una manera general, para dicha estructura. Dichos teoremas pueden visualizarse mediante diagramas de Venn o justificarse a partir de los conceptos intuitivos de conjunto y de elementos, como puede verse en las figuras 3.2 (propiedad asociativa) y 3.3 (Leyes de De Morgan).

2. *Propiedades de la relación de inclusión de conjuntos*

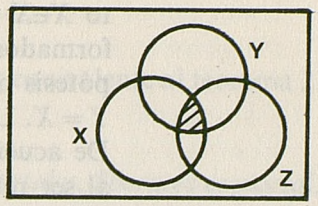
En el capítulo I se definió la notación $A \subseteq B$, que significa que el conjunto A está contenido dentro del conjunto B. Cuando queremos referirnos al símbolo $\subseteq$ sin hacer referencia específica a ningún conjunto, diremos *inclusión*, así como (+) se refiere a la unión. La rela-



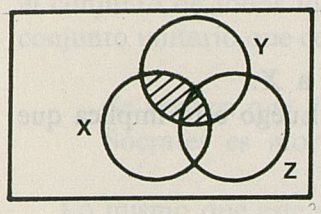
X



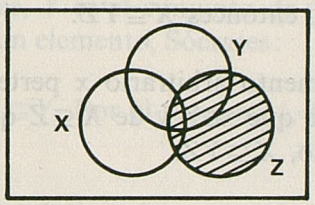
YZ



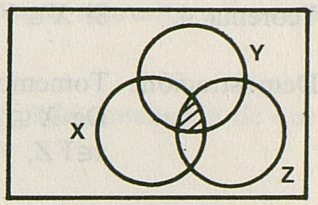
X (YZ)



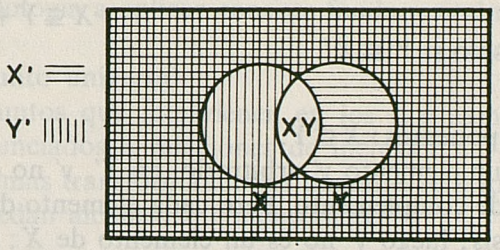
(XY)



Z



(XY) Z



ción de inclusión entre conjuntos cumple una serie de propiedades que pueden verificarse directamente a partir de las definiciones o haciendo uno de los diagramas de Venn. En la definición de $\subseteq$ se apuntó que

$$X \subseteq Y \quad \text{si y sólo si} \quad XY' = \phi$$

Teorema 1.º La relación de inclusión es reflexiva, ya que $X \subseteq X$ cualquiera que sea X.

Teorema 2.º La relación de inclusión es transitiva; es decir:
Si $X \subseteq Y$ y $Y \subseteq Z$, entonces $X \subseteq Z$.

Demostración: Tomemos un elemento arbitrario x del conjunto X.
Puesto que $X \subseteq Y$, por definición $x \in Y$. Como $Y \subseteq Z$, $x \in Z$, pero x era cualquier elemento de X; por tanto, $X \subseteq Z$.

Teorema 3.º Es antisimétrico; es decir,
Si $X \subseteq Y$ $Y \subseteq X$ si $X \neq Y$.
Supongamos que se verifica $X \subseteq Y$ e $Y \subseteq X$. Por lo primero, todo elemen-

to $X \in X$ es $X \in Y$, y por lo segundo, todo $y \in Y$ es $y \in X$; luego X e Y están formados por los mismos elementos, y por tanto son iguales, lo que por hipótesis no es cierto, por lo que no puede verificarse $X \subseteq Y$ e $Y \subseteq X$ sin ser $Y = X$. Luego la relación $\subseteq$ es antisimétrica.
De acuerdo con las tres propiedades anteriores vemos que la relación $\subseteq$, al ser reflexiva, transitiva y antisimétrica, el orden que establece entre los subconjuntos del conjunto universal U es parcial, ya que existen elementos no comparables por la relación $\subseteq$. Por ejemplo, X y X'.

Teorema 4.º Si $X \subseteq Y$ y $X \subseteq Z$, entonces $X \subseteq YZ$.

Demostración: Tomemos un elemento arbitrario x perteneciente a X.
De $X \subseteq Y$ se sigue que $x \in Y$ y de $X \subseteq Z$ que $x \in Z$. Luego esto implica que $x \in YZ$, y por tanto, $X \subseteq YZ$.

Teorema 5.º Si $X \subseteq Y$, entonces $X \subseteq Y + Z$ para cualquier Z.

Demostración: Puesto que $Y \subseteq Y + Z$, por el teorema 2.º $X \subseteq Y \subseteq Y + Z$
$X \subseteq Y + Z$

Teorema 6.º $X \subseteq Y$ si y sólo si $Y' \subseteq X'$.

Demostración: Primero suponemos: $X \subseteq Y$.
Tomemos un elemento y' arbitrario, en Y', y' no es un elemento de Y por definición de complemento. Pero cada elemento de X es un elemento de Y por hipótesis; luego y' no es un elemento de X; por tanto y' debe ser un elemento de X'. puesto que y' representa a cualquier elemento de Y': $Y' \subseteq X'$.
Segundo suponemos: $Y' \subseteq X'$.
Aplicando primero: $(X')' \subseteq (Y')'$ que se transforma en $X \subseteq Y$, por la ley 7, involutiva del complemento. Con lo que queda demostrado el teorema.

Teorema 7.º La condición necesaria y suficiente para que se verifique que $X \subseteq Y$ es $XY' = 0$.

1.º Si $X \subseteq Y$ $\quad XY' = 0$.
Esto es cierto, ya que por definición de complemento ningún elemento de Y puede ser elemento de Y': como todo elemento de X es elemento de Y, por definición de inclusión, ningún elemento de X puede pertenecer a Y', y por tanto la intersección de ambos debe ser el conjunto vacío.

2.º Si $XY' = 0$ $\quad X \subseteq Y$.
Si la intersección de X e Y' es el conjunto vacío, ello quiere decir que ningún elemento de X pertenece a Y'. Ahora bien, por definición de complementario todo elemento del conjunto universal U es elemento de Y o de Y'. Luego si ningún elemento de X pertenece a Y', es que todos son elementos de Y, y por tanto, $X \subseteq Y$.

APLICACION A LA LOGICA

Una de las leyes básicas de la lógica es la ley del *silogismo*, que es equivalente al teorema 2. Un ejemplo de silogismo es el siguiente:

Dado que Sócrates es un hombre y que todos los hombres son mortales, Sócrates es mortal.

La justificación de este razonamiento aplicando la relación de inclusión sería la siguiente: Consideremos el conjunto universal compuesto por todas las cosas animadas. Sea X el conjunto de todos los hombres, Y es el conjunto de todas las cosas mortales y S es un conjunto unitario que consta de un elemento, Sócrates:

Se verifica que $S \subseteq X$ y $X \subseteq Y$. Por el teorema 1, $S \subseteq Y$, que es la conclusión de que Sócrates es mortal.

Lo mismo que este problema relativo al teorema 2 se pueden plantear problemas que, más o menos artificiales, utilicen otras propiedades de la relación de inclusión.

El uso de notación simbólica hace trivial las conclusiones lógicas, que de otra manera serían difíciles. La metodología a aplicar consiste fundamentalmente en:

1.º Definir un conjunto universal.
2.º Definir los conjuntos que intervienen en los razonamientos.
3.º Traducir los enunciados a relaciones de inclusión.
4.º Aplicar los teoremas transformando las distintas relaciones de forma que mediante el teorema 2 puedan alcanzarse conclusiones.

Ejemplo: Hallar conclusiones de los siguientes enunciados:

(a) Un hombre que no es feliz no es dueño de sí mismo.
(b) Todos los hombres casados tienen responsabilidades.
(c) Todo hombre, o está bien casado, o es dueño de sí mismo (o ambas cosas).
(d) Ningún hombre con responsabilidades puede pescar todos los días.

Solución

Consideremos el conjunto universal formado por todos los hombres y definamos los siguientes conjuntos:

H es el conjunto de los hombres felices.
B es el conjunto de los hombres que son dueños de sí mismos.
M es el conjunto de los hombres casados.
R es el conjunto de los hombres con responsabilidades.
F es el conjunto de los hombres que pescan todos los días.

La primera fase (a) se representa $H' \subseteq B'$. Por el teorema 4 queda (a) $B \subseteq H$.
(b) nos dice $M \subseteq R$, que también puede expresarse $R' \subseteq M'$.
(c) nos da $M + B = 1$, o refiriéndonos a la equivalencia de $M'.B' = \phi$.

Estas frases, con una condición de inclusión, obtendrán (c) $M' \subseteq B$.
Finalmente, a partir de (d), se obtiene $RF = \phi$, que es equivalente (d) $F \subseteq R'$.
Combinando (d) y (b) por el teorema 1, (e) $F \subseteq R' \subseteq M' \Rightarrow F \subseteq M'$.
Combinando (e) y (c)$\Rightarrow$(f) $F \subseteq M' \subseteq B \Rightarrow F \subseteq B$.
Combinando (f) y (a)$\Rightarrow$(g) $F \subseteq B \subseteq M \Rightarrow F \subseteq M$.
Esta conclusión se lee: "Todos los hombres que pescan cada día son felices".

(e) y (f) también son conclusiones.

3. *Ecuaciones condicionales*

Ecuaciones condicionales, como en álgebra de números, son igualdades entre expresiones de conjuntos (monomios o polinomios) que no son válidas idénticamente para conjuntos arbitrarios, como ocurre con las leyes demostradas en 1, sino para determinados conjuntos, definidos precisamente por esa condición.

Considerando dos ecuaciones, diremos que la segunda es consecuencia de la primera, si puede obtenerse aplicando sobre la primera una secuencia de las siguientes reglas:

REGLA 1. Cualquier expresión, bien tanto a la izquierda como a la derecha del signo $=$ puede sustituirse por otra idéntica, es decir, obtenida por aplicación de una o varias de las leyes del álgebra de conjuntos. Es decir, se pueden realizar simplificaciones independientes en uno u otro miembro de la ecuación.

REGLA 2. Ambos miembros de la ecuación pueden sustituirse simultáneamente por los respectivos conjuntos complementarios.

REGLA 3. Se puede multiplicar cada miembro de la ecuación por el mismo o iguales conjuntos. Es decir, si son iguales dos conjuntos lo será la intersección con uno dado.

REGLA 4. Se puede sumar a cada miembro de la ecuación el mismo o iguales conjuntos. Como en el caso anterior, si son iguales dos conjuntos lo será su unión con uno dado.

Las reglas anteriores 1, 3 y 4 son válidas en el sentido de que si dos conjuntos verifican la condición de partida verificarán las obtenidas mediante las transformaciones indicadas en estas reglas; ello no implica la recíproca, es decir, que todo conjunto que verifique esta última verifique la primera; por ejemplo, si dos conjuntos son iguales lo es la intersección con uno dado (regla 3), pero, sin embargo, si las intersecciones de dos conjuntos con uno dado son iguales, ello no implica la igualdad de los dos conjuntos de partida, que sólo pueden tener común precisamente la intersección con el tercer conjunto; es decir, contrariamente al álgebra de números, de $X + Y = X + Z$ no se puede pasar a $Y = Z$, y de $XY = XZ$ tampoco puede pasarse $Y = Z$.

La regla 2 por la propiedad involutiva del complementario sí se verifica en ambas direcciones.

Como ejemplo, cada una de las ecuaciones siguientes es consecuencia de la precedente y, por tanto, de la primera ecuación:

$Y + X = XZ$	Ecuación dada.
$(Y + X)' = (XZ)'$	Regla 2.
$X'Y' = X' + Z'$	Reglas 1, 8a y 8b.
$WX'Y' = W(X' + Z')$	Regla 3.

$WX'Y' = WX' + WZ'$ Reglas 1, (3a).
$V + WX'Y' = V + WX' + WZ'$ Regla 4.

Podemos establecer otras dos reglas.

REGLA 5. Una ecuación de la forma $A + B = 0$ puede reemplazarse por dos ecuaciones simultáneas $A = 0$ y $B = 0$, y viceversa; es decir, si la unión de dos conjuntos es el conjunto vacío, necesariamente cada uno debe ser el conjunto vacío, ya que de otra forma la unión de ambos no sería este último.

Recíprocamente, si ambos son iguales a 0 su unión será también 0.

REGLA 6. Una ecuación de la forma $AB = 1$ puede reemplazarse por dos ecuaciones simultáneas $A = 1$ y $B = 1$, y viceversa; es decir, de manera análoga al caso anterior, si la intersección de dos conjuntos es el universal, es que cada uno de ellos es el universal, porque de otra forma no podrían tener a éste como parte común a ambos. Y recíprocamente, si cada uno es igual al universal, la intersección, parte común de ambos, deberá ser igual al conjunto universal.

Diremos de dos conjuntos de ecuaciones simultáneas que el segundo conjunto es consecuencia del primero, si cada ecuación del segundo se obtiene a partir de las ecuaciones del primero, aplicando una o más de las reglas 1 a la 6.

Diremos que dos conjuntos de ecuaciones son equivalentes *si cada uno es consecuencia del otro*. Conjuntos de ecuaciones equivalentes representan idénticas restricciones para los conjuntos que intervengan en las ecuaciones y son, por tanto, reemplazables unos por otros.

TEOREMA. Cualquier serie de condiciones impuestas a conjuntos que pueden expresarse en la notación del álgebra de conjuntos es equivalente a una sola ecuación con segundo miembro igual a cero.

Hay que hacer notar primero que *cualquier condición* expresable en notación algebraica debe ser necesariamente, *o una ecuación* que exprese la igualdad de dos conjuntos, *o una de inclusión* de conjuntos. Puesto que la condición $X \subseteq Y$ es equivalente a la ecuación $XY' = \phi$, es suficiente considerar solamente conjuntos de ecuaciones.

Haremos la demostración en dos etapas.

1.º Toda ecuación de la forma $A = B$ puede reducirse a otra equivalente con segundo miembro 0.

Para ello tenemos que obtener, aplicando una sucesión de las reglas 1 a 6, una ecuación con segundo miembro ϕ a partir de $A = B$. Para que la ecuación obtenida sea equivalente a $A = B$, tiene que poder obtenerse a partir de ella esta última aplicando otra sucesión de las reglas 1 a 6.

a) Obtención de una ecuación con segundo miembro nulo a partir de $A = B$ (I).
Si multiplicamos los dos miembros de (I) por B' (regla 3),

$$AB' = 0 \quad \text{(II)}$$

Si multiplicamos ambos miembros de (I) por A' (regla 3),

$$A'B = 0 \quad \text{(III)}$$

Sustituimos (II) y (III) por

$$AB' + A'B = 0 \quad \text{(IV)} \quad \text{(regla 5)}.$$

b) Obtención de $A = B$ a partir de (IV):
Multiplicamos ambos miembros de (IV) por B' (regla 3),

$$AB' = 0 \quad \text{(V)}$$

Si tomamos los complementos de ambos miembros en (IV) (regla 2),

$$(AB' + A'B)' = 1$$

Operando en el primer miembro mediante las leyes de De Morgan:

$$(A' + B)(A + B') = 1$$

Aplicando la propiedad distributiva:

$$AA' + BB' + A'B' + AB = 1. \text{ Es decir, } A'B' + AB = 1 \text{ (VI)}.$$

Si multiplicamos ambos miembros de (VI) por B:

$$AB = B \quad \text{(VII)}$$

Si sumamos (V) y (VII) (regla 4):

$$AB + AB' = B \qquad A(B + B') = B. \text{ Es decir, } A = B$$

Por tanto, toda ecuación de la forma $A = B$ es equivalente a $AB' + A'B = 0$.

2.º Si tenemos una serie de condiciones, éstas sólo pueden ser de la forma $A = B$ o $A \subseteq B$. Por el teorema anterior $A = B$ puede sustituirse por $AB' + A'B = 0$; por la propiedad 6 de la relación de inclusión $A \subseteq B$ es equivalente a $AB' = \phi$.

Por tanto, dada una serie de condiciones, éstas pueden ponerse siempre en forma de ecuaciones con segundo miembro 0.

Pero, dada una serie de ecuaciones con segundo miembro 0, por aplicación reiterada de la regla 5, éstas son equivalentes a la ecuación unión de todas las condiciones igualada a 0. Con lo que queda demostrado que todo conjunto de condiciones en álgebra de conjuntos es equivalente a una ecuación única con segundo miembro 0.

Ejemplo: Reemplazar el conjunto de condiciones (a) $X \subseteq Y$, (b) $X + Y = Z$ y (c) $Z + W = 1$ por una ecuación simple de la forma $A = 0$.

$X \subseteq Y \Leftrightarrow XY' = 0$
$X + Y = Z \Leftrightarrow (X + Y)Z' + (X + Y)'Z = 0$
$Z + W = 1 \Leftrightarrow Z'W' = 0$ tomando complementos en ambos miembros.

Sumando estas ecuaciones tenemos

$$XY' + XZ' + YZ' + X'Y'Z + Z'W' = 0$$

4. *Solución de ecuaciones*

Es posible encontrar solución para ecuaciones en álgebra de conjuntos, pero esta *solución no es* única: representará los límites superior e inferior del conjunto desconocido.

Supongamos una ecuación en la que aparece un conjunto X, desconocido, y que el resto de las letras que aparecen en la ecuación representan conjuntos conocidos. Esta ecuación se puede escribir

$$P(X) = 0, \text{ donde } P(X) \text{ representa una expresión booleana en conjuntos.}$$

Si $P(X)$ contiene términos en los que no aparece ni X ni X', cada término se puede multiplicar por $X + X'$ para producir una ecuación equivalente en la que aparezcan términos en X y X'. Agrupándolos, la ecuación quedará de la forma $AX + BX' = 0$. Esta ecuación es equivalente a dos ecuaciones $AX = 0$, $BX' = 0$, o a la condición $B \subseteq X \subseteq A'$ (teniendo en cuenta que $AX = 0$ es equivalente a $X \subseteq A'$ y $BX' = 0$ a $B \subseteq X$).

Cualquier conjunto que satisfaga esta condición es solución de la ecuación. B es la llamada *solución mínima* y A', *solución máxima* de la ecuación. Claramente se ve que la condición necesaria y suficiente para que exista solución es:

$$B \subseteq A \text{ o su equivalente } AB = 0$$

Esta ecuación es el llamado *eliminante de* X, o condición para que exista solución de la ecuación dada. La existencia de soluciones de una ecuación depende, en general, del significado de los conjuntos A y B. No obstante, en algunos casos puede o no puede satisfacerse $AB = 0$ independientemente del significado de los conjuntos. Por ejemplo, la ecuación $CDX + C'X' = 0$ tiene solución para conjuntos arbitrarios C y D, puesto que $(CD)(C') = 0$, cualquiera que sea el significado de C y D. La ecuación $(M + M')X + X' = 0$ no tiene solución, sea cual sea el significado de M. La solución de una ecuación es única sólo en el caso de que $B = A'$, en la notación anteriormente empleada. Principalmente porque raramente hay soluciones únicas, la resolución de ecuaciones juega un papel muy reducido en el álgebra de conjuntos.

Ejemplo 1. Resolver X en $BX = C$.

Solución

Esta ecuación es equivalente a $BXC' + C(BX)'$, es decir:

$$BC'X + B'C + CX' = 0.$$

Y si $B'C$ lo multiplicamos por $X + X'$, obtenemos

$$(B'C + BC')X + CX' = 0.$$

O sea que la solución general es $C \subseteq X \subseteq (B'C' + BC)$. El eliminante es $(B'C + BC')C = 0$ o $B'C = 0$. Si $C \subseteq B$, cualquier conjunto entre C y $B'C' + BC$ satisface la ecuación.

No sólo es posible resolver una ecuación simple para un conjunto X desconocido; pueden resolverse ecuaciones simultáneas o conjuntos de condiciones. Puesto que tal como se vio en 6, cualquier conjunto de condiciones es equivalente a una ecuación, las ecuaciones simultáneas siempre se reducirán a ecuaciones simples y se resolverán por el método anterior.

CAPITULO IV

LA LOGICA SIMBOLICA Y EL ALGEBRA DE PROPOSICIONES

1. *Proposiciones y funciones proposicionales*

En el presente capítulo se trata de la parte de la lógica simbólica (estudio mediante símbolos de la lógica) referente al cálculo proposicional.

El instrumento principal para el tratamiento de las proposiciones es el *álgebra de proposiciones*, que, como veremos, es un álgebra de Boole. Finalmente, a partir del álgebra de proposiciones, se estudian las fórmulas lógicas (razonamientos o argumentos) válidas para la demostración de teoremas.

1.1. DEFINICIONES

Lo mismo que en álgebra de conjuntos se partía de los conceptos intuitivos de conjunto y elemento, que no era posible definir para construir el álgebra de proposiciones, haremos algo análogo con los conceptos: *verdadero*, *falso*, *proposición*. Verdadero y falso se considerarán simplemente como atributos que se aplican a proposiciones. Por proposición se entenderá, por tanto, el contenido de cualquier clase de declaración que está libre de ambiguedad y que tiene la propiedad de ser verdadera o falsa, pero no ambas.

Ejemplos:

3 es un número primo.
Cuando 5 se suma a 4, la suma es 7.
En el planeta Venus existen criaturas vivas.

La primera proposición es verdadera, la segunda es falsa y la tercera puede ser verdadera o falsa, pero no ambas cosas a la vez. Las tres son, por tanto, proposiciones de acuerdo con la definición.

En cambio, la declaración:

La frase que está usted leyendo es falsa.

Si suponemos que es verdadera, del contenido deduciremos que es falsa, y viceversa. Su contenido, por tanto, es ambiguo, y por lo mismo no es una proposición.

Representaremos las proposiciones con letras minúsculas. Cuando no se den proposiciones específicas se les llamará *variables proposicionales*, y se usarán para representar proposiciones cualesquiera.

A partir de cualquier proposición, o grupo de proposiciones, se pueden formar proposiciones compuestas o funciones proposicionales mediante operaciones conectivas entre ellas. A continuación se describen algunas de estas conectivas.

2. *Conectivas lógicas*

2.1. NEGACION

Definiremos la negación de una proposición p, como la proposición "es falso que p". La notación que se adopta para esta proposición es p', aunque también se utilizan $\sim p$ y $\bar{p}$. Por ejemplo, supongamos que p es la proposición

Dormir es agradable.

La negación de esta proposición podrían ser las proposiciones:

Es falso que dormir es agradable.
Dormir no es agradable.
Dormir es desagradable.

Por tanto, *la negación es la opuesta a la proposición original.* Cuando p es verdadero, p' es falso, y cuando p' es falso, p' es verdadero. Esto se representa mediante la tabla siguiente:

P	P'
V	F
F	V

(V = verdadero)
(F = falso)

2.2. CONJUNCION

En general se define como conjunción de p y q para cualesquiera proposiciones arbitrarias p y q a la proposición "ambos p y q". La notación que se empleará es $p.q$ o pq, y se considerará verdadera en aquellos casos en que ambas, p y q, sean verdaderas, y falsa cuando lo sea p, q o ambas, lo que puede representarse por la tabla:

p	q	pq o $p.q$ o $p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Ejemplo

Si p es la proposición "llueve" y q es "me mojo", la conjunción de p y q es "llueve y me mojo".

2.3. DISYUNCION

Para proposiciones arbitrarias, p y q se define *la disyunción* de p y q, que se indicará con la notación $p+q$ o $p\ q$, a la proposición

"o bien p o q o ambas".

Las palabras "o ambas" usualmente se omiten, y también cuando no haya ambigüedad se puede omitir "o bien". Se considerará que $p+q$ es verdadera cuando bien p o q lo sean, o ambas a la vez, y falsa sólo cuando ambas lo sean, lo que puede representarse con la tabla:

p	q	$p+q$ o $p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

2.4. CONDICIONAL SIMPLE

Esta conectiva, también llamada implicación material, se indica con la notación

$$p \rightarrow q$$

p es el antecedente t q el consecuente de la implicación.

El significado es "si p entonces q". Equivalentes a esta definición son:

"p suficiente para q"
"q necesario para p"
"p solamente si q".

De acuerdo con la expresión gramatical de esta conectiva, cuando p es falso, q puede ser verdadero o falso, ya que no puede afirmarse nada sobre q, con lo que $p \rightarrow q$ podría ser verdadero o falso; sin embargo, dado que para el tratamiento matemático se precisa definir el valor de verdad en todos los casos posibles, se define el valor de verdad, a efectos de tratamiento matemático de esta conectiva, como verdadera en todos los casos, excepto cuando p es verdadera y q falsa. Lo que puede resumirse en el cuadro

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

A partir de la relación de *implicación* $p \rightarrow q$ se pueden definir otras implicaciones de uso corriente. La *recíproca de* $p \rightarrow q$ es $q \rightarrow p$, la inversa es $p' \rightarrow q'$, y *la contrarrecíproca es* $q' \rightarrow p'$.

De éstas, la implicación original y la contrarrecíproca son iguales entre sí, y la recíproca y la inversa también. La tabla siguiente establece estas declaraciones.

