# TEMARIO LMD

JESÚS MIRANDA GARCÍA

# Capítulo 1

# Inducción y recurrencia

## 1.1. Inducción y deducción.

Cuando realizamos una afirmación o proposición, una forma de clasificarla podría ser si corresponde con una proposición general (por ejemplo, una proposición general podría ser *a los niños les gusta el chocolate*), en la que se dice algo sobre todos los elementos de un conjunto, o con una proposición particular (por ejemplo, *al hijo de Juanito le gusta el chocolate*), en la que se afirma algo sobre algún elemento en particular de un conjunto.

Si admitimos como cierta una proposición general, podemos pasar a la certeza de las correspondientes proposiciones particulares. Por ejemplo, si fuera cierta la afirmación general que hemos puesto anteriormente de que a los niños les gusta el chocolate, de ahí podemos afirmar con seguridad que al hijo de Juanito (que es un niño) le gusta el chocolate.

El proceso por el cual inferimos la certeza de una proposición particular a partir de la certeza de una general, se llama *deducción.* Del hecho de que a los niños les gusta el chocolate hemos deducido que al hijo de Juanito le gusta el chocolate.

Recíprocamente, de la certeza de una o varias afirmaciones particulares, podemos inferir la certeza de una proposición general. A este proceso, se le suele llamar *inducción.* Por ejemplo, después de haber conocido a varios niños y haber comprobado que a todos ellos les gusta el chocolate podemos inducir que a todos los niños les gusta el chocolate.

En el avance científico están presentes ambos procesos. A partir de la observación de determinados fenómenos, se pasa a una afirmación general, que posteriormente permite deducir nuevos hechos. Por ejemplo, la ley de la Gravitación Universal fue una generalización de lo que se observaba que ocurría con los objetos que encontrábamos en la Tierra, así como el comportamiento de los planetas en su interacción con el Sol. Ahora, de esta afirmación general se han deducido gran cantidad de consecuencias que no son más que la particularización de esta ley al caso de dos o más objetos.

La certeza de una proposición general nos asegura la certeza de cada una de las proposiciones particulares. El proceso inverso (el paso de las proposiciones particulares a la general) sin embargo no es tan claro. Aunque hayamos observado que a cientos de niños les gusta el chocolate, no por ello podemos estar seguros de la certeza de que *a todos los niños les gusta el chocolate.*

En matemáticas, cuando afirmamos algo, hemos de tener la certeza absoluta de que lo que decimos es verdad. Nos preguntamos entonces: ¿tiene cabida la inducción en matemáticas?.

Para responder a esta pregunta, vamos a analizar qué ocurre cuando sumamos los números impares. Empezamos por la suma de sólo un número impar (el primero), continuamos calculando la suma de los dos primeros números impares, y así sucesivamente.

$$\begin{array}{lrcl} 1 & = & 1 & = 1^2 \\ 1+3 & = & 4 & = 2^2 \\ 1+3+5 & = & 9 & = 3^2 \\ 1+3+5+7 & = & 16 & = 4^2 \\ 1+3+5+7+9 & = & 25 & = 5^2 \\ 1+3+5+7+9+11 & = & 36 & = 6^2 \end{array}$$

Podemos comprobar, como por ejemplo, la suma $1+3+5+7+9+11+13+15+17+19$ vale 100, que es igual a $10^2$.

A la vista de esto, ¿podemos imaginarnos cuánto valdría, por ejemplo, la suma de los números impares desde el 1 hasta el 199, sin necesidad de realizar la suma?

Vemos como estamos sumando los 100 primeros números impares, luego esa suma parece que debe valer $100^2 = 10000$. Con un programa sencillo de ordenador podemos comprobar que eso es cierto.

¿Nos permiten estos ejemplos inducir una regla para calcular la suma de los $n$ primeros números enteros impares?. Todo apunta a que el valor de esa suma vale $n^2$.

Antes de continuar, vamos a tratar de escribir más formalmente esta regla. Lo primero que tenemos que ver es cómo hacer referencia al quinto número impar, o al vigésimo cuarto número impar. Fácilmente vemos que el quinto número impar es $9 = 2 \cdot 5 - 1$, y que el vigésimo cuarto es $47 = 2 \cdot 24 - 1$. Por tanto, el $n$-ésimo número impar es $2n - 1$. Entonces, lo que afirmamos es que la suma de los números impares, desde 1 hasta $2n - 1$, vale $n^2$.

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

O si adoptamos la notación de sumatoria

$$\sum_{k=1}^{n} (2k - 1) = n^2$$

Podemos ahora tomar números al azar, por ejemplo, $n = 47$, $n = 134$, $n = 3627$, y comprobar que esta afirmación ($\sum_{k=1}^{n} (2k - 1) = n^2$) es verdadera.

Pero por muchos números que elijamos, eso no nos garantiza que esta afirmación sea cierta para cualquiera de los infinitos números naturales que existen.

Supongamos, por un momento, que la afirmación es cierta para $n = 78$ (no hace falta que lo comprobemos), es decir,

$$1 + 3 + 5 + 7 + \cdots 151 + 153 + 155 = 78^2 = 6084$$

Entonces, para calcular la suma de los 79 primeros números impares, podemos aprovechar lo que tenemos

$$1 + 3 + 5 + 7 + \cdots 153 + 155 + 157 = 78^2 + 157 = 6084 + 157 = 6241 = 79^2$$

Y vemos que si la afirmación es cierta para $n = 78$ entonces es cierta para $n = 79$. Tendríamos entonces que

$$1 + 3 + 5 + 7 + \cdots 153 + 155 + 157 + 159 = 79^2 + 159 = 6241 + 159 = 6400 = 80^2$$

Y la afirmación sería cierta para $n = 80$. Es decir, el hecho de ser cierta para $n = 78$ nos garantiza que es cierta para $n = 79$, y para $n = 80$. ¿Podríamos repetir esto para obtener que es cierta para $n = 81$, $n = 82$, etc?

Vamos a escribirlo de otra forma

$$1+3+5+7+\cdots 153+155+157+159 = 79^2+159 = 79^2+2\cdot 79+1 = 79^2+2\cdot 79\cdot 1+1^2 = (79+1)^2 = 80^2$$

Y observamos que el valor concreto $n = 79$ no es relevante en el razonamiento anterior. Por tanto, para cualquier número natural $n$, si suponemos que

$$1 + 3 + 5 + \cdots + (2n - 3) + (2n - 1) = n^2$$

entonces

$$1 + 3 + 5 + \cdots + (2n - 3) + (2n - 1) + [2(n + 1) - 1] = n^2 + 2n + 1 = (n + 1)^2$$

Dicho de otra forma, si la suma de los primeros $n$ números impares vale $n^2$, entonces la suma de los $n+1$ primeros números impares vale $(n+1)^2$.

Entonces, si es cierto que $\sum_{k=1}^{78}(2k-1)=78^2$, también es cierto que $\sum_{k=1}^{79}(2k-1)=79^2$, y es cierto que $\sum_{k=1}^{80}(2k-1)=80^2$, y que $\sum_{k=1}^{81}(2k-1)=81^2$. Repitiendo este proceso las veces que haga falta, podríamos ver que es cierto que $\sum_{k=1}^{3421}(2k-1)=3421^2$, o que $\sum_{k=1}^{792348579}(2k-1)=792348579^2$.

Nosotros hemos comprobado que para $n=1$ la afirmación es cierta (y para $n=2,3,4,5,6$). Como cualquier número natural $n$ lo podemos obtener a partir de 1 sumándole uno unas cuantas veces, entonces, para cualquier número natural $n\geq 1$ podemos afirmar que la suma de los primeros $n$ números impares vale $n^2$, es decir,

$$\sum_{k=1}^{n}(2k-1)=n^2$$

Aquí termina el proceso de inducción. Si lo analizamos, vemos que lo que hemos hecho ha sido:

- A partir de unos cálculos, hemos inducido una regla que pensamos que debe ser válida para todos los números naturales.
- Hemos comprobado que esa regla vale para el número natural $n=1$.
- Suponiendo que la regla vale para un número natural $n$, hemos comprobado que vale para el número natural $n+1$.

Y esto nos garantiza la veracidad de la proposición general.

Para poder dar por cierta una afirmación matemática es necesario disponer de un argumento que asegure su veracidad. El hecho de comprobarla para unos cuantos casos particulares, por muchos que sean no nos garantiza nada. Por ejemplo, podemos observar lo siguiente:

$$4=2+2;\quad 6=3+3;\quad 8=3+5;\quad 10=3+7;\quad 12=5+7;\quad 14=3+11;\quad 16=5+11$$

Y vemos que los primeros números pares (salvo el 2) se pueden expresar como suma de dos números primos. Podemos pensar en otro número par, y probablemente comprobemos que esa afirmación sigue siendo cierta. De hecho, se ha comprobado para todos los números pares menores que $10^{18}$ (un trillón).

Pero no se ha encontrado ningún argumento para asegurar que la afirmación es cierta para cualquier número par. Por tanto, este resultado no pasa de ser una conjetura (con todos los visos de ser cierta) conocida como *conjetura de Goldbach*, en honor a Christian Goldbach, matemático prusiano (de Könisgberg) que en 1742 comunicó semejante enunciado por carta a Leonard Euler.

## 1.2. Números naturales. Principio de inducción.

El ejemplo que acabamos de analizar es una aplicación del conocido *principio de inducción*. El contexto natural donde aplicarlo es el conjunto de los números naturales (aunque con algunas modificaciones podría extenderse a cualquier conjunto bien ordenado, o también al conjunto de los números enteros). Todos sabemos que a dicho conjunto se le suele denominar como $\mathbb{N}$, y que está formado por los elementos $0,1,2,\cdots$. Es decir, $\mathbb{N}=\{0,1,2,\cdots\}$. Para llegar a este conjunto podemos basarnos en los axiomas de Peano, o bien, partir de una construcción basada en los axiomas de la teoría de conjuntos de Zermelo-Fraenkel, y de la que los axiomas de Peano son consecuencias de la construcción realizada.

No vamos a entrar en cómo obtener el conjunto $\mathbb{N}$. Lo que sí vamos a hacer es recordar algunas propiedades y características de este conjunto y sus elementos.

Para empezar, a los elementos del conjunto $\mathbb{N}$ los llamaremos números naturales. Dados dos números naturales $m, n$, tenemos definidos otros dos números naturales, llamados respectivamente suma y producto de $m$ y $n$, y representados mediante $m+n$ y $m \cdot n$ (o simplemente $mn$). Esto nos define dos operaciones en $\mathbb{N}$, que satisfacen las siguientes propiedades:

i) Para cualesquiera $m, n, p \in \mathbb{N}$, $(m+n)+p = m+(n+p)$ (es decir, la suma es asociativa).

ii) Para cualesquiera $m, n \in \mathbb{N}$, $m+n = n+m$ (es decir, la suma es conmutativa).

iii) Existe en $\mathbb{N}$ un elemento, representado por 0 tal que para cada $m \in \mathbb{N}$ se tiene que $m+0 = m$ (existencia de elemento neutro para la suma).

iv) Si $m+n = m+p$ entonces $n = p$ (Propiedad cancelativa).

v) Para cualesquiera $m, n, p \in \mathbb{N}$, $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ (es decir, el producto es asociativo).

vi) Para cualesquiera $m, n \in \mathbb{N}$, $m \cdot n = n \cdot m$ (es decir, el producto es conmutativo).

vii) Existe en $\mathbb{N}$ un elemento, representado por 1 tal que para cada $m \in \mathbb{N}$ se tiene que $m \cdot 1 = m$ (existencia de elemento neutro para el producto).

viii) Si $m \cdot n = m \cdot p$ y $m \neq 0$ entonces $n = p$.

ix) Para cualesquiera $m, n, p \in \mathbb{N}$, $m \cdot (n+p) = m \cdot n + m \cdot p$ (la suma es distributiva respecto al producto).

Al conjunto de los números naturales, salvo el cero, lo denotaremos como $\mathbb{N}^*$. Es decir, $\mathbb{N}^* = \{1, 2, 3, \cdots\}$

> Con estas propiedades, estamos diciendo que $\mathbb{N}$ es un semianillo conmutativo con elemento unidad. De momento hay muchos conjuntos para los que es cierto todo lo dicho hasta aquí. Por ejemplo, $\mathbb{Z}$ (los números enteros), $\mathbb{Q}$ (los números racionales), $\mathbb{R}$ (los números reales), $\mathbb{Q}^+$ (las fracciones mayores o iguales que cero), $\mathbb{R}^+$ (los números reales mayores o iguales que cero), los elementos de $\mathbb{Q}^+$ con denominador 5 ó 1, $\mathbb{C}$ (los números complejos), $\mathbb{Z}_p$, con $p$ primo (los enteros módulo $p$), $\mathbb{R}[x]$ (los polinomios con coeficientes reales), etc.

También en $\mathbb{N}$ hay definida una relación como sigue:

$$m \leq n \text{ si existe } p \in \mathbb{N} \text{ tal que } m+p = n$$

que satisface las siguientes propiedades:

x) $m \leq m$ para todo $m \in \mathbb{N}$ (la relación es reflexiva).

xi) Si $m \leq n$ y $n \leq m$ entonces $m = n$ (la relación es antisimétrica).

xii) Si $m \leq n$ y $n \leq p$ entonces $m \leq p$ (la relación es transitiva).

xiii) Para cualesquiera $m, n \in \mathbb{N}$, $m \leq n$ ó $n \leq m$.

Una relación que satisface estas tres las propiedades x), xi), xii) es lo que se conoce como una relación de orden (u orden parcial). Si además satisface la propiedad xiii) entonces lo que tenemos es un orden total.

> En todos los ejemplos vistos en la observación anterior podemos definir una relación de orden total. Sin embargo, la forma de definirlo en $\mathbb{C}$ o en $\mathbb{R}[x]$ es algo rebuscada y "poco natural". Por tanto, de los conjuntos anteriores, nos quedamos con $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p$, $\mathbb{Q}^+$, $\mathbb{R}^+$, o los números racionales con denominador 1 ó 5 (el orden en $\mathbb{Z}_p$ sería $0 \leq 1 \leq 2 \leq \cdots \leq p-1$).

xiv) $m \leq n$ implica que $m+p \leq n+p$ para todo $p \in \mathbb{N}$.

xv) $m+p \leq n+p$ implica que $m \leq n$.

xvi) $m \leq n$ implica que $m \cdot p \leq n \cdot p$.

xvii) Si $m \cdot p \leq n \cdot p$ y $p \neq 0$ entonces $m \leq n$.

Las propiedades xiv) y xv) fallan en $\mathbb{Z}_p$. Por ejemplo, en $\mathbb{Z}_7$ tendríamos $2 \leq 5$, pero $2+4$ no es menor o igual que $5+4$. Las propiedades xvi) y xvii) fallan también en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$. Por ejemplo, $2 \leq 5$ pero $2 \cdot (-1)$ no es menor o igual que $5 \cdot (-1)$.

Las 17 propiedades vistas hasta ahora valen, además de para $\mathbb{N}$, para otros conjuntos, como $\mathbb{Q}^+$, $\mathbb{R}^+$, los números racionales positivos con denominador 1 ó 5, etc. Lo que distingue a $\mathbb{N}$ de estos conjuntos es el *Principio de inducción*, que viene a decirnos que los números naturales podemos recorrerlos *de uno en uno, y empezando por cero.*

## Principio de inducción:

Si $A$ es un subconjunto de $\mathbb{N}$ tal que:

$0 \in A$

Si $n \in A$ entonces $n+1 \in A$

Entonces $A = \mathbb{N}$.

Es decir, cualquier número natural puede ser obtenido a partir del cero sin más que sumar uno las veces que sean necesarias. Si lo pensamos, para los conjuntos $\mathbb{Q}^+$ o $\mathbb{R}^+$ no se cumple esta propiedad, pues procediendo así siempre nos dejamos números "en medio".

También podemos enunciar este principio diciendo que si $A$ es un subconjunto de $\mathbb{N}^*$ tal que $1 \in A$ y $(n \in A \Longrightarrow n+1 \in A)$, entonces $A = \mathbb{N}^*$.

El ejemplo que hemos analizado en la sección anterior, podemos verlo ahora así.

Tomamos $A = \{n \in \mathbb{N}^* : \sum_{k=1}^{n} (2k-1) = n^2\}$.

Comprobamos que $1 \in A$ (de hecho, hemos comprobado que $1, 2, 3, 4, 5, 6 \in A$), y que si $n \in A$ entonces $n+1 \in A$.

Por el principio de inducción, tenemos que $A = \mathbb{N}^*$, luego para cualquier número natural $n \geq 1$ se tiene que $n \in A$, es decir, $\sum_{k=1}^{n} (2k-1) = n^2$.

El principio de inducción es la base de muchas demostraciones en las que intervienen los números naturales. Veamos un ejemplo.

**Ejemplo 1.2.1.** *Empezamos observando lo siguiente:*

$$\begin{array}{lrcl}
2^0 & = & 1 & = 2^1 - 1 \\
2^0 + 2^1 & = & 3 & = 2^2 - 1 \\
2^0 + 2^1 + 2^2 & = & 7 & = 2^3 - 1 \\
2^0 + 2^1 + 2^2 + 2^3 & = & 15 & = 2^4 - 1 \\
2^0 + 2^1 + 2^2 + 2^3 + 2^4 & = & 31 & = 2^5 - 1 \\
2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 & = & 63 & = 2^6 - 1
\end{array}$$

*Luego parece ser que, para cualquier número natural n se verifica que*

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

*Para esto, consideramos el conjunto A cuyos elementos son los números naturales para los que se verifica la propiedad anterior, es decir,*

$$A = \{n \in \mathbb{N} : 2^0 + \cdots + 2^n = 2^{n+1} - 1\}$$

*Claramente se tiene que* $0 \in A$, *pues* $2^0 = 2^{0+1} - 1$.

*Supongamos ahora que* $n \in A$, *y veamos que* $n+1 \in A$, *es decir, supongamos que* $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$ *y comprobemos que* $2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1$.

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$$

*Por el principio de inducción se tiene que $A = \mathbb{N}$, es decir, la propiedad es cierta para todo $n \in \mathbb{N}$.*

Una demostración basada en el principio de inducción es lo que se conoce como una demostración por inducción.

Si queremos demostrar por inducción que $P(n)$ es cierto para todo $n \in \mathbb{N}$ (donde $P(n)$ es una propiedad que hace referencia a $n$), podemos hacerlo como sigue:

- Caso base: Demostramos que $P(0)$ es cierto.
- Hipótesis de inducción: Suponemos que $P(n)$ es cierto.
- Paso inductivo: A partir de la hipótesis de inducción, demostramos que es cierto $P(n+1)$.

A continuación vamos a ver distintos ejemplos de aplicación de esto último.

**Ejemplo 1.2.2.**

1. *Vamos a comprobar que para todo $n \geq 1$ se verifica que*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

*Hacemos esto por inducción:*

- *Caso base: Para $n = 1$ el resultado es trivialmente cierto.*
- *Hipótesis de inducción: Para un número natural $n$ se tiene que $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.*
- *Paso inductivo: A partir de la hipótesis de inducción hemos de probar que $1 + 2 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}$*

$$(1 + 2 + \cdots + n) + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

*Cuentan que cuando Gauss tenía 10 años de edad, su profesor de aritmética, enfadado porque sus alumnos se portaban mal, los puso a calcular la suma de los primeros 100 números naturales. Mientras, el profesor se sentó en su silla a leer el periódico, confiando en que los niños tardarían bastante tiempo en realizar la suma. Sin embargo, en pocos minutos, el pequeño Gauss, llegó con el resultado de la suma: 5050.*

*El profesor, intrigado por el poco tiempo que había tardado le pidió que le explicara cómo había obtenido tal resultado. Gauss entonces explicó que podemos escribir la suma como $1+2+3+\cdots+99+100$, pero también como $100 + 99 + 98 + \cdots + 2 + 1$.*

*Escribimos ambas sumas (que son iguales) una debajo de otra*

$$\begin{array}{ccccccccccccc} 1 & + & 2 & + & 3 & + & \cdots & + & 98 & + & 99 & + & 100 \\ 100 & + & 99 & + & 98 & + & \cdots & + & 3 & + & 2 & + & 1 \end{array}$$

*Y ahora sumamos* en vertical

$$\begin{array}{ccccccccccccc} 1 & + & 2 & + & 3 & + & \cdots & + & 98 & + & 99 & + & 100 \\ 100 & + & 99 & + & 98 & + & \cdots & + & 3 & + & 2 & + & 1 \\ \hline 101 & + & 101 & + & 101 & + & \cdots & + & 101 & + & 101 & + & 101 \end{array}$$

*La suma inferior vale $101 \cdot 100$, y puesto que esta suma es 2 veces la suma que nos piden, la suma de los 100 primeros números es $\frac{101 \cdot 100}{2} = 5050$.*

*Utilizando esta técnica podríamos haber obtenido también la fórmula que hemos visto de que $1+2+\cdots+n = \frac{n(n+1)}{2}$.*

*Llamemos $S$ a la suma. Entonces:*

$$\begin{array}{ccccccccccccccc} S & = & 1 & + & 2 & + & 3 & + & \cdots & + & (n-2) & + & (n-1) & + & n \\ S & = & n & + & (n-1) & + & (n-2) & + & \cdots & + & 3 & + & 2 & + & 1 \\ \hline 2S & = & (n+1) & + & (n+1) & + & (n+1) & + & \cdots & + & (n+1) & + & (n+1) & + & (n+1) \end{array}$$

*Es decir, $2S = n(n+1)$, luego $S = \frac{n(n+1)}{2}$.*

2. *Vamos a demostrar que para cualquier número natural $n$, el número $7^n - 1$ es múltiplo de 6.*

   *Procedemos también por inducción.*

   - *Caso base: Aquí el primer caso es $n = 0$. Para $n = 0$ se tiene que $7^n - 1 = 7^0 - 1 = 1 - 1 = 0$, que claramente es múltiplo de 6.*
   - *Hipótesis de inducción: El número $7^n - 1$ es múltiplo de 6, es decir, para algún número entero $k$ se tiene que $7^n - 1 = 6k$.*
   - *Paso inductivo: Suponiendo que la hipótesis de inducción es cierta, tenemos que probar que $7^{n+1} - 1$ es también múltiplo de 6.*

     *Por la hipótesis de inducción sabemos que $7^n = 1 + 6k$. Entonces:*

     $$7^{n+1} - 1 = 7 \cdot 7^n - 1 = 7 \cdot (1 + 6k) - 1 = 7 + 7 \cdot 6k - 1 = 6 \cdot 7k + 6 = 6 \cdot (7k + 1)$$

     *que es múltiplo de 6.*

   *Con esto concluye la demostración.*

   *La inducción no es la única forma de demostrar afirmaciones sobre los números naturales. Por ejemplo, podemos demostrar la anterior afirmación operando como sigue:*

   $$7^n - 1 = (7 - 1) \cdot (7^{n-1} + 7^{n-2} + \cdots + 7^1 + 7^0) = 6 \cdot (7^{n-1} + 7^{n-2} + \cdots + 7 + 1)$$