			Implicación	Recíproca	Inversa	Contrarrecíproca
Fila	p	q	$p \to q$	$q \to p$	$p' \to q'$	$q' \to p'$
1	V	V	V	V	V	V
2	V	F	F	V	V	F
3	F	V	V	F	F	V
4	F	F	V	V	V	V

Ejemplo

Sea p la proposición "8 es un número par" y q la proposición "el bombón es dulce". Formar en palabras: (a) la implicación $p \to q$, (b) su recíproca, (c) su inversa, (d) su contrarrecíproca.

Solución

(a) Si 8 es un número par, entonces el bombón es dulce.
(b) Si el bombón es dulce, entonces 8 es un número par.
(c) Si 8 es un número impar, entonces el bombón no es dulce.
(d) Si el bombón no es dulce, entonces 8 es un número impar.

2.5. BICONDICIONAL

También llamada equivalencia material, se indica con la notación $p \leftrightarrow q$, y se lee "p si y solamente si q", o también, "p necesario y suficiente para q".

Esta proposición es verdadera siempre que p y q sean simultáneamente verdaderas o falsas, y falsa cuando una es verdadera y la otra falsa. Es decir,

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Mediante estas conectivas podemos definir, a partir de las variables proporcionales p,q,r representantes de proposiciones cualesquiera, funciones de las mismas formadas por estas variables o la negación de ellas separadas por los signos de conjunción o disyunción. Por ejemplo,

$$f(p,q,r) = (p + q'r + rp') \rightarrow (p \rightarrow qr')$$

3. *Tablas de verdad de funciones proposicionales*

Dada una función proposicional cualquiera $P(p,q,r, \ldots t)$ en donde $p,q,r, \ldots t$ son variables proposicionales, esta función puede definirse de manera análoga a las distintas operaciones conectivas del apartado anterior por los valores de verdad que atribuye a cada una de todas las combinaciones posibles de valores de verdad de las variables proposicionales.

Así, por ejemplo, las funciones proposicionales f,g,h de las variables p,q,r quedan totalmente definidas por la tabla de valores correspondientes a las 2^3 alternativas posibles de valores de las variables p,q,r indicadas en el cuadro siguiente.

p	q	r	$f(p,q,r)$	$g(p,q,r)$	$h(p,q,r)$
V	V	V	V	F	V
V	V	F	F	F	F
V	F	V	V	F	F
V	F	F	V	F	F
F	V	V	V	V	V
F	V	F	F	V	F
F	F	V	F	F	V
F	F	F	V	V	V

Por tanto, a una función proposicional le corresponde una tabla de este tipo que la define totalmente, llamada tabla de verdad.

Dos funciones proposicionales son iguales si tienen iguales tablas de verdad.

Dada una función proposicional expresada en función de las conectivas lógicas definidas en el apartado anterior, puede obtenerse su tabla de verdad a partir de las correspondientes a cada una de las conectivas.

Ejemplo

Dado $f(p,q,r) = (p \wedge q) \rightarrow r$ puede obtenerse su tabla de verdad obteniendo primero $h = p \wedge q$, la tabla de la función $h(p,q) = p \wedge q$ aplicando las reglas correspondientes a la conjunción, y a continuación la tabla de $f(p,q,r) = h \rightarrow r$ mediante las reglas de la implicación material o condicional entre los valores de h y r.

p	q	r	$h=p\wedge q$	$f=h\rightarrow r$
V	V	V	V	V
V	V	F	V	F
V	F	V	F	V
V	F	F	F	V
F	V	V	F	V
F	V	F	F	V
F	F	V	F	V
F	F	F	F	V

Una función proposicional tal que en su tabla de verdad, para todas las combinaciones posibles de valores de verdad de las variables, sólo aparece V, es decir, siempre verdadera, se llama *tautología.*

Recíprocamente, una función siempre falsa, es decir, aquella en que para todas las combinaciones de valores de las variables aparece F en la tabla de verdad, se llama *contradicción.*

4. *El álgebra de las funciones proposicionales*

Las definiciones anteriores nos permiten observar que sobre el conjunto $\{VF\}$ se han definido las operaciones $(+)$ y $(.)$ de acuerdo con las tablas

$+$	V	F
V	V	V
F	V	F

$.$	V	F
V	V	F
F	F	F

Por tanto, $(+)$ y $(.)$ son operaciones binarias definidas en $\{V,F\}$ que definen un álgebra con dicho conjunto. Vamos a demostrar que esta estructura, teniendo en cuenta la negación tal y como se ha definido, es un álgebra de Boole. Para ello basta comprobar que se verifican los axiomas de Huntington descritos en el capítulo II.

1.º Las dos operaciones conjunción y disyunción son conmutativas por definición.

2.º Cada una es distributiva respecto de la otra. Para comprobarlo basta demostrar la igualdad entre las funciones proposicionales

$$p+qr=(p+q)(p+r) \qquad p(q+r)=pq+pr \tag{1}$$

De acuerdo con la definición de igualdad entre funciones proposicionales, para que ésta exista deberán tener las mismas tablas de verdad.

En el cuadro siguiente se construyen las tablas correspondientes, pudiendo comprobarse las igualdades (1). Por ello, cada operación es distributiva con relación a la otra.

p	q	r	pq	pr	qr	$p+q$	$p+r$	$q+r$	$p+qr$	$(p+q)(p+r)$	$p(q+r)$	$pq+pr$
V	V	V	V	V	V	V	V	V	V	V	V	V
V	V	F	V	F	F	V	V	V	V	V	V	V
V	F	V	F	V	F	V	V	V	V	V	V	V
V	F	F	F	F	F	V	V	F	V	V	F	F
F	V	V	F	F	V	V	V	V	V	V	F	F
F	V	F	F	F	F	V	F	V	F	F	F	F
F	F	V	F	F	F	F	V	V	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F

3.º Existe un elemento neutro respecto a cada operación. En nuestro caso F es el neutro respecto a $(+)$ y V es el neutro respecto a $(.)$, como puede comprobarse por las tablas de las operaciones. Por ello podemos llamar $F=0$ y $V=1$.

4.º Para cada elemento existe otro complementario tal que

$$p+p'=1 \quad \text{y} \quad pp'=0$$

En nuestro caso el complementario (negación) de V es F, y recíprocamente.

Por tanto, se verifican los cuatro axiomas de Huntington, por lo que el cálculo proposicional obedece las leyes del cálculo booleano; es decir, pueden aplicarse los teoremas 1 a 9 demostrados en el capítulo II para las funciones proposicionales expresadas mediante las operaciones de conjunción y disyunción, ya que son funciones booleanas.

Por otra parte, las funciones definidas mediante una tabla de valores de verdad pueden ponerse en forma normal disyuntiva o conjuntiva, ya que al ser $V=1$ y $F=0$, la tabla de verdad proporciona un juego de valores 0,1 de la función correspondientes a valores 0,1 de las variables; por tanto, la función proposicional correspondiente puede ponerse siempre en función de las operaciones conjunción y disyunción.

Así, por ejemplo, la implicación material $p \rightarrow q$ tendrá como tabla de valores 0,1:

p	q	$p \rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

De acuerdo con ello, la función booleana correspondiente será en forma normal conjuntiva $p' + q$. Por tanto, $p \rightarrow q$ equivale a la disyunción de q y la negación de p. Análogamente puede verse que la conectiva bicondicional $p \rightarrow q$ equivale a $pq + p'q'$.

5. *Tratamiento de la lógica mediante teoría de conjuntos*

El desarrollo anterior del cálculo proposicional parte de las tablas de verdad de las funciones proposicionales, en la hipótesis de que todas las variables proposicionales pueden ser verdaderas o falsas, y son admisibles todas las combinaciones posibles de dichos valores en cada variable; esta hipótesis, que es válida para un tratamiento general del cálculo proposicional, puede no serlo al referirse a las funciones proposicionales de un conjunto *específico* de proposiciones que pueden estar relacionadas entre ellas.

Por ejemplo, consideremos la siguiente proposición con respecto a los enteros a y b. "O bien a es no menor que b o b es no menor que a". *Evidentemente esta proposición es una tautología.* Designando por p la proposición "a es menor que b" y por q la proposición "b es menor que a", si construimos la tabla de verificación para la proposición compuesta, no podremos demostrar que es una tautología, porque aparece 0 en la fila 1 de la tabla.

TABLA DE VERIFICACION $p' + q'$

Fila	p	q	p'	q'	$p'. + q'$
1	1	1	0	0	0
2	1	0	0	1	1
3	0	1	1	0	1
4	0	0	1	1	1

Ello es debido a que, considerando las proposiciones particulares de nuestro caso p y q, es imposible que sean verdad ambas simultáneamente, por lo que no es admisible la posibilidad lógica de la primera fila, suprimiéndola sí resulta una tautología.

Las proposiciones consideradas anteriormente constituyen un ejemplo de *proposiciones relacionadas*. Dado un conjunto específico de proposiciones son posibles distintas relaciones entre dos o más proposiciones, cada una identificada por el hecho de que una o más filas de una tabla de verificación correspondiente no representan posibles valores admisibles para las proposiciones. El ejemplo anterior pone de manifiesto la necesidad de discutir el hecho de las posibilidades lógicas de una manera general.

Veamos otro ejemplo.

Ejemplo: Una caja contiene quince bolas, de las cuales cinco son blancas, cinco rojas y cinco azules. Extraemos dos bolas a un tiempo. Estudiar las posibilidades lógicas de este suceso.

Supongamos las proposiciones

b = sale bola blanca
r = sale bola roja
a = sale bola azul

La tabla de todas las posibilidades lógicas es la indicada en el cuadro adjunto. Sin embargo, hay dos posibilidades, la primera y la última, que por la naturaleza del suceso no son admisibles, ya que sabemos que se han extraído dos bolas, por lo que al no haber más que de tres colores no pueden ser falsas las tres proposiciones simultáneamente, y por la misma razón es imposible que haya una de cada color. Por otro lado, la forma de realizarse la extracción de las bolas puede hacer que los casos en que salen dos bolas distintas constituyan una posibilidad doble según el orden de aparición.

	b	r	a
*	0	0	0
	0	0	1
	0	1	0
	1	0	0
	1	1	0
	1	0	1
	0	1	1
*	1	1	1

Vemos, por tanto, que al tratar un conjunto determinado de proposiciones se precisa realizar un análisis previo de las posibilidades lógicas de ese conjunto de proposiciones. El tratamiento puede hacerse mediante al álgebra de conjuntos, de la forma siguiente:

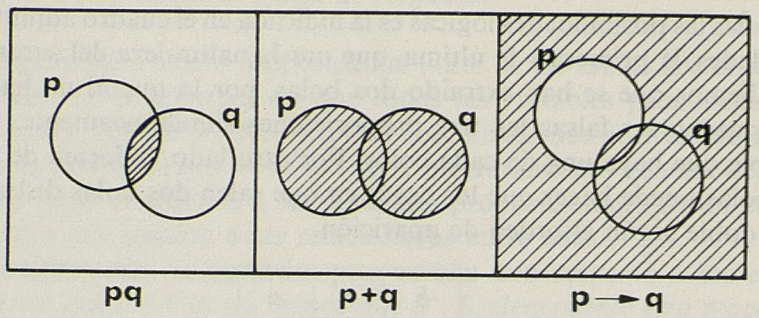
Se asigna al *conjunto de proposiciones* en estudio *un conjunto universal cuyos elementos son las posibilidades lógicas* para el conjunto de proposiciones. Esto puede hacerse de muchas maneras; en general se elegirá el conjunto de posibilidades más conveniente, que tiene las dos propiedades siguientes:

1.ª Las posibilidades elegidas son tales que en cualquier circunstancia presumible sólo puede suceder una de ellas.
2.ª Las posibilidades son tales que el valor verdadero de cada proposición puede determinarse por cualquiera de ellas.

Asimismo se asigna un subconjunto del conjunto universal a cada proposición tal que *el subconjunto contiene aquellas posibilidades para las cuales la proposición es cierta.* Este conjunto se llama "Conjunto de verdad de la proposición".

De acuerdo con lo anterior, *el conjunto de verdad para una función proposicional* del conjunto de proposiciones en estudio está formado por la composición de los conjuntos de verdad de las proposiciones que integran la función de acuerdo con las operaciones indicadas en la misma. Podemos representar conjuntos verdaderos abstractos por diagramas de Venn, exactamente como se hizo en el capítulo III, lo que ilustra la fuerte relación entre el

álgebra de conjuntos y el álgebra lógica. En la figura adjunta se incluyen los diagramas de Venn para mostrar los conjuntos verdaderos para pq, $p+q$, $p \rightarrow q$ en términos de conjuntos verdaderos para p y q. P y Q representan el conjunto verdadero para las proposiciones p y q, y las áreas sombreadas representan los conjuntos verdaderos para las proposiciones compuestas.



6. *Cuantificadores lógicos*

En el desarrollo de la lógica realizado hasta el momento se ha tratado de proposiciones y de las formas en que las mismas pueden combinarse para formar nuevas proposiciones, pero no se ha estudiado la estructura de las proposiciones simples. Para entender algunos tipos de proposiciones matemáticas muy importantes, es esencial hacer mención a las proposiciones que contienen *cuantificadores*. A continuación tenemos algunos ejemplos de las mismas:

algunos hombres son ricos;
todos los hombres están prevenidos;
ningún hombre es paciente.

Las palabras *algunos*, *todos*, *ningun*, son cuantificadores. Nos dicen "cuanto" se considera de un cierto conjunto de cosas. Muchas frases llevan implícito el cuantificador. Consideremos las siguientes proposiciones matemáticas en forma de ecuaciones:

$$x^2 + 4x = 7$$

$$x^2 - 4 = (x+2)(x-2)$$

La primera es cierta en el sentido de que por lo menos un número x hace $x^2 + 4x = 7$. La segunda es cierta en el sentido general de que para todo número x se verifica $x^2 - 4 = (x+2)(x-2)$. *La primera ecuación sería falsa únicamente* cuando ningún número x la satisfaga, *pero se puede demostrar que la segunda es falsa cuando* haya *un solo número* x que *no la satisfaga*. Es importante, pues, distinguir entre los dos tipos de proposiciones.

Diremos que $p(x)$ es una proposición o enunciado formal si al particularizar x para un determinado elemento de un conjunto se convierte en una proposición, es decir, verdadera o falsa. Por ejemplo, "x es mortal" es un enunciaco formal; al atribuir a x un elemento del conjunto de los hombres se convierte en una proposición.

Dado un conjunto C y un enunciado formal $p(x)$, puede definirse el conjunto de validez de dicho enunciado en C:

$$V_p = \{x \mid x \in C, \quad p(x) = \text{verdad}\}$$

La medida en que V_p se inscribe en C' se expresa con los cuantificadores lógicos.

1.º Si $V = C$, ello indica que $p(x)$ es cierto para todo elemento de C^p. Esto se expresa mediante el cuantificador universal $\forall$ de cualquiera de las formas:

$$\forall(x \mid x \in C)\ p(x) \qquad \forall(x \in C)\ p(x) \qquad \text{o bien } \forall x p$$

La notación del último caso se utilizará cuando se haya predefinido el conjunto a que pertenece x.

2.º Si $V_p \neq \phi$ y $V_p \neq C$, ello indica que si no todos los elementos de C', algunos hacen verdadero $p(x)$. Para expresarlo se emplea el cuantificador existencial $\exists$:

$$\exists(x \in C)\ p(x) \quad [\text{Existe al menos algún } x \in C \text{ que hace verdadero } p(x)]$$

También puede indicarse en la forma $\exists x^p$ si se ha definido previamente el conjunto a que pertenece x.

3.º Si $V_p = \phi$, no existe ningún elemento en C que verifique $p(x)$. Esto se expresa mediante el cuantificador universal $\forall$, ya que si $V_p = \phi$, todo elemento de C' hace que $p(x)$ sea falso.

$$\forall(x \in C)\ p'(x) \qquad \forall x p'$$

Ejemplos:
Si x es un número real

$$\exists_x(x^2 + 4x = 7),$$

o bien, si llamamos R al conjunto de los números reales

$$\exists(x \in R)(x^2 + 4x = 7)$$

Análogamente,

$$\forall_x(x^2 - 9 = (x - 3)(x + 3))$$

Las negaciones de las proposiciones que consideran cuantificadores obedecen las reglas

$$(\exists_x p)' = \forall_x p'$$
$$(\forall_x p)' = \exists_x p'$$

La justificación es inmediata a partir de la definición.

Puesto que no pueden manejarse los símbolos para cuantificación en el álgebra de proposiciones, no se usarán grandemente a continuación, se introducen para especificar las reglas de negación. En lo que sigue se usarán las letras para identificar proposiciones, incluyan o no cuantificadores.

7. *Razonamiento lógico*

A partir de un conjunto de proposiciones admitidas sin demostración, y mediante razonamiento lógico, se pueden obtener otras proposiciones. Por ejemplo, cuando afirmamos la veracidad del teorema de Pitágoras, queremos decir simplemente que se puede deducir a partir de los axiomas de la geometría plana de Euclides. No se verifica, por ejemplo, para triángulos en una superficie esférica.

Se define como "argumento" o razonamiento lógico un proceso que permite deducir una proposición llamada conclusión a partir de un conjunto de proposiciones llamadas premisas.

Se define como argumento o razonamiento *válido* aquel en que la conjunción de las premisas implica la conclusión.

Es decir, matemáticamente un razonamiento que produce una conclusión r a partir de las premisas $p_1, p_2, \ldots p_n$ será válido *si y solamente si* la proposición $(p_1, p_2, p_3 \ldots p_n) \rightarrow r$ *es una tautología.*

En general hay tres maneras de comprobar la validez de un argumento dado:

a) Comprobarlo directamente a partir de la definición usando una tabla de verificación, esto es, para demostrar que $(p_1, p_2, \ldots p_n) \rightarrow r$ es una tautología.
b) Demostrar que la proposición $(p_1, p_2, \ldots p_n) \rightarrow r$ puede reducirse a 1, usando los métodos normales de simplificación de funciones mediante el cálculo booleano.
c) A menudo la más sencilla de las tres, es reducir el argumento a una serie de argumentos, cada uno de los cuales previamente ha sido comprobada su validez por cualquiera de los métodos a) y b).

Dos de los argumentos usados normalmente son *la regla de desprendimiento* o *modus ponens* y la ley del silogismo.

La regla de desprendimiento viene dada por la forma

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline q \end{array}$$

En esta notación, que se empleará en lo sucesivo, se presentan primeramente las premisas y la conclusión debajo de una línea horizontal. Pueden escribirse comentarios a la derecha de cada proposición.

La ley del silogismo tiene la forma

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline p \rightarrow r \end{array}$$

La validez de ambos razonamientos se comprueba por el procedimiento b), a continuación.

1.º *Modus ponens*

Deberá ser una tautología:

$$p.(p \to q) \to q$$

Operando, esta expresión equivale a:

$$p.(p' + q) \to q$$

Teniendo en cuenta que $pp' = 0$, resulta

$$pq \to q$$

lo que equivale a

$$(pq)' + q = p' + q' + q = p' + 1 = 1.$$

2.º *Silogismo*

Análogamente, deberá ser una tautología:

$$\begin{aligned}
&(p \to q)(q \to r) \to (p \to r) \\
&(p' + q)(q' + r) \to (p \to r) = p'q' + p'r + qr \to (p \to r) = \\
&= (p'q' + p'r + qr)' + (p \to r) = \\
&= (p + q)(p + r')(q' + r') + (p' + r) = \\
&= (p + q)(pq' + r') + p' + r = pq' + pr' + qr' + p' + r = \\
&= (p + p')(p' + q') + pr' + qr' + r = p' + q' + pr' + qr' + r = \\
&= p' + q' + (p + q + r)(r + r') = p' + q' + p + q + r = \\
&= 1 + r = 1
\end{aligned}$$

Es importante hacer notar que la validez o no validez de un *argumento es independiente de la veracidad o falsedad de la conclusión.* Por ejemplo, consideremos los dos argumentos siguientes. El primero es válido, aunque la conclusión es falsa, y el segundo no es válido y la conclusión es verdadera.

Válido (modus ponens):

$p \to q$	Si el hielo está templado, entonces la nieve es negra.
p	El hielo está templado.
q	La nieve es negra.

No válido:

p	5 es un entero impar.
$q \rightarrow p$	Si 4 es un entero par, entonces 5 es un entero impar.
q	4 es un entero par.

También puede comprobarse la validez de los argumentos de la tabla siguiente:

Forma 1	Forma 2	Forma 3	Forma 4	Forma 5	Forma 6
p q pq	pq p	p' $p \rightarrow q$	$p+q$ p' q	p $p+q$	q $p \rightarrow q$

7.1. DEMOSTRACIONES INDIRECTAS DE LA VALIDEZ DE RAZONAMIENTOS

Si en un razonamiento lógico las premisas son $p_1, p_2, \ldots p_n$ y la conclusión q, si es válido un argumento que tiene como conclusión la negación p_i' de una cualquiera de las premisas, y como premisas las mismas con la sustitución de p_i por la negación, q' será válido el primer argumento.

Es decir, si

$$p_1\, p_2 \ldots q' \ldots p_n \rightarrow p_i'$$

es una tautología, también lo será

$$p_1\, p_2 \ldots p_i \ldots p_n \rightarrow q$$

En efecto, lo primero implica

$$(p_1\, p_2 \ldots q' \ldots p_n)' + p_i' = 1$$

lo que equivale a

$$(p_1' + p_2' + \ldots p_i' + \ldots p_n') + q = 1$$

Por tanto,

$$p_1\, p_2 \ldots p_i \ldots p_n \rightarrow q = 1$$

Este tipo de prueba de la validez de un razonamiento se llama indirecta, precisamente por apoyarse en otro, y puede ser de interés cuando el razonamiento obtenido, de acuerdo con las reglas anteriores, puede estructurarse como secuencia de razonamientos cuya validez se conoce.

Ejemplo

Comprobar la validez del siguiente argumento:

$$\begin{array}{l} p \\ pq \rightarrow r + s \\ q \\ s' \\ \hline r \end{array}$$

Solución: Tomaremos como premisas todas excepto s', y la negación de la conclusión. El argumento indirecto, por pasos, es como sigue:

p	premisa
q	premisa
———	
pq	forma 1 del cuadro anterior
$pq \rightarrow r + s$	premisa
$r + s$	conclusión por ley de desprendimiento
r'	premisa
———	
s	por forma 4 del cuadro

Pero esta conclusión es la negación de una de las premisas s' en el argumento directo; por lo tanto, éste es válido.

7.2. CONTRAEJEMPLO

Hay un tipo de pruebas especiales para demostrar que una implicación dada es falsa. El método trivial es demostrar que la negación de la implicación dada es cierta. No obstante, si la implicación concierne a propiedades de un conjunto de objetos, a menudo es sencillo rechazar la validez de la implicación mostrando un elemento específico del conjunto para el cual la proposición es falsa. Este procedimiento de comprobación se llama contraejemplo.

8. *Operaciones NAND y NOR*

Son éstas dos operaciones lógicas que permiten la expresión en función de ellas de las operaciones de conjunción, disyunción y negación; a continuación se describen ambas.

La operación NAND, también llamada anticonjunción u operación de Sheffer, se representa mediante un trazo vertical (trazo de Sheffer). Su tabla de verdad es:

p	q	$p \mid q$
1	1	0
1	0	1
0	1	1
0	0	1

El significado de $p|q$ es "no ambos p y q".

La representación en forma normal conjuntiva es, de acuerdo con la anterior tabla de verdad:

$$p|q = p' + q'$$

Por tanto,

$$p|p = p' + p' = p' \tag{1}$$
$$p + q = (p')' + (q')' = p'|q' = (p|p)|(q|q) \tag{2}$$
$$pq = (p' + q')' = (p|q)' = (p|q)|(p|q) \tag{3}$$

Las fórmulas (1), (2) y (3) muestran cómo las operaciones de negación de conjunción y disyunción pueden expresarse en función de NAND.

La operación NOR, también llamada antidisyunción u operación de Pierce, se representa mediante una flecha ↓ (flecha de Pierce). Su tabla de verdad es:

p	q	$p \downarrow q$
1	1	0
1	0	0
0	1	0
0	0	1

La significación de $p \downarrow q$ puede entenderse como "ni p ni q".

La expresión en forma normal disyuntiva de $p \downarrow q$, de acuerdo con la tabla anterior, es:

$$p \downarrow q = p'q'$$

Por tanto,

$$p \downarrow p = p'p' = p' \tag{4}$$

y teniendo en cuenta esto,

$$p + q = (p'q')' = (p \downarrow q)' = (p \downarrow q) \downarrow (p \downarrow q) \tag{5}$$
$$pq = (p')'(q')' = p' \downarrow q' = (p \downarrow p) \downarrow (q \downarrow q) \tag{6}$$

Las expresiones (4), (5) y (6) muestran cómo pueden ponerse en función de NOR las operaciones de negación, disyunción y conjunción.

Existen otras notaciones para estas operaciones. En algunos casos, para NAND se emplea ↓ y para NOR ↑.

Un conjunto de operaciones es funcionalmente completo cuando toda función proposicional puede expresarse enteramente en terminos relacionados por operaciones del conjunto. Para dar un conjunto funcionalmente completo, recordamos que *toda función proposicional tiene una tabla de verificación.* Más todavía, *toda tabla de verificación corresponde a una expresión en forma normal disyuntiva* (o conjuntiva), *usando solamente las operaciones* (+), (.) *y* (′). Por tanto, el conjunto $\{+ \ldots ')\}$ *es funcionalmente completo.*

Puesto que la proposición pq es igual a la proposición $(p' + q')'$ por la ley de De Morgan, es posible reemplazar la conjunción en cualquier función proposicional por una expresión equivalente con $(+)$ y $(')$. Esto demuestra que $\{+, '\}$ es un conjunto de operaciones funcionalmente completo. Otros conjuntos funcionalmente completos son: $\{.,'\}$ y $\{\rightarrow,'\}$.

En el caso particular de NOR y NAND puede demostrarse que son éstos los dos únicos conjuntos de operaciones funcionalmente completos con una sola operación.

9. *Tratamiento por cálculo proposicional de organigramas y tablas de decisión*

Las tablas de decisión constituyen una forma de expresar un proceso de selección de alternativas a partir de una serie de condiciones.

Una tabla de decisión tiene la siguiente estructura:

Lista de condiciones	Cuadro de posibilidades lógicas de condición
Lista de acciones posibles a tomar.	Cuadro de selección de acciones posibles.

Pueden ser de tres tipos: De entrada limitada.
De entrada extendida.
De entrada mixta.

Las tablas de entrada limitada son las de uso más generalizado. En ellas el juego de condiciones se organiza de forma que las posibilidades de contestación a cada una sean sí o no. Asimismo, el cuadro de acciones posibles es amplio, correspondiendo a cada acción una serie de condiciones para su realización.

Las tablas de entrada extendida presentan un juego de condiciones más reducido, pero para cada condición caben varias alternativas lógicas (no únicamente dos, como en el caso de entrada limitada). Asimismo, el juego de acciones es un único renglón constituido por una única variable que puede adoptar distintos estados para cada posibilidad lógica.

Las tablas mixtas son aquellas que participan de ambas posibilidades.

Ejemplos

Supongamos que en función de la raza (blanca, negra y amarilla), el sexo y la categoría profesional decidimos sobre una gama de acciones posibles (1, 2, 3, 4). La tabla de entrada extendida sería:

Raza	*B*	*B*	*B*	*N*	*N*	*N*	*A*	*A*	*A*	*B*	*B*	*B*	*N*	*N*	*N*	*A*	*A*	*A*
Sexo	*V*	*V*	*V*	*V*	*V*	*V*	*V*	*V*	*V*	*H*	*H*	*H*	*H*	*H*	*H*	*H*	*H*	*H*
Categoría	*A*	*B*	*C*	*A*	*B*	*C*	*A*	*B*	*C*	*A*	*B*	*C*	*A*	*B*	*C*	*A*	*B*	*C*
Acción	1	1	2	3	3	4	1	1	1	3	1	4	1	1	2	3	4	1

La de entrada limitada sería (en número de condiciones es superior al de la extendida; obsérvese que no son 2^8, ya que sólo pueden ser de una raza, un sexo y una categoría, por lo que las posibilidades lógicas se restringen).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Raza blanca	1	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Raza negra	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0	0	0
Raza amarilla	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1
Varón	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
Hembra	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
Categoría A	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
Categoría B	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0
Categoría C	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1
Acción 1	X	X					X	X	X		X		X	X				X
Acción 2			X												X			
Acción 3				X	X					X						X		
Acción 4						X						X					X	

1 – sí 0 – no

Suele hacerse también la tabla poniendo *si* o *no* en vez de 1 y 0.

Supongamos que queremos procesar una orden de suscripción a una revista. Esta puede ser de tipo normal o fruto de promoción, la suscripción puede ser por un año o dos años y puede acompañar el pago o no y el tipo de entrega es certificado o por correo normal. Las acciones a realizar son:

Incluir en el fichero promoción.
Incluir en el fichero normal.
Incluir en el fichero un año.
Incluir en el fichero dos años.
Incluir en el fichero pagado.
Incluir en el fichero a facturar.
Incluir en el fichero envío certificado.
Incluir en el fichero envío corriente.

Las decisiones dependen de la concurrencia de condiciones de acuerdo con la tabla siguiente:

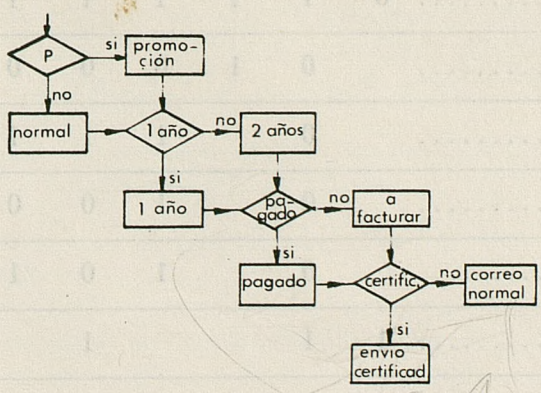
(Ponemos 1 – sí 0 – no)

C	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Promoción	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
Por un año	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
Pagado	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
Envío certificado	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
Incluir promoción	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
Incluir normal	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Incluir un año	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
Incluir dos años	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
Inclucir pagado	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
Incluir a facturar	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Incluir envío certificado	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
Incluir envío curriente	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

El organigrama correspondiente se indica en la figura.

En este caso el esquema lógico es sencillo y el número de consultas es el estrictamente necesario. En efecto, si llamamos a las condiciones p, q, r, s, y a las acciones A1, A2, A3, A4, A5, A6, A7, A8, las expresiones de cada una de estas acciones en función de las condiciones son:

$$A_1 = p \qquad A_2 = p'$$
$$A_3 = q \qquad A_4 = q'$$
$$A_5 = r \qquad A_6 = r'$$
$$A_7 = s \qquad A_8 = r'$$



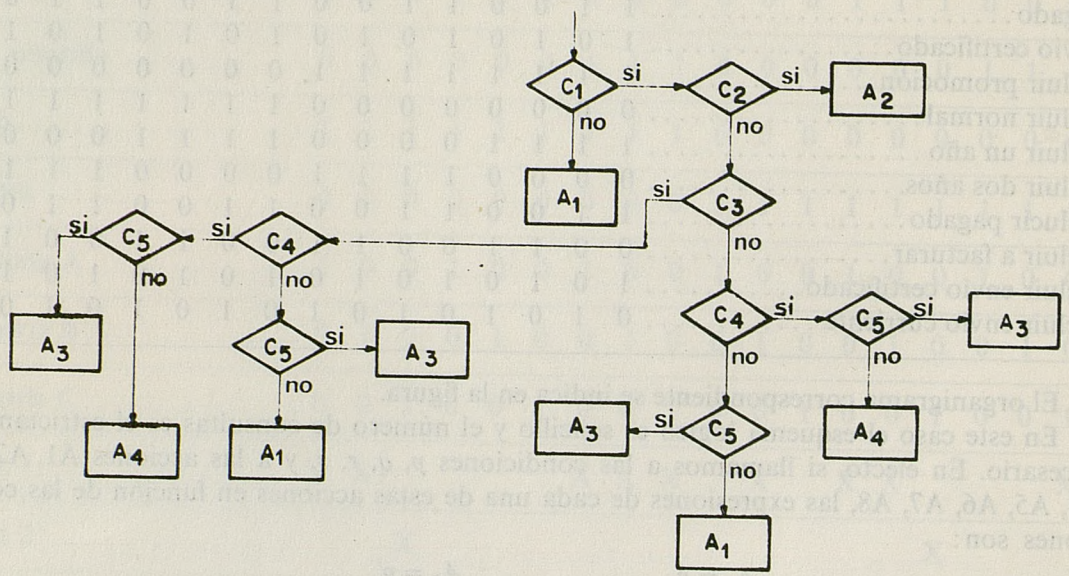
Es decir, las acciones aparecen en la forma más simplificada posible, y por tanto, el esquema lógico es el más simple posible.

Sin embargo, ese no es el caso más usual. La tabla de decisión, al establecer una relación lógica entre las acciones y las condiciones, permite, utilizando las reglas del cálculo proposicional, la simplificación de los procesos lógicos. Sea el ejemplo indicado en la figura de

organigrama de partida, en el que se preveen cinco condiciones y cuatro acciones de acuerdo con la estructura indicada. Las acciones se designan por A_i y las condiciones por C_i.

A continuación, de acuerdo con el proceso lógico del organigrama, se ha diseñado la tabla de decisión de entrada limitada correspondiente. Para ello basta atribuir a cada salida del organigrama una columna de la tabla de decisión (en nuestro caso, al haber diez salidas, habrá diez reglas en la tabla).

Se supone que en el organigrama están todas las posibilidades lógicas que dan lugar a acción; todas las demás dan cero a todas las acciones.



		1	2	3	4	5	6	7	8	9	10
x	Condición 1.	0	1	1	1	1	1	1	1	1	1
y	Condición 2.		0	1	0	0	0	0	0	0	0
z	Condición 3.		0		1	1	1	0	0	0	1
t	Condición 4.		0		1	0	0	1	0	1	1
u	Condición 5.		0		1	0	1	1	1	0	0
	Acción 1.	1	1			1					
	Acción 2.			1							
	Acción 3.				1		1	1	1		
	Acción 4.									1	1

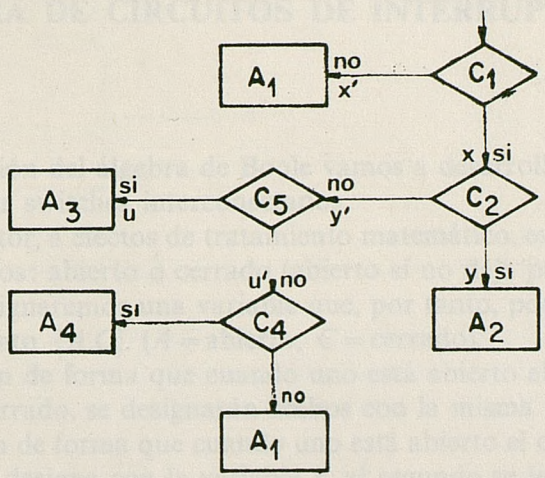
$$A_1 = x' + xy'z't'u' + xy'zt'u' = x' + xy't'u'$$
$$A_2 = xy$$
$$A_3 = xy'ztu + xy'zt'u + xy'z'tu + xy'z't'u = xy'zu + xy'z'u = xy'u$$
$$A_4 = xy'ztu' + y'z'tu' = xy'tu'$$

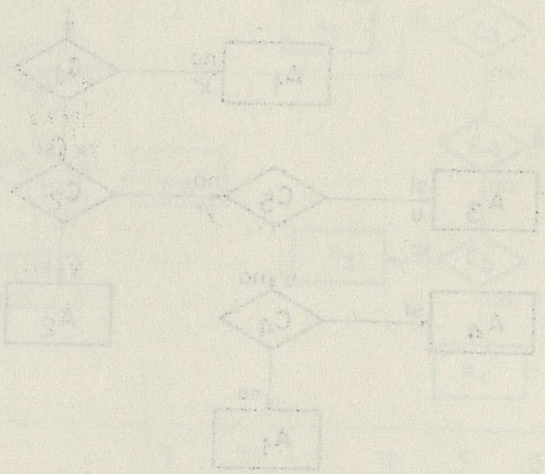
Por tanto, la condición z puede eliminarse.

Por otro lado, podemos organizar el organigrama de forma que se consulten primero las funciones de una, dos, tres, cuatro variables; es decir, consultaremos los términos

$$x',\ xy,\ xy'u,\ xy't'u',\ xy'tu'$$

De acuerdo con ello, resulta el organigrama adjunto mucho más simple que el inicial.





CAPITULO V

ALGEBRA DE CIRCUITOS DE INTERRUPTORES

1. *Definiciones*

Como tercera aplicación del álgebra de Boole vamos a desarrollar el tratamiento de los circuitos constituidos por switches interconectados.

Un switch, o interruptor, a efectos de tratamiento matemático, es un elemento que puede encontrarse en dos estados: abierto o cerrado (abierto si no deja pasar corriente y cerrado en caso contrario). Le asignaremos una variable que, por tanto, podrá tomar como valores los elementos del conjunto $\{A,C\}$ (A = abierto, C = cerrado).

Si dos switches actúan de forma que cuando uno está abierto el otro también, y análogamente en el caso de cerrado, se designarán ambos con la misma variable.

Si dos switches actúan de forma que cuando uno está abierto el otro está cerrado, y viceversa, si al primero se le designa con la variable x, al segundo se le asignará la variable x', o viceversa.

Dado un conjunto de switches interconectados, pueden definirse sobre el mismo dos puntos cualquiera como terminales. Como consecuencia de ella, para cada configuración de estados de los switches corresponderá un estado del circuito entre ambos terminales; es decir, estará abierto o cerrado.

En el estudio que sigue se desarrollará un método matemático de tratar los estados de los circuitos a partir de los de los switches que lo integran.

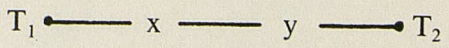
2. *Conexión de interruptores*

Vamos a estudiar el estado de un circuito de dos terminales constituido por dos switches en serie y paralelo.

2.1. CONEXION EN SERIE

Se define la variable correspondiente al estado del circuito como resultado de una operación que designaremos con el signo (.).

x	y	$x.y$
A	A	A
A	C	A
C	A	A
C	C	C

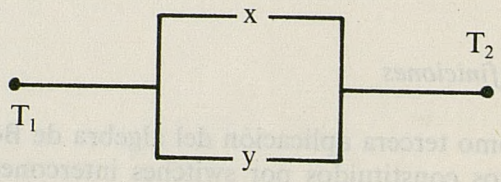


ya que si dos switches están en serie para que el circuito deje pasar la corriente se precisa que ambos estén cerrados.

2.2. CONEXION EN PARALELO

En este caso, para que el circuito esté cerrado, basta con que uno de los switches esté cerrado. Designaremos esta operación con el signo (+), la tabla de resultados será la siguiente:

x	y	$x+y$
A	A	A
A	C	C
C	A	C
C	C	C



3. *Función booleana correspondiente a un circuito serie-paralelo*

A partir de las tablas de definición de las operaciones (.) y (+), y teniendo en cuenta la definición de switch opuestos mediante la operación (′) dada en el apartado 1, la estructura constituida por el conjunto $\{A,C\}$ con las operaciones (+) (.) y (′) definidas por

+	A	C
A	A	C
C	C	C

.	A	C
A	A	A
C	A	C

$A' = C$
$C' = A$

es un álgebra de Boole, ya que el sistema es análogo al formado por las conectivas lógicas conjunción, disyunción y negación sobre el conjunto {verdadero o falso}, en el álgebra proposicional, que, como ya se vio en el capítulo IV, es un álgebra de Boole. En nuestro caso, $A = 0$ $C = 1$.

Por tanto, dado un circuito de switches conectados en serie-paralelo, si conocemos los estados del circuito para todas las combinaciones posibles de estados de los switches que lo integran, podremos de manera análoga al caso de funciones proposicionales obtener una función booleana de las variables correspondientes a los switches, bien en forma normal disyuntiva o conjuntiva. La función así obtenida representa el circuito serie paralelo entre los dos terminales definidos.

Dos circuitos son equivalentes si, para todas las combinaciones posibles de estados de los switches que los integran, se encuentran en el mismo estado.

Por tanto, dos circuitos serie-paralelo equivalentes tendrán iguales funciones booleanas representativas de los mismos.

Recíprocamente, dos funciones booleanas iguales se representarán por circuitos equivalentes. Por tanto, para simplificar un circuito bastará simplificar la función booleana que le representa y una vez verificada diseñar el circuito correspondiente a ésta. De acuerdo con lo anterior, el nuevo circuito será equivalente al anterior y más simple (lo que, en general, se traducirá en una mayor economía).

4. *Metodos de simplificación de circuitos.*

La importancia industrial de la simplificación de circuitos hace que se hayan desarrollado métodos sistemáticos para su realización, ya que cuando el número de variables es grande, así como el número de términos de la función, el ojo experimentado del calculista no garantiza la simplificación total de una función. Los métodos que se estudiarán son los de Karnaugh, procedimiento gráfico, y de McCluskey, procedimiento numérico sistemático que constituye en sí un algoritmo programable para su cálculo en ordenador.

4.1. METODO DE KARNAUGH

Este procedimiento es válido hasta 5 variables. Consiste en representar mediante un cuadro de doble, triple o cuádruple entrada todos los posibles términos en forma normal disyuntiva. En los cuadros adjuntos pueden verse los correspondientes cuadros o mapas de Karnaugh correspondientes a 1, 2, 3, 4 y 5 variables. Un término de la función en forma normal disyuntiva viene representado por un cuadro del mapa y está formado por el producto de las variables que representan la fila y columna que inciden en él. Así, en el mapa de Karnaugh correspondiente a cuatro variables el término correspondiente a la celda indicada con una cruz es $xy'z'w'$.

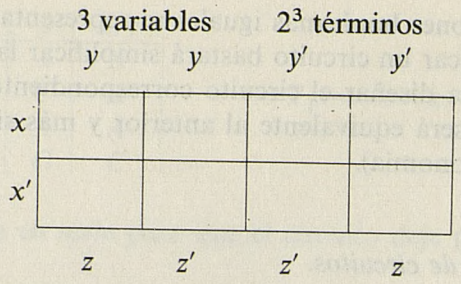
1 variable — 2^1 términos

x	x'

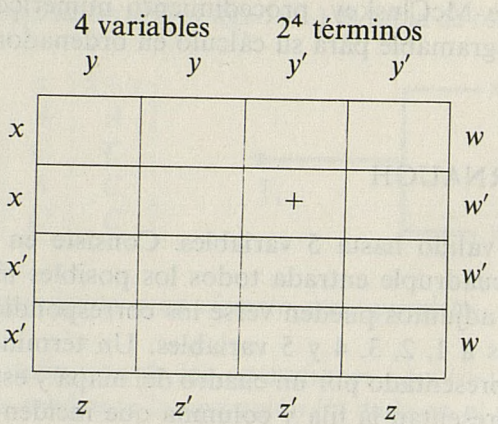
2 variables — 2^2 términos

	y	y'
x		
x'		

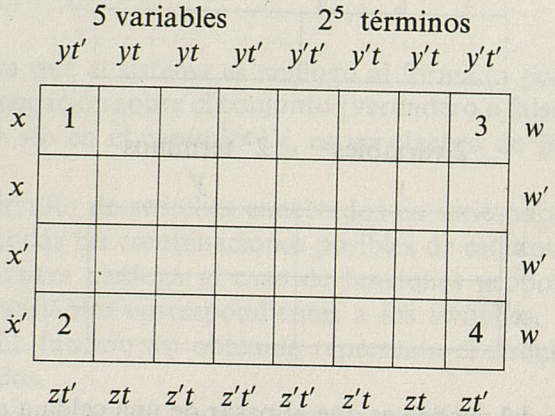
La regla de formación del cuadro es que al pasar de una celda a *otra adyacente sólo haya una variable que cambie de no estar complementada a estarlo, o viceversa, se consideran adyacentes o contiguos los bordes del cuadro.* Así, las celdas indicadas, en el cuadro correspondiente a cinco variables, con los números 1, 2, 3 y 4, son contiguas.



El procedimiento de utilización del mapa de Karnaugh para simplificar funciones booleanas en forma normal disyuntiva consiste en representar cada uno de los términos de la función por una celda en el cuadro y a continuación cubrir el conjunto de celdas afectadas por el menor número posible de rectángulos que comprendan celdas contiguas.



A cada rectángulo comprendiendo dos celdas contiguas corresponde un término con una variable menos (precisamente la única, por hipótesis de construcción del mapa, que cambia de estado al pasar de una a otra celda), formado por el producto de las variables con estados iguales en ambas celdas.



A cada rectángulo que comprende cuatro celdas contiguas le corresponde un único término con dos variables menos, precisamente aquellas que cambian de estado, y formado por el producto de las variables cuyos estados son comunes a las cuatro celdas.

Como ejemplo de aplicación, supongamos la función

$$f = xyzw + xyzw' + xyz'w' + x'yzw + x'yzw' + xy'z'w' + x'y'z'w'$$

Numerando los términos por el orden de aparición en la expresión, su representación en el mapa de Karnaugh es la indicada en la figura.

	y	y	y'	y'	
x	1				w
x	2	3	6		w'
x'	5		7		w'
x'	4				w
	z	z'	z'	z	

A efectos de simplificación pueden trazarse los rectángulos:

$$1-2-5-4$$
$$3-6$$
$$6-7$$

En el primer rectángulo, por corresponder a cuatro celdas contiguas, las variables que cambian de estado son x y w. Por tanto, equivale al término yz.

El segundo corresponde a $xw'z'$, y el tercero, a $y'z'w'$.

Obsérvese que, por la propiedad de absorción, puede incluirse un término dos veces. Por tanto, una forma simplificada de f será:

$$f = yz + xw'z' + y'w'z'$$

Otra posibilidad sería asociar el término 3 al 2, adoptándose los rectángulos

$$1-2-5-4$$
$$2-3$$
$$6-7$$

Con ello, otra forma de f con términos de segundo y tercer orden sería

$$f = yz + xyw' + y'z'w'$$

4.2. METODO DE MC CLUSKEY

Este procedimiento permite un tratamiento numérico de las funciones booleanas a efectos de su simplificación. Para ello parte de un método de representación de los términos

de la función y un proceso de simplificación. A continuación se describen ambos procedimientos.

4.2.1. Representación de los términos y la función

Se supone la función en forma normal disyuntiva, y por tanto todos los términos tendrán igual número de variables. Supuesto un orden entre ellas, se hará corresponder a cada variable si está en forma complementada, 0, y en caso contrario, 1. De acuerdo con este criterio, a cada término de la función se le hace corresponder un número en binario. Así, por ejemplo, al término $x'yzw't$ le corresponderá 01101.

Por tanto, una función booleana puede definirse por el orden de las variables y un conjunto de números binarios.

Por ejemplo, si el orden de las variables es x, y, z, t, la función f representada por

$$f = (0011, 0101, 0001, 1100, 1010)$$

Será en forma normal disyuntiva,

$$f = x'y'zt + x'yz't + x'y'z't + xyz't' + xy'zt'$$

Otra forma de representar una función es dar los números binarios representativos de sus términos en forma decimal; así, la función del ejemplo anterior puede representarse también en la forma:

$$f = (1, 3, 5, 10, 12)$$

4.2.2. Proceso sistemático de tratamiento

Representados los términos en forma binaria, el proceso a seguir es el siguiente:

1.º Se ordenan los términos en grupos según el número de "unos" con que cuentan. Así, en el grupo I se introducirán los que están formados por ceros; en el II, los que tienen solamente un "uno"; en el III, los que tienen dos, etc.

2.º Se compara cada término de un grupo con los del grupo siguiente y simplifican aquella que tengan iguales todas las cifras excepto una, suprimiendo precisamente este elemento distinto. Por ejemplo, si estamos comparando el grupo II con el III y dentro de ellos los elementos 0100 y 0101, se sustituirá en el grupo II 0100 por 010–. Esto equivale a prescindir de la última variable, ya que 0100 es $x'yz't'$ y 0101 es $x'yz't$, con lo que ambos pueden englobarse en el término $x'yz'$, teniendo en cuenta que $t + t' = 1$.

Como consecuencia de este proceso aparecerán en cada grupo elementos que no han podido englobar elementos del grupo inmediato y otros que sí incluyen términos del siguiente y que, por tanto, tienen algún guión en la posición correspondiente a la cifra simplificada.

Por el hecho de que un término de un grupo intermedio haya sido englobado en uno del grupo anterior, no debe eliminarse en su grupo, y debe utilizarse para ser comparado con los términos del grupo siguiente.

En cambio, de los elementos del último grupo se eliminarán los que se hayan podido englobar en los del anterior.

3.º Se aplica el mismo proceso que en 2.º en una nueva iteración, pero comparando ahora los términos de un grupo con los del siguiente que tengan guión en la misma posición.

Se realiza este proceso tantas veces como sea necesario hasta llegar a una situación en que, comparando cada término de un grupo con los del siguiente, no pueda hacerse ninguna simplificación.

En este momento se ha reducido el conjunto de términos iniciales a una serie de términos *con* y *sin* guiones que engloban a los de partida llamados implicantes primos, puesto que no son simplificables entre sí; cada uno de ellos incluirá varios de los términos de partida, incluso un término de los de partida podrá aparecer englobado en varios implicantes primos a la vez. La función de partida será igual a la formada por los implicantes primos encontrados por el proceso anterior. Sin embargo, debido a que dichos implicantes pueden contener varias veces a los términos de partida para representar a éstos no se precisará utilizar todos ellos, bastará, por tanto, seleccionar entre todos los implicantes primos el menor número de ellos que engloban a todos los términos de la función de partida.