   *lo que nos muestra que es múltiplo de 6.*

   *También podríamos haberlo hecho trabajando módulo 6. Decir que $7^n - 1$ es múltiplo de 6 es lo mismo que decir que $7^n - 1 = 0$ en $\mathbb{Z}_6$. Como en $\mathbb{Z}_6$ $7 = 1$, entonces $7^n - 1 = 1^n - 1 = 1 - 1 = 0$, como queríamos.*

3. *Puede ocurrir que al demostrar algo por inducción, en el proceso nos aparezca alguna propiedad que también podemos probar por inducción. Por ejemplo, vamos a demostrar que para cualquier número natural $n$, el número $n^3 + 3n^2 + 2n$ es múltiplo de 6.*

   *Como siempre, comprobamos el caso base, y demostramos el paso inductivo.*

   - *Caso base: El resultado es cierto para $n = 0$, es decir, $0^3 + 3 \cdot 0^2 + 2 \cdot 0$ es múltiplo de 6.*
   - *Hipótesis de inducción: Para un número natural $n$, el número $n^3 + 3n^2 + 2n$ es múltiplo de 6, es decir, $n^3 + 3n^2 + 2n = 6k$ para algún número entero $k$.*
   - *Paso inductivo: A partir de la hipótesis de inducción, demostremos que $(n+1)^3 + 3 \cdot (n+1)^2 + 2 \cdot (n+1)$ es múltiplo de 6.*

     $$\begin{aligned}(n+1)^3 + 3 \cdot (n+1)^2 + 2 \cdot (n+1) &= n^3 + 3n^2 + 3n + 1 + 3(n^2 + 2n + 1) + 2n + 2 = \\ &= n^3 + 3n^2 + 3n + 1 + 3n^2 + 6n + 3 + 2n + 2 = \\ &= (n^3 + 3n^2 + 2n) + (3n^2 + 3n + 1 + 6n + 3 + 2) = \\ &= 6k + (3n^2 + 3n + 6n + 6) = \\ &= 6(k + n + 1) + 3(n^2 + n).\end{aligned}$$

     *Si pudiéramos asegurar que el número $n^2 + n$ es múltiplo de 2 entonces $3(n^2 + n)$ sería múltiplo de 6, y con eso concluiríamos que $(n + 1)^3 + 3(n + 1)^2 + 2(n + 1)$ es múltiplo de 6, que es lo que queremos. Entonces abrimos aquí una nueva demostración.*

     > *Vamos a demostrar que para cualquier número natural $n$, $n^2 + n$ es múltiplo de 2. Lo hacemos por inducción.*
     >
     > - *Caso base: $0^2 + 0$ es múltiplo de 2. Claramente es cierto.*
     > - *Hipótesis de inducción: $n^2 + n$ es múltiplo de 2, es decir, $n^2 + n = 2l$ para algún número entero $l$.*

- *Paso inductivo: Hemos de comprobar, apoyándonos en que $n^2+n=2l$, que $(n+1)^2+(n+1)$ es múltiplo de 2.*

$$(n+1)^2+(n+1)=n^2+2n+1+n+1=n^2+n+2n+2=2l+2n+2=2(l+n+1)$$

*Y con esto, terminamos de demostrar que $n^2+n$ es múltiplo de 2 para cualquier número natural $n$.*
*También lo podríamos haber hecho factorizando $n^2+n$, ya que $n^2+n=n(n+1)$. Puesto que $n$ y $n+1$ son dos números consecutivos, uno de ellos tiene que ser múltiplo de 2, luego su producto es también múltiplo de 2.*

*Y ahora, como ya sabemos que $n^2+n=2l$ para algún número entero $l$ tenemos que*

$$(n+1)^3+3\cdot(n+1)^2+2\cdot(n+1)=6(k+n+1)+3\cdot 2l=6(k+n+1+l)$$

*Y esto concluye nuestra demostración por inducción de que $n^3+3n^2+2n$ es múltiplo de 6.*

*También aquí podríamos haber hecho la demostración sin usar el principio de inducción, ya que $n^3+3n^2+2n=n(n+1)(n+2)$. Entre los números $n$, $n+1$, $n+2$, uno de ellos es múltiplo de 3, luego su producto también lo es; y al menos uno de ellos es múltiplo de 2, luego su producto también lo es. Por tanto, $n^3+3n^2+2n$ es múltiplo de 2 y de 3, luego es múltiplo de 6.*

Como hemos dicho, para demostrar algún enunciado por inducción necesitamos dos cosas. Comprobar que el enunciado es cierto para el primer caso, y supuesto cierto para el caso $n$, comprobarlo para el caso $n+1$. Ambas cosas son importantes. La primera, nos permite arrancar el proceso de inducción. La segunda nos asegura que la máquina inductiva está en condiciones de hacer su trabajo. Pero si no la arrancamos, no conseguimos nada.

Por ejemplo, podríamos intentar probar que para cualquier $n\geq 1$, se verifica que $\sum_{k=1}^{n}(2k-1)=n^2+1$ (algo que sabemos que no es cierto).

Con lo visto anteriormente, es sencillo comprobar que si $\sum_{k=1}^{n}(2k-1)=n^2+1$ entonces $\sum_{k=1}^{n+1}(2k-1)=(n+1)^2+1$. Pero en cuanto intentamos comprobarlo para $n=1$ vemos que habría que probar que $1=2$, lo cual no es cierto.

Ya hemos hablado antes de lo que significan las demostraciones en matemáticas. Éstas son una herramienta que permiten afirmar que un determinado enunciado es cierto con total seguridad, en contraste con las ciencias experimentales, en las que esta seguridad no se alcanzará nunca. Por ejemplo, según la ley de gravitación universal dos cuerpos cualesquiera se atraen por una fuerza descrita en esa ley. Esto es algo que todos experimentamos día a día, al ver todos los objetos atraídos por la Tierra. Y se ha observado en miles de objetos celestes. A partir de esta experiencia se ha formulado una afirmación referente a todos los cuerpos en el espacio. ¿Podemos estar seguros de que nunca vamos a encontrar dos cuerpos que violen esta ley?.

Las distintas teorías físicas han ido cambiando a lo largo de la historia. Tras varias teorías sobre el Sistema Solar, se llegó a la Teoría de la Gravitación de Newton que logró dar una explicación bastante coherente del Universo a gran escala. Sin embargo, la concepción del Universo surgida a través de la ley de la Gravitación universal tuvo que ser modificada con la aparición de la Teoría de la Relatividad de Einstein.

En matemáticas, cuando se demuestra alguna afirmación o algún teorema se asegura que ese teorema es cierto, y que nada podrá ponerlo en entredicho (siempre que la demostración sea correcta).

Por ejemplo, podemos afirmar que para cualquier número natural $n$, la suma de las distintas potencias de 2 hasta $2^n$ vale $2^{n+1}-1$. Esta afirmación puede venir de la experimentación con números. $1+2=2^2-1$; $1+2+2^2=2^3-1$; $1+2+2^2+2^3=2^4-1$, y así con más números.

Podemos seguir realizando los cálculos para los 100 primeros números naturales, y en todos podríamos ver que se satisface nuestra afirmación. Podemos elegir más números al azar, y en todos veríamos que se satisface. Sin embargo, eso no es suficiente para poder decir que es cierto para todos los números. Por muchos números para los que lo comprobemos no podremos estar seguros de que no existe un número para el que no hayamos probado y que eche por tierra nuestra tesis. Sin embargo, la demostración que acabamos de hacer nos puede ahorrar todos esas comprobaciones y el resultado es

mucho más contundente. Nunca podremos encontrar un número natural que no cumpla la propiedad anterior ya que ese número no existe.

Sin ese paso de la demostración (el pasar de una comprobación para unos cuantos a la afirmación de que es cierta para todos) podríamos cometer errores, y dar por ciertas algunas propiedades que no lo son. Por ejemplo, para cada número natural $n \geq 3$ vamos a calcular $2^{n-1} - 1$ lo vamos a dividir entre $n$, y nos vamos a quedar con el resto.

- Para $n = 3$, $2^{n-1} - 1 = 3$, que dividido entre 3 da resto 0.
- Para $n = 4$, $2^{n-1} - 1 = 7$, que dividido entre 4 da resto 3.
- Para $n = 5$, $2^{n-1} - 1 = 15$, que dividido entre 5 da resto 0.
- Para $n = 6$, $2^{n-1} - 1 = 31$, que dividido entre 6 da resto 1.
- Para $n = 7$, $2^{n-1} - 1 = 63$, que dividido entre 7 da resto 0.
- Para $n = 8$, $2^{n-1} - 1 = 127$, que dividido entre 8 da resto 7.
- Para $n = 9$, $2^{n-1} - 1 = 255$, que dividido entre 9 da resto 3.
- Para $n = 10$, $2^{n-1} - 1 = 511$, que dividido entre 10 da resto 1.
- Para $n = 11$, $2^{n-1} - 1 = 1023$, que dividido entre 11 da resto 0.

Vemos que para los números 3, 5, 7 y 11 el resto de la división es 0, mientras que para los restantes es distinto de 0. Podemos seguir así, y si llegamos hasta 100 vemos que el resto de la división es 0 para los números 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, mientras que para los otros números el resto de la división es distinto de 0.

Es decir, dado $n \in \mathbb{N}$, $n \geq 3$, entonces $2^{n-1} - 1$ es múltiplo de $n$ implica que $n$ es primo. Dicho de otra forma, si llamamos $P(n)$ a la afirmación

$$2^{n-1} - 1 \text{ es múltiplo de } n \implies n \text{ es primo.}$$

hemos comprobado que $P(3)$, $P(4)$, $P(5)$, $P(6)$, $P(7)$, $P(8)$, $P(9)$, $P(10)$, $P(11)$ son ciertas, y hemos afirmado que la afirmación sigue siendo cierta hasta $n = 100$.

Esto nos induce a pensar que $P(n)$ es cierta para todo número natural $n$. Podríamos seguir comprobándolo para todos los números naturales hasta llegar a 200 ($2^{199}$ es un número de 61 cifras) y el resultado sería el mismo. Pero eso no nos garantiza ni mucho menos que el resultado no vaya a fallar alguna vez. De hecho, se tiene que

$$2^{340} - 1 = 22397447421778042105574422805684442781216454972346495348999891009637918711801609453808774932716071157 75$$

que es múltiplo de 341, y sin embargo 341 no es primo, pues es el producto de 11 y 31.

O fijémonos en lo siguiente:

| | | | | |
|---|---|---|---|---|
| | $4 = 2 + 2$ | $6 = 3 + 3$ | $8 = 3 + 5$ | $10 = 3 + 7$ |
| $12 = 5 + 7$ | $14 = 3 + 11$ | $16 = 3 + 13$ | $18 = 7 + 11$ | $20 = 3 + 17$ |
| $22 = 5 + 17$ | $24 = 11 + 13$ | $26 = 3 + 23$ | $28 = 5 + 23$ | $30 = 7 + 23$ |
| $32 = 3 + 29$ | $34 = 3 + 31$ | $36 = 5 + 31$ | $38 = 7 + 31$ | $40 = 3 + 37$ |
| $42 = 5 + 37$ | $44 = 3 + 41$ | $46 = 3 + 43$ | $48 = 5 + 43$ | $50 = 3 + 47$ |

Hemos tomado todos los números pares mayores que 2, hasta el 50, y todos los hemos podido expresar como suma de dos números primos.

No se ha encontrado ningún número par, mayor que 2, que no pueda expresarse como suma de dos números primos. De hecho, se ha comprobado para todos los números menores que 1 trillón. Sin embargo, eso es muy poco comparado con los infinitos números pares que existen.

Hasta el momento no se ha encontrado ningún argumento que permita afirmar que el resultado es cierto para todos los números pares. Por tanto, el resultado no pasa de ser una mera conjetura, conocida como *conjetura de Goldbach*.

El principio de inducción nos dice que si $A$ es un subconjunto de $\mathbb{N}$ que satisface las dos siguientes propiedades:

- $0 \in A$
- $n \in A \Longrightarrow n+1 \in A$

Entonces $A = \mathbb{N}$. Este axioma puede leerse de la forma siguiente:

> Si $A$ es un subconjunto de $\mathbb{N}$ que es distinto de $\mathbb{N}$, entonces, o $0 \notin A$, o existe $n \in \mathbb{N}$ tal que $n \in A$ y $n+1 \notin A$.

Esta formulación del principio de inducción (equivalente a la vista anteriormente) nos permite demostrar una propiedad importante de los números naturales.

**Teorema 1.2.1.** *[Principio de buena ordenación] Sea $A$ un subconjunto de $\mathbb{N}$ distinto del conjunto vacío. Entonces $A$ tiene mínimo.*

Se dice que $m$ es el mínimo de $A$ si $m \in A$ y $m \leq n$ para todo $n \in A$.

*Demostración:* Sea $B$ el conjunto de las cotas inferiores de $A$, es decir

$$B = \{m \in \mathbb{N} : m \leq n \ \text{ para todo } n \in A\}$$

Claramente $B \neq \mathbb{N}$ (pues si $m \in A$, $m+1 \notin B$).
También es cierto que $0 \in B$ (¿por qué?).
Por tanto, debe existir $m \in \mathbb{N}$ tal que $m \in B$ y $m+1 \notin B$
Por pertenecer $m$ a $B$ se tiene que $m \leq n$ para todo $n \in A$. Queda entonces comprobar que $m \in A$.
Ahora bien, supongamos que $m \notin A$, entonces, para cualquier $n \in A$ se tiene que $m \leq n$ (pues $m \in B$) y que $m \neq n$ (pues $m \notin A$), luego $m+1 \leq n$ para todo $n \in A$. Por tanto, tendríamos que $m+1 \in B$, lo cual no es posible.
Deducimos por tanto que $m \in A$, como queríamos. ■

El principio de inducción puede adoptar distintas formas. Por ejemplo, si queremos demostrar que una propiedad es cierta para todos los números naturales que son mayores o iguales que un cierto número $n_0 \in \mathbb{N}$, entonces podemos hacerlo demostrando que la propiedad es cierta para $n_0$, y supuesta cierta para un número $n$, entonces es cierta para $n+1$.

> Si queremos demostrar que la propiedad $P(n)$ es cierta para todo número natural $n \geq n_0$, tomamos $A = \{m \in \mathbb{N} : P(m+n_0)$ es cierta $\}$. Entonces:
>
> - Comprobamos que $0 \in A$. Esto es equivalente a comprobar que $P(n_0)$ es cierta.
> - Probamos que si $m \in A$ entonces $m+1 \in A$. Esto es lo mismo que probar que para $n \geq n_0$, si $P(n)$ es cierta, entonces $P(n+1)$ es cierta.

Incluso, en el comentario anterior podemos cambiar números naturales por *números enteros*. Es decir, para demostrar que una propiedad es cierta para todos los números enteros que son mayores o iguales que un cierto entero $n_0$, podemos proceder como acabamos de decir.

**Ejemplo 1.2.3.**

1. *Vamos a demostrar que para $n \geq 7$ se verifica que $3^n < n!$ (suponemos que es conocido lo que representa $n!$. De todas formas, más adelante, en el ejemplo 1.3.1 daremos una definición de esta función).*

   - *Caso base: En este caso es $n = 7$. En tal caso, y puesto que $3^7 = 2187$ y $7! = 5040$, lo que tenemos es que $2187 < 5040$, que claramente es cierto.*
   - *Hipótesis de inducción: Si $n \geq 6$, suponemos que $3^n < n!$.*
   - *Paso inductivo: Ahora, comprobamos que $3^{n+1} < (n+1)!$.*

   $$3^{n+1} = 3^n \cdot 3 < n! \cdot 3 < n! \cdot (n+1) = (n+1)!.$$

   *A partir de esto podemos afirmar que sea cual sea el número natural $n$ mayor que 6, se tiene que $3^n < n!$.*

2. *Vamos ahora a comprobar que para cualquier entero mayor o igual que* $-2$ *se verifica que* $n^2+7n+11>0$.

   - *Caso base: Lo comprobamos en primer lugar para* $n=-2$. *Puesto que* $(-2)^2+7\cdot(-2)+11=4-14+11=1>0$ *tenemos que para* $n=-2$ *es cierto.*
   - *Hipótesis de inducción:* $n^2+7n+11>0$ *para* $n\geq 2$.
   - *Paso inductivo: A partir de la hipótesis de inducción, tenemos que comprobar que* $(n+1)^2+7(n+1)+11>0$.

   $$(n+1)^2+7(n+1)+11=n^2+2n+1+7n+7+11=(n^2+7n+11)+(2n+1+7)>0+2n+8\geq 2(-2)+8=4>0$$

   *Por tanto, para cualquier entero* $n\geq -2$ *se verifica que* $n^2+7n+11$ *es un número natural.*

   *Notemos que* $(-3)^2+7\cdot(-3)+11=-1$. *Es decir, para* $n=-3$ *el enunciado anterior es falso.*

3. *Cuando intentamos dar el paso inductivo, hemos de prestar atención, pues ese paso debe ser válido para todos los números naturales para los que queremos que sea cierta la propiedad. Por ejemplo, demostremos que para cualquier número natural* $n$ *se verifica que* $2n<n^2+1$.

   - *Caso base: Para* $n=0$, *lo que tendríamos es* $0<1$, *que es verdad.*
   - *Hipótesis de inducción:* $2n<n^2+1$ *para* $n\geq 0$.
   - *Paso inductivo: Tenemos que comprobar que* $2(n+1)<(n+1)^2+1$.

     $$2(n+1)=2n+2<n^2+1+2<n^2+2n+2=n^2+2n+1+1=(n+1)^2+1.$$

     *Donde en la segunda desigualdad hemos sustituido* $1$ *por* $2n$ *(es decir, hemos usado la desigualdad* $1<2n$*). Esta desigualdad vale si* $n\geq 1$, *pero para* $n=0$ *es falsa. Por tanto, el paso inductivo no nos permite pasar de 0 hasta 1.*

     *De hecho, la desigualdad no es cierta para* $n=1$ *(en tal caso tenemos* $2<2$, *que no es verdad).*

     *El paso inductivo sí nos permitiría pasar desde 1 hasta 2, pero para eso necesitamos que sea cierta para* $n=1$, *que ya sabemos que no es así.*

     *Para* $n=2$ *sí es cierta (*$4<5$*), y el paso inductivo permite pasar desde 2 hasta 3, desde 3 hasta 4, y así sucesivamente. Por tanto, esta desigualdad es cierta para* $n\geq 2$.

4. *Ahora vamos a demostrar que para cualquier número natural* $n$, *se tiene que* $2n\leq n^2+1$. *Esta desigualdad sí es cierta para todos los números naturales, pero si intentamos demostrarla por inducción, nos encontramos con el mismo problema de antes. El paso inductivo no nos deja pasar desde cero hasta uno.*

   *Entonces, podemos demostrar la desigualdad para todos los números naturales mayores o iguales que 1 (aquí no habría problema en demostrarlo por inducción), y posteriormente comprobarla para* $n=0$.

   *También tenemos la alternativa de no usar el principio de inducción. Para esto escribimos la desigualdad como* $0\leq n^2-2n+1$. *Y esta podemos verla como* $0\leq(n-1)^2$. *Claramente, eso es verdad para cualquier número natural (y entero).*

5. *Comprobemos que para* $n\geq 2$ *se tiene que* $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}<2-\frac{1}{n}$.

   - *Caso base: Ahora es para* $n=2$, *nos diría* $1+\frac{1}{4}<2-\frac{1}{2}$. *Es decir,* $\frac{5}{4}<\frac{3}{2}$.
   - *Hipótesis de inducción: Para un número natural* $n$ *se verifica que* $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}<2-\frac{1}{n}$.
   - *Paso inductivo: Demostremos que* $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}+\frac{1}{(n+1)^2}<2-\frac{1}{n+1}$.

$$\begin{aligned}
1+\tfrac{1}{4}+\cdots+\tfrac{1}{n^2}+\tfrac{1}{(n+1)^2} &< 2-\tfrac{1}{n}+\tfrac{1}{(n+1)^2}\\
&= 2-\tfrac{(n+1)^2}{n(n+1)^2}+\tfrac{n}{n(n+1)^2}\\
&= 2-\tfrac{n^2+2n+1}{n(n+1)^2}+\tfrac{n}{n(n+1)^2}\\
&= 2-\tfrac{n^2+2n+1-n}{n(n+1)^2}\\
&= 2-\tfrac{n^2+n+1}{n(n+1)^2}\\
&< 2-\tfrac{n^2+n}{n(n+1)^2}\\
&= 2-\tfrac{n(n+1)}{n(n+1)^2}\\
&= 2-\tfrac{1}{n+1}
\end{aligned}$$

*Donde* $2-\frac{n^2+n}{n(n+1)^2} > 2-\frac{n^2+n+1}{n(n+1)^2}$ *ya que la cantidad que le restamos a 2 en el primer caso es más pequeña que la que le restamos en el segundo.*

> *El problema de Basilea consistía en calcular el valor de la serie* $\sum_{k=1}^{\infty}\frac{1}{k^2}$*. En 1735, Leonhard Euler calculó el valor de dicha suma, que resulta ser* $\frac{\pi^2}{6}$*, y cuyo valor numérico es* $1'6449...$ *A partir de esto, lo que acabamos de demostrar resulta obvio.*

6. *Dado un número natural* $n$*, mayor que cero, demostremos que* $\frac{1}{2^1}+\frac{1}{2^2}+\cdots+\frac{1}{2^n}<1$*.*

   *Antes de dar la demostración, vamos a fijarnos en lo siguiente:*

$$\begin{aligned}
\tfrac{1}{2} &= \tfrac{1}{2} < 1\\
\tfrac{1}{2}+\tfrac{1}{4} &= \tfrac{3}{4} < 1\\
\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{8} &= \tfrac{7}{8} < 1\\
\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{8}+\tfrac{1}{16} &= \tfrac{15}{16} < 1\\
\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{8}+\tfrac{1}{16}+\tfrac{1}{32} &= \tfrac{31}{32} < 1
\end{aligned}$$

   *Notemos como cada una de las sumas que tenemos a la izquierda de las desigualdades se obtiene de la suma anterior sumándole la mitad de lo que le falta para llegar a la unidad. En el primer caso, la suma vale* $\frac{1}{2}$*. Falta* $\frac{1}{2}$ *para llegar a la unidad, y se le suma* $\frac{1}{4}$ *(que es la mitad de* $\frac{1}{2}$*).*

   *La segunda suma vale* $\frac{3}{4}$*, luego falta* $\frac{1}{4}$ *para llegar a la unidad. La mitad es* $\frac{1}{8}$*, que es lo que se suma en el siguiente.*

   *Y eso es lo que ocurre en los casos siguientes. Por ejemplo, la cuarta suma vale* $\frac{15}{16}$*, luego falta* $\frac{1}{16}$ *para llegar a la unidad. La mitad es* $\frac{1}{32}$*, y eso es lo que sumamos en la quinta.*

   *Se ve entonces que como siempre sumamos la mitad de lo que falta para llegar a la unidad, siempre nos vamos a mantener por debajo, luego la suma debe ser menor que 1 en cualquier caso.*

   *Vamos a intentar demostrarlo.*

   - *Caso base: Para* $n=1$ *ya lo hemos comprobado.*
   - *Hipótesis de inducción:* $\sum_{k=1}^{n}\frac{1}{2^k}<1$*.*
   - *Paso inductivo: Demostremos que* $\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^n}+\frac{1}{2^{n+1}}<1$*, a partir de la hipótesis de inducción.*

*Pero si lo intentamos de la forma que parece más natural, nos encontramos con* $\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^n}+\frac{1}{2^{n+1}}<1+\frac{1}{2^{n+1}}$.
*Y ahora, no hay forma de demostrar que esto último es menor o igual que 1.*

*Para intentar resolver el problema, vamos a escribirlo de otra forma. Probaremos dos maneras distintas:*

*i) Multiplicamos ambos miembros de la desigualdad por* $2^n$ *(que al ser un número positivo no cambia la desigualdad). En tal caso, lo que tenemos que demostrar es que* $\frac{2^n}{2^1}+\frac{2^n}{2^2}+\cdots+\frac{2^n}{2^n}<2^n$*, o lo que es lo mismo,* $1+2+\cdots+2^{n-1}<2^n$.
*Y ahora esto lo demostramos por inducción:*

- *Caso base: Que es para* $n=0$*. Lo que nos dice es* $1<2$.
- *Hipótesis de inducción. Para un número* $n\geq 1$ *se verifica que* $1+2+\cdots+2^{n-1}<2^n$.
- *Paso inductivo: A partir de la hipótesis de inducción veamos que* $1+2+\cdots+2^{n-1}+2^n<2^{n+1}$.

$$1+2+\cdots+2^{n-1}+2^n<2^n+2^n=2^{n+1}$$

*ii) Observando con detalle los cinco ejemplos que hemos puesto antes, podemos inducir la igualdad* $\frac{1}{2}+\cdots+\frac{1}{2^n}=1-\frac{1}{2^n}$.
*Si conseguimos demostrar esto, habremos demostrado lo que buscábamos, ya que* $1-\frac{1}{2^n}<1$*. De hecho, demostrar que* $\frac{1}{2}+\cdots+\frac{1}{2^n}=1-\frac{1}{2^n}$ *es demostrar más de lo que nos pedían, pues no sólo demostramos que la suma* $\frac{1}{2}+\cdots+\frac{1}{2^n}$ *es menor que 1, sino que calculamos exactamente cuánto le falta a esa suma para llegar a 1.*

- *Caso base: Ya está hecho. Es simplemente comprobar que* $\frac{1}{2}=1-\frac{1}{2}$.
- *Hipótesis de inducción: Si* $n\geq 1$, $\frac{1}{2}+\cdots+\frac{1}{2^n}=1-\frac{1}{2^n}$.
- *Paso inductivo: Demostremos que* $\frac{1}{2}+\cdots+\frac{1}{2^n}+\frac{1}{2^{n+1}}=1-\frac{1}{2^{n+1}}$

$$\frac{1}{2}+\cdots+\frac{1}{2^n}+\frac{1}{2^{n+1}}=1-\frac{1}{2^n}+\frac{1}{2^{n+1}}=1-\frac{2}{2^{n+1}}+\frac{1}{2^{n+1}}=1-\frac{1}{2^{n+1}}$$

Entre las distintas formas que puede adoptar el principio de inducción, una de ellas es la que se denomina *inducción fuerte* o *segundo principio de inducción.*

**Teorema 1.2.2.** *[Segundo principio de inducción]*
*Sea* $A$ *un subconjunto de* $\mathbb{N}$*. Supongamos que se verifica:*

1. $0\in A$.
2. *Para cualquier* $n$, $\{0,1\cdots n-1\}\subseteq A\Longrightarrow n\in A$

*Entonces* $A=\mathbb{N}$.