4.º Para definir un proceso sistemático de selección del subconjunto de implicantes primos más simple que comprende a la totalidad de los términos de la función de partida, se utiliza un cuadro de doble entrada (para proceso con ordenador sería una matriz), en el que por un lado (borde horizontal) se indican los términos de partida y en el otro los implicantes primos. Para indicar que un implicante primo comprende a un término de la función primitiva, se incluye un asterisco en la columna correspondiente a ambos.

Para elegir el grupo de implicantes primos que comprende a todos los términos, se procederá en la forma siguiente:

Se eligen en primer lugar los implicantes primos correspondientes a los términos de la función que aparecen solamente en un implicante primo y cuya elección por tanto es obligatoria, ya que, de no incluirse, la función resultante no englobaría todos los términos.

Una vez elegidos estos implicantes se suprimen las columnas correspondientes a los términos de la función incluidos en ellos. A continuación se van seleccionando nuevos implicantes primos en orden preferente por el número de términos que engloban, cada vez que se selecciona uno se tachan las columnas correspondientes a los términos incluidos en él. Se continúa con el proceso hasta que se tachan todas las columnas. Cuando varios términos implicantes primos engloban el mismo número de términos de la función de partida el criterio indicado de selección es ambiguo, y lo que puede hacerse es estudiar tantas alternativas como términos de características análogas aparezcan simultáneamente en un momento del proceso y seleccionar la más interesante según el resultado final.

El proceso se ilustra con el ejemplo siguiente:

Simplificar la función de x, y, z, t:

$$f = (0, 1, 2, 3, 4, 6, 7, 8, 9, 11, 15)$$

En el cuadro adjunto se presenta la organización en cinco grupos de los distintos términos con la notación binaria y decimal. Se aplica el proceso descrito, que tiene dos etapas, resultando como implicantes primos los términos *A*, *B*, *C*, *D*, *E*, *F*. En el cuadro, como resultado de cada iteración, se indican los términos que engloba de la función primitiva, descritos éstos en forma decimal. Así, el implicante *A* engloba los términos 0, 1, 2, 3.

A partir de esta información se construye el cuadro de doble entrada que relaciona los implicantes y los términos de partida.

Dado que los términos 4 y 15 aparecen en un único implicante, debe obligatoriamente seleccionarse aquellos que los contienen, es decir, *B* y *F*.

Una vez seleccionados *B* y *F*, se rayan las columnas de los términos que contienen; de los implicantes restantes, el que engloba más términos es el *C*; una vez seleccionado *C*, pueden rayarse todas las columnas, con lo que el proceso puede darse por terminado y la expresión simplificada de la función es *B*, *C*, *F*, o sea

$$x't' + y'z' + zt$$

ESTADO INICIAL			1.ª ITERACION		2.ª ITERACION		
Grupo	Número decimal	Número binario	Notación decimal	Notación binaria	Notación decimal	Notación binaria	Nombre del implicante
I	0	0000	0,1	000–	0,1,2,3	00––	*A*
			0,2	00–0	0,2,4,6	0––0	*B*
			0,4	0–00	0,4,2,6	0––0	*B*
			0,8	–000	0,1,8,9	–00–	*C*
II	1	0001	1,3	00–1	2,3,6,7	0–1–	*D*
	2	0010	2,3	001–	1,3,9,11	–0–1	*E*
	4	0100	2,6	0–10	2,6,3,7	0–1–	*D*
	8	1000	4,6	01–0			
			8,9	100–			
III	3	0011	3,7	0–11	3,7,11,15	––11	*F*
	6	0110	3,11	–011	3,11,7,15	––11	*F*
	9	1001	6,7	011–			
			9,11	10–1			
IV	7	0111	7,15	–111			
	11	1011	11,15	1–11			
V	15	1111					

Términos implicantes	0	1	2	3	4	6	7	8	9	11	15
A	*	*	*	*							
B	*		*		*	*					
C	*	*						*	*		
D			*	*		*	*				
E		*		*					*	*	
F				*			*			*	*

5. *Circuito de varios terminales*

En los apartados anteriores hemos comprobado como a un circuito de dos terminales le correspondían una función booleana siempre que este circuito estuviera formado por conexiones en serie y paralelo. Cabe estudiar el comportamiento de los circuitos en los que se definen más de dos terminales y cuyas conexiones pueden no estar en serie y paralelo.

En general un circuito de n terminales se define como un conjunto de switches interconectados entre sí, en los cuales se han definido una serie de puntos como terminales del circuito.

Para estudiar los circuitos de varios terminales no solamente se precisará una función booleana, sino que serán necesarias tantas como pares de terminales se puedan elegir entre las n existentes, es decir, si en un circuito se han definido n terminales, el número de funciones booleanas correspondientes será $\frac{n(n-1)}{2}$.

Dos circuitos de n terminales serán equivalentes si son iguales las funciones representativas de cada pareja de terminales, es decir, si tenemos un circuito con 4 terminales T_1, T_2, T_3, T_4, que comprenden los switches $xyzw$, en el primer circuito podrán definirse las funciones $f_{12}(x,y,z,w)$, $f_{13}(x,y,z,w)$, $f_{14}(x,y,z,w)$, $f_{23}(x,y,z,w)$, $f_{24}(x,y,z,w)$ y $f_{34}(x,y,z,w)$.

Asimismo, en el otro circuito podrán definirse las funciones $g_{12}(x,y,z,w)$, $g_{13}(x,y,z,w)$, $g_{14}(x,y,z,w)$, $g_{23}(x,y,z,w)$, $g_{24}(x,y,z,w)$ y $g_{34}(x,y,z,w)$.

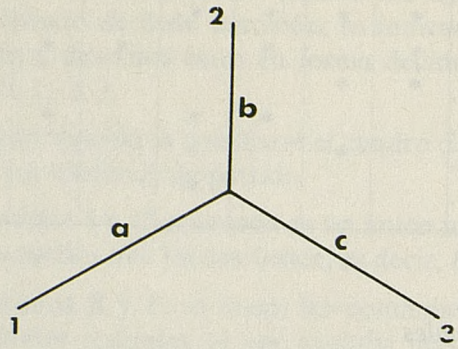
Para que sean equivalentes estos circuitos, por definición tendrá que verificarse $f_{ij} = g_{ij}$ para todo i,j.

Un circuito de n terminales puede sustituirse por otro equivalente, de acuerdo con la definición anterior, ya que ambos se comportarán de la misma forma para iguales estados de los switches, lo que permite su aplicación para la sustitución de los tipos de conexión entre los switches de forma que puedan pasarse a una conexión en serie paralelo de los mismos switches a partir de otra que no está en esa forma. Un ejemplo de este tipo de sustitución es el caso de estrella triángulo que se detalla a continuación.

En una conexión en estrella como la indicada en la figura nos encontramos con un circuito formado por tres terminales, T_1, T_2 y T_3, con un punto triple al cual están conectados los tres terminales, encontrándose situados en cada uno de los ramales de conexión un switch de los tres existentes en el circuito a,b,c.

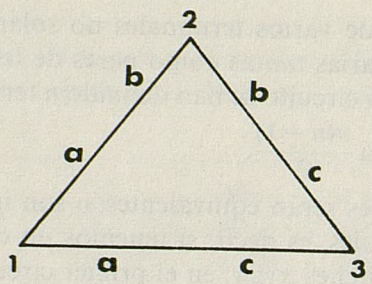
Puede sustituirse este circuito entre los mismos tres terminales por una conexión en triángulo de los mismos switches, de la forma indicada en la figura, siendo entonces la co-

nexión en triángulo un circuito equivalente al primero con los switches que aparecen en la figura.



En efecto, las funciones booleanas entre cada pareja de terminal en el circuito estrella son las siguientes:

$$f_{12} = ab$$
$$f_{13} = ac$$
$$f_{23} = bc$$



En la conexión en triángulo dispuesto tal como se indica en la figura, las funciones booleanas son las siguientes:

$$f_{12} = ab + bc.ca = ab + abc = ab$$
$$f_{13} = ac + abbc = ac + abc = ac$$
$$f_{23} = bc + baac = bc + bac = bc$$

Vemos, por tanto, que las funciones representativas son iguales y, por tanto, ambos circuitos son equivalentes. Este resultado puede aplicarse de manera sucesiva a la reducción de nudos con conexiones múltiples en circuitos complejos, haciendo progresivas sustituciones de estrellas por los correspondientes circuitos en triángulo, con lo que se va reduciendo de los grados la multiplicidad de los nudos.

6. *Función booleana correspondiente a un circuito de switches no conectados en serie paralelo*

Dado un circuito de switches interconectados en forma cualquiera con dos terminales definidos sobre el mismo, puede definirse una función booleana que represente el compor-

tamiento de dicho circuito relativo a los dos terminales; para ello pueden seguirse los tres métodos siguientes: Método de los caminos, método de los cortes y método de sustitución progresiva de nudos múltiples.

Los dos primeros procedimientos son métodos, en una cierta medida, de tanteo, y el único procedimiento sistemático es el tercero de reducción progresiva de nudos múltiples aplicando la sustitución estrella triángulo descrita en el apartado anterior. A continuación se describen en líneas generales las características en cada uno de estos procedimientos.

6.1. METODO DE LOS CAMINOS

Este procedimiento consiste en describir todas las secuencias de switch que conducen de un terminal a otro. El procedimiento tiene que ser lo suficientemente sistemático como para estar seguro de que se han descrito todos los caminos posibles de acceso desde el terminal de origen al terminal de salida.

Una vez obtenidas todas las secuencias de switches que conducen de un terminal al otro, la función booleana correspondiente puede formarse mediante la suma de los productos de los switches integrantes de cada camino.

En efecto, la función booleana formada de esta manera se comporta, en cuanto a la representación del circuito, de la misma forma que éste, ya que cualquier combinación de valores 1 de los switches integrantes correspondientes a un camino dará 1 como valor de la función, por estar todos los switches en forma de producto en un término, que tomará, por tanto, el valor 1. Sin embargo, cualquier otra combinación de switches que no haga 1 todos los integrantes al menos de uno de los términos, hará 0 el valor de la función, ya que en cada término habrá al menos un factor 0 que, por tanto, hará nulo el valor del mismo. La función obtenida de esta forma se comporta en cuanto a representación del circuito igual que éste, ya que vale 0 en las mismas condiciones de situación de los switches que abren en el circuito, y vale 1 para las situaciones de los switches que lo cierran.

6.2. METODOS DE LOS CORTES

El método de los cortes consiste en obtener todos los grupos de switches cuya apertura simultánea impida el paso de la corriente en el circuito, es decir, lo ponen en estado abierto entre los dos terminales.

Debe aplicarse un procedimiento sistemático que asegure que se han obtenido todos los cortes posibles. Una vez seleccionados todos los grupos de switches que corten el circuito, la función booleana correspondiente estará formada por el producto de las sumas de todos los switches de cada grupo.

La función construida de esta forma representa el comportamiento del circuito en todos los casos posibles. En efecto, cualquier juego de valores de los switches que hace 0, las integrantes de un factor cerrarán el circuito y por hipótesis de formación de los factores hará el valor de la función 0, ya que uno de sus factores será nulo. Inversamente, cualquier combinación de valores de los switches que no anule ningún factor dará 1 como valor de la función, ya que todos sus factores valdrán 1.

Como cada uno de los factores representa una de las posibilidades de cierre y en conjunto todos los factores representan todas las posibilidades de cierre, la función construida

se comporta exactamente igual que el circuito, tomando valores 0 cuando éste está abierto y 1 cuando está cerrado.

6.3. METODO DE REDUCCION DE NUDOS MULTIPLES

Este método, si bien en algunos casos puede ser más prolijo que los dos anteriores, tiene la ventaja de que al ser sistemático asegura la resolución de los problemas sin las dudas que puedan presentarse en los dos anteriores como consecuencia del procedimiento de enumeración de posibles caminos o las posibilidades de corte.

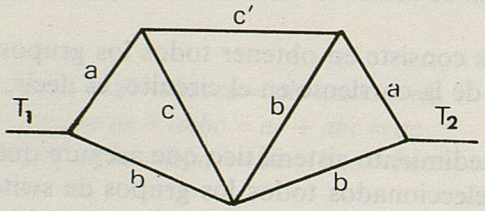
Consiste este procedimiento fundamentalmente en ir sustituyendo cada uno de los nudos múltiples, aplicando la sustitución estrella triángulo para circuito de tres terminales de forma sucesiva.

Para ello se seleccionan tres puntos interiores al circuito como terminales, que estén conectados a un nudo múltiple, y este circuito inmediatamente se sustituirá por el equivalente conectado en triángulo con los mismos terminales; de esta forma el nudo central quedará reducido una unidad en su grado. Actuando de esta manera sucesivamente se podrá llegar a configurar un circuito en el cual todos los nudos son de grado 2 y, por tanto, es un circuito conectado en serie paralelo, que, por haber aplicado sustituciones parciales sucesivas de circuitos equivalentes, será en conjunto equivalente al de partida y, por tanto, para obtener la función booleana correspondiente al primitivo circuito bastará traducir a expresiones booleanas las conexiones en serie-paralelo del circuito equivalente resultante del proceso.

6.4. EJEMPLO DE APLICACION

A continuación se ilustra la aplicación de los tres métodos anteriores a la obtención de la función booleana de un circuito cuyas conexiones no son en serie paralelo.

Sea el circuito de dos terminales de la figura, en el que aparecen interconectados los switches a,b,c; vamos a obtener la función booleana correspondiente al mismo por los tres métodos antes descritos.



1.º Método de los caminos.

Los caminos posibles desde T_1 a T_2 son:

Pasando por a:

1 $ac'a$
2 $ac'bb$
3 acb
4 $acba$

Pasando por b:

5 $bcc'a$
6 $bcc'bb$
7 bba
8 bb

Por tanto, la función booleana correspondiente al circuito será:

$$f = ac'a + ac'bb + acb + acba + bcc'a + bcc'bb + bba + bb.$$

Simplificando los términos nulos y aplicando la ley de idempotencia:

$$f = ac' + ac'b + acb + ab + b = ac' + ab + ab + b = b + ac'.$$

2.º Método de los cortes.

El cierre del paso de corriente entre T_1 y T_2 puede hacerse de las formas siguientes:

a) Cortando dos ramales de conexión:

1 a,b

b) Cortando tres ramales de conexión:

2 bcc'
3 bbc'

c) Cortando cuatro ramales:

4 $acbb$
5 $bcba$

De acuerdo con estos cortes la función booleana correspondiente será:

$$f = (a + b)(b + c + c')(b + b + c')(a + c + b + b)(b + c + b + a),$$

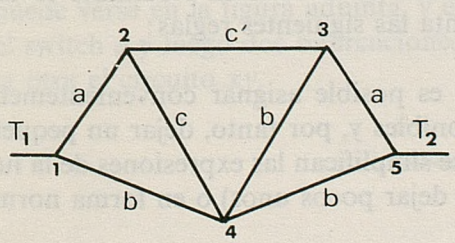
teniendo en cuenta que $c + c' = 1$ y la supresión de factores iguales por idempotencia:

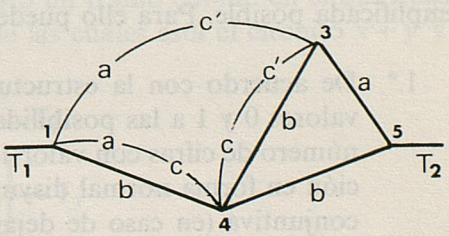
$$f = (a + b)(b + c')(a + b + c) = (b + ac')(b + a + c) = b + ac'(a + c) = b + ac'.$$

3.º Método de sustitución de puntos múltiples.

Si consideramos el circuito que tiene como terminales los nudos 1, 4 y 3, puede entenderse como conectado en estrella en el nudo 2 como punto múltiple, aplicando la transformacón estrella-triángulo se obtiene el circuito equivalente indicado en la figura en el que desaparece el punto múltiple 2.

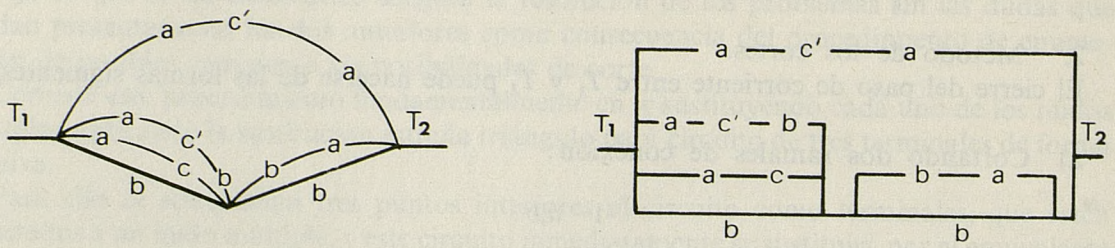
Por otra parte, el ramal entre los puntos 3 y 4, formado por c,c' en serie, puede suprimirse, por ser ambos switches complementarios y, por tanto, estar el ramal siempre abierto. Una vez suprimido este ramal reducimos el punto múltiple 3.





Sustituyendo el circuito con terminales 1, 4 y 5 conectados en estrella con 3, por el equivalente conectado en triángulo. Resultando finalmente el circuito indicado en la figura con conexiones en serie y paralelo, cuya función booleana es, por tanto,

$$f = ac' + (abc' + ac + b)(b + ab).$$



Operando y simplificando:

$$ac' + b(abc' + b + ac) = ac' + b(b + ac) = ac' + b.$$

La última igualdad es debido a que $b(b + ac) = b$ (ley de absorción).

7. *Diseño de circuitos de propiedades dadas con varios terminales*

En general, cuando un circuito tiene dos terminales, la forma de diseñar uno que cumpla una determinada propiedad de comportamiento con relación a ambos terminales consiste en describir esta propiedad mediante las correspondientes tablas de valores 0 y 1 de los switches y los correspondientes estados que se deseen presentar en circuitos. Esta tabla permite la obtención de las funciones representativas del circuito en forma normal disyuntiva o bien en forma normal conjuntiva, una vez obtenida la función; de esta forma puede diseñarse el circuito correspondiente conectado en serie paralelo, simplificando la función obtenida y representando las distintas operaciones de la función resultante con la correspondiente operación de conexión.

Puede ocurrir que las propiedades exigidas a la función no cubran todas las posibilidades lógicas que serían necesarias para definir la función en forma normal disyuntiva. En ese caso pueden obtenerse distintos circuitos que tengan las propiedades dadas, adaptando valores arbitrarios para las posibilidades lógicas sobre las que no se manifieste ningún deseo en cuanto al comportamiento del circuito. En general, estas posibilidades lógicas disponibles se utilizan como elemento que conduce a una expresión de la función resultante lo más simplificada posible. Para ello pueden tenerse en cuenta las siguientes reglas:

1.º De acuerdo con la estructura de la función es posible asignar convenientemente valores 0 y 1 a las posibilidades lógicas disponibles y, por tanto, dejar un pequeño número de cifras con valor 1 ó 0, con lo cual se simplifican las expresiones de la función en forma normal disyuntiva (en caso de dejar pocos unos) o en forma normal conjuntiva (en caso de dejar pocos ceros).

2.º Es posible asignar valores 0 y 1 de forma que se consiga hacer que la función sea independiente de alguna variable, con lo cual el circuito resultante se simplificará.

La aplicación de esta regla puede verse en el ejemplo siguiente.

Ejemplo

Diseñar un circuito con las propiedades definidas en la tabla siguiente:

Línea	X	Y	Z	$G(X,Y,Z)$
1	1	1	1	1
2	1	1	0	0
3	1	0	1	0
4	1	0	0	0
5	0	1	1	?
6	0	1	0	?
7	0	0	1	0
8	0	0	0	?

SOLUCION 1:

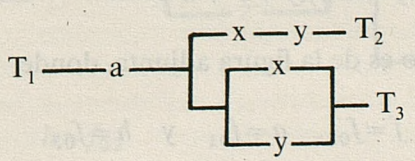
Usando la regla primera y notando que aparece solamente un 1 en la columna de la función, si asignamos 0 a cada una de las columnas ambiguas resultará la función $f = xyz$. El circuito es una conexión en serie de los switches x,y,z.

SOLUCION 2:

Si usamos la regla 2 y notamos que si asignamos 1 a la línea 5 y 0 a cada una de las líneas 6 y 8, la función llegará a ser independiente de x y puede escribirse como $f = yz$. El circuito es ahora una conexión en serie de y y z solamente, el cual es simplemente el circuito de la solución 1.

Naturalmente, los dos circuitos no son equivalentes, pero varían solamente en los casos cuyo resultado es indiferente, por lo que cualquiera de los dos reflejará el comportamiento en los aspectos que interesan.

Cuando se trata de diseñar circuitos con más de dos terminales se tratará la resolución de este problema en el sentido de combinar un conjunto de circuitos de dos terminales en un circuito de N terminales, de tal manera que existan switches comunes en el mayor número posible. Para ilustrar este procedimiento cabe considerar, como ejemplo, el caso de construir un circuito de tres terminales tal que $f_{12} = a(x + y)$ y $f_{13} = axy$. El circuito combinado puede verse en la figura adjunta, y en él se ha dispuesto un tramo común en el que aparece el switch a y luego dos bifurcaciones, en la primera de las cuales está el circuito $x + y$ y en la otra el circuito xy.



De esta forma se dispone un circuito con terminal inicial común T_1 y finales T_2 y T_3, de forma que las funciones entre 1 y 2 y 1 3 son las dadas.

Generalizando, si consideramos un conjunto de funciones $f_1, f_2, \ldots f_n$ donde alguno de los switches incluidos en los mismos son comunes, se puede diseñar un circuito de $N+1$ terminales. T_0, T_1, T_2, etc., T_n, de tal forma que la función f_i represente el circuito que une T_0 con T_i. Este enfoque del problema no es el único posible, ya que pueden existir otros circuitos con n terminales tal que N de las (n_2) funciones posibles sean las funciones dadas. Sin embargo, la expresión adoptada permite representar con un terminal común las series de funciones dadas.

El problema consistirá en estructurar algebraicamente las N funciones de manera que tengan los circuitos la mayor cantidad de tramos comunes.

Si las funciones están dadas explícitamente, un procedimiento a seguir consistirá en factorizar cada una de ellas por distintas alternativas, intentando encontrar factores comunes en la mayor cantidad posible, y todos ellos, una vez localizados estos factores comunes, pueden diseñarse los circuitos de forma análoga al ejemplo anterior.