Formalmente, la primera condición no es necesaria, pues para $n=0$ la segunda condición afirma $\emptyset\subseteq A\Longrightarrow 0\in A$, y puesto que la primera parte es siempre cierta ($\emptyset\subseteq A$), la condición 2 implica que $0\in A$. Sin embargo, en la práctica suele ser necesario comprobar que $0\in A$.

Notemos también que si la condición 1 se cambia por una de la forma $0,1,\cdots,k\in A$, la tesis del teorema sigue siendo cierta.

También, si queremos demostrar que una propiedad $P(n)$ es cierta para todo número natural (o entero) mayor o igual que $n_0$, podemos usar este segundo principio de inducción. Probamos que $P(n_0)$ es cierta, y que si $P(n_0),\ P(n_0+1),\cdots,P(n-1)$ son ciertas (sea quien sea $n>n_0$) entonces $P(n)$ es cierta.

*Demostración:* Supongamos que $A\neq\mathbb{N}$. Entonces el conjunto $B=\mathbb{N}\setminus A$ es distinto del conjunto vacío. Por tanto, por el principio de buena ordenación tenemos que $B$ tiene un mínimo. Sea este $n_0$. Esto implica que $\{0,1,\cdots,n_0-1\}\subseteq A$ (pues ninguno de sus elementos pertenece a $B$), luego por la condición 2 tenemos que $n_0\in A$, lo que es imposible, pues $n_0\in B$. Deducimos entonces que $A=\mathbb{N}$ ■

Es decir, para demostrar que la propiedad $P(n)$ es cierta para cualquier número natural $n$:

- Demostramos que $P(0)$ es cierta.
- Dado un número natural $n$, si $P(0),\ P(1),\ \cdots P(n-1)$ son ciertas, entonces demostramos que $P(n)$ es cierta.

En cuyo caso, por el segundo principio de inducción, la propiedad es cierta para todo número natural $n$.

**Ejemplo 1.2.4.** *Vamos a usar este segundo principio de inducción para demostrar un conocido resultado. El* Teorema fundamental de la aritmética. *Es decir, vamos a ver que dado $n \geq 2$, entonces, o $n$ es primo, o $n$ se puede descomponer como producto de primos.*

- *Tenemos que para $n = 2$ el resultado es cierto, pues 2 es un número primo.*
- *Sea $n \geq 3$, y supongamos que todos los números menores que $n$, o son primos, o se descomponen como producto de números primos.*

  *Pueden ocurrir dos cosas:*

  - *Que $n$ sea primo. En tal caso, el resultado es cierto para $n$.*
  - *Que $n$ no sea primo. En este caso, $n$ tiene un divisor que no es ni 1 ni $n$. Sea este $a$. Eso significa que $n = a \cdot b$ para algún número natural $b$.*

    *Es claro que tanto $a$ como $b$ son distintos de 1, y son menores que $n$. Por tanto, ambos números son producto de números primos (o son ellos números primos). Es decir, $a = p_1 p_2 \cdots p_r$ y $b = q_1 q_2 \cdots q_s$ para algunos números primos $p_1, \cdots p_r, q_1, \cdots, q_s$ (donde bien $r$, bien $s$ podrían valer 1). De aquí deducimos que*

$$n = a \cdot b = (p_1 p_2 \cdots p_r) \cdot (q_1 q_2 \cdots q_s)$$

    *Es decir, $n$ es producto de números primos, como queríamos.*

## 1.3. Recurrencia.

### 1.3.1. Definiciones recursivas.

Vamos a centrarnos a continuación en las aplicaciones cuyo dominio es el conjunto de los números naturales. Recordemos que dados dos conjuntos $X$ e $Y$, una aplicación de $X$ en $Y$ es una forma de asignar, a cada elemento de $X$, un elemento (y sólo uno) de $Y$. A las aplicaciones cuyo dominio son los números naturales, las denominaremos sucesiones.

**Definición 1.** *Sea $X$ un conjunto. Una sucesión en $X$ es una aplicación $x : \mathbb{N} \to X$.*

Si $x : \mathbb{N} \to X$ es una sucesión, denotaremos normalmente al elemento $x(n)$ como $x_n$.

A la hora de definir una sucesión en $X$ podemos definir explícitamente la forma de asignar a cada número natural $n$ el elemento $x_n \in X$ mediante alguna regla. Por ejemplo, podemos definir la sucesión $x : \mathbb{N} \to \mathbb{Z}$ como $x_n = n - n^2$.

Hemos dado una regla que nos permite calcular la imagen de cualquier número natural. Por ejemplo, $x_{25} = 25 - 25^2 = -600$, $x_{100} = 100 - 100^2 = -9900$. Y así para cualquier $n \in \mathbb{N}$.

Pero en ocasiones puede resultar más sencillo definir la imagen de un número natural $n$ en términos de la imagen de otros números naturales. Es decir, para definir la sucesión recurrimos a la propia sucesión. Esta forma de hacerlo se llama *recursión.*

La estructura de los números naturales, que queda reflejada en el principio de inducción, da muchas posibilidades para la recursión.

Supongamos que queremos definir una sucesión $x : \mathbb{N} \to X$ recursivamente. La primera forma de hacerlo es siguiendo los siguientes pasos:

- Paso base: Se elige un elemento $x_0 \in X$, que va a ser el valor de la sucesión en $n = 0$.

- Paso recursivo: Dado un número natural $n$, se proporciona una regla para definir $x_{n+1}$ a partir del conocimiento de $x_n$.

El principio de inducción nos garantiza que de esta forma tenemos definida de forma única una función $x : \mathbb{N} \to X$.

**Ejemplo 1.3.1.**

1. *Definimos la siguiente sucesión $x : \mathbb{N} \to \mathbb{N}$:*

$$x_0 = 1; \qquad x_{n+1} = 2 \cdot x_n$$

*Vamos a calcular los primeros términos de la sucesión:*

- $x_0 = 1$. *Por definición.*
- $x_1 = 2 \cdot x_0 = 2 \cdot 1 = 2$ *(el paso recursivo para $n = 0$).*
- $x_2 = 2 \cdot x_1 = 2 \cdot 2 = 4$ *(el paso recursivo para $n = 1$).*
- $x_3 = 2 \cdot x_2 = 2 \cdot 4 = 8$ *(el paso recursivo para $n = 2$).*
- $x_4 = 2 \cdot x_3 = 2 \cdot 8 = 16$ *(el paso recursivo para $n = 3$).*
- $x_5 = 2 \cdot x_4 = 2 \cdot 16 = 32$ *(el paso recursivo para $n = 4$).*

*Vemos que lo que hemos definido es la sucesión $x_n = 2^n$. Esto habría que probarlo por inducción.*

2. *De forma análoga a como hemos definido la sucesión $x_n = 2^n$, podemos definir, dado $a \in \mathbb{R}$ la siguiente sucesión.*

$$y_0 = 1; \qquad y_{n+1} = a \cdot y_n$$

*Que no es sino una forma de definir el valor de $a^n$.*

3. *Vamos a definir el factorial de un número natural. Para esto definimos la sucesión $z : \mathbb{N} \to \mathbb{N}$ como sigue:*

$$z_0 = 1; \qquad z_{n+1} = (n+1) \cdot z_n$$

*Al número $z_n$ se le conoce como el* factorial *de $n$, y se representa como $n!$.*

*Por ejemplo, se tiene que $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$, $6! = 720$.*

4. *Sea $u : \mathbb{N} \to \mathbb{N}$ la sucesión:*

$$u_0 = 0; \qquad u_{n+1} = u_n + 5$$

*Calculamos los primeros términos de esta sucesión. $u_0 = 0$, $u_1 = 5$, $u_2 = 10$, $u_3 = 15$, $u_4 = 20$. Y vemos que en realidad, lo que tenemos es que $u_n = 5 \cdot n$.*

*Si en lugar del número 5 hubiéramos tomado otro número natural $m$, entonces lo que habríamos hecho es definir la sucesión $u_n = m \cdot n$.*

> *Todos sabemos que la multiplicación de números naturales no es más que "sumar muchas veces la misma cantidad". Así, para multiplicar números naturales sólo necesitamos saber sumar. Esta idea queda reflejada en la anterior definición. Hemos definido la multiplicación $m \cdot n$ a partir únicamente de la suma. Para formalizar el sumar muchas veces utilizamos la recursión. Así, para multiplicar $5 \cdot 4$ lo que hacemos es sumar el 5 cuatro veces.*
>
> *De la misma forma, sabemos que multiplicar muchas veces la misma cantidad es lo mismo que calcular una potencia. Esto ha quedado plasmado en las sucesiones $x_n$ e $y_n$ definidas previamente.*
>
> *También podemos ver la suma como "sumar muchas veces uno". Y así, a partir del conocimiento de como sumar uno (es decir, de contar), podemos definir la suma de dos números naturales. Esto es lo que hacíamos cuando usábamos los dedos para sumar.*

5. *Definimos la sucesión $w_n$ como sigue:*

   - $w_1 = 1$.
   - $w_{n+1} = w_n + (n+1)$.

   *Notemos que aquí hemos definido una función $w : \mathbb{N}^* \to \mathbb{N}$. Dos formas de escribir la sucesión serían:*

$$w_n = 1 + 2 + \cdots + n; \qquad w_n = \sum_{k=1}^{n} k$$

   *Vamos a demostrar que $w_n = \frac{n(n+1)}{2}$. Para esto, utilizamos el principio de inducción.*

   - *Caso base: $w_1 = \frac{1(1+1)}{2}$. Eso es cierto, pues por definición $w_1 = 1$, que es igual $\frac{1(1+1)}{2}$.*
   - *Suponemos que $w_n = \frac{n(n+1)}{2}$, y queremos demostrar que $w_{n+1} = \frac{(n+1)(n+1+1)}{2}$, es decir, $w_{n+1} = \frac{(n+1)(n+2)}{2}$.*
     *Tenemos que:*

$$w_{n+1} = w_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{n(n+1)+2(n+1)}{2} =$$
$$= \frac{(n+2)(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Vamos a considerar la siguiente sucesión:
$f_0 = 0;\ f_1 = 1;\ f_2 = 1;\ f_3 = 2;\ f_4 = 3;\ f_5 = 5;\ f_6 = 8;\ f_7 = 13;\ f_8 = 21;\ f_9 = 34;\ f_{10} = 55;\ f_{11} = 89; \cdots$

Podemos ver la regla que seguimos para calcular un término de la sucesión. Es sumar los dos términos anteriores. Obviamente, para poder aplicar esta regla es necesario tener dos términos de la sucesión. Por tanto, $f_0$ y $f_1$ no siguen ese criterio. Una definición entonces podría ser:

- $f_0 = 0;\ f_1 = 1$.
- $f_n = f_{n-1} + f_{n-2}$ si $n \geq 2$.

De esta forma, parece claro que está bien definido el valor de $f_n$ para cualquier $n \in \mathbb{N}$. Sin embargo, esta definición no se ajusta al método de recurrencia dado anteriormente (pues en este caso, para calcular un término es necesario recurrir a los dos términos anteriores, mientras que en el método dado anteriormente, únicamente necesitamos conocer el término anterior).

La sucesión aquí definida se denomina *sucesión de Fibonacci*. Esta sucesión fue estudiada por Leonardo de Pisa, a principios del siglo XIII, mientras intentaba encontrar un modelo numérico para determinar el número de conejos que resultan en un año si se parte de una sola pareja. Más tarde, el alemán Johannes Kepler la utilizó en su estudio de cómo se ordenan las hojas de una planta alrededor de su tallo.

Esta sucesión satisface lo que se conoce como una *relación de recurrencia lineal homogénea.*

### 1.3.2. Recurrencia lineal homogénea.

**Definición 2.** *Sea $x : \mathbb{N} \to \mathbb{R}$ una sucesión. Decimos que dicha sucesión satisface una relación de recurrencia lineal homogénea con coeficientes constantes si existe $k \in \mathbb{N}$ y $a_1, \cdots, a_k \in \mathbb{R}$ tales que para cualquier $n \geq k$ se verifica que*

$$\sum_{j=0}^{k} a_j \cdot x_{n-j} = a_0 \cdot x_n + a_1 \cdot x_{n-1} + \cdots + a_k \cdot x_{n-k} = 0$$

*donde $a_0 = 1$.*

*Al número $k$ se le denomina* orden de la relación.

*A una sucesión que satisface una relación de recurrencia lineal homogénea la llamaremos* sucesión lineal homogénea.

**Observación:**

Vamos a comentar brevemente el nombre que le hemos puesto a las sucesiones que satisfacen esta tipo de relaciones.

1. Se llama lineal pues todos los términos de la sucesión aparecen elevados a exponente 1. Es decir, no aparece en ningún sumando expresiones de la forma $x_i x_j$, $(x_i)^2$, $\sqrt{x_i}$, $sen(x_i)$, etc.

2. Se llama homogénea porque está igualada a cero.

**Ejemplo 1.3.2.**

1. *La sucesión de Fibonacci satisface una relación de recurrencia lineal homogénea de orden 2. Esto es fácil de ver, pues* $f_n - f_{n-1} - f_{n-2} = 0$ *para cualquier* $n \geq 2$. *En este caso,* $a_1 = -1$ *y* $a_2 = -1$.

2. *La primera sucesión definida en el ejemplo 1.3.1 satisface también una relación de recurrencia lineal homogénea de orden 1, en la que* $a_1 = -2$.

   *Notemos que esta sucesión satisface una relación de recurrencia lineal homogénea de orden 2, pues si* $n \geq 2$ *se tiene que* $x_n = 2x_{n-1} = 2(2x_{n-2}) = 4x_{n-2}$, *es decir,* $x_n - 4x_{n-2} = 0$.

   *Esa no es la única forma de obtener una reclación de recurrencia lineal homogénea de orden 2 para* $x_n$. *Por ejemplo, podríamos haber operado asi:* $x_n = x_{n-1} + x_{n-1} = x_{n-1} + 2 \cdot x_{n-2}$.

En general, si $x_n$ es una sucesión que satisface una relación de recurrencia lineal homogénea de orden $k$, entonces para cualquier $m \geq k$, $x_n$ satisface una relación de recurrencia lineal homogénea de orden $m$.

Llamaremos *orden* de una sucesión lineal homogénea al menor grado de las relaciones de recurrencia lineal homogénea que satisface la sucesión.

Así, la sucesión de Fibonacci es una sucesión lineal homogénea de grado 2.

Lo que vamos a hacer a continuación es, dada una sucesión lineal homogénea, encontrar una expresión del término general.

En primer lugar, notemos que si $x_n$ e $y_n$ son dos sucesiones que satisfacen ambas una misma relación de recurrencia lineal homogénea, entonces para cualesquiera $a, b \in \mathbb{R}$, la sucesión $z_n = ax_n + by_n$ satisface esa relación.

**Ejemplo 1.3.3.** *Sabemos que la sucesión* $x_n = 2^n$ *satisface la relación* $x_n - 4x_{n-2} = 0$.

*La sucesión* $y_n = (-2)^n$ *satisface esa misma relación (*$y_n - 4y_{n-2} = 0$*).*

*Entonces, la sucesión* $z_n = 2^n + (-2)^n$ *satisface esa relación. Los primeros términos de la sucesión son*

$z_0 = 2$, $z_1 = 0$, $z_2 = 8$, $z_3 = 0$, $z_4 = 32$, $z_5 = 0$, $z_6 = 128$, $z_7 = 0$.

*Esta sucesión podría haber sido definida recursivamente como*

- $z_0 = 2$; $z_1 = 0$.
- $z_n = 4 \cdot z_{n-2}$ *para* $n \geq 2$.

**Observación:**

Si tenemos una sucesión lineal homogénea de orden $k$, entonces para calcular cada término de la sucesión necesitamos conocer los $k$ términos anteriores. Por tanto, para poder poner a funcionar la recurrencia nos son necesarios los $k$ primeros términos de la sucesión. Estos términos de la sucesión es lo que se conoce como **condiciones iniciales.**

Dada una relación de recurrencia (no necesariamente lineal homogénea), nos vamos a plantear el problema de encontrar sucesiones que satisfagan dicha relación de recurrencia. Tenemos así, para cada relación de recurrencia, un *problema de recurrencia* (en el caso de que la recurrencia sea lineal homogénea, hablaremos de un problema de recurrencia lineal homogénea). A cada una de esas sucesiones las llamaremos *soluciones del problema de recurrencia* correspondiente.

Por ejemplo, planteamos el problema de recurrencia lineal homogénea siguiente: $x_n - 4x_{n-2} = 0$.

Son soluciones a dicho problema las sucesiones $u_n = 2^n$, $y_n = (-2)^n$, $z_n = 2^n + (-2)^n$, $w_n = 0$. Lo que diferencia a estas cuatro sucesiones son las condiciones iniciales. Estas son, para la primera sucesión $u_0 = 1$, $u_1 = 2$; para la segunda, $y_0 = 1$, $y_1 = -2$; para la tercera, $z_0 = 2$, $z_1 = 0$; y para la cuarta, $w_0 = 0$, $w_1 = 0$.

Hemos visto que si $x_n$ e $y_n$ son soluciones de un mismo problema recurrencia lineal homogénea con coeficientes constantes, entonces cualquier combinación lineal suya es solución de la misma relación de recurrencia. Como consecuencia, el conjunto de las soluciones a un problema de recurrencia lineal homogénea es un espacio vectorial. Puede comprobarse que la dimensión de este espacio vectorial coincide con el orden de la relación.

**Ejemplo 1.3.4.** *Vamos a buscar la solución al problema de recurrencia lineal homogénea $x_n = x_{n-1} + 2x_{n-2}$ con condiciones iniciales $x_0 = 2$, $x_1 = 1$. Para esto, calculamos unos cuantos términos de dicha sucesión:*

$$x_2 = 1+2\cdot 2 = 5; \quad x_3 = 5+2\cdot 1 = 7; \quad x_4 = 7+2\cdot 5 = 17; \quad x_5 = 17+2\cdot 7 = 31; \quad x_6 = 31+2\cdot 17 = 65$$

*Comparamos ahora la sucesión $x_n$ con la sucesión $2^n$*

$$\begin{array}{cccccccc} x_n & \to & 2 & 1 & 5 & 7 & 17 & 31 & 65 \\ 2^n & \to & 1 & 2 & 4 & 8 & 16 & 32 & 64 \end{array}$$

*Y vemos que la diferencia entre los términos de ambas sucesiones es $1$ ó $-1$, dependiendo de que correspondan a un término par o impar. Por tanto, parece que el término general de la sucesión podría ser $x_n = 2^n + (-1)^n$.*

*Vamos a probar que esto es cierto. Para eso, usaremos el segundo principio de inducción.*

*Para $n = 0$ y $n = 1$ sabemos que es cierto, pues lo hemos comprobado (de hecho, está comprobado para $n = 2, 3, 4, 5, 6$).*

*Sea $n \geq 2$, y suponemos que para cualquier $k < n$ se verifica que $x_k = 2^k + (-1)^k$. Entonces:*

$$\begin{aligned} x_n = x_{n-1} + 2x_{n-2} &= 2^{n-1} + (-1)^{n-1} + 2(2^{n-2} + (-1)^{n-2}) = 2^{n-1} + 2\cdot 2^{n-2} + (-1)^{n-1} + 2\cdot(-1)^{n-2} = \\ &= 2^{n-1} + 2^{n-1} + (-1)^{n-2}(-1+2) = 2\cdot 2^{n-1} + (-1)^{n-2} = 2^n + (-1)^n \end{aligned}$$

*Y de aquí podemos deducir que el término general de la sucesión es $x_n = 2^n + (-1)^n$.*

A continuación vamos a intentar ver cómo son las soluciones a un problema de de recurrencia lineal homogénea con coeficientes constantes. Hemos comentado anteriormente que el conjunto de las soluciones forma un espacio vectorial. Lo que pretendemos es encontrar una base de ese espacio vectorial.