Este procedimiento general se ilustra en el ejemplo siguiente:

Ejemplo 1

Diseñar un circuito de 4 terminales que realice las tres funciones siguientes, usando switches comunes, siempre que sea posible:

$$f = xy'z + (xy' + x'y)zw$$
$$g = xy'zw' + x'yzw'$$
$$h = x'y + (xy' + x'y)(z' + w')$$

g se puede factorizar fácilmente:

$$g = (zy' + x'y)zw'$$

Examinando en f y h los posibles factores comunes con g, resulta:

$$\begin{aligned} f &= z(xy' + (xy' + x'y)w) \\ &= z(xy'y' + x'yy' + (xy' + x'y)w) \\ &= z(xy' + x'y)y' + (xy' + x'y)w) \\ &= (xy' + x'y)z(y' + w). \end{aligned}$$

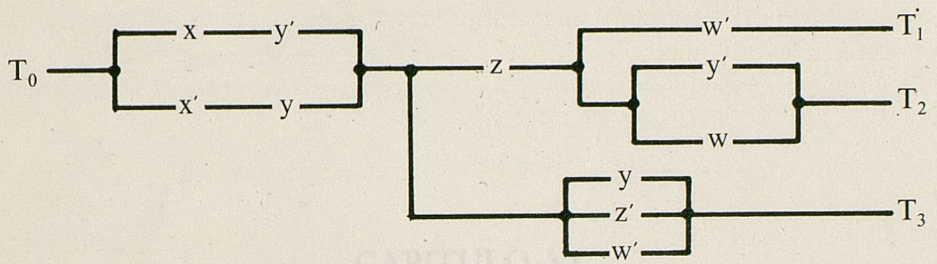
Igualmente,

$$\begin{aligned} h &= x'y + (xy' + x'y)(z' + w') \\ &= x'yy + xy'y + (xy' + x'y)(z' + w') \\ &= (xy' + x'y)(y + z' + w') \end{aligned}$$

Por tanto, el circuito elegido es de la figura adjunta, donde

$$f = f_{02}, \quad g = f_{01} \quad \text{y} \quad h = f_{03}.$$

Si las funciones no se dan explícitamente, pero se especifican mediante una tabla de valores 0,1, el mejor procedimiento es primero escribir cada función en forma normal conjuntiva, localizando a continuación los factores comunes y diseñando el circuito de forma que se haga el mejor uso posible de ellos. Este procedimiento se aplica en el ejemplo siguiente:



Ejemplo 2

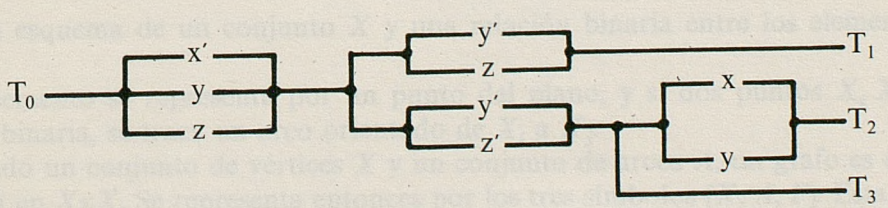
Construir un circuito de cuatro terminales con las propiedades siguientes:

	x	y	z	f	g	h
1	1	1	1	1	0	0
2	1	1	0	0	1	1
3	1	0	1	1	1	1
4	1	0	0	0	0	0
5	0	1	1	1	0	0
6	0	1	0	0	1	1
7	0	0	1	1	0	1
8	0	0	0	1	0	1

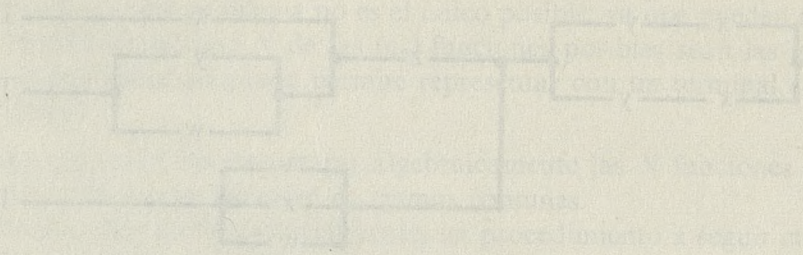
Cada función en forma normal conjuntiva es:

$$f=(x'+y+z)(x'+y'+z)(x+y'+z)$$
$$g=(x'+y+z)(x'+y'+z')(x+y'+z')(x+y+z)(x+y+z')$$
$$h=(x'+y+z)(x'+y'+z')(x+y'+z')$$

Lo que se refleja en el circuito de la figura



en donde $f=f_{01}$ $\quad g=f_{02}$ $\quad h=f_{03}$

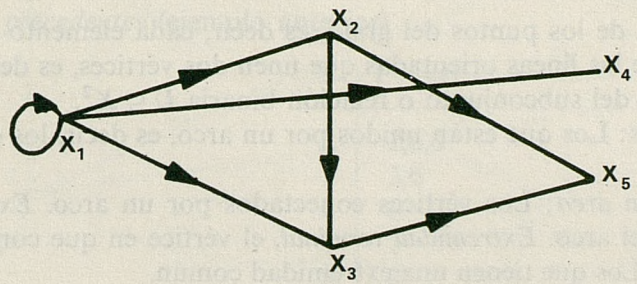


CAPITULO VI

INTRODUCCION A LA TEORIA DE GRAFOS

1. *Concepto de grafo*

Un grafo orientado es una red que consta de un conjunto $X=\{X_1,X_2,X_3,X_4,X_5\}$ de puntos y un cierto número de arcos orientados que unen varios pares de estos puntos (ver figura).



En un lenguaje matemático estos puntos y flechas pueden representar:

1.º Una aplicación Γ de un conjunto X en el conjunto de sus partes $X \to P(X)$.

En el grafo de la figura se tiene:

$$\Gamma(X_1)=\{X_1,X_2,X_3,X_4\} \qquad \Gamma(X_4)=\phi$$
$$\Gamma(X_2)=\{X_3,X_5\} \qquad \Gamma(X_5)=\phi$$
$$\Gamma(X_3)=\{X_5\}$$

2.º Un esquema de un conjunto X y una relación binaria entre los elementos de ese conjunto.

Cada elemento se representa por un punto del plano, y si dos puntos X_i X_j verifican la relación binaria, se traza un arco orientado de X_i a X_j.

3.º Dado un conjunto de vértices X y un conjunto de arcos A, un grafo es una aplicación F de A en $X \times X$. Se representa entonces por los tres símbolos (X, A, F). Esta definición, para ser equivalente a las anteriores, requiere que dos arcos distintos no tengan el mismo elemento $(X_iX_j) \in X \times X$ correspondiente; es decir, que F sea inyectiva.

El estudio teórico de estas redes, llamadas comunmente GRAFOS, efectuado con independencia de cualquier hipótesis sobre los elementos del conjunto representado por vértices o arcos, tiene un interés evidente por las múltiples aplicaciones que se derivan en la práctica: Esquemas eléctricos, estudio funcional de sistemas técnicos, relaciones humanas, estructuras administrativas, redes de transporte, problemas de planificación y ordenación de tareas, etc., pueden representarse esquemáticamente por medio de estas redes, generalmente de gran tamaño.

La teoría de grafos permite elaborar algoritmos de cálculo o procesos heurísticos para tratar estas redes complejas en ordenadores.

NOTA

Un algoritmo de cálculo es un proceso sistemático que permite obtener el resultado deseado (un óptimo, por ejemplo) en un número finito de pasos.

Un proceso heurístico permite solamente el estudio del problema considerado, sin que se tenga la certeza de obtener el resultado deseado, y será tanto mejor cuanto mayor porcentaje de buenas soluciones proporcione su explotación.

2. *Definiciones y notaciones*

— *Vértice*: Cada uno de los puntos del grafo, es decir, cada elemento del conjunto X.
— *Arco*: Cada una de las líneas orientadas que unen dos vértices, es decir, cada uno de los elementos (x,y) del subconjunto o relación binaria $U \subseteq X^2$.
— *Vértices adyacentes*: Los que están unidos por un arco, es decir, los que satisfacen la relación binaria.
— *Extremidades de un arco*: Los vértices conectados por un arco. *Extremidad inicial*, el vértice origen del arco. *Extremidad terminal*, el vértice en que concluye el arco.
— *Arcos adyacentes*: Los que tienen una extremidad común.
— *Bucle*: Un arco que es adyacente de sí mismo.
— *Precedente*: Todo vértice extremidad inicial respecto al vértice extremidad terminal. El conjunto de los precedentes de un vértice x se representa así:

$$\Gamma^{-1}(x)$$

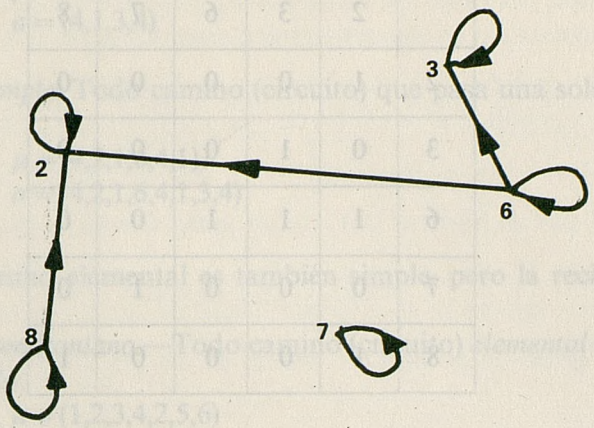
siendo $\Gamma^{-1}(x) = \{y \,/\, (y,x) \in U\}$.

Ejemplo (en el grafo de la figura adjunta):

$$\Gamma^{-1}(2) = \{2, 6, 8\}$$

— *Siguiente*: Todo vértice extremidad terminal respecto al vértice extremidad inicial. El conjunto de los siguientes de un vértice x se representa así: $\Gamma(x) = \{y \,/\, (x,y) \in U\}$.
— *Incidente interior de un vertice*: Todo arco que tiene a dicho vértice como extremidad terminal.

— *Incidente exterior de un vértice*: Todo arco que tiene a dicho vértice como extremidad inicial.



Diccionario de un grafo

Todo grafo puede ser representado en forma de diccionario de alguna de las dos maneras siguientes:

Diccionario de precedentes (ejemplo anterior)

x	$\Gamma^{-1}(x)$
2	2,6,8
3	3,6
6	6
7	7
8	8

Diccionario de siguientes (ejemplo anterior)

x	$\Gamma(x)$
2	2
3	3
6	2,3,6
7	7
8	2,8

Matriz booleana de un grafo (matriz asociada a un grafo)

Una tercera forma de representar un grafo se obtiene por medio de una matriz de Boole; es decir, una matriz cuadrada cuyas líneas y columnas representan los vértices del grafo y cuyas casillas indican si su línea y columna respectivas verifican la relación (1) o no (0).

Ejemplo (grafo anterior):

	2	3	6	7	8
2	1	0	0	0	0
3	0	1	0	0	0
6	1	1	1	0	0
7	0	0	0	1	0
8	1	0	0	0	1

Caminos y circuitos de un grafo

Consideremos el grafo siguiente:

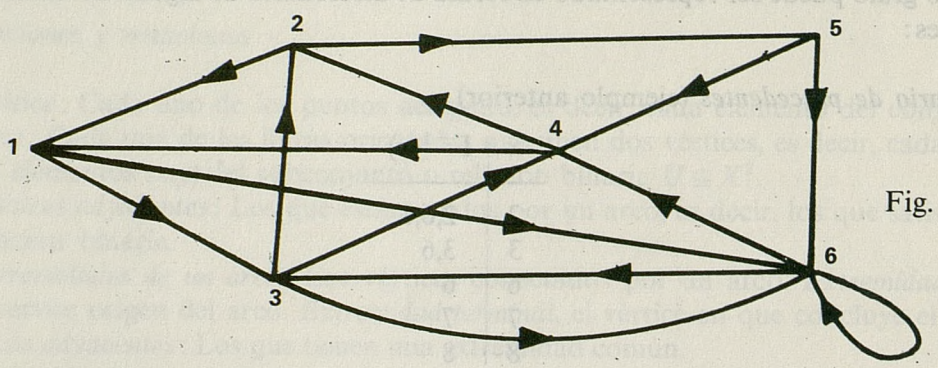


Fig. 1

— *Camino* (μ) en un grafo $G=(X,U)$, es una sucesión de *arcos*, tales que la extremidad terminal de cada uno coincide con la inicial del siguiente.
Camino de x_i a x_{iq},

$$m(x_i,x_{iq})=\{(x_{i1},x_{i2}),(x_{i2},x_{i3}),\ldots(x_{ip},x_{ip+1}),\ldots(x_{iq-1},x_{iq})\},$$

de modo que $\forall p\in\{1,\ldots q-1\}$, $(x_{ip},x_{ip+1})\in U$.
Ejemplo: $\mu=(1,3,6,3,4)$ (representación esquemática).

— *Circuito* (σ) es una sucesión cíclica de arcos tales que la extremidad terminal de cada uno coincide con la extremidad inicial del siguiente.

$$m(x_{i1},x_{iq}) \text{ tal que } x_{i1}=x_{iq}$$

Ejemplo (fig. 1): $\sigma=(1,3,4,1.6,4,2,1)$ (representación esquemática).

— *Camino* (*circuito*) *elemental*: Todo camino (circuito) que pasa una sola vez por cada uno de sus vértices.
Ejemplo (fig. 1): $\mu = (4,1,3)$
$\sigma = (4,1,3,4)$

— *Camino* (*circuito*) *simple*. Todo camino (circuito) que pasa una sola vez por cada uno de sus arcos.
Ejemplo (fig. 1): $\mu = (4,2,1,6,4,1)$
$\sigma = (4,2,1,6,4,1,3,4)$

NOTA.—Todo camino elemental es también simple, pero la recíproca no es cierta.

— *Camino* (*circuito*) *hamiltoniano*.—Todo camino (circuito) *elemental* que pasa por todos los vértices del grafo.
Ejemplo (fig. 1): $\mu = (1,2,3,4,2,5,6)$
$\sigma = (1,3,2,5,6,4,1)$

— *Camino* (*circuito*) *euleriano*. Todo camino (circuito) *simple* que pasa por todos los *arcos* del grafo.

NOTA.—En el grafo de la figura 1 no existe ningún camino ni circuito euleriano alguno.

— *Ascendiente de un vértice* x. Todo vértice situado en un camino que concurre sobre x.

x' es ascendiente de x si $\exists m(x',x)$.

— *Descendiente de un vértice* x. Todo vértice situado en un camino que parte de x.

x'' es descendiente de x si $\exists m(x,x'')$.

NOTA.—Todo precedente (siguiente) es un ascendiente (descendiente), pero la recíproca es falsa.

— *Raíz* (*antiraíz*). Todo vértice que tiene como descendientes (ascendientes) a los demás vértices del grafo.

x es una raíz $\Leftrightarrow \forall x' \in X,\ x' \neq x,\ \exists m(x,x')$
x es un antiraíz $\Leftrightarrow \forall x' \in X,\ x' \neq x,\ \exists m(x',x)$
Ejemplo (fig. 1):

El vértice 5 es una raíz del grafo.
El vértice 1 es una antiraíz del grafo.

NOTA.—Desde la raíz se puede "caminar" hasta cualquier vértice de un grafo.
NOTA.—A una antiraíz se puede llegar desde cualquier vértice de un grafo.
NOTA.—Las raíces (antiraíces) pueden no existir, ser únicas o múltiples.

Cadenas y ciclos de un grafo

Los conceptos de cadena y ciclo son paralelos a los de camino y circuito. Estos últimos se aplican a los grafos provistos de orientación (arcos), y los primeros a los grafos en los que la orientación no existe o en los que se hace caso omiso de ella.

NOTA.—Para indicar que un grafo carece de orientación se suele utilizar la representación simbólica $H=(X,V)$ en vez de $G=(X,U)$. Estos grafos se denominan *simétricos.*

— *Arista.* Es un par de vértices (x,y) de un grafo $G=(X,U)$ tal que:

$$(x,y)\in U \quad y/o \quad (y,x)\in U \quad y\neq x$$

Ejemplo: El grafo de la figura 1 consta de las aristas que se indican en la figura 2.

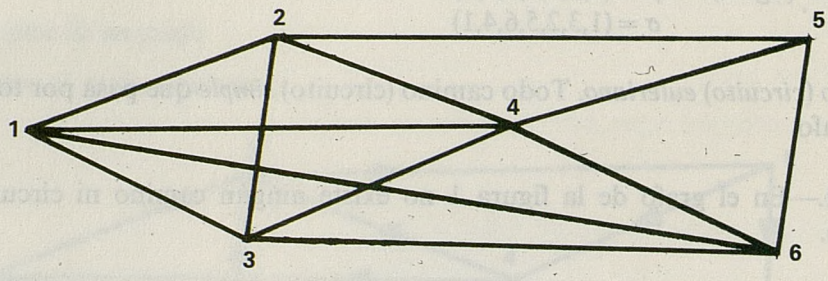


Fig. 2

— *Cadena.* Es una sucesión de aristas tales que la extremidad terminal de cada una coincide con la extremidad inicial de la que le sigue.
Ejemplo (fig. 2): (1,2,3,4,5,2) (representación esquemática).

— *Ciclo.* Es una sucesión circular de aristas, tales que la extremidad terminal de cada una coincide con la extremidad inicial de la siguiente.
Ejemplo (fig. 2): (3,4,5,2,4,1,3)

— *Cadena* (*ciclo*) *elemental.* Es una cadena (ciclo) que pasa una sola vez por cada uno de sus vértices.
Ejemeplo (fig. 2): Cadena: (2,4,3,6)
Ciclo: (2,4,3,1,2)

— *Cadena* (*ciclo*) *simple.* Es una cadena (ciclo) que pasa una sola vez por cada una de sus aristas.
Ejemplo (fig. 2): Cadena: (1,2,4,1,3)
Ciclo: (1,2,4,5,6,3,4,1)

— *Cadena* (*ciclo*) *hamiltoniano.* Es una cadena (ciclo) *elemental* que pasa por todos los *vértices* del grafo.
Ejemplo (fig. 2): Cadena: (1,2,3,4,5,6)
Ciclo: (1,2,3,4,5,6,1)

— *Cadena* (*ciclo*) *euleriano.* Es una cadena (ciclo) *simple* que pasa por todas las *aristas* del grafo.

Ejemplo (fig. 2): Cadena: (5,2,4,5,6,1,3,4,6,3,2,1,4)
Ciclo: No existe ninguno.

NOTA.—Ciertos autores llaman a las cadenas (ciclos), así definidos seudocadenas (seudociclos), reservando la denominación cadena (ciclo) para aquellas seudocadenas (seudociclos) que no poseen parejas de aristas consecutivas idénticas.

Grado de un vértice

Se llama *semigrado interior* de un vértice al número de arcos que inciden interiormente sobre él (exceptuados los posibles bucles).

Se representa así: $d'(x)$ o $d^-(x)$
Ejemplo (fig. 1): $d'(3)=2$ o $d^-(3)=2$

Paralelamente, se llama *semigrado exterior* de un vértice al número de arcos que inciden exteriormente sobre el mismo.

Se representa así: $d''(x)$ o $d^+(x)$
Ejemplo: (fig. 1): $d''(3)=3$

Grado de un vértice es, finalmente, el número de aristas que inciden en él Se representa por $d(x)$.

Ejemplo (fig. 1): $d(3)=4$

Corte, cociclo y cocircuito

Sea A una parte cualquiera de X en el grafo $G=(X,U)$.

Recibe el nombre de *corte interior* de A el conjunto de arcos que inciden interiormente sobre alguno de los vértices de A y tienen como extremidad inicial algún vértice de $(X-A)$. Se representa así: $w'(A)$ o $w-(A)$.

$$(a,b)\in w'(A) \text{ si } a \notin A \text{ y } b\in A$$

Ejemplo (fig. 1): $A=\{1,2\}$ " $w'(A)=\{(4,2), (3,2), (4,1)\}$.

Paralelamente, se da el nombre de *corte exterior* de A al conjunto de arcos que inciden exteriormente sobre alguno de los vértices de A y tienen como extremidad terminal algún vértice de $(X-A)$. Se representa así: $w''(A)$ o $w^+(A)$.

$$(a,b)\in w''(A) \text{ si } a\in A \text{ y } b \notin A$$

Ejemplo (fig. 1): $A=\{1,2)$ " $w''(A)=\{(2,5), (1,6), (1,3)\}$.

NOTA.—La supresión de los arcos $w'(A)$ (resp. $w''(A)$) lleva consigo el aislamiento hacia el interior (resp. hacia el exterior) de los vértices pertenecientes a A.

Se llama *grado interior* (exterior) de A al número de arcos de que consta el corte interior (exterior) de A. Se representa así:

$$d'(A) = / w'(A) / \ (d''(A) = / w''(A) /)$$

Se llama *cociclo* de A al conjunto $w'(A) \cup w''(A)$, es decir, al conjunto de arcos que inciden sobre A. Su representación: $w(A)$.

Ejemplo (fig. 1): $A = \{1,2\}$ $w(A) = \{(2,5), (4,2), (3,2), (4,1), (1,6), (1,3)\}$.

$NOTA.$—$w(A) = w(X - A)$ para $\forall A \subset X$.

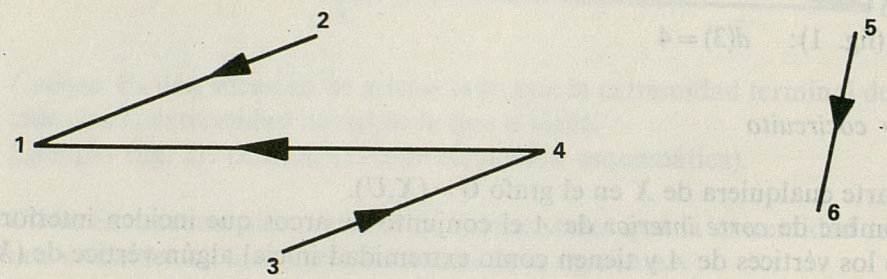
Por último, cuando para $B \subset X$, $w'(B) = \phi$, o bien $w''(B) = \phi$, el cociclo de B recibe la denominación de *cocircuito*. En este caso, las "comunicaciones" de B con $(X - B)$ tienen lugar en un solo sentido.

Grafo parcial, subgrafo y subgrafo parcial

Si conservando todos los vértices de un grafo (G) eliminamos una parte de sus arcos, el grafo resultante (G') recibe el nombre de *grafo parcial* de G.

$$G' = (X, U') \text{ “ } U' \subset U$$

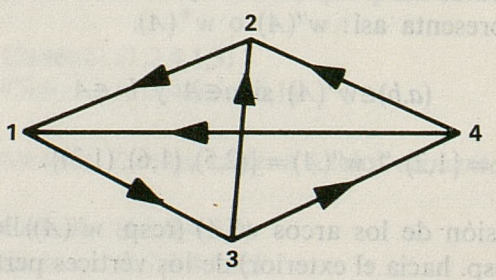
Ejemplo (fig. 1): El grafo G' siguiente es un grafo parcial del grafo G de la figura 1.



Si abandonando una parte de los vértices mantenemos todos los arcos, salvo aquellos que incidan sobre los vértices abandonados, el grafo (G_A) resultante se denomina *subgrafo* de G.

$G = (A, U_A)$ “ $A \subset X, U_A =$ Conjuntos de arcos de $\cup$ que tienen sus extremidades en A. $U_A \subset U$.

Ejemplo: La figura siguiente representa un subgrafo del grafo de la figura 1.

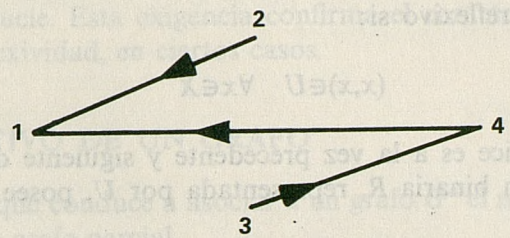


NOTA.—Adviértase que en el subconjunto $(U - U_A)$ de arcos desaparecidos se encuentran los del cociclo de A más aquellos que tienen sus dos extremidades en los vértices desaparecidos.

Por último, la yuxtaposición de las dos operaciones anteriores da lugar a un subgrafo parcial.

$$G'^A = (A, U'_A),\ A \subset X,\ U'_A \subset U_A$$

Ejemplo: El grafo siguiente es un subgrafo parcial del grafo de la figura 1.



EJEMPLOS DE GRAFOS EN UNA EMPRESA

Organigrama jerárquico

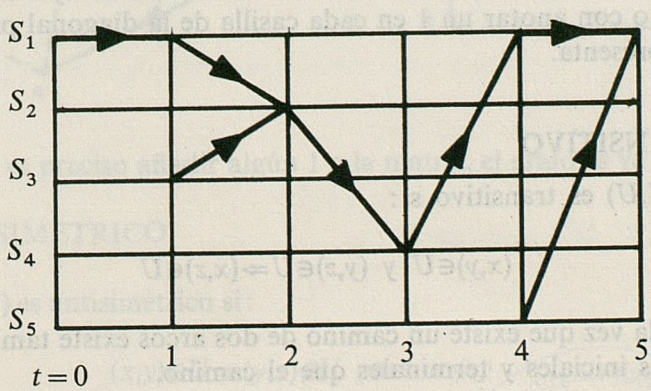
Los elementos del conjunto X son individuos y/o grupos de individuos.
La relación binaria es la dependencia jerárquica y/o funcional.

Grafo de relaciones

X es el conjunto de servicios de la empresa.
$(x_i, x_j) \in U$ si algún documento o material va desde x_i a x_j.

Grafo de circulación

Sea S el conjunto de servicios y T el conjunto de períodos de tiempo o fechas $(t = 1,2, \ldots)$.
El conjunto X es entonces el producto cartesiano $S \times T$.
Relación binaria: $[(S_i t), (S_j t+1)] \in U$ si algo circula de S_i a S_j entre t y $t+1$.



Grafo de sucesión de operaciones

X es el conjunto de etapas materiales (operaciones) de un proceso.
$(x_i,x_j)\in U$ si la operación x_i debe preceder inmediatamente a la operación x_j.

Organigrama de la programación, etc.

3. *Grafos particulares*

3.1. GRAFO REFLEXIVO

Un grafo $G=(X,U)$ es reflexivo si:

$$(x,x)\in U \quad \forall x\in X$$

Es decir, cuando todo vértice es a la vez precedente y siguiente de sí mismo.

En este caso, la relación binaria R, representada por U, posee la propiedad reflexiva; es decir,

$$\forall x,\ xRx$$

Ejemplos:
— "tener el mismo sexo que"
— "ser igual o mayor que".
— etcétera.

NOTA.—El concepto de reflexibilidad tiene un carácter un tanto convencional. A veces, basta forzar un poco el sentido de las palabras para hacer reflexiva una relación que podría muy bien no serlo. Se acepta esta convención para facilitar el razonamiento en ciertos casos.

3.2. CIERRE REFLEXIVO DE UN GRAFO

Es aquella aplicación que consiste en asociar a un grafo G el "más pequeño" grafo reflexivo que lo contiene como grafo parcial. Para ello basta con dibujar un bucle en cada uno de los vértices de G o con anotar un 1 en cada casilla de la diagonal principal de la matriz de Boole que lo representa.

3.3. GRAFO TRANSITIVO

Un grafo $G=(X,U)$ es transitivo si:

$$(x,y)\in U \text{ y } (y,z)\in U \Rightarrow (x,z)\in U$$

Es decir, cuando cada vez que existe un camino de dos arcos existe también un arco con las mismas extremidades iniciales y terminales que el camino.

Paralelamente al caso anterior, la relación binaria R representada por U es una relación transitiva, es decir, xRy y $yRz \Rightarrow xRz$.

Ejemplos:

— "ser más joven que"
— "tener la misma edad que"
— "estar incluido en"

NOTA.—En un grafo transitivo, el conjunto de los precedentes de un vértice se identifica con el de sus ascendientes y el conjunto de los siguientes con el de sus descendientes.

NOTA.—En un grafo transitivo todo vértice perteneciente a un circuito posee obligatoriamente un bucle. Esta exigencia confirma el carácter convencional, e incluso artificial, de la reflexividad, en ciertos casos.

3.4. CIERRE TRANSITIVO DE UN GRAFO

Es aquella aplicación que conduce a asociar a un grafo G "el más pequeño" grafo transitivo que lo contiene como grafo parcial.

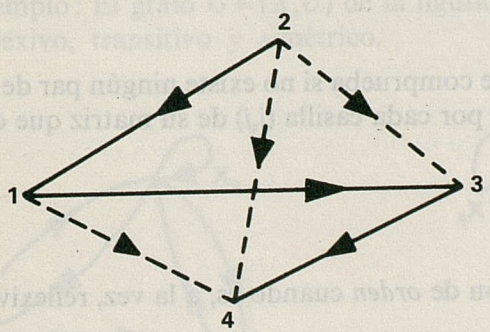
El procedimiento a emplear se basa en las reglas siguientes:

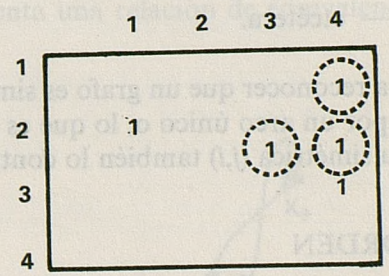
1.º Identificar para cada vértice x,$\Gamma(x)$ $y\Gamma^{-1}(x)$.
2.º Crear los arcos necesarios para unir todo elemento de $\Gamma^{-1}(x)$ con todo elemento de $\Gamma(x)$.

Prácticamente, este procedimiento consiste en:

1.º Poner el grafo en forma matricial.
2.º Recorrer de arriba a abajo todas las líneas efectuando las operaciones siguientes: Reproducir todos los 1 que existan en la línea i, sobre toda línea h que tenga un 1 en la columna i.

Ejemplo:





NOTA.—Si no es preciso añadir algún 1 a la matriz, el grafo es ya transitivo.

3.5. GRAFO ANTISIMETRICO

Un grafo $G=(X,U)$ es antisimétrico si:

$$(x,y)\in U \Rightarrow (y,x)\notin U \text{ para } x\neq y$$

Es decir, si el número de arcos entre dos cualesquiera de sus vértices es igual a 0 ó 1.

La relación binaria R correspondiente será asimismo antisimétrica, que es aquella en que

$$aRb \text{ y } bRa \Rightarrow a = b$$

Ejemplos:
— "estar a más distancia que"
— "ser hijo de"
— "tener más graduación que"

Para reconocer si un grafo es antisimétrico basta con verificar si no existe ningún par de vértices unidos por dos arcos o comprobar que para toda casilla (i,j) de la matriz que contiene un 1, su casilla simétrica (j,i) no lo contiene.

3.6. GRAFO SIMETRICO

Un grafo $G = (X,U)$ es simétrico cuando:

$$(x,y) \in U \Rightarrow (y,x) \in U \qquad (x \neq y)$$

o sea cuando entre cualquier par de vértices del grafo el número de arcos es 0 ó 2.

La relación binaria correspondiente R se denomina relación simétrica. En ella se verifica:

$$aRb \Rightarrow bRa \qquad (a \neq b)$$

Ejemplos:
— "tener igual empleo que"
— "haber nacido el mismo año que"
— "ser perpendicular a"
— etcétera.

Para reconocer que un grafo es simétrico se comprueba si no existe ningún par de vértices unidos por un arco único o, lo que es igual, si por cada casilla (i,j) de su matriz que contiene un 1, su simétrica (j,i) también lo contiene.

3.7. ORDEN

Un grafo $G = (X,U)$ representa una relación de *orden* cuando es, a la vez, reflexivo, transitivo y antisimétrico.

Ejemplo de relaciones de orden:
— "ser igual o mayor que"
— "tener tanta o más autoridad que"
— "ocurrir no más tarde que"
— etcétera.

Cando una relación binaria (y el grafo que la representa) es únicamente transitiva y simétrica, dicha relación se llama de *orden estricto*.

Ejemplos de relaciones de orden estricto:

— "ser mayor que"
— "tener más autoridad que"
— "ocurrir antes que"
— etcétera.

3.8. EQUIVALENCIA

Un grafo $G=(X,U)$ representa una relación de *equivalencia* cuando es a la vez reflexivo, transitivo y simétrico.

Ejemplos de relaciones de equivalencia:

— "ser pariente de"
— "pertenecer a la misma promoción que"
— "tener la misma calificación que"

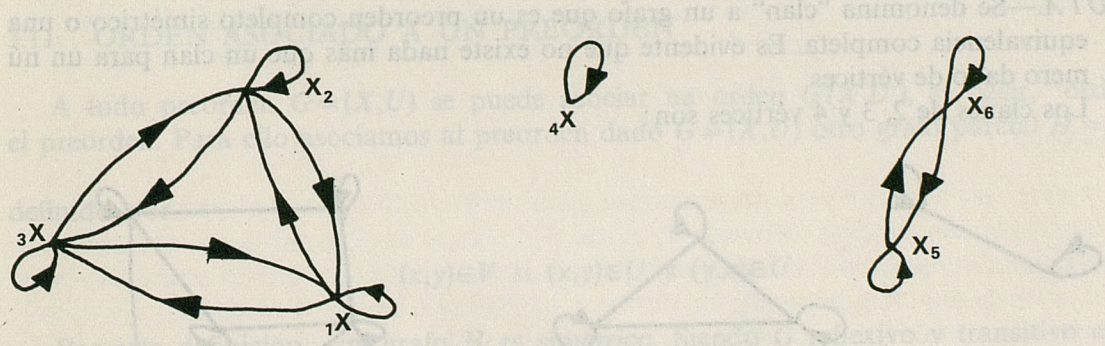
En una relación de equivalencia, a un elemento x se puede asociar el conjunto $\Gamma(x)$ de los elementos y que verifican $(x,y)\in U$. Este conjunto define una *clase de equivalencia* en el grafo G.

Estas clases tienen las propiedades siguientes:

Si $x'\in\Gamma(x)$ $\quad\Gamma(x')=\Gamma(x)$
Si $z\notin\Gamma(x)$ $\quad\Gamma(z)\cap\Gamma(x)=\phi$

El conjunto de las clases de equivalencia constituye, por tanto, una partición que se llama *cociente* del conjunto X por la relación de equivalencia. Recíprocamente, si se ha definido sobre un conjunto X una partición, la relación R (tal que xRy si x e y pertenecen a una misma clase), define sobre el conjunto X un grafo que representa una relación de equivalencia.

Ejemplo: El grafo $G=(X,U)$ de la figura, representa una relación de equivalencia, pues es reflexivo, transitivo y simétrico.



Como se observa fácilmente, son tres las clases de equivalencia:

$$C_1=\{x_1,x_2,x_3\};\quad C_2=\{x_4\};\quad C_3=\{x_5,x_6\}$$

El cociente del conjunto X por la relación de equivalencia representada por U, constituye la partición $X/U = \{C_1, C_2, C_3\}$.

NOTA.—Hablar de relación de equivalencia es lo mismo que hablar de relación de clasificación (clasifica en clases).

3.9. PREORDEN

Recibe el nombre de *preorden* todo grafo o relación binaria reflexiva y transitiva.
Luego un preorden simétrico es una relación de equivalencia y un preorden antisimétrico es un orden.

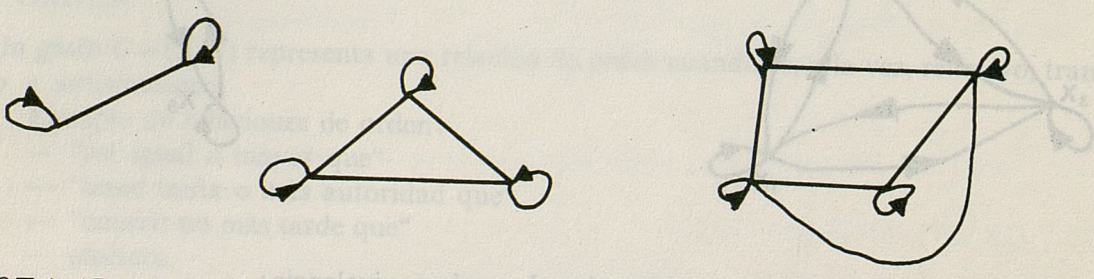
3.10. CLASIFICACION DE LOS PREORDENES

Si añadimos a las propiedades ya estudiadas la de *totalidad*, que la posee todo grafo $G = (X,U)$ tal que $\forall x \in X$; $\forall y \in X$; $(x,y) \in U$ o/y $(y,x) \in U$.
Podemos hacer la siguiente clasificación:

Reflexivo + transitivo	Preorden	S	AS	T	ϕ
				P	Yuxtaposición de bucles
			$\overline{AS}$	T	Clan
				P	Equivalencia
		$\overline{S}$	AS	T	Orden total
				P	Orden
			$\overline{AS}$	T	Preorden total
				P	Preorden

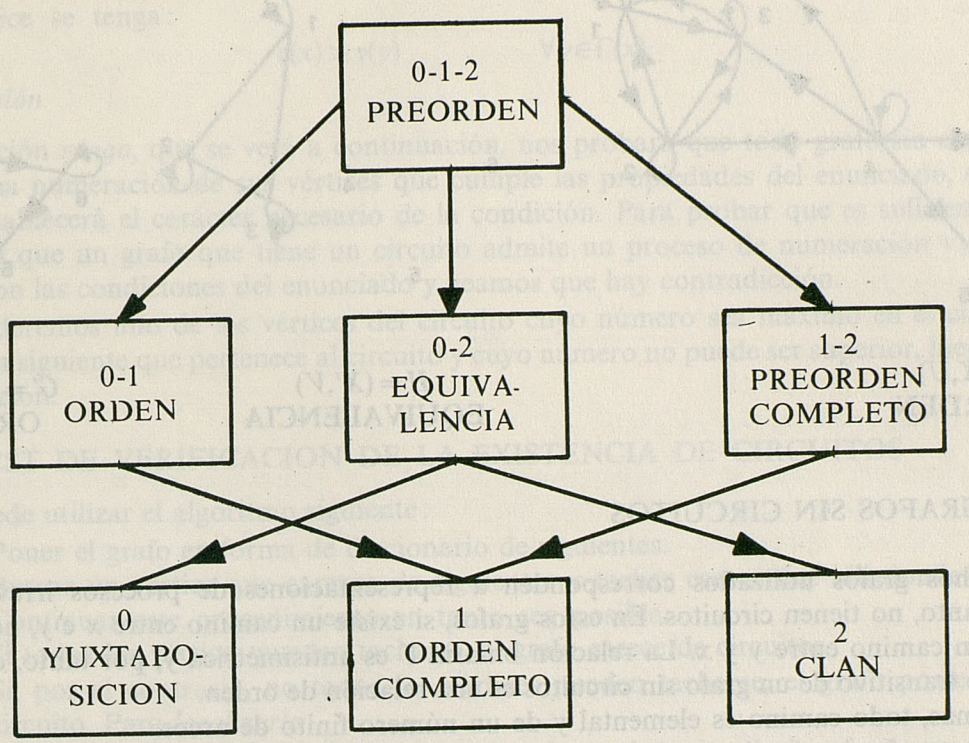
(Indicándose las propiedades de simétrico, antisimétrico, total y parcial por sus iniciales y la ausencia de ellas por un signo $-$).

NOTA.—Un grafo total se denomina también completo.
NOTA.—Se denomina "clan" a un grafo que es un preorden completo simétrico o una equivalencia completa. Es evidente que no existe nada más que un clan para un número dado de vértices.
Los clanes de 2, 3 y 4 vértices son:



NOTA.—La "yuxtaposición de bucles" es el único grafo a la vez simétrico y antisimétrico.
NOTA.—Una equivalencia no es más que una yuxtaposición de clases (cada una de ellas constituye una clase de equivalencia).

Otra clasificación interesante es aquella que podemos hacer en función del número de arcos que ligan dos vértices distintos cualesquiera:



NOTA.—Los arcos del grafo que esquematiza esta clasificación traducen la inclusión de los conjuntos de los preórdenes que le son "adyacentes". Por ejemplo, todo orden completo es un preorden completo, un clan es una equivalencia.

3.11. ORDEN ASOCIADO A UN PREORDEN

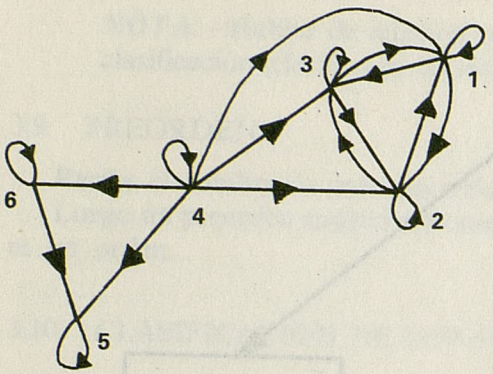
A todo preorden $G=(X,U)$ se puede asociar un orden $G'(X'U')$, es decir, "ordenar" el preorden. Para ello asociamos al preorden dado $G=(X,U)$ otro grafo parcial $H=(X,V)$ definido por

$$(x,y)\in V \text{ si } (x,y)\in U \text{ y } (y,x)\in U$$

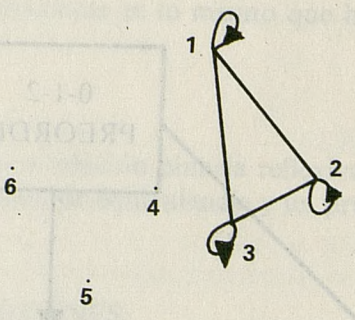
Por esta definición, este grafo H es simétrico. Siendo G reflexivo y transitivo es fácil de deducir que H lo es también. Por tanto, $H=(X,V)$ es una equivalencia llamada *equivalencia asociada* al preorden G.

Si designamos por $X'=X/V$ el conjunto de clases de la equivalencia definida por H, podemos considerar el grafo $G'=(X'U')$ resultante del grafo G, al agrupar todos los vértices de cada clase en uno solo.

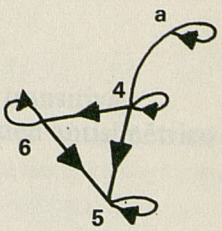
Ejemplo:



$G=(X,U)$
PREORDEN



$H=(X',V)$
EQUIVALENCIA



$G'=(X',U')$
ORDEN

3.12. GRAFOS SIN CIRCUITOS

Muchos grafos utilizados corresponden a representaciones de procesos irreversibles y, por tanto, no tienen circuitos. En estos grafos, si existe un camino entre x e y, no puede existir un camino entre y y x. La relación binaria Γ es antisimétrica y, por tanto, el cierre reflexivo transitivo de un grafo sin circuitos es una relación de orden.

Además, todo camino es elemental y de un número finito de arcos.

En un grafo sin circuitos existen necesariamente vértices tales que $\Gamma(x)=\phi$, pues si no al final de un camino del máximo número de arcos nos encontraríamos con uno de sus vértices. Recorriéndolo en sentido contrario se ve que deben existir vértices tales que $\Gamma^{-1}(x)=\phi$.

3.13. TEOREMA

Una condición necesaria y suficiente para que un grafo no tenga circuitos es que todo subconjunto A no vacío del conjunto de sus vértices admita al menos un elemento que no sea siguiente de ningún elemento de A.

Demostración

Necesaria: Supongamos que no se verifica para un grafo G y sea A un subconjunto no vacío de vértices tal que cada elemento de A sea el siguiente de al menos un elemento de A. Consideremos el subgrafo G_A de G que engendra A. Cada uno de sus vértices posee al menos un precedente en G_A. Si a partir de un vértice a_1 se elige uno de sus precedentes, por ejemplo a_2, después uno de los precedentes de a_2, etcétera, se forma una sucesión que hará aparecer inevitablemente una repetición y, por tanto, un circuito de G_A, que es también un circuito de G.

Suficiente: La condición no se cumple por un grafo que posea un circuito, pues el conjunto A de los vértices del circuito verifica precisamente que todo elemento es siguiente de algún elemento de A, contra la hipótesis.

3.14. TEOREMA

Una condición necesaria y suficiente para que un grafo no tenga circuitos es que exista un proceso de numeración v de sus vértices (con valores enteros y no negativos), tal que para cada vértice se tenga:

$$v(x) > v(y) \qquad \forall y \in \Gamma(x)$$

Demostración

La noción *rango*, que se verá a continuación, nos probará que todo grafo sin circuitos admite una numeración de sus vértices que cumple las propiedades del enunciado, con lo que se establecerá el carácter necesario de la condición. Para probar que es suficiente supongamos que un grafo que tiene un circuito admite un proceso de numeración v de sus vértices con las condiciones del enunciado y veamos que hay contradicción.

Consideremos uno de los vértices del circuito cuyo número sea máximo en el circuito. Admite un siguiente que pertenece al circuito y cuyo número no puede ser superior, luego hay contradicción.

3.15. TEST DE VERIFICACION DE LA EXISTENCIA DE CIRCUITOS

Se puede utilizar el algoritmo siguiente:

1.º Poner el grafo en forma de diccionario de siguientes.
2.º Buscar un vértice que carezca de siguientes y tachar ese vértice allí donde figure.
3.º Continuar este procedimiento en tanto sea posible.
4.º Si todos los vértices pueden tacharse, el grafo carece de circuitos.
5.º Si, por el contrario, no todos los vértices pueden tacharse, el grafo posee algún circuito. Para *localizarlo*:
6.º Iniciar una lista en la que figure, como primer elemento de la misma, un vértice cuyos siguientes no hayan sido tachados y añadir a la lista el primero no tachado.
7.º Buscar la línea correspondiente a este vértice y añadir a la lista su primer siguiente no tachado.
8.º Continuar este proceso hasta que aparezca en la lista repetido alguno de los elementos que figuran ya en ella. La secuencia de vértices comprendida entre los vértices repetidos constituye un circuito.

Ejemplo:

x	$\Gamma(x)$
1	3
2	1,4
3	2,4
4	5,~~6~~
5	3,~~6~~
~~6~~	

$\sigma_1 = (1,3,2,1)$

3.16. ELIMINACION DE TODOS LOS CIRCUITOS DE UN GRAFO

Puesto que la existencia de un circuito indica que los elementos que los constituyen son equivalentes entre sí, cabe sustituirlos por un solo vértice ficticio que los represente y que se haga cargo de las relaciones de aquéllas con los demás vértices del grafo.

Eliminando el circuito σ_1 del grafo anterior y llamando a al vértice ficticio que representará a sus componentes (1,3,2), el grafo transformado quedará como sigue:

x	$\Gamma(x)$
a	4
4	5,ϕ
5	a,ϕ
ϕ	

Repitiendo el algoritmo expuesto en 3.13., llegamos a la detección de un nuevo circuito $\sigma_2 = (a,4,5,a)$, que, representado por un nuevo vértice ficticio b, nos conduce finalmente al siguiente grafo sin circuitos:

3.17. RANGO DE UN VERTICE

Se denomina rango de un vértice (simbólicamente se representa por $r(x)$), a un número entero no negativo que se utiliza como indicador de la categoría jerárquica que ocupa el vértice dentro de todo grafo sin circuitos.

Para determinar el rango de los vértices de un grafo se utiliza el algoritmo siguiente:

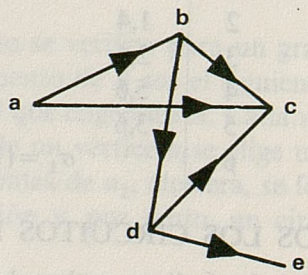
1.º Asignar rango cero $r(x) = 0$ a todos los vértices que carezcan de precedentes en el grafo. Al conjunto de vértices cuyo $r(x) = 0$, denominémosle Xo.

2.º Entre los vértices pertenecientes a $X - Xo$, seleccionar aquellos que no tengán ningún precedente en $X - Xo$ (es decir, aquellos cuyos precedentes tengan ya un rango asignado). A todos estos vértices —que constituyen un nuevo conjunto X_1— asígnesele el rango $r(x) = 1$.

3.º Proseguir con este procedimiento hasta lograr asignar un rango a todos los vértices del grafo.

Ejemplo:

$Xo = \{a\}$ $\quad r(a) = 0$
$X_1 = \{b\}$ $\quad r(b) = 1$
$X_2 = \{d\}$ $\quad r(d) = 2$
$X_3 = \{c,e\}$ $\quad r(c) = 3,\ r(e) = 3$



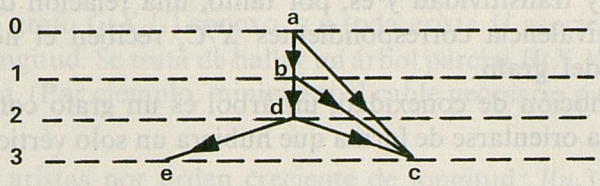
NOTA.—Puede definirse un rango similar —pero en sentido contrario— cambiando la palabra precedente por la palabra siguiente, en el algoritmo anterior.

3.18. GRAFO DE RANGOS

Una vez determinado el rango de cada vértice puede construirse un grafo equivalente al anterior, en el que los vértices aparezcan situados por nivel jerárquico.

Ejemplos:

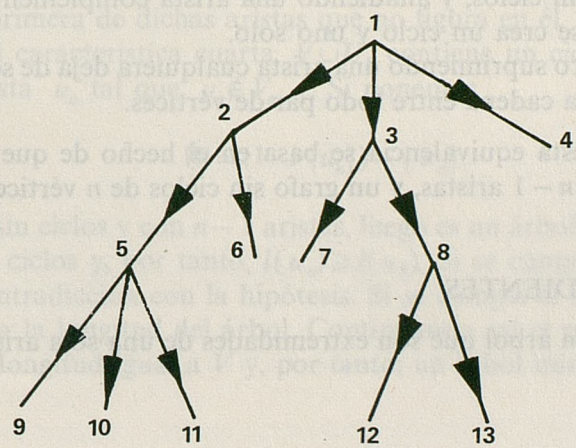
Tomando el mismo grafo del ejemplo anterior, su grafo equivalente de rangos será el siguiente:



4. *Arborescencias y árboles*

4.1. DEFINICION

Una arborescencia es un grafo sin circuitos tal que exista un solo vértice cuyo grado interior es cero (raíz de la arborescencia) y el resto de sus vértices tienen un grado interior igual a uno.



Las arborescencias intervienen en numerosos esquemas muy conocidos:

— Clasificación de constituyentes sucesivos: conjunto, subconjunto, piezas. La relación binaria es en este caso una relación de inclusión.

— Organigrama jerárquico de una empresa: Es una arborescencia si toda persona distinta al director general tiene un solo superior jerárquico.

Arbol: Reemplazando los arcos por aristas en una arborescencia se obtiene lo que se llama un árbol. Recíprocamente, si tomamos un vértice cualquiera como origen en un árbol definimos una arborescencia. De un árbol pueden obtenerse, por consiguiente, tantas arborescencias como vértices posee.

4.2. GRAFO CONEXO

Se dice que un grafo es conexo si dados dos vértices distintos cualesquiera x,y, existe al menos una cadena entre x e y. Considerando un grafo cualquiera, podemos siempre definir sobre el conjunto X de sus vértices la relación binaria C_s tal que (x,y) verifica C_s si existe una cadena entre x e y o si $x = y$.

Esta relación binaria recibe el nombre de conexidad simple, posee las propiedades de reflexividad, simetría y transitividad y es, por tanto, una relación de equivalencia.

Las clases de equivalencia correspondientes X/C_s reciben el nombre de *componentes simplemente conexas* del grafo.

Introduciendo la noción de conexidad, un árbol es un grafo conexo y sin ciclos (si no fuera conexo no podría orientarse de forma que hubiera un solo vértice con un grado interior igual a cero).

4.3. TEOREMA 1

Sea G un grafo de n vértices ($n > 1, |X| = n$). Un árbol se puede caracterizar por cualquiera de las propiedades siguientes, equivalentes entre sí:

1.º G es conexo y sin ciclos.
2.º G es un grafo sin ciclos y admite $n - 1$ aristas.
3.º G es conexo y admite $n - 1$ aristas.
4.º G es un grafo sin ciclos, y añadiendo una arista complementaria entre dos vértices no adyacentes se crea un ciclo y uno solo.
5.º G es conexo, pero suprimiendo una arista cualquiera deja de serlo.
6.º Existe una única cadena entre todo par de vértices.