**Definición 3.** *Dada el problema de recurrencia lineal homogénea con coeficientes constantes*

$$x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0$$

*Al polinomio $x^k + a_1 x^{k-1} + \cdots + a_{k-1}x + a_k$ se le conoce como* polinomio característico *de la relación, y a la ecuación $x^k + a_1 x^{k-1} + \cdots + a_{k-1}x + a_k = 0$ la ecuación característica.*

**Ejemplo 1.3.5.**

1. *La ecuación característica del problema de recurrencia $x_n = 2x_{n-1}$ es $x - 2 = 0$.*
2. *La ecuación característica de la recurrencia que nos da la sucesión de Fibonacci es $x^2 - x - 1 = 0$.*
3. *La ecuación característica de la sucesión estudiada en el ejemplo 1.3.4 es $x^2 - x - 2 = 0$.*

Los ejemplos que hemos estado analizando nos conducen a la siguiente proposición.

**Proposición 1.3.1.** *Si $\alpha$ es una solución de la ecuación característica de un problema de recurrencia, entonces la sucesión $x_n = \alpha^n$ es una solución a dicho problema.*

*Demostración:*

Supongamos que la relación de recurrencia es $x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0$. En tal caso, por ser $\alpha$ una raíz del polinomio característico se tiene que $\alpha^k + a_1\alpha^{k-1} + \cdots + a_{k-1}\alpha + a_0 = 0$.

Sea $x_n = \alpha^n$. Vamos a ver que esta sucesión satisface la relación de recurrencia.

$x_n+a_1x_{n-1}+\cdots+a_kx_{n-k} = \alpha^n+a_1\alpha^{n-1}+\cdots+a_k\alpha^{n-k} = \alpha^{n-k}\cdot(\alpha^k+a_1\alpha^{k-1}+\cdots+a_{k-1}\alpha+a_0) = \alpha^k\cdot 0 = 0$

■

**Observación:**

Si $\alpha_1$ y $\alpha_2$ son dos raíces del polinomio característico de una relación de recurrencia, entonces $x_n = (\alpha_1)^n$ e $y_n = (\alpha_2)^n$ son dos soluciones a dicha relación de recurrencia. Entonces también son soluciones todas las combinaciones lineales de estas dos sucesiones, es decir, todas las sucesiones de la forma $a(\alpha_1)^n + b(\alpha_2)^n$.

En general, si $\alpha_1, \alpha_2, \cdots, \alpha_k$ son todas las raíces del polinomio característico de una relación de recurrencia, entonces cualquier sucesión de la forma $x_n = b_1(\alpha_1)^n + b_2(\alpha_2)^n + \cdots + b_k(\alpha_k)^n$ es solución a la relación de recurrencia.

Además, es fácil ver que dichas soluciones son linealmente independientes.

En el caso de que la relación de recurrencia fuera de orden $k$, entonces, las sucesiones $(\alpha_1)^n$, $(\alpha_2)^n$, $\cdots$, $(\alpha_k)^n$ forman una base del espacio de dimensiones, y por tanto, cualquier solución sería de la forma anterior.

Las condiciones iniciales son las que nos determinarían cuáles son los coeficientes $b_1, b_2, \cdots, b_k$.

**Ejemplo 1.3.6.**

1. *Consideramos la sucesión definida por $x_n = 2x_{n-1}$, $x_0 = 1$.*

   *La ecuación característica es $x - 2 = 0$, cuya única solución es $\alpha = 2$. Puesto que la relación es de orden 1, la sucesión $x_n$ es de la forma $x_n = b \cdot 2^n$. A partir de la condición $x_0 = 1$, obtenemos que $1 = b \cdot 2^0$, luego $b = 1$.*

   *Por tanto, $x_n = 2^n$.*

   *Si tomamos la sucesión $y_n = 2y_{n-1}$, $y_0 = 3$, entonces la ecuación característica es la misma, luego $y_n = b \cdot 2^n$.*

   *Ahora, tenemos que $3 = y_0 = b \cdot 2^0 = b$. Por tanto, $y_n = 3 \cdot 2^n$.*

2. *Para esta sucesión, ver el ejemplo 1.3.4.*

   *Consideramos la sucesión definida por $x_n = x_{n-1} + 2x_{n-2}$, $x_0 = 2$, $x_1 = 1$. Vamos a hallar el término general de esta sucesión. Para esto, vamos a seguir los siguientes pasos:*

   - *Calculamos el polinomio característico. Este vale $x^2 - x - 2$.*
   - *Hallamos sus raíces. Podemos hacerlo siguiendo la fórmula $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, o bien, usando la regla de Ruffini. En cualquier caso, obtenemos que las raíces son $\alpha_1 = 2$, $\alpha_2 = -1$.*
   - *Escribimos la forma general de la sucesión.*

     *Puesto que tenemos dos raíces, y la relación de recurrencia es de orden 2, la forma general es $x_n = a \cdot 2^n + b \cdot (-1)^n$.*
   - *Planteamos, a partir de las condiciones iniciales, las ecuaciones para hallar $a$ y $b$.*
     - *De la condición $x_0 = 2$ nos queda la ecuación $2 = a \cdot 2^0 + b \cdot (-1)^0 = a + b$.*
     - *De la condición $x_1 = 1$ nos queda la ecuación $1 = a \cdot 2^1 + b \cdot (-1)^1 = 2a - b$.*
   - *Resolvemos el sistema que nos ha quedado:*

     $$\left.\begin{array}{rcrcl} a & + & b & = & 2 \\ 2a & - & b & = & 1 \end{array}\right\}$$ *Fácilmente vemos que la solución es $a = 1$ y $b = 1$*
   - *Sustituimos las soluciones obtenidas en la expresión de la forma general de la sucesión, para hallar el término n-ésimo de la sucesión.*

     $$x_n = 1 \cdot 2^n + 1 \cdot (-1)^n = 2^n + (-1)^n$$

     *Y vemos que coincide con el obtenido en el ejemplo 1.3.4.*

3. *Vamos a encontrar el término general de la sucesión definida por la relación* $x_n = 3x_{n-1} + 4x_{n-2}$, *con las condiciones iniciales* $x_0 = 0$, $x_1 = 1$.

   *Seguimos los mismos pasos que en el ejemplo precedente.*

   - *Polinomio característico:* $x^2 - 3x - 4$.
   - *Raíces del polinomio característico:* $\alpha_1 = 4$, $\alpha_2 = -1$.
   - *Forma general de la solución:* $x_n = a \cdot 4^n + b \cdot (-1)^n$.
   - *Sistema de ecuaciones para calcular los coeficientes:* $\left.\begin{array}{r} a + b = 0 \\ 4a - b = 1 \end{array}\right\}$
   - *Resolvemos el sistema.* $a = \frac{1}{5}$, $b = \frac{-1}{5}$.
   - *Sustituimos en la forma general de la solución.*

   $$x_n = \frac{1}{5}(4^n - (-1)^n)$$

   *Ahora, podemos calcular algunos términos, y así comprobar que el resultado obtenido es correcto.*

   | | |
   |---|---|
   | $x_2 = 3x_1 + 4x_0 = 3 \cdot 1 + 4 \cdot 0 = 3.$ | $\frac{1}{5}(4^2 - (-1)^2) = \frac{1}{5}(16 - 1) = \frac{15}{5} = 3.$ |
   | $x_3 = 3x_2 + 4x_1 = 3 \cdot 3 + 4 \cdot 1 = 13.$ | $\frac{1}{5}(4^3 - (-1)^3) = \frac{1}{5}(64 - (-1)) = \frac{65}{5} = 13.$ |
   | $x_4 = 3x_3 + 4x_2 = 3 \cdot 13 + 4 \cdot 3 = 51.$ | $\frac{1}{5}(4^4 - (-1)^4) = \frac{1}{5}(256 - 1) = \frac{255}{5} = 51.$ |
   | $x_5 = 3x_4 + 4x_3 = 3 \cdot 51 + 4 \cdot 13 = 205.$ | $\frac{1}{5}(4^5 - (-1)^5) = \frac{1}{5}(1024 - (-1)) = \frac{1025}{5} = 205.$ |

4. *Vamos a calcular la expresión general del término n-ésimo de la sucesión de Fibonacci.*

   - *Polinomio característico:* $x^2 - x - 1$.
   - *Raíces del polinomio característico:* $\alpha = \frac{1 \pm \sqrt{1+4}}{2}$. $\alpha_1 = \frac{1+\sqrt{5}}{2}$, $\alpha_2 = \frac{1-\sqrt{5}}{2}$.
   - *Forma general de la solución:* $f_n = a\left(\frac{1+\sqrt{5}}{2}\right)^n + b\left(\frac{1-\sqrt{5}}{2}\right)^n$.
   - *Sistema de ecuaciones:*

   $$\begin{array}{rcrcl} a & + & b & = & 0 \\ \frac{1+\sqrt{5}}{2}\, a & + & \frac{1-\sqrt{5}}{2}\, b & = & 1 \end{array}$$

   - *Resolución del sistema.*
     *De la primera ecuación, tenemos que* $b = -a$. *Sustituimos en la segunda y operamos:*

     $$1 = a\frac{1+\sqrt{5}}{2} - a\frac{1-\sqrt{5}}{2} = a\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = a\frac{2\sqrt{5}}{2} = a \cdot \sqrt{5}$$

     *Luego* $a = \frac{1}{\sqrt{5}} = \frac{\sqrt{5}}{5}$. *Por tanto,* $b = -\frac{\sqrt{5}}{5}$.
   - *Sustituimos.*
     $f_n = \frac{\sqrt{5}}{5}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{\sqrt{5}}{5}\left(\frac{1-\sqrt{5}}{2}\right)^n$. *De donde:*

     $$f_n = \frac{\sqrt{5}}{5}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

5. *Vamos a hacer un ejemplo donde las raíces del polinomio característico no sean números reales.*
   *Sea la sucesión* $u_n = 2u_{n-1} - 2u_{n-2}$; $u_0 = 0$, $u_1 = 1$.

   - *Polinomio característico:* $x^2 - 2x + 2$.
   - *Soluciones de la ecuación característica:* $\alpha = \frac{2 \pm \sqrt{4-2\cdot 4}}{2} = \frac{2 \pm \sqrt{-4}}{2} = \frac{2 \pm 2\sqrt{-1}}{2} = 1 \pm i$. *Es decir* $\alpha_1 = 1 + i$, $\alpha_2 = 1 - i$.
   - *Forma general de la sucesión:* $u_n = a(1+i)^n + b(1-i)^n$.

- *Sistema de ecuaciones:*

$$\begin{array}{rcrcl} a & + & b & = & 0 \\ (1+i)a & + & (1-i)b & = & 1 \end{array}$$

- *Resolución del sistema.*
  *De la primera ecuación tenemos que $a=-b$. Sustituimos en la segunda:*
  $1=(1+i)a+(1-i)a=a(1+i-1+i)=a\cdot 2i$. *Por tanto,* $a=\frac{1}{2i}=\frac{i}{2i^2}=\frac{i}{-2}=\frac{-i}{2}$, *de donde* $b=\frac{i}{2}$.
- *Sustituimos:*

$$u_n=\frac{-i}{2}(1+i)^n+\frac{i}{2}(1-i)^n=\frac{i}{2}\big((1-i)^n-(1+i)^n\big)$$

*Podemos dejar así la sucesión, pero vamos a transformar la anterior expresión. Para ello:*
$1+i=\sqrt{2}\left(cos\frac{\pi}{4}+i\ sen\frac{\pi}{4}\right)$, *o si queremos,* $1+i=\sqrt{2}e^{i\frac{\pi}{4}}$. *De donde*
$(1+i)^n=\sqrt{2^n}\left(cos\frac{n\pi}{4}+i\ sen\frac{n\pi}{4}\right)$
*Esta última expresión puede obtenerse de:*

$$(1+i)^n=(\sqrt{2})^n\left(e^{i\frac{\pi}{4}}\right)^n=\sqrt{2^n}e^{i\frac{n\pi}{4}}=\sqrt{2^n}\left(cos\frac{n\pi}{4}+i\ sen\frac{n\pi}{4}\right),\quad pues\ e^{ix}=cos(x)+i\ sen(x)$$

*De la misma forma, se tiene que*
$(1-i)^n=\sqrt{2^n}\left(cos\frac{-n\pi}{4}+isen\frac{-n\pi}{4}\right)=\sqrt{2^n}\left(cos\frac{n\pi}{4}-isen\frac{n\pi}{4}\right)$
*Por tanto, tenemos que*

$$\begin{aligned} u_n &= \tfrac{i}{2}\big((1-i)^n-(1+i)^n\big)= \\ &= \tfrac{i}{2}\sqrt{2^n}\left[\left(cos\tfrac{n\pi}{4}-i\ sen\tfrac{n\pi}{4}\right)-\left(cos\tfrac{n\pi}{4}+i\ sen\tfrac{n\pi}{4}\right)\right] \\ &= \tfrac{i}{2}\sqrt{2^n}\left(-2i\ sen\tfrac{n\pi}{4}\right)=-i^2\sqrt{2^n}\ sen\tfrac{n\pi}{4} \end{aligned}$$

*Es decir,* $u_n=\sqrt{2^n}\ sen\frac{n\pi}{4}$.
*Como ejercicio, demuestra por inducción que esta expresión se corresponde con la sucesión $u_n$ que acabamos de definir.*

6. *Vamos a estudiar la sucesión* $x_n=5x_{n-1}-8x_{n-2}+4x_{n-3}$; $x_0=2$, $x_1=1$, $x_2=-3$. *Procedemos como en los casos anteriores.*

- *Polinomio característico:* $x^3-5x^2+8x-4$.
- *Raíces del polinomio:*

$$\begin{array}{r|cccc} & 1 & -5 & 8 & -4 \\ 1 & & 1 & -4 & 4 \\ \hline & 1 & -4 & 4 & 0 \end{array}\qquad \begin{array}{r|ccc} & 1 & -4 & 4 \\ 2 & & 2 & -4 \\ \hline & 1 & -2 & 0 \end{array}\qquad \begin{array}{r|cc} & 1 & -2 \\ 2 & & 2 \\ \hline & 1 & 0 \end{array}$$

*Es decir, tiene dos raíces que son* $\alpha_1=1$, $\alpha_2=2$.
- *Escribimos la forma de la solución* $x_n=a\cdot 1^n+b\cdot 2^n=a+b\cdot 2^n$.
- *Planteamos el sistema.*

$$\begin{array}{rcrcl} a & + & b & = & 2 \\ a & + & 2b & = & 1 \\ a & + & 4b & = & -3 \end{array}$$

- *Resolvemos el sistema. Podemos ver que el sistema es incompatible.*

En este último ejemplo tenemos un problema de recurrencia de lineal homogénea de orden 3. Resolviendo la ecuación característica hemos encontrado dos sucesiones que son solución de ese problema de recurrencia: la sucesión $1^n$ y la sucesión $2^n$. Pero como la dimensión del espacio de soluciones tiene dimensión 3, no todas las sucesiones son combinación lineal de esas dos. En concreto, la solución concreta al problema planteado no puede expresarse como combinación lineal de estas dos sucesiones (por eso el sistema nos ha salido incompatible).

La siguiente proposición nos va a decir cómo encontrar una base del espacio de soluciones cuando el número de raíces del polinomio característico sea menor que el orden de la relación.

**Proposición 1.3.2.** *Supongamos que tenemos el problema de recurrencia $x_n + a_1x_{n-1} + \cdots + a_kx^{n-k}$, que $p(x)$ es el polinomio característico de esa relación y que $\alpha$ es una raíz doble de dicho polinomio. Entonces la sucesión $x_n = n \cdot \alpha^n$ es una solución a dicho problema.*

*Demostración:* Tenemos que demostrar que para cualquier $n \geq k$ se verifica que

$$n \cdot \alpha^n + (n-1) \cdot a_{n-1} \cdot \alpha^{n-1} + \cdots + (n-k) \cdot a_k \cdot \alpha^{n-k} = 0$$

Tomamos el polinomio $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_kx^{n-k} = x^{n-k} \cdot p(x)$. Es claro que $\alpha$ es una raíz doble de $q(x)$ (pues $(x-\alpha)^2$ es un divisor de $q(x)$, ya que lo es de $p(x)$). Por tanto, $\alpha$ es una raíz de $q'(x)$.

Calculamos la derivada de $q(x)$. $q'(x) = n \cdot x^{n-1} + (n-1) \cdot a_{n-1} \cdot x^{n-2} + \cdots + (n-k) \cdot a_{n-k} \cdot x^{n-k-1}$. Y ahora, sabemos que $q'(\alpha) = 0$, luego $\alpha\ q'(\alpha) = 0$. Por tanto

$$\begin{array}{rcl} 0 = \alpha\ q'(\alpha) & = & \alpha \cdot (n \cdot \alpha^{n-1} + (n-1) \cdot a_{n-1} \cdot \alpha^{n-2} + \cdots ' + (n-k) \cdot a_{n-k} \cdot \alpha^{n-k-1}) = \\ & = & n \cdot \alpha^n + (n-1) \cdot a_{n-1} \cdot \alpha^{n-1} + \cdots + (n-k) \cdot a_k \cdot \alpha^{n-k} \end{array}$$

Como queríamos. ■

**Ejemplo 1.3.7.** *Retomamos el último ejemplo analizado.*

*Teníamos la sucesión $x_n = 5x_{n-1} - 8x_{n-2} + 4x_{n-3}$; $x_0 = 2$, $x_1 = 1$, $x_2 = -3$. Veíamos que el polinomio característico tenía dos raíces $\alpha_1 = 1$ y $\alpha_2 = 2$, lo que nos daba dos soluciones de la recurrencia $x_n = 5x_{n-1} - 8x_{n-2} + 4x_{n-3}$.*

*Pero la raíz $\alpha_2 = 2$ es una raíz doble. Por tanto, según la proposición anterior, tenemos una nueva solución, que es $n \cdot 2^n$.*

*La solución general es entonces $x_n = a + b \cdot 2^n + c \cdot n \cdot 2^n$. El sistema que hay que resolver es entonces*

$$\begin{array}{rcrcrcr} a & + & b & & & = & 2 \\ a & + & 2b & + & 2c & = & 1 \\ a & + & 4b & + & 8c & = & -3 \end{array}$$

*Y la solución del sistema es $a = 1$, $b = 1$, $c = -1$. Por tanto, la expresión del término general de la sucesión es*

$$x_n = 1 + 2^n - n \cdot 2^n$$

*Se puede probar por inducción que esta expresión es correcta.*

**Observación:**

Hemos visto cómo resolver el problema de recurrencia lineal homogénea cuando el polinomio característico tiene una raíz doble. En el caso de que $\alpha$ sea una raíz de multiplicidad $r$, se tiene que las sucesiones $\alpha^n,\ n \cdot \alpha^n,\ \cdots, n^{r-1} \cdot \alpha^n$ son soluciones del problema de recurrencia.

**Ejemplo 1.3.8.** *Consideramos la sucesión definida por la recurrencia $x_n = 3x_{n-1} - 3x_{n-2} + x_{n-3}$, y las condiciones iniciales $x_0 = 4$, $x_1 = 2$, $x_2 = 2$.*

*El polinomio característico es $x^3 - 3x^2 + 3x - 1$, que se factoriza como $(x-1)^3$. Por tanto, la solución general es $x_n = a \cdot 1^n + bn \cdot 1^n + cn^2 \cdot 1^n = a + bn + cn^2$.*

*Sustituyendo las ecuaciones iniciales nos queda el sistema*

$$\begin{array}{rcrcrcl} a & & & & & = & 4 \\ a & + & b & + & c & = & 2 \\ a & + & 2b & + & 4c & = & 2 \end{array}$$

*Cuya solución es $a = 4$, $b = -3$, $c = 1$. Por tanto, la sucesión es $x_n = n^2 - 3n + 4$.*

### 1.3.3. Recurrencia lineal no homogénea.

**Definición 4.** *Sea $x : \mathbb{N} \to \mathbb{R}$ una sucesión. Decimos que dicha sucesión satisface una relación de recurrencia lineal con coeficientes constantes si existe $k \in \mathbb{N}$, $a_1, \cdots, a_k \in \mathbb{R}$ y $f : \mathbb{N} \to \mathbb{R}$ tales que para cualquier $n \geq k$ se verifica que*

$$\sum_{j=0}^{k} a_j \cdot x_{n-j} = a_0 \cdot x_n + a_1 \cdot x_{n-1} + \cdots + a_k \cdot x_{n-k} = f(n)$$

*donde $a_0 = 1$.*

*Al número $k$ se le denomina* orden de la relación.

**Ejemplo 1.3.9.** *La sucesión definida como $x_1 = 1$, $x_n = 2x_{n-1} + 1$ satisface una relación de recurrencia lineal no homogénea.*

*Puedes comprobar por inducción que $x_n = 2^n - 1$. Más adelante veremos cómo llegar a esta solución.*

Dado un problema de recurrencia lineal no homogénea $x_n + a_1 x_{n-1} + \cdots a_k x_{n-k} = f(n)$, al problema de recurrencia lineal homogénea $x_n + a_1 x_{n-1} + \cdots a_k x_{n-k} = 0$ lo llamaremos el *problema de recurrencia lineal homogénea asociado.*

**Proposición 1.3.3.** *Sea $x_n + a_1 x_{n-1} + \cdots a_k x_{n-k} = f(n)$ un problema de recurrencia lineal no homogénea.*

- *Supongamos que $u_n$ y $v_n$ son soluciones a dicho problema. Entonces la sucesión $u_n - v_n$ es una solución al problema de recurrencia lineal homogénea asociado.*
- *Si $y_n$ es una solución al problema no homogéneo, entonces todas las soluciones a dicho problema son de la forma $y_n + h_n$, donde $h_n$ es una solución al problema homogéneo.*

*Demostración:*

Por ser $u_n$ y $v_n$ soluciones al problema no homogéneo se tiene que $u_n + a_1 u_{n-1} + \cdots a_k u_{n-k} = f(n)$, y que $v_n + a_1 v_{n-1} + \cdots a_k v_{n-k} = f(n)$. Por tanto:

$$\begin{array}{rcl} u_n - v_n & = & a_1(u_{n-1} - v_{n-1} + \cdots a_k(u_{n-k} - v_{n-k}) = \\ & = & u_n + a_1 u_{n-1} + \cdots a_k u_{n-k} - (v_n + a_1 v_{n-1} + \cdots a_k v_{n-k}) = \\ & = & f(n) - f(n) = 0 - 0 = 0 \end{array}$$

La segunda parte se prueba de forma análoga.

■

**Ejemplo 1.3.10.** *Vamos a encontrar la solución general al problema de recurrencia lineal no homogénea $x_n = 2x_{n-1} + 1$.*

*Vimos en el ejemplo anterior que $x_n = 2^n - 1$ es una solución particular a dicha recurrencia.*

*La recurrencia lineal homogénea asociada es $x_n = 2x_{n-1}$, cuya solución general es $a \cdot 2^n$.*

*Por tanto, la solución general es $y_n = a \cdot 2^n - 1$.*

A la solución general del anterior problema de recurrencia hemos llegado a partir del conocimiento de una solución particular (y de cómo son las soluciones de la recurrencia homogénea asociada). Pero, ¿cómo obtener esa solución particular?.