La justificación de esta equivalencia se basa en el hecho de que un grafo conexo de n vértices posee al menos $n - 1$ aristas, y un grafo sin ciclos de n vértices posee como máximo $n - 1$ aristas.

4.4. VERTICES PENDIENTES

Son los vértices de un árbol que son extremidades de una sola arista.

4.5. TEOREMA 2.

Un árbol admite al menos dos vértices pendientes.

En efecto: Supongamos que admitiera menos de dos vértices pendientes, es decir, 0 ó 1 solamente. Si recorremos el grafo a partir de un vértice cualquiera, en el primer caso, o del vértice pendiente, en el segundo, no pasando dos veces por la misma arista, no podríamos pasar dos veces por el mismo vértice, pues no existen ciclos. Por otra parte, desde cualquier vértice x podremos recorrer una nueva arista, pues x no puede ya ser pendiente, y así continuaríamos indefinidamente, lo que no es posible, al ser finito el número de vértices del grafo.

4.6. TEOREMA 3.

Un grafo $G(X,U)$ admite un grafo parcial que sea un árbol, si y solamente si, G es conexo.

En efecto, si G no es conexo, ninguno de sus grafos parciales lo es; luego no admite árboles parciales.

Si G es conexo, busquemos una arista tal que su supresión convierta el grafo en no conexo.

Si la arista no existe, G es un árbol; si existe, la suprimimos y continuamos hasta que no podamos suprimir nuevas aristas. Tendremos entonces un árbol cuyo conjunto de vértices es precisamente X.

ALGORITMO DE KRUSKAL

Consideremos un grafo $G(X,U)$ conexo, y a toda arista U asociemos un número $l(u) \geqslant 0$, que llamaremos su longitud. Se trata de hallar un árbol parcial $H(X,V)$ del grafo cuya longitud total $\Sigma l(u)$ sea mínima. (Por ejemplo, minimizar el cable necesario para unir n puntos dados.) Se procede así:

1.º Ordenar las aristas por orden creciente de longitud: $l(u_1) \leqslant l(u_2) \ldots$

2.º Se elige la menor de todas ellas, luego la que viene después que no forme ciclo e iteramos eligiendo siempre la primera de la lista que no forme ciclo con las ya elegidas anteriormente hasta terminarla.

Se obtiene así un árbol de longitud mínima.

En efecto, por este proceso de elección llegamos a obtener un grafo tal que si añadimos una nueva arista distinta de las elegidas creamos un ciclo, luego es un árbol, y por la propiedad segunda tiene $n-1$ aristas: $V_{n-1} = \{u_1, u_2, \ldots u_{n-1}\}$.

Supongamos ahora que el árbol de longitud mínima V no contuviera alguna de las aristas elegidas y sea u_k la primera de dichas aristas que no figura en él.

Por la propiedad característica cuarta, $V \cup U_k$ contiene un ciclo y uno solo, existiendo en este ciclo una arista u_o tal que $u_o \notin V_{n-1}$. Si ponemos

$$W = (V \cup \{u_k\}) - \{u_o\}$$

obtenemos un grafo sin ciclos y con $n-1$ aristas, luego es un árbol; pero $V_{k-1} \cup \{u_o\}$ evidentemente no contiene ciclos y, por tanto, $l(u_o) \geqslant l(u_k)$. Si se cumple el signo $>$, V no es el árbol mínimo, en contradicción con la hipótesis. Si se cumple el signo $=$, la sustitución de u_o por u_k no aumenta la longitud del árbol. Continuando así el proceso, demostramos que V_{n-1} es un árbol de longitud igual a V y, por tanto, un árbol mínimo.

5. *Problemas secuenciales*

En el vasto dominio de los fenómenos orgánicosociales se presentan con gran frecuencia problemas cuya solución se alcanza a través de un proceso secuencial, es decir, mediante una sucesión, temporal o espacial, de opciones intermedias. Los problemas que poseen esta estructura se agrupan bajo la denominación genérica de problemas secuenciales.

Citaremos como muestra de problemas de esta clase los siguientes:

a) Determinación de la ruta más corta entre dos localidades geográficas.

b) Determinación del camino más corto que permite unir entre sí todos los puntos de una extensa red de comunicaciones.

c) Hallar un camino cualquiera para desplazarse de un punto a otro.

d) Establecer un programa temporal de actividades.

e) Llegar a la decisión final, en una situación determinada, empleando para ello el menor número posible de decisiones parciales intermedias.
f) Enumerar todas las soluciones posibles de un problema; etcétera.

5.1. PLANTEAMIENTO DEL PROBLEMA

Todo problema secuencial puede ser planteado sobre un grafo orientado $G=(X,U)$, en el cual:

X representa el conjunto de opciones, actividades, puntos, localidades geográficas, etc.
U representa el conjunto de conexiones, relaciones, etc., que existen entre los elementos de X.

Representada así la estructura del problema, su solución consiste, en la mayoría de los casos, en localizar en el grafo G un camino o un conjunto de caminos, que reúnan ciertas características. Los vértices del camino (o caminos), tomados en el orden en que en él figuran, constituyen la secuencia (o secuencias) solución del problema.

5.2. PROBLEMAS ESPECIFICOS

En el marco de este apartado analizaremos los problemas específicos siguientes:

— Hallar un camino *cualquiera* para ir de un vértice a otro.
— Hallar un camino que permita ir desde un vértice (xo) a otro vértice (xm), utilizando el número mínimo *de arcos.*
— Hallar un camino de *valor mínimo* (tiempo, distancia, costo, etc.) o de *valor máximo* entre un vértice (xo) y otro vértice (xm).

A continuación se describen algunos algoritmos referentes a estos temas.

Además de estos problemas (que en realidad se reducen a la búsqueda de un subconjunto de arcos o aristas, conforme a unas reglas estrictas), existen otros, cuyo objetivo es la búsqueda de un subconjunto de vértices, dotado de alguna propiedad interesante.

5.3. ALGORITMO DE TARRY PARA LA BUSQUEDA DE UN CAMINO

Se trata del problema del "laberinto", partiendo de un vértice a de un grafo sin bucles (hipótesis aplicable a todos los grafos de este capítulo); llegar a otro vértice b.

Supongamos el caso más difícil, es decir, aquel en que el grafo carece de orientación. Cada arista puede ser recorrida en los dos sentidos.

Se procede así:

1.º No recorrer jamás dos veces la misma arista en el mismo sentido.
2.º Si uno se encuentra en un vértice cualquiera (Z), no tomar la arista que nos ha conducido la primera vez al vértice (Z), salvo que no exista otra posibilidad.

Si existe un camino para ir de a a b, es evidente que b será, tarde o temprano, encontrado.

5.4. ALGORITMO PARA LOCALIZAR UN CAMINO DE LONGITUD MINIMA

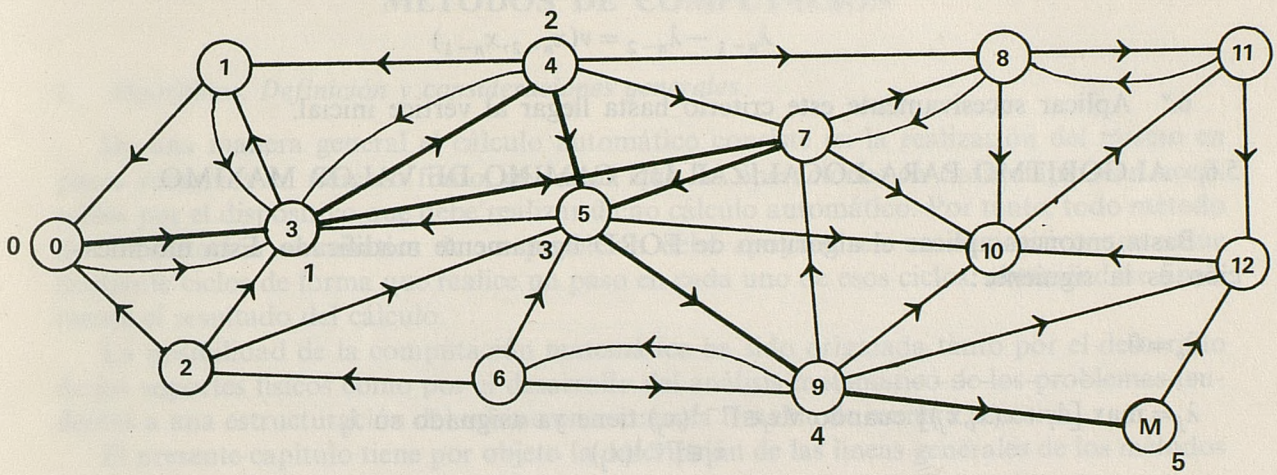
NOTA.—Se le llama longitud de un camino $1(\mu)$ al número de arcos que lo componen.

Para localizar un camino de longitud mínima se procede así:

1.º Asignar la cota 0 al vértice inicial x_o.
2.º Asignar la cota 1 a todos los vértices de $\Gamma(x_o)$.
3.º Asignar la cota 2 a todos los vértices de $\Gamma^2(x_o)$, no todavía marcados.
4.º Proseguir este proceso hasta que le sea asignada una cota al vértice terminal y, aumentando, a cada paso, en una unidad el valor de la cota.
5.º Si p es el valor de la cota que ha correspondido al vértice final y, p es la longitud del más corto camino que permite ir de x_o a y.
6.º La composición del camino o caminos óptimos se obtiene descendiendo desde y por los vértices cuya cota disminuye progresivamente, en una unidad.

Ejemplo:

En el ejemplo de la figura, los caminos de longitud mínima entre O y M son $\mu_1 = (0,3,4,5,9,M)$ y $\mu_2 = (0,3,7,5,9,M)$.



5.5. ALGORITMO PARA LOCALIZAR UN CAMINO DE VALOR MINIMO (algoritmo de FORD)

Sea un grafo $G = (X,U)$ a cada uno de cuyos arcos u se le ha asociado un valor $v(u)$ denominado "valor de u" ($v(u) \geqslant 0$).

El camino de valor mínimo entre dos vértices x_o y x_n será aquel que verifique la relación siguiente:

$$v(\mu) = \sum_{u \in \mu} v(u) \text{ mínimo}$$

En el concepto de valor de un arco pueden incluirse cualidades tales como distancia, tiempo, costo, etc.

Para resolver este problema existen diversos algoritmos. Citaremos aquí el llamado algoritmo de FORD. Una variante del cual, reservada a los grafos sin circuitos, comprende las fases siguientes:

1.º Se marca cada vértice x_i del grafo con un índice λ_i, comenzando por asignar el vértice inicial x_o el valor $\lambda_o = 0$.

2.º El valor λ_i para cada uno de los otros vértices se obtiene así: $\lambda_j = \min [\lambda_i + v(x_i,x_j)]$, para $x_i \in \Gamma^{-1}(x_j)$ cuando $\forall x_i \in \Gamma^{-1}(x_j)$ tiene ya asignado su índice λ_i.

$$x_i \in \Gamma^{-1}(x_i)$$

3.º Detener el proceso en cuanto se le haya podido asignar al último vértice del camino x_n su correspondiente λ_n. El valor del camino óptimo es λ_n.

4.º Para determinar cuáles son los arcos que componen dicho camino se parte del vértice terminal x_n. El último arco del camino será aquel (o aquellos, si hay más de un camino óptimo) para los cuales:

$$\lambda_n - \lambda_{n-1} = v(x_{n-1},\ x_n)$$

5.º Análogamente, el penúltimo arco del camino óptimo (x_{n-2},x_{n-1}) será aquel que cumple la siguiente igualdad:

$$\lambda_{n-1} - \lambda_{n-2} = v(x_{n-2},x_{n-1})$$

6.º Aplicar sucesivamente este criterio hasta llegar al vértice inicial.

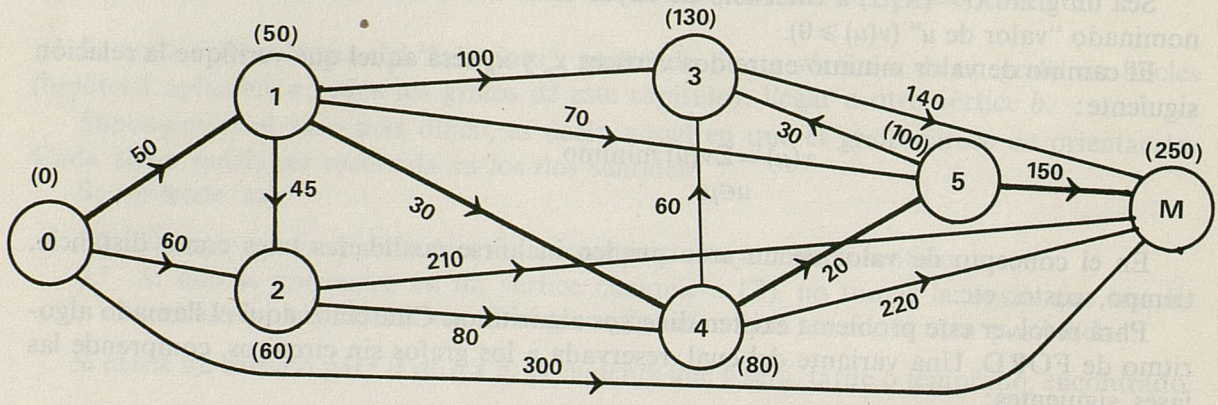
5.6. ALGORITMO PARA LOCALIZAR UN CAMINO DE VALOR MAXIMO

Basta entonces aplicar el algoritmo de FORD ligeramente modificado. Esta modificación es la siguiente:

$\lambda_o = 0$

$\lambda_j = \max [\lambda_i + v(x_i,x_j)]$ cuando $\forall x_i \in \Gamma^{-1}(x_j)$ tiene ya asignado su λ_i
$x_i \in \Gamma^{-1}(x_j)$

Ejemplo:
Calcular el camino más corto entre O y M:



Aplicando el algoritmo de Ford, encontramos como valores de λ los indicados en la figura, resultando el camino más corto $\mu = (0,1,4,5,M)$ y $v(\mu) = 250$.

CAPITULO VII

METODOS DE COMPUTACION

1. *Algoritmos. Definición y consideraciones generales*

De una manera general el cálculo automático consiste en la realización del mismo en pasos sucesivos en número finito, de forma que las operaciones en cada etapa sean aceptables por el dispositivo que debe realizar dicho cálculo automático. Por tanto, todo método de computación automática de un problema debe apoyarse en un dispositivo que actúe mediante ciclos de forma que realice un paso en cada uno de esos ciclos, obteniéndose finalmente el resultado del cálculo.

La posibilidad de la computación matemática ha sido originada tanto por el desarrollo de los soportes físicos como por el desarrollo del análisis matemático de los problemas tendentes a una estructuración del mismo en secuencia tratable de manera sucesiva.

El presente capítulo tiene por objeto la descripción de las líneas generales de los métodos matemáticos de resolución de problemas.

Un algoritmo, de acuerdo con las consideraciones generales anteriores, puede definirse como un método de resolución de un tipo de problemas por aplicación de sucesivas transformaciones, de forma que al final pueda obtenerse bien la solución del problema o bien la decisión de que dicho problema no tiene solución. Caso de que el método de resolución no cumpla esta última condición de posibilidad de análisis de la existencia de solución en el problema, dicho método se llama un semialgoritmo.

Se han hecho distintos esfuerzos en el campo matemático por encontrar métodos generales de definición de algoritmos; dichos métodos tratan de englobar los distintos aspectos que comprenden la estructura de un algoritmo, es decir:

a) Un método de descripción de los tipos de problemas a resolver; ello requiere la definición de un lenguaje con el cual puede describirse dicho problema.
b) Un método de descripción de las transformaciones posibles a aplicar a las distintas palabras del lenguaje, de forma que una sucesión de transformaciones pueda describir un algoritmo.
c) Un criterio para definir la forma de aplicar una secuencia de transformaciones descriptiva del algoritmo a una sucesión de palabras del lenguaje con que se describe el problema.

Los problemas se describen por el método a) y los algoritmos se describen por el método b) y se aplican a los problemas con los criterios c).

La resolución de un problema requiere la utilización de un dispositivo capaz de aceptar los lenguajes a) y b) y que aplique el criterio c) al operar la secuencia de transformaciones sobre el problema.

Los distintos procedimientos matemáticos de estructuración normalizada de algoritmos se basan en distintas hipótesis y procedimientos para los apartados a), b) y c). En el presente capítulo se describen los algoritmos de Markov, las máquinas de Turing y los autómatas finitos, como procedimientos más generalizados de estructuración normalizada de algoritmos.

2. *Algoritmos de Markov*

Este método de normalización de algoritmos tiene la siguiente estructura.

a) Los problemas a tratar estarán constituidos por sucesiones de símbolos de un alfabeto finito prefijado $A = \{a_0, a_1, a_2, \ldots a_n\}$.

b) Un algoritmo consta de una secuencia ordenada de transformaciones o producciones del tipo $X \to Y$ (transformación simple)
$X \to Y.$ (transformación conclusiva)

siendo X e Y sucesiones de elementos del alfabeto A (X antecedente, Y consecuente).

El símbolo $\to$ indica que la transformación sustituye, en la secuencia que define el problema, la aparición de la sucesión delante del signo por la que aparece detrás.

Así, si una secuencia dada es del tipo *mnpXrst*, al aplicar la transformación $X \to Y$ se convertirá en

mnpYrst

Si la transformación es simple el algoritmo continuará, pero si es conclusiva ($X \to Y.$), al aplicar esta transformación se dará por terminado el proceso.

c) La forma de aplicar un algoritmo definido por una secuencia ordenada de transformaciones del tipo descrito en b) a una sucesión de símbolos descriptivos del problema a procesar, consiste en aplicar a la sucesión, en primer lugar, *la primera transformación que aparece en el orden en que se escribe el algoritmo, cuyo antecedente aparece primero en la sucesión estudiada*, si no aparece en la sucesión ninguno de los antecedentes del algoritmo, la sucesión permanece invariable por aplicación del algoritmo programado; si la transformación a aplicar es conclusiva, una vez aplicada se da por terminado el paso del algoritmo a la sucesión propuesta. Caso de que la transformación no sea conclusiva, a la sucesión resultante de la aplicación de la transformación se le aplica el algoritmo de manera análoga, es decir, aplicando la transformación cuyo antecedente aparece primero al recorrer la nueva sucesión de izquierda a derecha; si no aparece ningún antecedente se da por terminado el algoritmo, si aparece y la transformación es conclusiva se aplica ésta, y se da por terminado el algoritmo y si no se continúa de la misma forma.

Ejemplo:

Vamos a definir el algoritmo que, dada una sucesión de elementos del alfabeto {0,1} detecte si el número de unos es par o impar.

Definimos el algoritmo mediante los elementos 0,1, par, impar, y el blanco λ, mediante la siguiente secuencia:

1. par 1——→ impar
2. par 0——→ par
3. impar 1—→ par
4. impar 0—→ impar
5. par λ——→ par.
6. impar λ—→ impar.

conclusivas

7. 0————→ par
8. 1————→ impar

Sea la sucesión 011100110λ; vamos a describir la aplicación del algoritmo anterior a esta sucesión:

Primer paso: Recorremos la sucesión de izquierda a derecha para cada una de las transformaciones de que consta el algoritmo; la primera cuyo antecedente aparece es la 7, que transforma la sucesión en

par 11100110 λ

Segundo paso: Estudiando la sucesión resultante del primer paso, la primera transformación cuyo antecedente aparece en ella es la 1, que transforma par 1→impar, resultando la sucesión:

impar 1100110 λ

Tercer paso: Análogamente, la primera transformación cuyo antecedente aparece es la 3, que transforma impar 1→par, resultando:

par 100110 λ

Cuarto paso: par 1→impar, y resulta:

impar 00110 λ

Quinto paso: impar 0→impar, resulta:

impar 0110 λ

Sexto paso: impar 0→impar, resulta:

impar 110 λ

Séptimo paso: impar $1 \rightarrow$ par, resulta:

par $1\ 0\ \lambda$

Octavo paso: par $1 \rightarrow$ impar, resulta:

impar $0\ \lambda$

Noveno paso: impar $0 \rightarrow$ impar, resulta:

impar λ

Décimo paso: impar $\lambda \rightarrow$ impar. conclusiva.

Por tanto, el algoritmo aplicado a la sucesión dada produce como resultado: "impar", el algoritmo propuesto permite definir, por tanto, en una sucesión de 0,1 cuyo final se indica con un carácter *blanco* si el número de 1 es par o impar.

En el ejemplo descrito la sucesión a tratar podía estar formada por los elementos 0,1, par, impar y λ (blanco), y las transformaciones del algoritmo estaban formadas por estos mismos elementos; sin embargo, cabe la definición de un algoritmo de Markov *sobre* un alfabeto dado, es decir, de forma que se utilicen en la definición de las transformaciones del algoritmo no sólo a sucesiones con elementos del alfabeto de la sucesión a transformar, sino también incluyendo además determinados elementos a efectos de facilitar determinadas operaciones. La necesidad de estos elementos viene impuesta por el hecho de que a efectos de aplicar las transformaciones se manipula la sucesión de izquierda a derecha, seleccionando aquella transformación cuyo antecedente aparece primero en ese orden.

Así, si se quiere transformar S en AS, basta incluir $\lambda \rightarrow A$, ya que la sucesión S siempre puede considerarse $\lambda S \lambda$; pero si se quiere transformar S en SA no hay forma de hacerlo mediante esta instrucción, ya que *siempre se aplicará al primer blanco que aparece a la izquierda de S y no al que aparece detrás*, con lo cual no podría conseguirse. Sin embargo, utilizando el símbolo α no comprendido en el alfabeto M de la sucesión S, podemos definir el siguiente algoritmo:

$$\begin{array}{ll} \alpha\zeta \rightarrow \zeta\alpha & (\zeta \in M) \\ \alpha \rightarrow A & \\ \lambda \rightarrow \alpha & \end{array}$$

La aplicación de este algoritmo permite que la primera operación de λ a la izquierda de S dé lugar a αS, a continuación la primera transformación es aplicable, produciendo:

$$\alpha S \rightarrow S\alpha$$

y la segunda:

$$S\alpha \rightarrow SA$$

La introducción del elemento α, llamado marcador, permite el manejo de la sucesión en un orden distinto del automático, impuesto por las hipótesis de definición de los algoritmos, ya que si bien se lee la sucesión de izquierda a derecha, se puede procesar de derecha a izquierda.

Una ilustración del empleo de marcadores puede verse en el ejemplo siguiente.

Ejemplo

Si queremos implementar un algoritmo de Markov que transforme una cinta constituida por números decimales en el producto de la misma por tres, habremos de emplear marcadores, ya que el orden de lectura de la cinta es de izquierda a derecha y el de proceso en la multiplicación de derecha a izquierda. Utilizando marcadores conseguiremos procesar el elemento de la cinta que interese, de acuerdo con el orden del proceso. En nuestro caso, el alfabeto de la sucesión de entrada es:

$$A = \{0,1,2,3,4,5,6,7,8,9,\$\}$$

\$ es un carácter indicador de principio y final de la sucesión.

Emplearemos los marcadores α, β y γ; a la par de controlar el elemento de la sucesión a tratar, indicarán el acarreo; α indicará que no existe acarreo, β que el acarreo vale 1 y γ que vale 2. El algoritmo es el siguiente:

1. $0\$ \to \alpha 0\$$
2. $1\$ \to \alpha 3\$$
3. $2\$ \to \alpha 6\$$
4. $3\$ \to \alpha 9\$$
5. $4\$ \to \beta 2\$$
6. $5\$ \to \beta 5\$$
7. $6\$ \to \beta 8\$$
8. $7\$ \to \gamma 1\$$
9. $8\$ \to \gamma 4\$$
10. $9\$ \to \gamma 7\$$
11. $0\alpha \to \alpha 0$
12. $1\alpha \to \alpha 3$
13. $2\alpha \to \alpha 6$
14. $3\alpha \to \alpha 9$
15. $4\alpha \to \beta 2$
16. $5\alpha \to \beta 5$
17. $6\alpha \to \beta 8$
18. $7\alpha \to \gamma 1$
19. $8\alpha \to \gamma 4$
20. $9\alpha \to \gamma 7$
21. $0\beta \to \alpha 1$
22. $1\beta \to \alpha 4$
23. $2\beta \to \alpha 7$
24. $3\beta \to \beta 0$
25. $4\beta \to \beta 3$
26. $5\beta \to \beta 6$
27. $6\beta \to \beta 9$
28. $7\beta \to \gamma 2$
29. $8\beta \to \gamma 5$
30. $9\beta \to \gamma 8$
31. $0\gamma \to \alpha 2$
32. $1\gamma \to \alpha 5$
33. $2\gamma \to \alpha 8$
34. $3\gamma \to \beta 1$
35. $4\gamma \to \beta 4$
36. $5\gamma \to \beta 7$
37. $6\gamma \to \gamma 0$
38. $7\gamma \to \gamma 3$
39. $8\gamma \to \gamma 6$
40. $9\gamma \to \gamma 9$
41. $\$\alpha \to \$$.
42. $\$\beta \to \$1$.
43. $\$\gamma \to \$2$.