Un forma consiste en intentar transformar la relación de recurrencia en una relación lineal homogénea.

Vamos a ver algún ejemplo.

**Ejemplo 1.3.11.**

- *Nos situamos de nuevo en el problema de recurrencia lineal no homogénea* $x_n = 2x_{n-1} + 1$. *Lo que hace que no sea homogénea es el término* 1. *Vamos a tratar de "eliminarlo". Para esto, y puesto que la relación de recurrencia es válida para todos los números naturales mayores o iguales que 1, tomamos* $n \geq 2$ *y se tiene:*

$$\begin{array}{rcl} x_n & = & 2x_{n-1} + 1 \\ x_{n-1} & = & 2x_{n-2} + 1 \end{array}$$

*Y restando ambas igualdades nos queda:*

$$x_n - x_{n-1} = 2x_{n-1} - 2x_{n-2} \implies x_n - 3x_{n-1} + 2x_{n-2} = 0$$

*Y así vemos que toda solución al problema de recurrencia lineal no homogénea* $x_n = 2x_{n-1} + 1$ *es solución al problema de recurrencia lineal homogénea* $x_n = 3x_{n-1} - 2x_{n-2}$ *(el recíproco no es cierto. Basta tomar la sucesión constante* $x_n = 1$*).*

*La ecuación característica de este problema es* $x^2 - 3x + 2 = 0$, *cuyas soluciones son* $\alpha_1 = 2$ *y* $\alpha_2 = 1$. *Por tanto, todas las soluciones son de la forma* $x_n = a \cdot 2^n + b$

*Ahora, seleccionamos aquellas que sean solución al problema* $x_n = 2x_{n-1} + 1$. *Si* $x_n$ *es una solución a tal problema, tenemos:*

$x_1 = 2a + b$

$x_1 = 2x_0 + 1 = 2(a + b) + 1 = 2a + 2b + 1$

*Por tanto,* $2a + b = 2a + 2b + 1$, *de donde deducimos que* $b = -1$.

*Luego la solución general al problema* $x_n = 2x_{n-1} +$ *es* $x_n = a \cdot 2^n - 1$.

- *Vamos a resolver el problema de recurrencia lineal no homogénea* $x_n + x_{n-1} = 2n$.

*En primer lugar, tratamos de transformar la recurrencia no homogénea en una homogénea. Entonces, para cada* $n \geq 2$ *tenemos:*

$$\begin{array}{l} x_n + x_{n-1} = 2n \\ x_{n-1} + x_{n-2} = 2(n-1). \end{array}$$

*Restamos ambas igualdades, y nos queda que para* $n \geq 2$, $x_n - x_{n-2} = 2$. *Por tanto, para* $n \geq 3$,

$$\begin{array}{l} x_n - x_{n-2} = 2. \\ x_{n-1} + x_{n-3} = 2. \end{array}$$

*Y volviendo a restar, tenemos* $x_n - x_{n-1} - x_{n-2} + x_{n-3} = 0$. *La ecuación característica es* $x^3 - x^2 + x + 1 = 0$, *cuyas raíces son* $\alpha_1 = -1$ *(simple) y* $\alpha_2 = 1$ *(doble).*

*La solución general al problema de recurrencia lineal homogénea es* $x_n = a(-1)^n + b + cn$.

*Ahora, de todas esas soluciones hemos de seleccionar aquéllas que sean soluciones del problema* $x_n + x_{n-1} = 2n$.

$$\left.\begin{array}{l} \left.\begin{array}{l} x_0 = a + b \\ x_1 = -a + b + c \end{array}\right\} \Rightarrow \begin{array}{c} x_1 + x_0 = 2b + c \\ x_1 + x_0 = 2 \cdot 1 = 2 \end{array} \Big\} \Rightarrow\ 2b + c = 2 \\ \left.\begin{array}{l} x_1 = -a + b + c \\ x_2 = a + b + 2c \end{array}\right\} \Rightarrow \begin{array}{c} x_2 + x_1 = 2b + 3c \\ x_2 + x_1 = 2 \cdot 2 = 4 \end{array} \Rightarrow\ 2b + 3c = 4 \end{array}\right\} \Rightarrow\ c = 1;\ b = \frac{1}{2}$$

*Luego la solución general al problema de recurrencia* $x_n + x_{n-1} = 2n$ *es* $x_n = a(-1)^n + n + \frac{1}{2}$.

Vamos a fijarnos con un poco más de detalle en este ejemplo.

Partimos de una recurrencia lineal no homogénea ($x_n + x_{n-1} = 2n$) cuya relación homogénea asociada es $x_n + x_{n-1} = 0$, y por tanto su polinomio característico es $x + 1$.

Lo que hemos hecho ha sido intentar eliminar la parte no homogénea. En un primer paso, hemos llegado a la relación $x_n - x_{n-2} = 1$, cuya relación homogénea asociada es $x_n - x_{n-2} = 0$, y su polinomio característico es $x^2 - 1 = (x + 1)(x - 1)$.

En un segundo paso hemos llegado a la relación de recurrencia $x_n - x_{n-1} - x_{n-2} + x_{n-3} = 0$, cuyo polinomio característico es $x^3 - x^2 - x + 1 = (x + 1)(x - 1)^2$.

Vemos que en cada uno de los pasos, hemos disminuido en 1 el grado de la parte no homogénea, mientras que el polinomio característico se multiplica por $(x - 1)$.

Como conclusión de esto, podemos decir:

**Proposición 1.3.4.** *Supongamos que $x_n$ es una sucesión que satisface una relación de recurrencia lineal no homogénea*

$$x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = f(n)$$

*donde $f(n)$ es un polinomio de grado $r$.*

*Entonces $x_n$ satisface una relación de recurrencia lineal homogénea cuyo polinomio característico es $(x^k + a_1 x^{k-1} + \cdots + a_k)(x - 1)^{r+1}$.*

La demostración de esta proposición se haría por inducción, siguiendo la idea que hemos mostrados en el ejemplo precedente.

**Ejemplo 1.3.12.** *Sea $x_n$ la sucesión definida por $x_n - x_{n-2} = n + 1$, $x_0 = 1$, $x_1 = -1$. Vamos a buscar el término general de la sucesión $x_n$.*

*El polinomio característico de la relación lineal homogénea asociada es $x^2 - 1$. Como $n + 1$ es un polinomio de grado 1, la sucesión $x_n$ satisface una recurrencia lineal homogénea cuyo polinomio característico es $(x^2 - 1)(x - 1)^2 = (x + 1) \cdot (x - 1)^3$.*

*Por tanto, la sucesión $x_n$ es de la forma $x_n = a \cdot (-1)^n + b + cn + dn^2$. Puesto que $x_2 = x_0 + 3 = 4$ y $x_3 = x_1 + 4 = 3$ tenemos que:*

$$\begin{array}{rcrcrcrcr} a & + & b & & & & & = & 4 \\ -a & + & b & + & c & + & d & = & -1 \\ a & + & b & + & 2c & + & 4d & = & 4 \\ -a & + & b & + & 3c & + & 9d & = & 3 \end{array}$$

*Y al resolver el sistema nos queda $a = \frac{13}{8}$, $b = \frac{-5}{8}$, $c = 1$, $d = \frac{1}{4}$. Por tanto, la forma general de $x_n$ es*

$$x_n = \frac{13 \cdot (-1)^n - 5 + 8n + 2n^2}{8}$$

Vamos a modificar la forma de la función $f(n)$. Para esto, analizamos el siguiente ejemplo:

**Ejemplo 1.3.13.** *Vamos a encontrar la solución al problema de recurrencia lineal $x_n = 2x_{n-1} + n \cdot 4^n$.*

*Ahora, el término no homogéneo es $n \cdot 4^n$.*

*El polinomio característico de la relación de recurrencia homogénea asociada es $x - 2$.*

*Vemos que si procedemos como antes, restando $x_n - x_{n-1}$, no conseguimos nada. Pero si calculamos $x_n - 4x_{n-1}$, el término no homogéneo se simplifica.*

$$\begin{array}{rcrcl} x_n & = & 2x_{n-1} & + & n \cdot 4^n \\ 4x_{n-1} & = & 8x_{n-2} & + & (n-1) \cdot 4^n \\ \hline x_n - 4x_{n-1} & = & 2x_{n-1} - 8x_{n-2} & + & [n - (n-1)] \cdot 4^n \\ x_n & = & 6x_{n-1} - 8x_{n-2} & + & 4^n \end{array}$$

*El polinomio característico de la recurrencia homogénea asociada es ahora $x^2 - 6x + 8 = (x-2) \cdot (x-4)$.*

*Y si ahora repetimos, nos queda:*

$$\begin{array}{rcrcl} x_n & = & 6x_{n-1} - 8x_{n-2} & + & 4^n \\ 4x_{n-1} & = & 24x_{n-2} - 32x_{n-3} & + & 4^n \\ \hline x_n - 4x_{n-1} & = & 6x_{n-1} - 32x_{n-2} + 32x_{n-3} & & \\ x_n & = & 10x_{n-1} - 32x_{n-2} + 32x_{n-3} & & \end{array}$$

*Y vemos que nos queda una relación de recurrencia lineal homogénea cuyo polinomio característico es* $x^3 - 10x^2 + 32x - 32 = (x-2)\cdot(x-4)^2$.

*La solución de esta recurrencia es* $x_n = a\cdot 2^n + b\cdot 4^n + cn\cdot 4^n$. *Puesto que* $x_1 = 2x_0 + 4$ *y* $x_2 = 2x_1 + 32 = 2(2x_0+4) + 32 = 4x_0 + 40$, *para hallar la relación entre* $a$, $b$ *y* $c$ *planteamos el sistema:*

$$\begin{array}{rcrcrcl} a & + & b & & & = & x_0 \\ 2a & + & 4b & + & 4c & = & 2x_0 + 4 \\ 4a & + & 16b & + & 32c & = & 4x_0 + 40 \end{array}$$

*cuya solución es* $a = x_0 + 2$, $b = -2$, $c = 2$.

*Si sustituimos en la sucesión tenemos la solución al problema de recurrencia:*

$$x_n = 2^n x_0 + 2^{n+1} + (2n-2)\cdot 4^n$$

*Que vemos que se corresponde con lo que habíamos dicho antes. La solución general de la recurrencia no homogénea es la solución de la recurrencia lineal homogénea* $(2^n x_0)$ *más una solución particular* $(2^{n+1} + (2n-2)4^n)$.

A la luz de estos ejemplos, tenemos un resultado similar a la proposición 1.3.4.

**Proposición 1.3.5.** *Supongamos que* $x_n$ *es una sucesión que satisface una relación de recurrencia lineal no homogénea*

$$x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = b^n \cdot f(n)$$

*donde* $f(n)$ *es un polinomio de grado* $r$.

*Entonces* $x_n$ *satisface una relación de recurrencia lineal homogénea cuyo polinomio característico es* $(x^k + a_1 x^{k-1} + \cdots + a_k)(x-b)^{r+1}$.

Vamos a concluir con algunos ejemplos que ilustran lo dicho hasta el momento.

**Ejemplo 1.3.14.**

1. *Nos preguntamos cuantos números hay cuya expresión en binario tiene* $n$ *cifras, y no contiene dos ceros consecutivos.*

   *Vamos a llamar a este número* $x_n$, *y vamos a determinar el valor de* $x_n$.

   *Sea* $a$ *un número de tales características. Entonces, la cifra de la izquierda de* $a$ *vale 1 (en su expresión binaria). Si la quitamos, nos quedan* $n-1$ *cifras. Pueden darse dos casos:*

   - *Que la cifra de la izquierda de este número sea también 1. En este caso, lo que nos queda es un número cuya expresión en binario tiene* $n-1$ *cifras, y no contiene dos ceros consecutivos. Números de estas características hay* $x_{n-1}$.
   - *Que la cifra de la izquierda de este número sea cero. En este caso, la siguiente debe ser 1 (pues si no, el número a tendría dos ceros consecutivos). Si quitamos también el cero, lo que nos queda es un número de* $n-2$ *cifras en binario, y que no contiene dos ceros consecutivos. Números de estas características hay* $x_{n-2}$.

   *Por tanto, tenemos que* $x_n = x_{n-1} + x_{n-2}$.

   *Además,* $x_1 = 1$ *(el único número con una cifra es 1), y* $x_2 = 2$ *(los números con dos cifras son* 10 *y* 11*).*

   *Tenemos entonces que* $x_n$ *es la solución al problema de recurrencia lineal no homogénea* $x_n = x_{n-1} + x_{n-2}$, $x_1 = 1$, $x_2 = 2$. *La solución sabemos que es* $x_n = f_{n+1}$, *donde* $f_n$ *es la sucesión de Fibonacci.*

2. *Comenzamos el capítulo calculando la suma de los n primeros números impares. Es decir, teníamos la sucesión*

$$\begin{array}{lcl} x_1 & = & 1 \\ x_2 & = & 1+3 \\ x_3 & = & 1+3+5 \\ x_4 & = & 1+3+5+7 \\ \dots & \dots & \dots\dots\dots\dots \\ x_n & = & 1+3+5+\cdots+(2n-1) \end{array}$$

*Y vemos que la sucesión $x_n$ podemos definirla por recurrencia como $x_n = x_{n-1} + (2n-1)$, $x_1 = 1$.*

*Tenemos entonces una relación de recurrencia lineal no homogénea donde la parte no homogénea es un polinomio de grado 1, y la parte homogénea tiene polinomio característico $x-1$.*

*Por tanto, $x_n$ satisface una relación de recurrencia lineal homogénea cuyo polinomio característico es $(x-1)^3$, y por tanto, el término general es $x_n = a + bn + cn^2$.*

*El conocimiento de los tres primeros términos nos da el sistema*

$$\begin{array}{rcrcrcl} a & + & b & + & c & = & 1 \\ a & + & 2b & + & 4c & = & 4 \\ a & + & 3b & + & 9c & = & 9 \end{array}$$

*cuya solución es $a = 0$, $b = 0$, $c = 1$. Es decir, $x_n = n^2$.*

Como ejercicio, encuentra el término general de la sucesión $x_n = 1^2 + 2^2 + \cdots + n^2$.

# Capítulo 2

# Conjuntos ordenados. Retículos y álgebras de Boole.

## 2.1. Conjuntos ordenados.

En este capítulo vamos a estudiar el concepto de retículo. Hay dos caminos para llegar a esta estructura. Uno es mediante un conjunto con dos operaciones binarias que satisfacen una serie de axiomas. El otro es a partir del concepto de conjunto ordenado. Nosotros aquí hemos adoptado el segundo. Si enriquecemos la estructura de retículo con unos axiomas adicionales obtenemos lo que se conoce como *Álgebra de Boole.* Analizaremos su estructura, y llegaremos a que en el caso finito, las álgebras de Boole tiene una forma muy particular. Estudiaremos el álgebra de Boole de las funciones booleanas, y el teorema de estructura nos conducirá a las formas normales. Terminaremos viendo algunas aplicaciones de las álgebras de Boole al diseño de circuitos lógicos.

**Definición 5.** *Sea $X$ un conjunto, y $\leq$ una relación binaria en $X$. Se dice que $\leq$ es una relación de orden si se verifican las siguientes propiedades.*

*Reflexiva: $x \leq x$ para todo $x \in X$.*

*Antisimétrica: Si $x \leq y$ e $y \leq x$ entonces $x = y$.*

*Transitiva: Si $x \leq y$ e $y \leq z$ entonces $x \leq z$.*

*Si $X$ es un conjunto en el que tenemos definida una relación de orden $\leq$, se dice que $(X, \leq)$ es un conjunto ordenado (o, si está claro cual es la relación $\leq$ se dice simplemente que $X$ es un conjunto ordenado).*

*Si $\leq$ es una relación de orden en $X$ que satisface la propiedad adicional de que dados $x, y \in X$ entonces $x \leq y$ ó $y \leq x$, se dice entonces que $\leq$ es una relación de orden total, y que $(X, \leq)$ (o $X$) es un conjunto totalmente ordenado (en ocasiones, para destacar que $(X, \leq)$ es una relación de orden, pero que no es total se dice que $\leq$ es una relación de orden parcial y que $(X, \leq)$ es un conjunto parcialmente ordenado).*

**Ejemplo 2.1.1.**

1. *El conjunto de los números naturales, con el orden natural ($m \leq n$ si existe $k \in \mathbb{N}$ tal que $n = m+k$) es un conjunto totalmente ordenado. De la misma forma, también lo son $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ y $(\mathbb{R}, \leq)$.*

2. *Dado un conjunto $X$, entonces $\mathcal{P}(X)$, con el orden dado por la inclusión es un conjunto ordenado. Si $X$ tiene más de un elemento, este orden no es total, pues dados $x, y \in X$ distintos se tiene que $\{x\} \not\subseteq \{y\}$ y $\{y\} \not\subseteq \{x\}$.*

3. *En el conjunto de los números naturales, la relación de divisibilidad es una relación de orden que no es total. Esta relación viene dada por $a|b$ si existe $c \in \mathbb{N}$ tal que $b = a \cdot c$ (compara con la relación de orden natural). Sin embargo, en el conjunto de los números enteros esta relación no es de orden pues no es antisimétrica, ya que $2|-2$, $-2|2$ y sin embargo $2 \neq -2$.*

4. *Para cualquier número natural $n$ consideramos el conjunto*

$$D(n) = \{m \in \mathbb{N} : m|n\}$$

*Entonces $(D(n), |)$ es un conjunto (parcialmente) ordenado.*

5. *Sea $(X, \leq)$ es un conjunto ordenado, e $Y$ un subconjunto de $X$. Definimos en $Y$ el orden $x \preceq y$ si $x \leq y$ (vistos como elementos de $X$). Entonces, $(Y, \preceq)$ es un conjunto ordenado. De ahora en adelante, el orden en $Y$ lo denotaremos igual que en $X$.*

   *Un ejemplo de esto último podría ser el caso de los divisores de un número natural $n$.*

   *Si $(X, \leq)$ es un conjunto totalmente ordenado, entonces, para cualquier $Y \subseteq X$ se tiene que $(Y, \leq)$ es un conjunto totalmente ordenado.*

La definición de conjunto ordenado puede hacerse también a partir de la noción de *orden estricto*.

**Definición 6.** *Sea $X$ un conjunto, $y <$ una relación binaria en $X$. Se dice que $<$ es un orden estricto si se verifican las siguientes propiedades:*

*Antirreflexiva Para cualquier $x \in X$ se tiene que $x \not< x$.*

*Transitiva Si $x < y$ e $y < z$ entonces $x < z$.*

Es fácil comprobar que si $\leq$ es una relación de orden en un conjunto $X$, entonces si definimos

$$x < y \text{ si } x \leq y \text{ y } x \neq y$$

se tiene que $<$ es una relación de orden estricto en $X$.

De la misma forma, si $<$ es una relación de orden estricto en $X$ entonces la relación siguiente:

$$x \leq y \text{ si } x < y \text{ o } x = y$$

es una relación de orden en $X$.

Vemos entonces que los conceptos de *relación de orden* y *relación de orden estricto* son equivalentes, pues dada una relación de orden tenemos determinada una relación de orden estricto y viceversa. Además, los caminos para pasar de orden a orden estricto, y de orden estricto a orden, son uno el inverso del otro.

A continuación vamos a construir un grafo (dirigido) asociado a una relación de orden. Aún cuando los grafos serán estudiados con posterioridad, la representación de una relación de orden mediante este grafo ayuda a visualizar mejor el orden dado.

**Definición 7.** *El diagrama de Hasse de un conjunto ordenado $(X, \leq)$ es un grafo dirigido cuyos vértices son los elementos de $X$, y existe un lado de $x$ a $y$ si $x < y$ y no existe $z$ tal que $x < z < y$.*

El diagrama de Hasse está definido para cualquier conjunto ordenado. Sin embargo, en general dicho diagrama no permite recuperar el orden. Por ejemplo, en el caso del conjunto $(\mathbb{R}, \leq)$, dado cualquier $x \in \mathbb{R}$ no existe ningún $y \in \mathbb{R}$ que esté conectado a $x$ por algún lado.

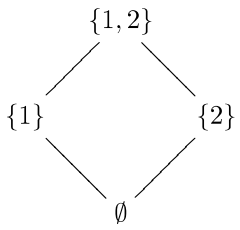
Sin embargo, si el conjunto $X$ es finito, entonces dados $x, y \in X$ se tiene que $x \leq y$ si $x = y$ o existe algún camino que parta de $x$ y termine en $y$.

Una forma habitual de representar el diagrama de Hasse es dibujar los lados como líneas ascendentes, lo que implica colocar los vértices de forma apropiada.

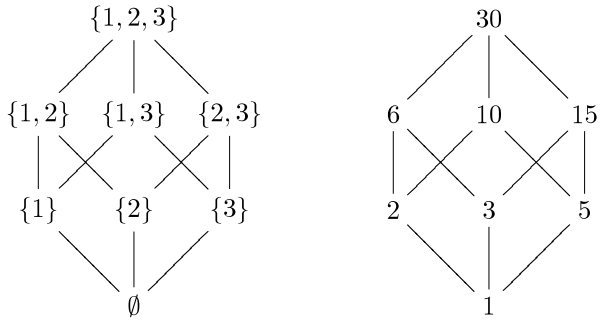
**Ejemplo 2.1.2.**

1. *El diagrama de Hasse del conjunto* $(\mathbb{N}, \leq)$ *sería*


2. *Consideramos el conjunto ordenado* $(\mathcal{P}(\{1,2\}, \subseteq)$. *Entonces el diagrama de Hasse sería:*

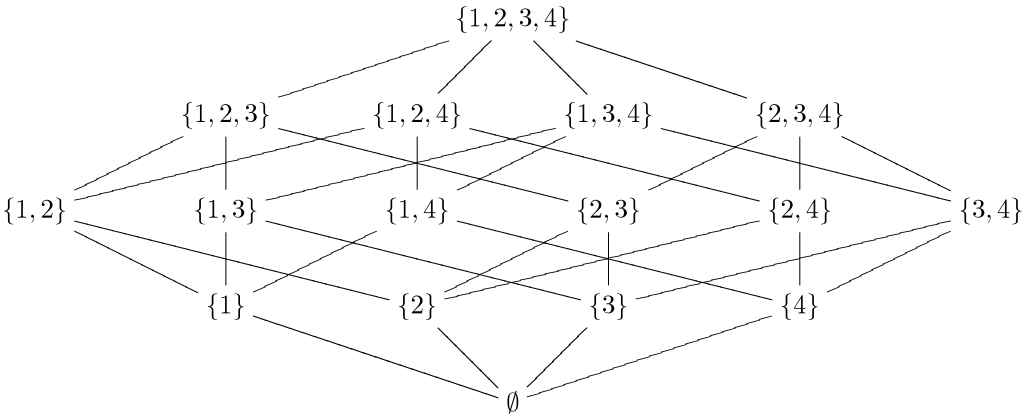



3. *Vamos a representar los diagramas de Hasse de los conjuntos ordenados* $\mathcal{P}(\{1,2,3\})$ *y* $D(30)$.



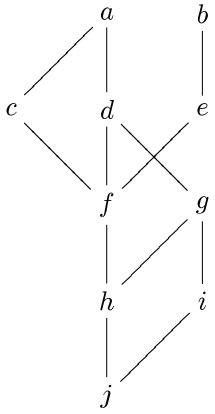

*Observa como la estructura de conjunto ordenado es igual en ambos casos.*

4. *Vamos a representar el diagrama de Hasse de* $\mathcal{P}(\{1,2,3,4\})$.




*Prueba a dibujar el diagrama de Hasse de los divisores de 210 y compáralo con este último.*

5. *Si tenemos un grafo dirigido que no contiene caminos cerrados, entonces podemos definir un orden en el conjunto de los vértices. $x \leq y$ si $x = y$ o existe un camino con inicio $x$ y fin $y$. Si en el grafo no hay caminos entre dos vértices adyacentes, entonces el grafo es el diagrama de Hasse de un conjunto ordenado.*




*tenemos definido un orden en el conjunto $X = \{a, b, c, d, e, f, g, h, i\}$. Con este orden se tiene, por ejemplo que,*

*$h \leq e$, pues tenemos un camino $h - f - e$ que empieza en $h$ y termina en $e$.*

*$i \leq a$, pues el camino $i - g - d - a$ empieza en $i$ y termina en $a$.*

*$i \not\leq e$, pues ningún camino empieza en $i$ y termina en $e$.*

**Definición 8.** *Sea $(X, \leq)$ un conjunto ordenado.*

1. *Un elemento $x \in X$ se dice que es maximal, si no existe $y \in X$ tal que $x \leq y$ y $x \neq y$.*
2. *Un elemento $x \in X$ se dice que es máximo, si para todo $y \in X$ se verifica que $y \leq x$.*

De la misma forma se puede definir lo que es un elemento minimal y lo que es un mínimo.

**Ejemplo 2.1.3.** *En el último conjunto ordenado del ejemplo anterior se tiene que $a$ y $b$ son elementos maximales, pues no hay ningún elemento que sea mayor que ellos. Sin embargo, el conjunto $X$ no tiene máximo.*

*El elemento $j$ es un elemento minimal, y además es mínimo.*

*En el conjunto de los divisores de 30 (ver ejemplo anterior) tenemos que 10 no es un elemento maximal, pues $10 \leq 30$. Sí se tiene que 30 es un elemento maximal, pues no hay ningún elemento que sea mayor que él. También se tiene que 30 es un máximo de ese conjunto.*

*En el conjunto $(\mathbb{N}, \leq)$, el cero es el mínimo y es el único elemento minimal. Este conjunto no tiene máximo ni elementos maximales.*

*Si $(X, \leq)$ es un conjunto ordenado finito, entonces $X$ tiene al menos un elemento maximal y un elemento minimal.*

Nótese, que si un conjunto tiene máximo, entonces este es único. Además, en el caso de que tenga máximo, entonces tiene sólo un elemento maximal, que coincide con el máximo.

Idéntica observación vale para mínimo y elemento minimal.

Denotaremos por máx$(X)$ al máximo del conjunto $X$, en el caso de que exista, y por mín$(X)$ al mínimo.

En el ejemplo que hemos estudiado anteriormente no existe máx$(X)$, mientras que mín$(X) = j$.

**Definición 9.** *Sea $(X, \leq)$ un conjunto ordenado, e $Y$ un subconjunto de $X$. Consideramos en $Y$ el orden inducido de $X$.*

1. *Un elemento $x \in X$ se dice que es* cota superior *de $Y$ si $x \geq y$ para todo $y \in Y$.*

2. *Un elemento $x \in X$ se dice que es* supremo *de $Y$ si es el mínimo del conjunto de las cotas superiores de $Y$.*

De la misma forma se define lo que es una cota inferior y un ínfimo.

**Ejemplo 2.1.4.** *Si $X = \{a, b, c, d, e, f, g, h, i, j\}$ con el orden dado anteriormente, e $Y = \{c, d, f, g, h\}$ entonces:*

*El conjunto de las cotas superiores de $Y$ es $\{a\}$.*

*Puesto que este conjunto tiene mínimo, que es a, entonces a es el supremo de $Y$.*

*Los elementos c y d son elementos maximales de $Y$.*

*El conjunto de las cotas inferiores es $\{h, j\}$.*

*De éstas, h es el máximo, luego h es el ínfimo de $Y$.*

*h es además el único elemento minimal y el mínimo de $Y$.*

Cuando un conjunto tiene supremo éste es único. Podemos entonces hablar de *el supremo de $Y$*, y lo representaremos mediante $\sup(Y)$.

De la misma forma, denotaremos por $\text{ínf}(Y)$ al ínfimo del conjunto $Y$ cuando exista.

Cuando un conjunto tiene máximo, entonces también tiene supremo, y coincide con él. En el último ejemplo vemos como el recíproco no es cierto, pues $Y$ tiene supremo pero no tiene máximo.

Cuando el supremo de un conjunto pertenezca al conjunto, entonces será también el máximo.

**Definición 10** (Buen orden)**.** *Sea $(X, \leq)$ un conjunto ordenado. Se dice que $\leq$ es un buen orden si todo subconjunto no vacío de $X$ tiene mínimo. En tal caso, se dice que $(X, \leq)$ (o $X$) es un conjunto bien ordenado.*

**Observación:** Todo conjunto bien ordenado es un conjunto totalmente ordenado, pues dados dos elementos $x, y \in X$ el subconjunto $\{x, y\}$ tiene mínimo. Si $\text{mín}(\{x, y\}) = x$ entonces $x \leq y$, mientras que si $\text{mín}(\{x, y\}) = y$ entonces $y \leq x$.

El recíproco no es cierto. Busca un ejemplo.

**Ejemplo 2.1.5.** *El conjunto de los números naturales, con el orden usual, es un conjunto bien ordenado, como demostramos en el Teorema 1.1.1.*

**Definición 11.** *Sean $(X_1, \leq_1)$ y $(X_2, \leq_2)$ dos conjuntos ordenados.*

*Se define el* orden producto *en $X_1 \times X_2$ como sigue:*

$$(x_1, x_2) \leq_{prod} (y_1, y_2) \text{ si } x_1 \leq_1 y_1 \text{ y } x_2 \leq_2 y_2.$$

*Se define el* orden lexicográfico *en $X_1 \times X_2$ como sigue:*

$$(x_1, x_2) \leq_{lex} (y_1, y_2) \overset{def}{\iff} \begin{cases} x_1 <_1 y_1 & \text{ó} \\ x_1 = y_1 \text{ y } x_2 \leq_2 y_2. \end{cases}$$

Claramente, si $(x_1, x_2) \leq_{prod} (y_1, y_2)$ entonces $(x_1, x_2) \leq_{lex} (y_1, y_2)$.

**Proposición 2.1.1.** *Si $(X_1, \leq_1)$ y $(X_2, \leq_2)$ son dos conjuntos ordenados, entonces $(X_1 \times X_2, \leq_{prod})$ y $(X_1 \times X_2, \leq_{lex})$ son conjuntos ordenados.*

*Además, si $\leq_1$ y $\leq_2$ son órdenes totales (resp. buenos órdenes) entonces $\leq_{lex}$ es un orden total (resp. buen orden).*

*Demostración:* La demostración de que el orden producto es una relación de orden es fácil, y se deja como ejercicio. Centrémonos pues en el orden lexicográfico.

Notemos en primer lugar que si $(x_1, x_2) \leq_{lex} (y_1, y_2)$ entonces $x_1 \leq_1 y_1$.

Veamos que la relación es de orden.

Reflexiva: Si $(x_1, x_2) \in X_1 \times X_2$ entonces $(x_1, x_2) \leq_{lex} (x_1, x_2)$, pues se da la segunda opción ($x_1 = x_1$ y $x_2 \leq x_2$).

Simétrica: Supongamos que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ y $(y_1, y_2) \leq_{lex} (x_1, x_2)$. Entonces se tiene que $x_1 \leq_1 y_1$ e $y_1 \leq_1 x_1$, de donde $x_1 = y_1$. Deducimos entonces que $x_2 \leq_2 y_2$ e $y_2 \leq_2 x_2$, lo que implica que $x_2 = y_2$.

Transitiva: Supongamos ahora que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ y $(y_1, y_2) \leq_{lex} (z_1, z_2)$. Pueden darse entonces tres opciones(no excluyentes):

- $x_1 <_1 y_1$, en cuyo caso $x_1 <_1 z_1$, luego $(x_1, x_2) \leq_{lex} (z_1, z_2)$.
- $y_1 <_1 z_1$, en cuyo caso $x_1 <_1 z_1$ y concluimos como en la opción anterior.
- $x_1 = y_1$ e $y_1 = z_1$. En tal caso, $x_2 \leq_2 y_2$ e $y_2 \leq_2 z_2$, de donde $x_1 = z_1$ y $x_2 \leq_2 z_2$, es decir, $(x_1, x_2) \leq_{lex} (z_1, z_2)$.

Supongamos ahora que $\leq_1$ y $\leq_2$ son órdenes totales. Sean $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$. Aquí pueden darse tres opciones (mutuamente excluyentes):

- $x_1 <_1 y_1$. En tal caso $(x_1, x_2) \leq_{lex} (y_1, y_2)$.
- $y_1 <_1 x_1$. En este caso $(y_1, y_2) \leq_{lex} (x_1, x_2)$.
- $x_1 = y_1$. Entonces dependiendo de que $x_2 \leq_2 y_2$ o $y_2 \leq_2 x_2$ se tendrá que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ o que $(y_1, y_2) \leq_{lex} (x_1, x_2)$.

Por último, supongamos que $\leq_1$ y $\leq_2$ son buenos órdenes, y sea $Y \subseteq X_1 \times X_2$ un subconjunto no vacío.

Nos quedamos con el conjunto de todas las primeras coordenadas de los elementos de $A$, es decir, tomamos

$$Y_1 = \{x_1 \in X_1 : (x_1, x_2) \in A \text{ para algún } x_2 \in X_2\}.$$

Sea $a = \text{mín}(Y_1)$. Tomamos entonces $Y_2 = \{x_2 \in X_2 : (a, x_2) \in A\}$. Como $Y_2 \neq \emptyset$, tiene mínimo. Sea éste $b$. Entonces $(a, b) = \text{mín}(A)$. ■

**Observación:** Si tenemos $n$ conjuntos ordenados $X_1, X_2, \ldots, X_n$, podemos definir recursivamente el orden producto y el orden lexicográfico en $X_1 \times X_2 \times \cdots \times X_n$.

Supuesto definido el orden producto $\leq_{prod}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{prod} (y_1, \ldots, y_{n-1}, y_n) \text{ } si \text{ } (x_1, \ldots, x_{n-1}) \leq_{prod} (y_1, \ldots, y_{n-1}) \text{ y } x_n \leq y_n,$$

es decir, definimos el orden producto en $(X_1 \times \cdots \times X_{n-1}) \times X_n$.

Supuesto definido el orden lexicográfico $\leq_{lex}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{lex} (y_1, \ldots, y_{n-1}, y_n) \overset{\text{def}}{\iff} \begin{cases} (x_1, \ldots, x_{n-1}) <_{lex} (y_1, \ldots, y_{n-1}) & \text{ó} \\ (x_1, \ldots, x_{n-1}) = (y_1, \ldots, y_{n-1}) \text{ y } x_n \leq y_n. \end{cases}$$

Sea el conjunto

$$\mathcal{A} = \{\ , a, b, c, d, e, f, g, h, i, j, l, l, m, n, \tilde{n}, o, p, q, r, s, t, u, v, w, x, y, z\},$$

es decir, las 27 letras del alfabeto junto con el espacio en blanco.

Claramente, $\mathcal{A}$ tiene un orden total de todos conocido.

Supongamos que $n$ es el número de letras de la palabra más larga de la lengua española. Entonces, cada palabra puede representarse como un elemento de $\mathcal{A}^n$ (poniendo tantos espacios al final como sea necesario).

Cuando ordenamos las palabras, tal y como vienen en un diccionario, nos fijamos en la primera letra, y es la que nos da el orden. Cuando ésta coincide, pasamos a la segunda, y es ésta entonces la que nos da el orden. De coincidir también, nos fijamos en la tercera, y así sucesivamente. Es decir, las palabras de la lengua están ordenadas siguiendo el orden lexicográfico.

**Ejemplo 2.1.6.**

*Consideramos en* $\mathbb{N}\times\mathbb{N}$ *los órdenes producto* ($\leq$) *y lexicográfico* $\leq_{lex}$ *deducidos a partir del orden usual en* $\mathbb{N}$. *Entonces:*

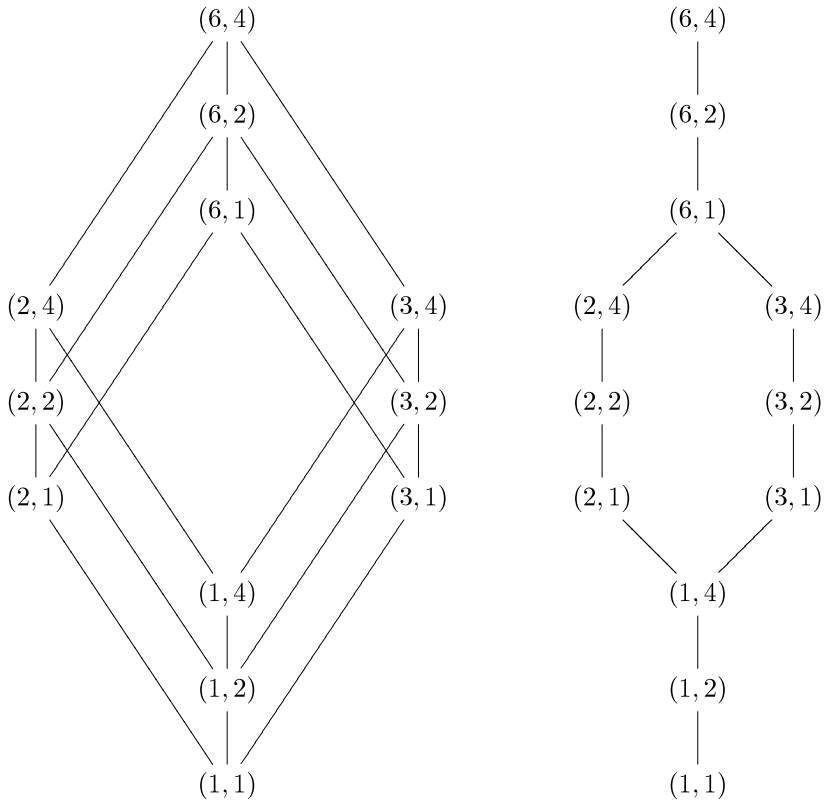
*Los elementos* $(0,n),(1,n-1),\ldots,(n-1,1),(n,0)$ *están ordenados según el orden lexicográfico, mientras que con el orden producto ninguna pareja de ellos es comparable.*

*Se puede ver entonces que la propiedad de ser orden total o buen orden no se mantiene al tomar el orden producto.*

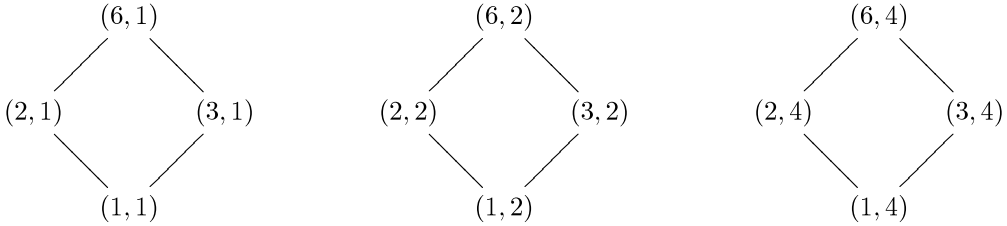
*Si* $X=\{(0,n),(1,n-1),\ldots,(n-1,1),(n,0)\}$ *entonces:*

- *El conjunto de cotas inferiores con respecto al orden lexicográfico es* $\{(0,0),(0,1),\ldots,(0,n)\}$, *mientras que con respecto al orden producto tiene una única cota inferior, que es* $(0,0)$.
- *El ínfimo, respecto al orden lexicográfico es* $(0,n)$, *que es también el mínimo. Con respecto al orden producto es* $(0,0)$, *y no tiene mínimo.*
- *Con respecto al orden lexicográfico tiene un elemento minimal, que es* $(0,n)$ *y un elemento maximal, que es* $(n,0)$. *Con respecto al orden producto, todos los elementos son maximales y minimales.*

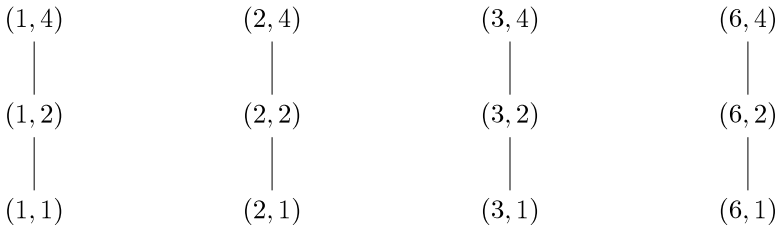
*Sean ahora los conjuntos ordenados* $(D(6),|)$ *y* $(D(4),|)$. *Entonces los diagramas de Hasse de* $D(6)\times D(4)$ *con el orden producto y el orden lexicográfico son respectivamente:*



*Nótese como el diagrama de Hasse de $D(6) \times D(4)$ con el orden producto consiste en "pegar" tres diagramas como el de $D(6)$*

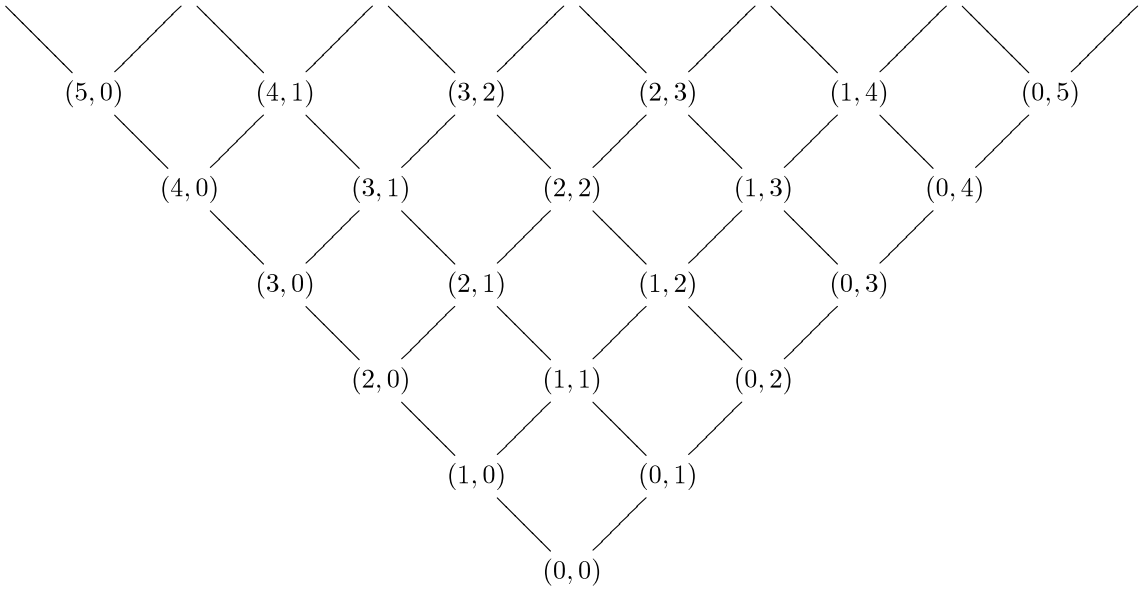



*y cuatro diagramas como el de $D(4)$*




*mientras que el diagrama de Hasse de $D(6) \times D(4)$ con el orden lexicográfico tiene la "misma forma" que el de $D(6)$, salvo que en cada vértice tenemos un diagrama de $D(4)$.*

*El diagrama de Hasse de $(\mathbb{N}^2, \leq_{prod})$ sería como sigue:*




## 2.2. Retículos.

**Definición 12.** *Un retículo es un conjunto ordenado, $(L, \leq)$ en el que cualquier conjunto finito tiene supremo e ínfimo.*

Si $(L, \leq)$ es un retículo y $x, y \in L$, denotaremos por $x \vee y$ al supremo del conjunto $\{x, y\}$ y por $x \wedge y$ al ínfimo del conjunto $\{x, y\}$.

Nótese que $x \vee y$ está definido por la propiedad:

$$x \leq x \vee y;\ y \leq x \vee y \qquad (x \leq z \text{ e } y \leq z) \Longrightarrow x \vee y \leq z$$

La primera parte dice que $x \vee y$ es una cota superior del conjunto $\{x, y\}$, mientras que la segunda dice que es la menor de las cotas superiores.

**Proposición 2.2.1.** *Si $(L, \leq)$ es un retículo, las operaciones $\vee$ y $\wedge$ satisfacen las siguienes propiedades:*

$$\begin{array}{rl} \textit{Conmutativa} & \left\{ \begin{array}{l} x \vee y = y \vee x \\ x \wedge y = y \wedge x. \end{array} \right. \\ \textit{Asociativa} & \left\{ \begin{array}{l} x \vee (y \vee z) = (x \vee y) \vee z \\ x \wedge (y \wedge z) = (x \wedge y) \wedge z. \end{array} \right. \\ \textit{Absorción} & \left\{ \begin{array}{l} x \vee (x \wedge y) = x \\ x \wedge (x \vee y) = x. \end{array} \right. \\ \textit{Idempotencia} & \left\{ \begin{array}{l} x \vee x = x \\ x \wedge x = x. \end{array} \right. \end{array}$$

*Demostración:* La demostración de la propiedad conmutativa, así como la de idempotencia es inmediata. Para demostrar la propiedad asociativa basta comprobar que tanto $x \vee (y \vee z)$ como $(x \vee y) \vee z$ representa el supremo del conjunto $\{x, y, z\}$, y lo mismo para el ínfimo. Veamos que $\sup(\{x, y, z\}) = x \vee (y \vee z)$.

Es claro que $x \leq x \vee (y \vee z)$, $y \leq x \vee (y \vee z)$ y $z \leq x \vee (y \vee z)$. Por otra parte,

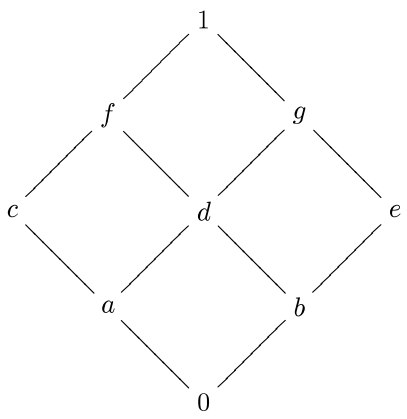
$$\left.\begin{array}{l} x \leq u \\ y \leq u \\ z \leq u \end{array}\right\} \Longrightarrow y \vee z \leq u \left.\right\} \Longrightarrow x \vee (y \vee z) \leq u.$$

Por tanto, $x \vee (y \vee z)$ es el supremo del conjunto $\{x, y, z\}$.