El algoritmo descrito anteriormente aplicado a la sucesión

\$ 4 9 7 8 5 3 6 \$

produce sucesivamente:

a) $\$497853\beta 8\$$ $(6\$ \to \beta 8\$)$
b) $\$49785\beta 08\$$ $(3\beta \to \beta 0)$
c) $\$4978\beta 608\$$ $(5\beta \to \beta 6)$
d) $\$497\gamma 5608\$$ $(8\beta \to \gamma 5)$
e) $\$49\gamma 35608\$$ $(7\gamma \to \gamma 3)$
f) $\$4\gamma 935608\$$ $(9\gamma \to \gamma 9)$
g) $\$\beta 4935608\$$ $(4\gamma \to \beta 4)$
h) \$14935608\$ $(\$\beta \to \$1.)$

La sucesión resultante es el producto de la inicial por tres.
El algoritmo permite multiplicar cualquier sucesión por tres.

3. *Máquinas de Turing*

Es éste un método de estructuración de algoritmos, descrito por Turing en 1936, que lo concibió como una máquina automática para resolver problemas. Esta máquina puede definirse matemáticamente de la forma siguiente:

a) La máquina tiene como posibles un conjunto finito S de estados.
b) La máquina tiene una cinta infinita dividida en tramos, cada uno de ellos conteniendo un carácter, elemento de un alfabeto dado A. Esta cinta debe estar inicialmente en blanco con la excepción de un número finito de tramos, cada uno de ellos con un carácter.
c) La máquina puede mover la cinta en ambas direcciones y pararla mediante un código de movimiento (izquierda, derecha y alto).

Es decir, la máquina está formada por un conjunto de cinco elementos (A, S, γ, ζ, δ), constituidos por dos conjuntos y tres aplicaciones, con las siguientes características:

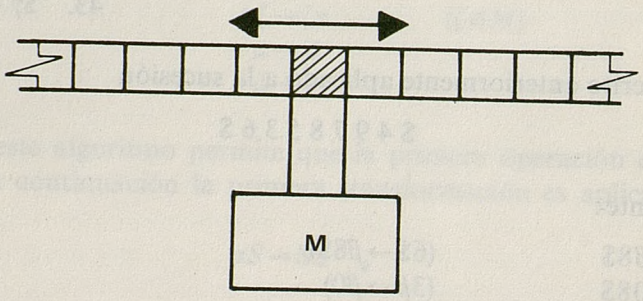
$A = \{a_0, a_1, \ldots a_n\}$, alfabeto formado por un conjunto finito de símbolos.

$S = \{S_0, S_1, \ldots S_m\}$, conjunto finito de estados de la máquina.

$\nu =$ Aplicación de $S \times A \rightarrow S$, que define a partir de cada pareja estado actual-símbolo leído el estado siguiente.

$\zeta =$ Aplicación de $S \times A \rightarrow A$, que define a partir de cada pareja estado actual-símbolo leído, el símbolo a escribir.

$\delta =$ Aplicación de $S \times A \rightarrow$ {izquierda, derecha, parado}, que define a partir de cada pareja estado actual-símbolo leído la estrategia de movimiento de la cinta; es decir, si ésta debe moverse un lugar hacia la izquierda o derecha o debe quedarse parada.



El conjunto del dispositivo puede verse en el gráfico adjunto; la forma de operar es un ciclo indefinido consistente en:

1.º La máquina lee un símbolo de la cinta.
2.º Aplicando la función ζ sustituye en la cinta el símbolo leído por el correspondiente a la pareja estado-símbolo.

3.º Aplicando la función v cambia de estado.
4.º De acuerdo con la pareja estado símbolo leído, decide el movimiento de la cinta y vuelve de acuerdo con ello a 1.º).

La estructuración de un algoritmo se produce con este dispositivo lógico, de la forma siguiente:

a) El problema a tratar se describe mediante una sucesión de símbolos del alfabeto A.
b) El algoritmo de tratamiento de una sucesión se define mediante las funciones v de cambio de estado y δ de movimiento de la cinta.
c) El criterio de aplicación de un algoritmo a un problema viene dado por la forma ya descrita de funcionamiento de la máquina.

Puede darse esta otra definición de la máquina de Turing:

Una máquina de Turing es un conjunto finito de quíntuples S_i^0, a_i^0, a_i^1, M_i, S_i^1, en donde

$S_i^0, S_i^1, \in S$ siendo S el conjunto de estados posibles de la máquina.

$a_i^0, a_i^1, \in A$ siendo A el alfabeto de símbolos descriptivos de los problemas a tratar por la máquina.

$M_i \in$ {izquierdo, derecho, parado}, conjunto de movimientos posibles de la cinta, *con la condición de que dos quíntuples distintos deben tener distintas parejas iniciales* (S_i^0, a_i^0).

El significado de los distintos elementos está relacionado con la definición dada previamente; cada quíntuple representa un conjunto completo de operaciones a realizar por la máquina *en un solo paso*, condicionadas por la pareja S_i^0 a_i^0.

En efecto, S_i^0 a_i^0 constituyen la pareja estado inicial al comienzo del paso, y símbolo leído de la cinta; los otros elementos del quíntuple indican las operaciones a realizar correspondientes a la pareja S_i^0, a_i^0; en efecto,

a_i^1 indica el símbolo a escribir en la cinta; es, por tanto, el elemento que la función ζ aplica a (S_i^0, a_i^0).

M_i indica el movimiento a realizar; representa, por tanto, el elemento que δ hace corresponder a la pareja (S_i^0, a_i^0).

S_i^1 indica el estado final del paso; es decir, es el elemento correspondiente a la pareja (S_i^0, a_i^0), atribuido por la función v.

La descripción de la máquina de Turing mediante el conjunto de quíntuples es la forma más directa de describirla, si bien la estructura corresponde a la definición inicial. *Dentro del quíntuple, los dos primeros elementos son selectores de la operación a realizar; los tres restantes elementos del quíntuple reflejan la operación en sus distintos aspectos*: movimiento de la cinta, transición al estado siguiente y carácter a imprimir en la cinta. Esta estructura de los distintos quíntuples permite la representación de una máquina de Turing mediante una tabla de doble entrada con filas estados iniciales y columnas caracteres leídos, incluyéndose en cada punto de la tabla los tres elementos definitorios de la operación a realizar correspondiente.

Ejemplo

Vamos a definir una máquina de Turing que lea una cinta formada por 0 y 1, indicando su origen y final mediante el signo $ e imprima al comienzo de la misma el símbolo "par" o "impar", según sea par o impar el número de unos de la cinta.

La máquina tiene cinco estados: S_0,S_1,S_2,S_3 y S_4, y un alfabeto formado por los signos {$, 0, 1, par, impar}. λ simboliza el blanco.

Utilizamos el signo α como marcador. Puede definirse mediante la tabla siguiente:

Entrada / Estado actual	$	1	0	impar	par	α	λ
S_0	$\$DS_1$	$1IS_0$	$0IS_0$	impar DS_0	par DS_0		
S_1	$\$HS_0$	αIS_2	$0DS_1$				
S_2	$\$IS_3$	$1IS_2$	$0IS_2$				
S_3				par DS_4	impar DS_4		impar DS_4
S_4	$\$DS_4$	$1DS_4$	$0DS_4$			$1DS_1$	

λ = blanco

La definición de la máquina mediante el conjunto de quíntuples es:

1. $S_0\$\$DS_1$
2. S_011IS_0
3. S_000IS_0
4. S_0 impar impar DS_0
5. S_0 par par DS_0
6. $S_1\$\$HS_0$
7. $S_11\alpha IS_2$
8. S_100DS_1
9. $S_2\$\$IS_3$
10. S_211IS_2
11. S_200IS_2
12. S_3 impar par DS_4
13. S_3 par impar DS_4
14. $S_3\lambda$ impar S_4
15. $S_4\$\$DS_4$
16. S_411DS_4
17. S_400DS_4
18. $S_4\alpha 1DS_1$

Para comprobar la forma de operar de esta máquina, supongamos que la cinta a leer es:

011101

El estado inicial es S_0.

1.º Lee $, escribe $, se desplaza a la derecha y pasa al estado S_1 (quíntuple 1).
2.º Lee 0, escribe 0, se desplaza a la derecha y sigue en S_1 (q. 8).
3.º Lee 1, escribe α, se desplaza a la izquierda y pasa a S_2 (q. 7).
4.º Lee 0, escribe 0, se desplaza a la izquierda y sigue en S_2 (q. 11).
5.º Lee $, escribe $, se desplaza a la izquierda y pasa a S_3 (q. 9).
6.º Lee un blanco, λ, escribe "impar" y pasa a S_4 (q. 14).
7.º Lee $, escribe $, se desplaza a la derecha y sigue en S_4 (q. 15).
8.º Lee 0, escribe 0, se desplaza a la derecha y sigue en S_4 (q. 17).
9.º Lee α, escribe 1, se desplaza a la derecha y pasa a S_1 (q. 18).

A continuación ocurre igual desde 3.º, con la única diferencia de que se desplaza un lugar más a la izquierda y en lugar de leer λ en S_4 lee impar y pasa a par al final de la lectura de la cinta, la máquina acaba en S_0 y la cinta acaba en la forma:

par 011101

Ejemplo

Vamos a describir una máquina de Turing que realice la operación de multiplicación decimal por tres. La máquina leerá una cinta de números acotada inicialmente por $ y finalmente por un blanco.

El algoritmo consistirá en recorrer toda la cinta de izquierda a derecha hasta llegar al final de la misma; recorrerá la cinta de derecha a izquierda, sustituyendo cada cifra por su producto por tres, teniendo en cuenta las cifras que se llevan del producto anterior.

Lectura / Estado	0	1	2	3	4	5	6	7	8	9	$	λ
S_0	$0DS_0$	$1DS_0$	$2DS_0$	$3IS_0$	$4DS_0$	$5DS_0$	$6DS_0$	$7DS_0$	$8DS_0$	$9DS_0$	$\$DS_0$	λIS_1
S_1	$0IS_1$	$3IS_1$	$6IS_1$	$9IS_1$	$2IS_2$	$5IS_2$	$8IS_2$	$1IS_3$	$4IS_3$	$7IS_3$	$\$HS_0$	
S_2	$1IS_1$	$4IS_1$	$7IS_1$	$0IS_2$	$3IS_2$	$6IS_2$	$9IS_2$	$2IS_3$	$5IS_3$	$8IS_3$	$1IS_4$	
S_3	$2IS_1$	$5IS_1$	$8IS_2$	$1IS_2$	$4IS_2$	$7IS_2$	$0IS_3$	$3IS_3$	$6IS_3$	$0IS_3$	$2IS_4$	
S_4												$\$HS_0$

Así, por ejemplo, la máquina antes descrita leería la cinta \$845601λ y la transformaría en \$2536803λ.

Ejemplo

Vamos a diseñar una máquina de Turing para identificar la paridad de números en base 10. Se supondrá que el número viene representado por una sucesión de cifras entre dos marcas \$. La máquina leerá la cinta y escribirá al principio de la cinta "par" o "impar". Se supone inicialmente en el estado S_0

	\$	0	1	2	3	4	5	6	7	8	9	Par	Impar	Blanco
S_0	$\$DS_1$	$0DS_0$	$1DS_0$	$2DS_0$	$3DS_0$	$4DS_0$	$5DS_0$	$6DS_0$	$7DS_0$	$8DS_0$	$9DS_0$			
S_1	$\$IS_2$	$0DS_1$	$1DS_1$	$2DS_1$	$3DS_1$	$4DS_1$	$5DS_1$	$6DS_1$	$7DS_1$	$8DS_1$	$9DS_1$			
S_2	$\$HS_0$	$0IS_4$	$1IS_3$	$2IS_4$	$3IS_3$	$4IS_4$	$5IS_3$	$6IS_4$	$7IS_3$	$8IS_4$	$9IS_3$			
S_3	$\$IS_3$	$0IS_3$	$1IS_3$	$2IS_3$	$3IS_3$	$4IS_3$	$5IS_3$	$6IS_3$	$7IS_3$	$8IS_3$	$9IS_3$	impar DS_5	impar DS_5	impar DS_5
S_4	$\$IS_4$	$0IS_4$	$1IS_4$	$2IS_4$	$3IS_4$	$4IS_4$	$5IS_5$	$6IS_4$	$7IS_4$	$8IS_4$	$9IS_4$	par DS_5	par DS_5	par DS_5
S_5	$\$DS_6$	$0DS_5$	$1DS_5$	$2DS_5$	$3DS_5$	$4DS_5$	$5DS_5$	$6DS_5$	$7DS_5$	$8DS_5$	$9DS_5$			
S_6	$\$HS$	$0DS_6$	$1DS_6$	$2DS_6$	$3DS_6$	$4DS_6$	$5DS_6$	$6DS_6$	$7DS_6$	$6DS_6$	$9DS_6$			

La máquina descrita recorre la sucesión de izquierda a derecha, y cuando detecta el último signo \$ vuelve atrás comprobando la paridad de la última cifra, adoptando un estado u otro, según la misma; recorre la cinta en dirección contraria hasta encontrar el primer signo \$, a cuya izquierda escribe par o impar, y recorre de nuevo la cinta de derecha a izquierda, para parar y pasar a S_0 finalmente.

4. *Autómatas finitos*

Un autómata finito (también llamado máquina de estado finito) puede definirse matemáticamente como constituido por cinco elementos $\{A, S, Z, v, \zeta\}$, siendo:

A = Alfabeto de símbolos de entrada, en número finito.

$$A = \{a_0, a_1, a_2, \ldots a_n\}$$

S = Conjunto finito de estados posibles de la máquina.

$$S = \{S_0, S_1, S_2, \ldots S_n\}$$

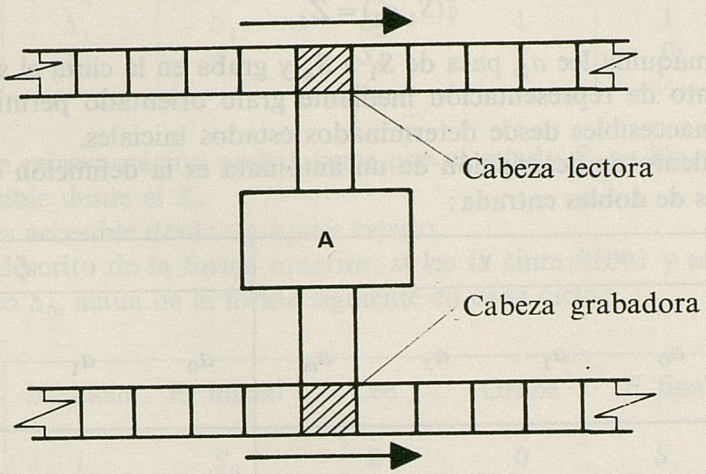
Z = Alfabeto de símbolos de salida, con número finito de símbolos.

$$Z = \{Z_0, Z_1, Z_2, \ldots Z_n\}$$

v = Aplicación $A \times S \rightarrow S$, que permite definir a partir de un símbolo de entrada leído y el estado actual del autómata el estado siguiente.

ζ = Aplicación $A \times S \rightarrow Z$ que permite definir a partir de un símbolo de entrada y el estado del autómata el símbolo inmediato de salida, elemento de Z.

A partir de esta definición el funcionamiento del autómata puede representarse de la forma indicada en la figura, constituido por una máquina en la que aparecen dos cabezas, una lectora y otra grabadora, sobre sendas cintas. El funcionamiento arranca de un estado inicial en la máquina $e_1 (e \in S$, lee un símbolo de la cinta de lectura, l_1 $(l_1 \in A)$.



Mediante la función v atribuye a la pareja e_1, l_1 el estado siguiente a tomar, e_2 (e_2 es el elemento de S definido por v (e_1, l_1).

La cinta grabadora se llama también cinta de memoria, y sólo puede moverse en un sentido, a diferencia de la máquina de Turing.

Mediante la función ζ atribuye a la pareja e_1, l_1 un elemento g_1 de Z, y entonces la máquina graba en la cinta de memoria g_1.

Vemos, por tanto, que en esta etapa de funcionamiento la máquina ha partido de un estado inicial e_1, ha leído un símbolo l_1, ha grabado otro g_1 y ha pasado al estado e_2; el funcionamiento continúa de manera análoga; en el estado e_2 leerá de la cinta de lectura un nuevo símbolo l_2 $(l_2 \in A)$, grabará en la cinta de memoria otro símbolo g_2 $(g \in Z)$ y pasará de e_2 a un nuevo estado e_3 $(e_3 \in S)$.

De acuerdo con la descripción anterior vemos que en una sucesión de ciclos de operación mediante las funciones v y ζ y la definición del estado inicial de la máquina, puede pasarse de una sucesión de elementos del alfabeto A leídos en una cinta a otra sucesión de elementos del alfabeto Z grabados en otra cinta.

En este caso, la normalización del algoritmo se produce en la siguiente forma:

a) El problema se describe mediante una sucesión de elementos del alfabeto de entrada.

b) El proceso de tratamiento se describe mediante el alfabeto de salida y las funciones v y δ de transición entre estados y de relación entre entrada y salida.

c) La forma de aplicación consiste en utilizar los criterios de funcionamiento antes descritos.

Si las funciones v y ζ están completamente definidas, es decir, para cada elemento de $S \times A$ está definido el correspondiente en S (función v) o en Z (función ζ), se dice que la máquina está completamente definida; en este caso, dado un estado inicial a cada secuencia leída de elementos de A, le corresponde una única secuencia de elementos de Z grabados.

La visualización de un autómata definido en la forma anterior puede realizarse mediante un grafo orientado en el que los nudos son los estados y los arcos son parejas de elementos (l_i, g_i) de los alfabetos A y Z de entrada y salida, ligados mediante v a los estados extremos del arco; así, si entre dos estados S_1 y S_4 existe un arco cuyo sentido va de S_1 a S_4, al que se le atribuye la pareja de elementos (a_2, Z_4), ello representa que

$$v(S_1,a_2) = S_4$$
$$\zeta(S_1,a_2) = Z_4$$

Es decir, si la máquina lee a_2, pasa de S_1 a S_4 y graba en la cinta el símbolo Z_4.

El procedimiento de representación mediante grafo orientado permite visualizar muy bien los estados inaccesibles desde determinados estados iniciales.

Otro procedimiento de descripción de un autómata es la definición de las funciones v y ζ mediante tablas de dobles entrada:

Funciones	v				ζ			
Símbolo leído / Estado actual	a_0	a_1	a_2	a_m	a_0	a_1	a_2	$a_3 \ldots a_m$
S_0 S_1 S_2 S_3 S_n			S_4				Z_4	

En cada elemento de la cuadrícula se incluye el valor atribuido por v y ζ a la pareja de elementos de cabecera de fila y columna.

A continuación se indican algunos ejemplos de autómatas y sus representaciones correspondientes.

Ejemplos de autómatas finitos

Ejemplo 1

Supongamos el alfabeto de entrada $A = \{0,1\}$ y el de salida $Z = \{0,1\}$; sea el conjunto de estados S constituido por tres estados $S = \{S_0,S_1,S_2\}$.

Las funciones v y ζ, $S \times A \to S$ y $S \times A \to Z$ se definen de la forma siguiente:

$(0,S_0) \to S_1$	$(0,S_0) \to 0$
$(1,S_0) \to S_0$	$(1,S_0) \to 1$
$(0,S_1) \to S_1$	$(0,S_1) \to 1$
$(1,S_1) \to S_2$	$(1,S_1) \to 1$
$(0,S_2) \to S_1$	$(0,S_2) \to 1$
$(1,S_2) \to S_0$	$(1,S_2) \to 0$

La representación mediante tabla es la siguiente:

Funciones	ν		ζ	
Entrada / Estado actual	0	1	0	1
S_0	S_1	S_0	0	1
S_1	S_1	S_2	1	1
S_2	S_1	S_0	1	0

En el grafo de representación podría verse que el estado S_0 es inaccesible desde el S_1, y el S_2 es inaccesible desde el S_0.

El estado S_1 es accesible desde cualquier estado.

El autómata descrito de la forma anterior, si lee la cinta 01001 y se encuentra inicialmente en el estado S_0, actúa de la forma siguiente en cada ciclo:

N.º ciclo	E. inicial	Lee	Graba	E. final
1	S_0	0	0	S_1
2	S_1	1	1	S_2
3	S_2	0	1	S_1
4	S_1	0	1	S_1
5	S_1	1	1	S_2

Por tanto, en la cinta de memoria graba 01111 y el estado final es S_2.

Ejemplo 2.

Supongamos la máquina de dos estados S_0,S_1 con alfabetos A y Z, como en el ejemplo 1, constituidos por $\{0,1\}$, definidos por la tabla siguiente:

Funcion	ν		ζ	
Entrada / Estado actual	0	1	0	1
S_0	S_0	S_1	0	1
S_1	S_1	S_0	0	1

De acuerdo con la descripción del autómata, éste reproduce exactamente cualquier secuencia leída y se encuentra en un estado u otro según el número de *unos* leídos sea par o impar, ya que si lee 0, permanece en el estado en que se encontraba, y si lee 1 pasa de S_0 a S_1 o de S_1 a S_0, según el estado en que se encuentre; de esta forma, si el estado inicial es S_0, si el número de unos leídos es par se encontrará en estado S_0, y si es impar, en S_1.

El autómata definido de esta forma es una máquina para detectar el error de paridad (*parity check*) en secuencias dadas. Puede incluirse un dispositivo para que la máquina imprima *par* o *impar*, añadiendo en el alfabeto de lectura un carácter E y en el de escritura los símbolos *par* e *impar*:

$$A = \{0,1,E\} \qquad Z = \{0,1, \text{par, impar}\}$$

Cuando la máquina está en S_0 y lee E escribe *par*; si está en S_1 y lee E escribe *impar*. El nuevo autómata se describe mediante la tabla siguiente:

Función	v			ζ		
Entrada / Estado actual	0	1	E	0	1	E
S_0	S_0	S_1	S_0	0	1	Par
S_1	S_1	S_0	S_1	0	1	Impar

Ejemplo

Vamos a diseñar un autómata que transforme números decimales en su producto por tres.

El alfabeto de entrada y salida es: $A = \{1,2,3,4,5,6,7,8,9,\$,\lambda\}$. \$, carácter indicador de fin de cinta; λ, carácter blanco.

La cinta de entrada se supone que se lee de derecha a izquierda y se considera que la de salida se escribe en la misma forma.

Un autómata que realiza esta operación es el siguiente:

Funciones	v											ζ											
Entrada / E. actual	0	1	2	3	4	5	6	7	8	9	\$	0	1	2	3	4	5	6	7	8	9	\$	λ
S_0	S_0	S_0	S_0	S_0	S_1	S_1	S_1	S_2	S_2	S_2	S_0	0	3	6	9	2	5	8	1	4	7	\$	λ
S_1	S_0	S_0	S_0	S_1	S_1	S_1	S_1	S_2	S_2	S_2	S_1	1	4	7	0	3	6	9	2	5	8	1	\$
S_2	S_0	S_0	S_0	S_1	S_1	S_1	S_2	S_2	S_2	S_2	S_2	2	5	8	1	4	7	0	3	6	9	2	\$

El autómata definido lee de derecha a izquierda una cinta y graba otra en la misma dirección con el producto de la misma por tres; se supone que el estado inicial es S_0 y al final del proceso continúa en S_0.

Así, la cinta \$865432 se procesa de la manera siguiente: Suponemos el autómata en estado S_0:

Estado	Lee	Escribe	Estado siguiente
S_0	2	6	S_0
S_0	3	9	S_0
S_0	4	2	S_1
S_1	5	6	S_1
S_1	6	9	S_1
S_1	8	5	S_2
S_2	\$	2	S_2
S_2		\$	S_0

Es decir, la cinta resultante es \$2596296, que es el producto del número leído por tres.

BIBLIOGRAFIA

El curso del que se han tomado estos apuntes tiene como base los siguientes textos, cuya lectura se recomienda:

S. MAC LANE G. BIRCKHOFF, *Algebra*. Mac Millan, 1967, New York.

G. BIRKHOFF y T. C. BARTEE, *Modern Applied Algebra*. Mc Graw Hill, 1970, New York.

B. ROY y M. HORPS, *Algebre Moderne et Theorie des Graphes*. Dunod, Paris, 1970.

E. J. WHITESITT, *Boolean Algebra and its applications*. Addison Wesley, 1961.

D. KAYE, *Sistemas booleanos*. Editorial Alhambra, 1970.

R. R. KORFHAGE, *Lógica y algoritmos*. Limusa Wiley, 1970.

INDICE POR CAPITULOS


MEC

METODOS MATEMATICOS DE APLICACION A LA INFORMATICA • SISTEMAS