En cuanto a la absorción, la primera se deduce fácilmente del hecho de que $x \wedge y \leq x$ y la segunda de que $x \leq x \vee y$. ■

**Ejemplo 2.2.1.**

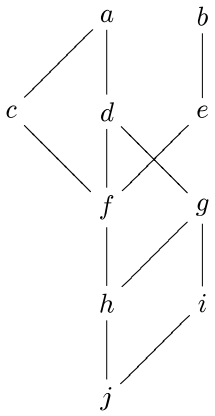
1. *Si $X$ es un conjunto totalmente ordenado, entonces $X$ es un retículo. Dados $x, y \in X$ se tiene que $x \vee y = \textit{máx}(\{x, y\})$ mientras que $x \wedge y = \textit{mín}(\{x, y\})$.*
2. *El conjunto ordenado $(\mathbb{N}, |)$ es un retículo. En este caso se tiene que $x \vee y = mcm(x, y)$ mientras que $x \wedge y = mcd(x, y)$. De la misma forma, si $n \in \mathbb{N}$ entonces $D(n)$, con el orden dado por la divisibilidad es un retículo. Supremo e ínfimo vienen dado por el mínimo común múltiplo y el máximo común divisor respectivamente.*
3. *Si $X$ es un conjunto, entonces $\mathcal{P}(X)$ es un retículo. En este caso supremo e ínfimo vienen dados por la unión y la intersección respectivamente; es decir, $A \vee B = A \cup B$ y $A \wedge B = A \cap B$.*
4. *Si $V$ es un $K$-espacio vectorial, el conjunto de los subespacios vectoriales de $V$ es un retículo, con el orden dado por la inclusión. Aquí, dado dos subespacios vectoriales $V_1$ y $V_2$ se tiene que $V_1 \vee V_2 = V_1 + V_2$ mientras que $V_1 \wedge V_2 = V_1 \cap V_2$.*
5. *El conjunto ordenado cuyo diagrama de Hasse es*



*es un retículo.*

*Se tiene, por ejemplo:* $c \vee d = f$, $c \wedge d = a$, $b \vee c = f$, $b \wedge c = 0$, $c \vee e = 1$, $c \wedge e = 0$.

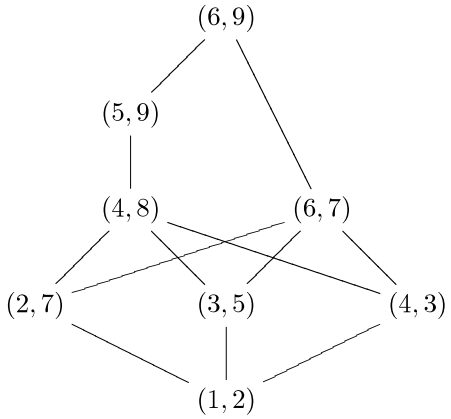
6. *El conjunto ordenado cuyo diagrama de Hasse es*




*no es un retículo, pues por ejemplo, no existe el supremo del conjunto* $\{a, e\}$. *Sin embargo, el conjunto* $\{f, i\}$ *sí tiene supremo (d) e ínfimo (j).*

7. *Dado el conjunto* $A = \{(1,2);\ (4,3);\ (3,5);\ (2,7);\ (4,8);\ (6,9);\ (6,7);(5,9)\} \subseteq \mathbb{N}^2$, *consideramos en A el orden inducido del orden producto en* $\mathbb{N}^2$.

*El diagrama de Hasse de A sería:*




*Este conjunto no es un retículo. Por ejemplo, tomamos* $x = (2,7)$ *e* $y = (3,5)$. *El conjunto de las cotas superiores de x e y es* $\{(4,8);\ (6,7);\ (5,9);\ (6,9)\}$. *Y ese conjunto no tiene mínimo. Por tanto, no existe la menor de las cotas superiores, luego no existe el supremo de x e y.*

Nótese que si $(L, \leq)$ es un retículo, entonces dados $x, y \in L$ se verifica que $x \leq y$ si, y sólo si, $x \vee y = y$, o si queremos, $x \leq y$ si, y sólo si, $x \wedge y = x$. Es decir, podemos recuperar el orden dentro del retículo a partir del conocimiento de las operaciones supremo o ínfimo.

La siguiente proposición nos da condiciones suficientes para que dos operaciones definidas en un conjunto puedan ser el supremo y el ínfimo de alguna relación de orden en ese conjunto.

**Proposición 2.2.2.** *Sea L un conjunto en el que tenemos definidas dos operaciones* $\vee$ *y* $\wedge$ *que satisfacen las propiedades conmutativa, asociativa, idempotencia y de absorción. Supongamos que en L definimos la relación*

$$x \leq y \quad \text{si } x \vee y = y.$$

*Entonces,* $(L, \leq)$ *es un retículo donde las operaciones supremo e ínfimo vienen dadas por* $\vee$ *y* $\wedge$ *respectivamente.*

*Demostración:*

1. Veamos en primer lugar que $(L, \leq)$ es un conjunto ordenado. Para esto, comprobemos que la relación $\leq$ es reflexiva, antisimétrica y transitiva.

   Reflexiva. Puesto que $x \vee x = x$ se tiene que $x \leq x$ para cualquier $x \in L$.

   Antisimétrica. Supongamos que $x \leq y$ e $y \leq x$. Esto implica que $x \vee y = y$ y que $y \vee x = x$. Puesto que $\vee$ es conmutativa deducimos que $x = y (= x \vee y)$.

   Transitiva. Supongamos ahora que $x \leq y$ y que $y \leq z$, es decir, $x \vee y = y$ e $y \vee z = z$. Entonces:

   $$x \vee z = x \vee (y \vee z) = (x \vee y) \vee z = y \vee z = z$$

   luego $x \leq z$.

2. Comprobemos ahora que dados $x, y \in L$ se verifica que $\sup(\{x, y\}) = x \vee y$.

   Puesto que $x \vee (x \vee y) = (x \vee x) \vee y = x \vee y$ se tiene que $x \leq x \vee y$. De la misma forma se comprueba que $y \leq x \vee y$.

   Si $x \leq u$ e $y \leq u$ (es decir, $x \vee u = u$ e $y \vee u = u$). Entonces:

   $$(x \vee y) \vee u = x \vee (y \vee u) = x \vee u = u,$$

   de donde se deduce que $x \vee y \leq u$.

3. Por último, veamos que $\text{ínf}(\{x, y\}) = x \wedge y$.

   $(x \wedge y) \vee x = x \vee (x \wedge y) = x$ luego $x \wedge y \leq x$.

   De la misma forma se comprueba que $x \wedge y \leq y$.

   Si $u \leq x$ y $u \leq y$ (es decir, $u \vee x = x$ y $u \vee y = y$) se tiene que:

   $$u \wedge x = u \wedge (u \vee x) = u \qquad u \wedge y = u \wedge (u \vee y) = u,$$

   $$u \wedge (x \wedge y) = (u \wedge x) \wedge y = u \wedge y = u,$$

   $$u \vee (x \wedge y) = (u \wedge (x \wedge y)) \vee (x \wedge y) = (x \wedge y) \vee ((x \wedge y) \wedge u) = x \wedge y,$$

   luego $u \leq x \wedge y$.

■

Nótese que se tiene que $x \vee y = y$ si, y sólo si, $x \wedge y = x$, luego podría haberse hecho la demostración definiendo la relación

$$x \leq y \quad \text{si } x \wedge y = x.$$

Nótese también que la propiedad de idempotencia se puede deducir a partir de la de absorción, pues

$$x \vee x = x \vee [x \wedge (x \vee x)] = x,$$

luego podemos demostrar la proposición anterior partiendo de que las operaciones $\vee$ y $\wedge$ satisfacen las propiedades asociativa, conmutativa y de absorción.

Esta proposición permite definir un retículo, bien dando la relación de orden, bien dando las operaciones $\vee$ y $\wedge$.

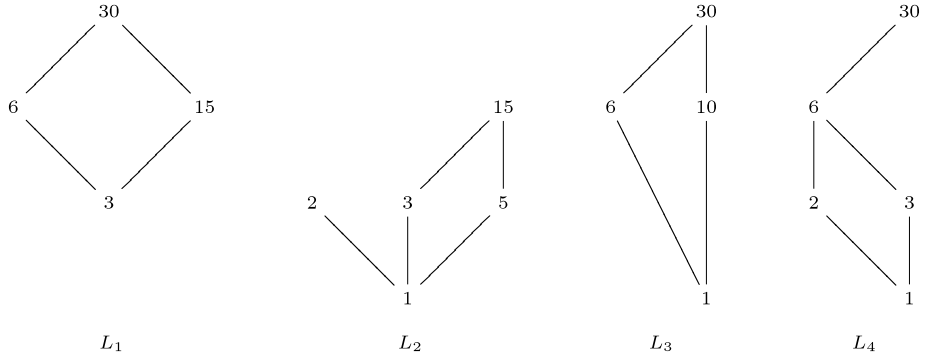
Si $(L, \leq)$ es un retículo y $L$ tiene máximo, denotaremos a éste por 1, mientras que si tiene mínimo lo denotaremos por 0. Se tiene entonces, $x \vee 1 = 1$, $x \wedge 1 = x$, $x \vee 0 = x$ y $x \wedge 0 = 0$.

Un retículo finito siempre tiene máximo y mínimo. Si el retículo es infinito, puede tenerlo o no. Así, por ejemplo, $(\mathbb{N}, \leq)$ tiene mínimo pero no tiene máximo; $(\mathbb{Z}, \leq)$ no tiene ni mínimo ni máximo. El retículo $(\mathbb{N}, |)$ es infinito y tiene máximo y mínimo. En este caso, el máximo es 0 mientras que el mínimo es 1.

**Definición 13.** *Sea $(L, \leq)$ un retículo, y $L' \subseteq L$ un subconjunto de $L$. Entonces $L'$ es un subrretículo si para cualesquiera $x, y \in L'$ se verifica que $x \vee y \in L'$ y $x \wedge y \in L'$.*

**Ejemplo 2.2.2.** *Consideramos el retículo $D(30)$.*

*Sean $L_1 = \{3, 6, 15, 30\}$, $L_2 = \{1, 2, 3, 5, 15\}$, $L_3 = \{1, 6, 10, 30\}$ y $L_4 = \{1, 2, 3, 6, 30\}$. Sus diagramas de Hasse son:*




$L_1$ $L_2$ $L_3$ $L_4$

*Entonces $L_1$ y $L_4$ son subrretículos de $D(30)$, mientras que $L_2$ y $L_3$ no lo son. $L_2$ no es subrretículo porque el supremo de 2 y 3 es 6, que no pertenece a $L_2$. $L_3$ no es subrretículo porque el ínfimo de 6 y 10 vale 2, que no pertenece a $L_3$. Nótese que $L_3$, con el orden que hereda de $D(30)$, es un retículo, pero no es subrretículo de $L_3$.*

**Definición 14.** *Sea $L$ un retículo. Se dice que $L$ es distributivo si para cualesquiera $x, y, z \in L$ se verifica que*

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad y \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

En general, si $L$ es un retículo se tiene que $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$.

$$\left.\begin{array}{l} \left.\begin{array}{l} x \leq x \vee y \\ x \leq x \vee z \end{array}\right\} \implies x \leq (x \vee y) \wedge (x \vee z) \\ \left.\begin{array}{l} y \wedge z \leq x \vee y \\ y \wedge z \leq x \vee z \end{array}\right\} \implies y \wedge z \leq (x \vee y) \wedge (x \vee z) \end{array}\right\} \implies x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z),$$

y de la misma forma se tiene que $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$. Por tanto, se tiene que un retículo es distributivo si $(x \vee y) \wedge (x \vee z) \leq x \vee (y \wedge z)$ y $(x \wedge (y \vee z) \leq x \wedge y) \vee (x \wedge z)$.

Por otra parte, si $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ para cualesquiera $x, y, z \in L$ se tiene que

$$\begin{array}{rcll} (x \wedge y) \vee (x \wedge z) & = & [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z] & \text{propiedad distributiva} \\ & = & [x \vee (x \wedge y)] \wedge [z \vee (x \wedge y)] & \text{pues } \vee \text{ es conmutativa} \\ & = & [(x \vee x) \wedge (x \vee y)] \wedge [(z \vee x) \wedge (z \vee y)] & \text{propiedad distributiva} \\ & = & (x \vee x) \wedge (x \vee y) \wedge (x \vee z) \wedge (y \vee z) & \text{propiedad asociativa y conmutativa} \\ & = & [x \wedge (x \vee y) \wedge (x \vee z)] \wedge (y \vee z) & \text{idempotencia y propiedad asociativa} \\ & = & x \wedge (y \vee z) & \text{Absorción} \end{array}$$

mientras que si $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ para cualesquiera $x, y, z \in L$ entonces se verifica que $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ también para cualesquiera $x, y, z \in L$.

Es decir, basta con que se dé una de las dos posibles propiedades distributivas para que se dé la otra.

**Ejemplo 2.2.3.**

1. *Si $L$ es un conjunto totalmente ordenado, entonces $L$ es un retículo distributivo. Basta comprobar que para cualesquiera $x, y, z \in L$ se verifica que*

$$máx\{x, mín\{y, z\}\} = mín\{máx\{x, y\}, máx\{x, z\}\},$$

*lo cual puede hacerse fácilmente comprobando que se da la igualdad en cualquiera de los seis casos siguientes:*

$$x \leq y \leq z; \quad x \leq z \leq y; \quad y \leq x \leq z; \quad y \leq z \leq x; \quad z \leq x \leq y; \quad z \leq y \leq x,$$

*y puesto que en la igualdad el papel que juegan $y$ y $z$ es el mismo, bastaría con comprobarlo en los casos*

$$x \leq y \leq z; \qquad y \leq x \leq z; \qquad y \leq z \leq x.$$

2. *El retículo $(\mathbb{N}, |)$ es un retículo distributivo. Basta ver que en este caso, el cálculo del supremo y el ínfimo se reduce al cálculo del máximo y el mínimo de los exponentes, y entonces reducirse al caso anterior.*

   *Por el mismo motivo, para cada número natural $n \in \mathbb{N}$ el retículo $D(n)$ es distributivo.*

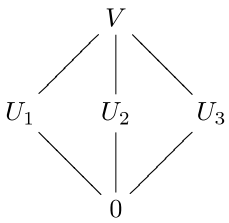
3. *Si $X$ es un conjunto, entonces $(\mathcal{P}(X), \subseteq)$ es un retículo distributivo, pues la unión y la intersección de conjuntos son distributivas la una con respecto de la otra.*

4. *Si $V$ es un $K$-espacio de dimensión mayor que $1$, entonces el retículo de los subespacios vectoriales de $V$ es un retículo que no es distributivo.*

   *Como ejemplo, sea $K = \mathbb{Z}_2$ y $V = \mathbb{Z}_2^2$. Entonces $V$ tiene $5$ subespacios vectoriales que son:*

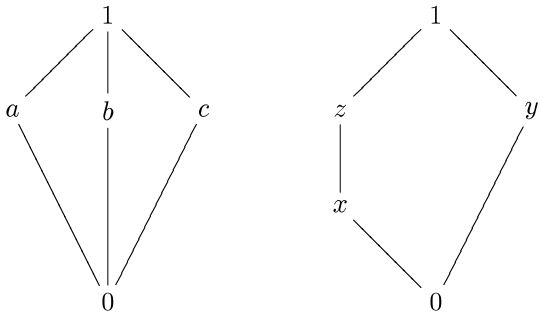
$$V; \quad U_1 = \{(0,0),(1,0)\}; \quad U_2 = \{(0,0),(0,1)\}; \quad U_3 = \{(0,0),(1,1)\}; \quad 0.$$

   *y se tiene que $U_2 \cap U_3 = 0$, luego $U_1 + (U_2 \cap U_3) = U_1$, mientras que $(U_1 + U_2) \cap (U_1 + U_3) = V \cap V = V$. El diagrama de Hasse de este retículo es:*




   *En general, si $V$ es un $K$-espacio de dimensión mayor o igual que $2$, y $u, v$ son dos vectores linealmente independientes, consideramos $U_1 = L\{u\}$, $U_2 = L\{v\}$ y $U_3 = L\{u+v\}$ y se verifica que $U_1 + (U_2 \cap U_3) = U_1$, mientras que $(U_1 + U_2) \cap (U_1 + U_3) = L\{u, v\}$.*

5. *Consideramos los siguientes retículos:*




   *denominados respectivamente* diamante *y* pentágono. *En el ejemplo anterior hemos visto que el diamente no es distributivo. En cuanto al pentágono, se tiene que*

$$x \vee (y \wedge z) = x \vee 0 = x, \qquad (x \vee y) \wedge (x \vee z) = 1 \wedge z = z.$$

*luego tampoco es distributivo.*

*En general, se tiene que un retículo es distributivo si no contiene como subrretículos ni al pentágono ni al diamante. En el apartado anterior hemos visto como el retículo de subespacios vectoriales de un espacio vectorial tiene al diamante como subrretículo.*

**Proposición 2.2.3.** *Sea $L$ un retículo distributivo, y sen $x, y, z \in L$ tales que $x \vee y = x \vee z$ y $x \wedge y = x \wedge z$. Entonces $y = z$.*

*Demostración:* Se tiene que

$$y = y \vee (x \wedge y) = y \vee (x \wedge z) = (y \vee x) \wedge (y \vee z) = (z \vee x) \wedge (z \vee y) = z \vee (x \wedge y) = z \vee (x \wedge z) = z.$$

■

**Ejemplo 2.2.4.** *En el diamante se tiene que $a \vee b = a \vee c = 1$, y $a \wedge b = a \wedge c = 0$, y sin embargo, $b \neq c$.*
*En el pentágono, $y \vee x = y \vee z = 1$ e $y \wedge x = y \wedge z = 0$, y sin embargo, $x \neq z$.*

**Definición 15.** *Sea $L$ un retículo que tiene máximo y mínimo (a los que denotaremos por 1 y 0 respectivamente), y $x \in L$. Se dice que $y \in L$ es un complemento de $x$ si $x \vee y = 1$ y $x \wedge y = 0$.*
*Un reticulo en el que todo elemento tiene complemento se dice complementado.*

Obviamente, si $y$ es un complemento de $x$ entonces $x$ es un complemento de $y$.

Por otra parte, si $L$ es un retículo distributivo y $x$ un elemento de $L$ que tiene complemento, entonces el complemento es único (ver Proposicion 2.2.3).

Si $L$ es un retículo distributivo y $x$ es un elemento que tiene complemento, denotaremos por $x'$ o $\overline{x}$ al único complemento de $x$.

**Ejemplo 2.2.5.**

1. *Si $L$ tiene máximo (1) y mínimo (0), entonces 0 es un complemento de 1.*
2. *El retículo $(\mathcal{P}(X), \subseteq)$ es un retículo complementado. Dado $A \in \mathcal{P}(X)$ se verifica que $A \cup (X \setminus A) = X$ y $A \cap (X \setminus A) = \emptyset$. Por ser un retículo distributivo, el complemento de cada elemento es único.*
3. *El pentágono y el diamente son retículos complementados. Vemos sin embargo, que los complementos de algunos elementos no son únicos.*

   *Así, en el diamante, tanto b como c son complementos de a; tanto a como c son complementos de b y tanto a como b son complementos de c.*

   *En el pentágono, tanto $x$ como $z$ son complementos de $y$. Sin embargo, $x$ tiene un único complemento, que es $y$, al igual que $z$.*
4. *Si $L$ es un conjunto totalmente ordenado con más de dos elementos, entonces es un retículo distributivo, pero no es complementado.*
5. *Si $V$ es un $K$-espacio vectorial de dimensión finita (esto último no es necesario) entonces el retículo de los subespacios vectoriales de $V$ es un retículo complementado.*

   *Para ver esto, tomamos $U$ un subespacio vectorial de $V$. Supongamos que $\mathcal{B}_U = \{u_1, \ldots, u_m\}$ es una base de $U$. Esta base puede ser ampliada hasta una base de $V$. Si dicha base ampliada es $\mathcal{B} = \{u_1, \ldots, u_m, u_{m+1}, \ldots, u_n\}$ entonces el subespacio generado por $\{u_{m+1}, \ldots, u_n\}$ es un complemento de $U$.*

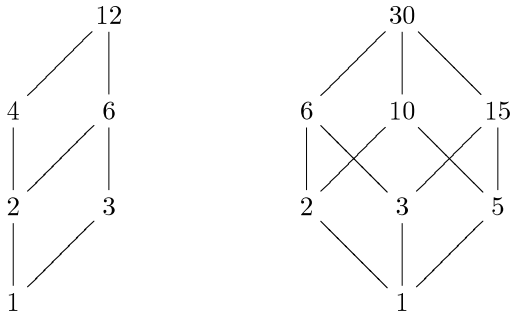
   *Puesto que en general hay muchas formas de completar una base de $V$ a partir de una base de $U$, el subespacio $U$ puede tener muchos complementos.*

   *Así, si tomamos $U = \mathbb{R}^2$ y $U = L[(1, 0)]$ (es decir, el eje $OX$) entonces cualquier recta que pase por el origen distinta del eje $OX$ es un complemento de $U$.*

6. *Dado un número natural $D(n)$, el retículo $D(n)$ no tiene por qué ser un retículo complementado. Por ejemplo, $D(4)$ no es complementado (es un conjunto totalmente ordenado con 3 elementos), mientras que $D(6)$ sí lo es.*

   *Se pide, determinar qué elementos de $D(n)$ tienen complemento, y a partir de ahí, determinar para qué valores de $n$ es $D(n)$ un retículo complementado.*

   *Así, por ejemplo, en $D(12)$ tienen complemento $1, 3, 4, 12$ mientras que no tienen $2, 6$. En $D(30)$ todos los elementos tienen complemento.*




$D(12)$ $D(30)$

**Proposición 2.2.4.** *Sean $(L_1, \leq)$ y $(L_2, \leq)$ dos conjuntos ordenados. Consideramos en $L_1 \times L_2$ el orden producto. Entonces:*

- *Si $L_1$ y $L_2$ son retículos, también lo es $L_1 \times L_2$. Las operaciones supremo e ínfimo en $L_1 \times L_2$ vienen dadas por*

$$(x_1, x_2) \vee (y_1, y_2) = (x_1 \vee y_1, x_2 \vee y_2) \qquad (x_1, x_2) \wedge (y_1, y_2) = (x_1 \wedge y_1, x_2 \wedge y_2)$$

- *Si $L_1$ y $L_2$ son retículos distributivos, también lo es $L_1 \times L_2$.*
- *Si $L_1$ y $L_2$ son retículos complementados, también lo es $L_1 \times L_2$.*

## 2.3. Álgebras de Boole

### 2.3.1. Generalidades sobre álgebras de Boole

**Definición 16.** *Un* álgebra de Boole *es un retículo distributivo y complementado.*

**Ejemplo 2.3.1.**

1. *Dado un conjunto $X$, el conjunto $\mathcal{P}(X)$, con el orden dado por la inclusión es un álgebra de Boole.*
2. *$D(6)$, o $D(30)$ son álgebras de Boole. No es álgebra de Boole $D(4)$ o $D(12)$.*

Al igual que los retículos se pueden definir sin mencionar el orden, sino únicamente las operaciones supremo e ínfimo, con las respectivas propiedades, un álgebra de Boole puede definirse también a partir de las operaciones $\vee$ y $\wedge$.

**Definición 17** (Segunda definición de álgebra de Boole)**.** *Sea $B$ un conjunto. Supongamos que en $B$ tenemos definidas dos operaciones, $\vee$ y $\wedge$ tales que:*

1. $x \vee (y \vee z) = (x \vee y) \vee z, \qquad x \wedge (y \wedge z) = (x \wedge y) \wedge z.$
2. $x \vee y = y \vee x, \qquad x \wedge y = y \wedge z.$

3. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), \qquad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$

4. $x \vee (x \wedge y) = x, \qquad x \wedge (x \vee y) = x.$

5. *Existen* $0, 1 \in B$ *tales que* $x \vee 0 = x, \quad x \wedge 0 = 0, \quad x \vee 1 = 1, \quad x \wedge 1 = x.$

6. *Para cada* $x \in B$ *existe* $\overline{x} \in B$ *tal que* $x \vee \overline{x} = 1$ *y* $x \wedge \overline{x} = 0.$

Es fácil comprobar que las definiciones 16 y 17 son equivalentes.

**Proposición 2.3.1** (Leyes de De Morgan)**.** *Sea* $B$ *un álgebra de Boole, y* $x, y \in B$*. Entonces:*

$$\overline{x \vee y} = \overline{x} \wedge \overline{y}, \qquad \overline{x \wedge y} = \overline{x} \vee \overline{y}.$$

*Demostración:* Se verifica que:

$$(x \vee y) \vee (\overline{x} \wedge \overline{y}) = [(x \vee y) \vee \overline{x}] \wedge [(x \vee y) \vee \overline{y}] = (x \vee \overline{x} \vee y) \wedge (x \vee y \vee \overline{y}) = (1 \vee y) \wedge (x \vee 1) = 1 \wedge 1 = 1,$$

$$(x \vee y) \wedge (\overline{x} \wedge \overline{y}) = [x \wedge (\overline{x} \wedge \overline{y})] \vee [y \wedge (\overline{x} \wedge \overline{y})] = (0 \wedge \overline{y}) \vee (\overline{x} \wedge 0) = 0 \vee 0 = 0.$$

■

**Ejemplo 2.3.2.**

1. *Consideremos el conjunto* $\mathbb{Z}_2$*. En él, consideramos las operaciones*

$$x \wedge y = xy, \qquad x \vee y = x + y + xy.$$

*Entonces* $\mathbb{Z}_2$*, con estas operaciones es un álgebra de Boole. De hecho, es el álgebra de Boole más simple (a excepción de un álgebra de Boole con un elemento). Representaremos a este álgebra de Boole como* $\mathbb{B}$*.*

*Nótese que este álgebra de Boole se corresponde con el orden* $0 \leq 1$*.*

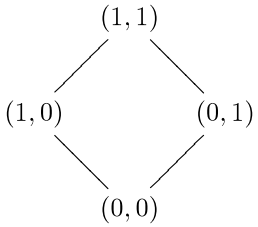
2. *Puesto que el producto de álgebras de Boole es un álgebra de Boole, tenemos, para cada número natural* $n$ *el álgebra de Boole* $\mathbb{B}^n$ *que tiene* $2^n$ *elementos. En este caso, las operaciones del álgebra de Boole vienen dadas por:*

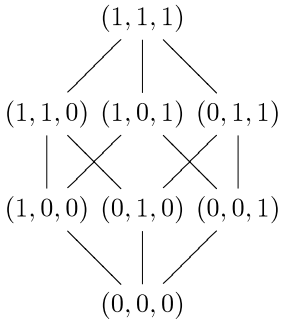
$$(x_1, x_2, \ldots, x_n) \vee (y_1, y_2, \ldots, y_n) = (x_1 \vee y_1, x_2 \vee y_2, \ldots, x_n \vee y_n),$$

$$(x_1, x_2, \ldots, x_n) \wedge (y_1, y_2, \ldots, y_n) = (x_1 \wedge y_1, x_2 \wedge y_2, \ldots, x_n \wedge y_n),$$

$$\overline{(x_1, x_2, \ldots x_n)} = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}).$$

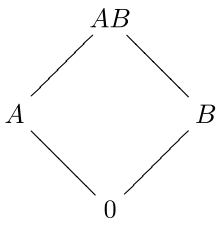
*Veamos los diagramas de Hasse de* $\mathbb{B}^2$ *y* $\mathbb{B}^3$*.*



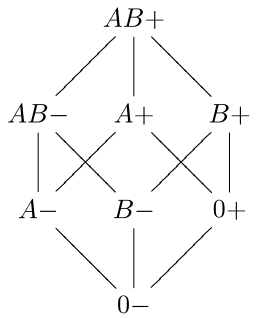

*Podemos comparar las estructuras de álgebra de Boole de* $\mathbb{B}^2$ *y* $\mathbb{B}^3$ *con las de* $\mathcal{P}(\{a, b\})$ *y* $\mathcal{P}(\{a, b, c\})$*.*

*3. Consideramos las álgebras de Boole siguientes:*





*que como podemos ver tienen una estructura semejante a $\mathbb{B}^2$ y $\mathbb{B}$ respectivamente. Su producto, tendrá entonces la misma estructura que $\mathbb{B}^3$. El diagrama de Hasse de dicho álgebra sería*




*y vemos que los elementos que la forman son los ocho grupos sanguíneos. En este caso, ser* menor o igual *significa* puede donar*. Así, el grupo* 0− *es el donante universal, mientras que el grupo* $AB+$ *es el receptor universal.*

**Definición 18.** *Sea $B$ un álgebra de Boole y $x \in B$. Se dice que $x$ es un átomo si $x$ es un elemento minimal de $B \setminus \{0\}$.*

**Nota:** Si $(X, \leq)$ es un conjunto ordenado que tiene mínimo (que llamaremos 0), podemos también definir los átomos de $X$ como los elementos minimales del conjunto $X \setminus \{0\}$.

**Ejemplo 2.3.3.** *Si $X$ es un conjunto, los átomos del álgebra de Boole $\mathcal{P}(X)$ son los subconjuntos unitarios.*

*Los átomos del álgebra de Boole $\mathbb{B}^n$ son aquellos que tienen todas las coordenadas nulas salvo una.*

*En el álgebra de Boole $D(30)$ los átomos son los divisores primos de* 30.

**Teorema 2.3.1.** *Sea $B$ un álgebra de Boole finita, y $x \in B \setminus \{0\}$. Entonces, $x$ se expresa de forma única como supremo de átomos.*

Antes de demostrar el teorema, veamos el siguiente lema:

**Lema 2.3.1.** *Sea $B$ un álgebra de Boole finita y $x \in B \setminus \{0\}$. Entonces existe $a \in B$, átomo, y tal que $a \leq x$.*

*Demostración:* Basta tomar el conjunto $A_x = \{y \in B : 0 < y \leq x\}$, que es distinto del vacío (pues $x$ es un elemento suyo). Se tiene que un elemento minimal de $A_x$ (que existe por ser $A_x$ finito) es un átomo de $B$. ■

Dado cualquier elemento $x \in B \setminus \{0\}$, denotaremos por $\mathcal{A}_x$ al conjunto de todos los átomos de $B$ que son menores o iguales que $x$.

*Demostración:*(teorema 2.3.1)

Supongamos que $\mathcal{A}_x = \{a_1, a_2, \ldots, a_m\}$. Sea entonces $z = a_1 \vee a_2 \vee \ldots \vee a_m$. Comprobemos que $z = x$.

Puesto que $a_i \leq x$ se tiene que $z \leq x$. Supongamos que $z \neq x$.

Consideramos $\overline{z}$. Se tiene entonces que $1 = z \vee \overline{z} \leq x \vee \overline{z}$ de donde $x \vee \overline{z} = 1$. Por tanto, $x \wedge \overline{z} \neq 0$ (si valiera 0 tendríamos que $\overline{z} = \overline{x}$, lo que implicaría que $z = x$).

Sea $a$ un átomo menor o igual que $x \wedge \overline{z}$. Entonces, $a \leq x$, luego $a = a_i$ para algún $i$. Supongamos que $a = a_1$. En ese caso, se tiene que:

$$0 = \overline{z} \wedge z = \overline{z} \wedge (a_1 \vee \cdots \vee a_m) \geq a \wedge (a_1 \vee \cdots \vee a_m) = (a \wedge a_1) \vee (a \wedge a_2) \vee \cdots \vee (a \wedge a_m) = a_1,$$

lo cual no es posible.

Deducimos por tanto que $z = x$, es decir, $x$ se expresa como supremo de átomos.

Supongamos ahora que podemos expresar $x$ como supremo de átomos de la forma $x = b_1 \vee \cdots \vee b_k$. Entonces:

$$b_i = b_i \wedge x = b_i \wedge (a_1 \vee \cdots \vee a_m) = (b_i \wedge a_1) \vee (b_i \wedge a_2) \vee \cdots \vee (b_i \wedge a_m),$$

y puesto que el ínfimo de dos átomos vale cero salvo que los dos átomos coincidan deducimos que $b_i = a_j$ para algún $j$. Por tanto, se tiene que

$$\{b_1, \ldots, b_k\} \subseteq \{a_1, \ldots, a_m\}.$$

De forma análoga se demuestra la otra inclusión. ■

Este teorema nos dice que si $B$ es un álgebra de Boole finita, y $X = \{a_1, \ldots, a_n\}$ son sus átomos (es decir, $X = \mathcal{A}_1$) entonces los elementos de $B$ son:

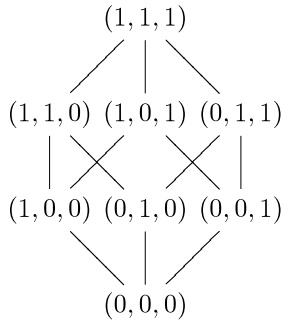
$$B = \left\{ \bigvee_{x \in A} x : \ A \in \mathcal{P}(X) \right\},$$

donde se ha empleado la notación $0 = \bigvee_{x \in \emptyset} x$.

Vemos entonces que $B$ tiene tantos elementos como $\mathcal{P}(X)$. Por tanto, el número de elementos de $B$ es $2^n$, donde $n$ es el número de átomos. Es más, tenemos que las álgebras de Boole $B$, $\mathbb{B}^n$ y $\mathcal{P}(X)$ con $X = \{1, 2, \ldots, n\}$ son isomorfas.

**Ejemplo 2.3.4.**

1. *Consideramos el álgebra de Boole* $\mathbb{B}^3$.

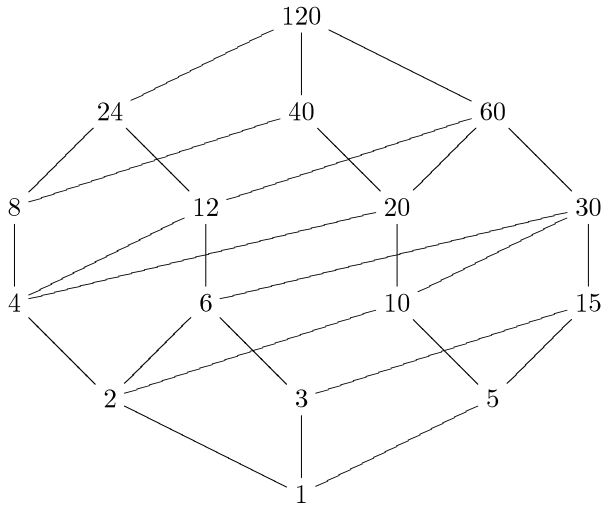



*Vemos que los átomos son* $(1, 0, 0)$, $(0, 1, 0)$ *y* $(0, 0, 1)$. *Si tomamos cualquier elemento distinto de* $(0, 0, 0)$, *por ejemplo,* $(1, 0, 1)$ *podemos comprobar fácilmente que se puede expresar como supremo de átomos. En este caso,* $(1, 0, 1) = (1, 0, 0) \vee (0, 0, 1)$.

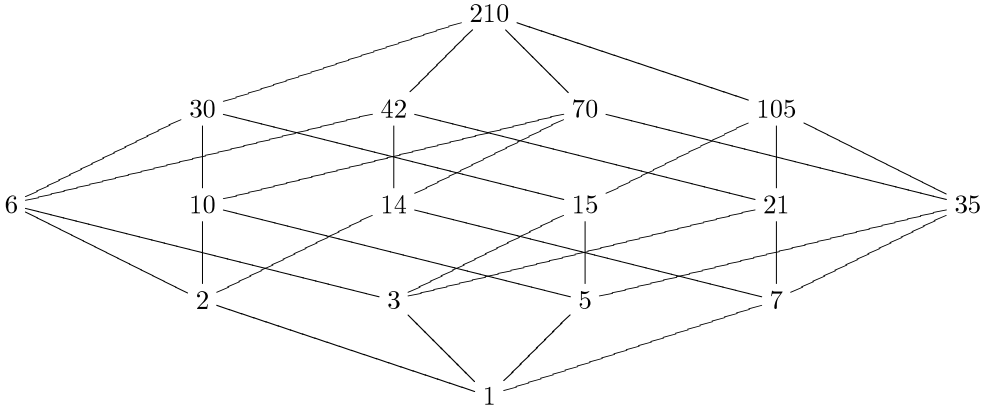
*Con cualquier otro elemento podríamos hacer lo mismo.*

2. *Sean ahora los conjuntos ordenados $D(120)$ y $D(210)$, cuyos diagramas de Hasse son:*

$D(120)$




$D(210)$



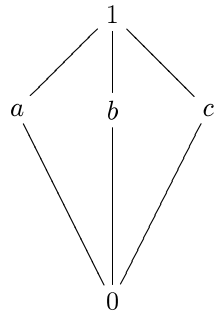

*Los átomos del primer conjunto ordenado serían los elementos $2, 3, 5$. Si tomamos por ejemplo el elemento $30$ vemos que podemos ponerlo como supremo de átomos, pues $30 = 2 \vee 3 \vee 5$. Pero, por ejemplo, si tomamos $x = 20$ vemos que no podemos ponerlo como supremo de átomos. Los átomos que son menores que 20 son 2 y 5, y como podemos comprobar, $2 \vee 5 = 10 \neq 20$.*

*Por tanto, aquí hay elementos que no se pueden poner como supremo de átomos. Esto nos dice que $D(120)$ no es un álgebra de Boole.*

*Los átomos del segundo conjunto son $2, 3, 5, 7$. Podemos tomar cualquier elemento distinto de 1, y comprobar que puede expresarse como supremo de átomos. Por ejemplo: $42 = 2 \vee 3 \vee 7$, $35 = 5 \vee 7$, $105 = 3 \vee 5 \vee 7$.*

*El conjunto de los divisores de 210 es un álgebra de Boole.*

3. *Consideramos el diamante, que sabemos que no es un álgebra de Boole, pues es distributivo.*



*Los átomos aquí serían a, b, c. La situación aquí es que todo elemento (salvo 0) se expresa como supremo de átomos. Pero la forma no es única, pues* $1 = a \vee b = a \vee c = b \vee c = a \vee b \vee c$.

### 2.3.2. Funciones y expresiones booleanas

**Definición 19.** *Una función booleana con n variables es una aplicación* $f : \mathbb{B}^n \to \mathbb{B}$.
*Denotaremos por* $\mathcal{F}_n$ *al conjunto de las funciones booleanas con n variables. Es decir:*

$$\mathcal{F}_n = \{f : \mathbb{B}^n \to \mathbb{B} \quad f \text{ es aplicación}\}.$$

**Ejemplo 2.3.5.**

1. *La aplicación* $f : \mathbb{B} \to \mathbb{B}$ *dada por* $f(0) = 1$; $f(1) = 0$ *es una función booleana en* 1 *variable (es decir, un elemento de* $\mathcal{F}_1$. *Esta aplicación responde a la expresión* $f(x) = \overline{x}$.

2. *Sea* $f : \mathbb{B}^2 \to \mathbb{B}$ *la aplicación* $f(x, y) = x \vee y$. *Entonces f es una aplicación booleana en* 2 *variables* ($f \in \mathcal{F}_2$). *Esta aplicación, elemento a elemento es:*

$$(0,0) \mapsto 0, \qquad (1,0) \mapsto 1, \qquad (0,1) \mapsto 1, \qquad (1,1) \mapsto 1.$$

**Definición 20.** *Dadas* $f, g : \mathbb{B}^n \to \mathbb{B}$ *se dice que* $f \leq g$ *si* $f(x_1, x_2, \ldots, x_n) \leq g(x_1, x_2, \ldots x_n)$ *para todo* $(x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$.

Es fácil comprobar que esta relación convierte a $\mathcal{F}_n$ en un álgebra de Boole. Las operaciones *supremo* e *ínfimo*, así como el complementario vienen dador por

$$f \vee g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \vee g(x_1, \ldots x_n),$$

$$f \wedge g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \wedge g(x_1, \ldots x_n),$$

$$\overline{f}(x_1, \ldots, x_n) = \overline{f(x_1, \ldots, x_n)},$$

mientras que el máximo y el mínimo son las aplicaciones constantes 1 y 0 respectivamente.

Los átomos de este álgebra de Boole son las aplicaciones que valen 1 en un elemento de $\mathbb{B}^n$, y 0 en el resto. Puesto que en $\mathbb{B}^n$ hay $2^n$ elementos, tenemos que $\mathcal{F}_n$ tiene $2^n$ átomos, lo que nos dice que $\mathcal{F}_n$ tiene $2^{2^n}$ elementos.

**Ejemplo 2.3.6.**

1. *El álgebra* $\mathcal{F}_1$ *tiene* $2^2 = 4$ *elementos. Éstos son:*

$$\begin{array}{cccc} 0 \mapsto 0 & 0 \mapsto 0 & 0 \mapsto 1 & 0 \mapsto 1 \\ 1 \mapsto 0 & 1 \mapsto 1 & 1 \mapsto 0 & 1 \mapsto 1. \end{array}$$

   *Los átomos son las aplicaciones segunda y tercera.*

2. *El álgebra* $\mathcal{F}_2$ *tiene* 4 *átomos, y por tanto* 16 *elementos. Los átomos son:*

$$\begin{array}{cccc} (0,0) \mapsto 1 & (0,0) \mapsto 0 & (0,0) \mapsto 0 & (0,0) \mapsto 0 \\ (1,0) \mapsto 0 & (1,0) \mapsto 1 & (1,0) \mapsto 0 & (1,0) \mapsto 0 \\ (0,1) \mapsto 0 & (0,1) \mapsto 0 & (0,1) \mapsto 1 & (0,1) \mapsto 0 \\ (1,1) \mapsto 0 & (1,1) \mapsto 0 & (1,1) \mapsto 0 & (1,1) \mapsto 1. \end{array}$$

### 2.3.3. Expresiones booleanas

**Definición 21.** *Sea $S$ un conjunto. Se definen las expresiones booleanas sobre el conjunto $S$ de forma recursiva como sigue:*

1. *Si $x \in S \cup \{0,1\}$ entonces $x$ es una expresión booleana.*
2. *Si $e_1, e_2$ son expresiones booleanas, entonces también lo son $e_1 \vee e_2$, $e_1 \wedge e_2$ y $\overline{e_1}$.*

*A las expresiones booleanas que sean elementos de $S$, o complementos suyos, los denominaremos* literales.

**Ejemplo 2.3.7.** *Si $S = \{x, y, z\}$ son expresiones booleanas $x$, $x \vee z$, $\overline{x \wedge \overline{y}}$, $1$.*
*Son literales, $x$, $\overline{z}$, $z$.*

A la hora de representar las expresiones booleanas, emplearemos la notación $x\,y$ o $x{\cdot}y$ para la expresión $x \wedge y$, mientras que usaremos la notación $x + y$ para la expresión $x \vee y$.
Así, la expresión booleana $x \vee (y \wedge \overline{z})$ la representaremos como $x + (y\,\overline{z})$.

Supongamos que tenemos un conjunto $S$ con $n$ elementos, es decir, $S = \{x_1, x_2, \ldots, x_n\}$. A cada elemento de $S$ le vamos a asignar un elemento de $\mathcal{F}_n$. Concretamente, al elemento $x_i$ le asignamos la función $x_i : \mathbb{B}^n \to \mathbb{B}$ dada por $x_i(a_1, \ldots, a_i, \ldots, a_n) = a_i$. De esta forma, a cada expresión booleana sobre el conjunto $S$ le podemos hacer corresponder una función $\mathbb{B}^n \to \mathbb{B}$.
Por ejemplo, si $S = \{x, y, z\}$ y consideramos la expresión booleana $x \vee (\overline{y} \wedge z)$, le corresponde la función booleana

$$\begin{array}{ll} (0,0,0) \mapsto 0 \vee (1 \wedge 0) = 0, & (0,0,1) \mapsto 0 \vee (1 \wedge 1) = 1, \\ (0,1,0) \mapsto 0 \vee (0 \wedge 0) = 0, & (0,1,1) \mapsto 0 \vee (0 \wedge 1) = 0, \\ (1,0,0) \mapsto 1 \vee (1 \wedge 0) = 1, & (1,0,1) \mapsto 1 \vee (1 \wedge 1) = 1, \\ (1,1,0) \mapsto 1 \vee (0 \wedge 0) = 1, & (1,1,1) \mapsto 1 \vee (0 \wedge 1) = 1. \end{array}$$

Puesto que cada expresión booleana determina una función booleana, podremos referirnos a las funciones mencionando las expresiones que las representan. Así, la función que acabamos de ver podría definirse como $f(x, y, z) = x \vee (\overline{y} \wedge z)$. Ahora, para calcular la imagen de un elemento de $\mathbb{B}^3$ basta sustituir en la expresión booleana $x$, $y$ y $z$ por los valores en los que queremos evaluar, y efectuar las operaciones en el álgebra de Boole $\mathbb{B}$. Por ejemplo

$$f(0,0,1) = 0 \vee (\overline{0} \wedge 1) = 0 \vee (1 \wedge 1) = 0 \vee 1 = 1.$$

Nótese que en el Ejemplo 2.3.5 ya se ha empleado esta forma de definir una función booleana.
Si ahora quisiéramos emplear la notación introducida anteriormente, la función $f$ adoptaría la forma $f(x, y, z) = x + (\overline{y}\,z)$.
A la hora de emplear esta notación hemos de tener cuidado en no confundir con las operaciones suma y producto hecho en $\mathbb{Z}_2$. En relación al producto no hay problema, pues vimos como la operación $\wedge$ se corresponde con el producto en $\mathbb{Z}_2$. Sin embargo, en $\mathbb{Z}_2$ se tiene que $x \vee y = x + y + x\,y$, lo cual hace que la operación $+$ difiera de la operación $\vee$, pues $1 + 1 = 0$ mientras que $1 \vee 1 = 1$. Para el resto de parejas, ambas operaciones coinciden ($0 + 0 = 0 \vee 0$; $0 + 1 = 0 \vee 1$; $1 + 0 = 1 \vee 0$). El contexto nos aclarará en cada caso si al emplear el símbolo $+$ nos estamos refiriendo a la suma (en $\mathbb{Z}_2$) o al supremo (en $\mathbb{B}$).
Por ejemplo, si decimos *sea $f$ la función booleana dada por $f(x, y, z) = x\,y + y\,\overline{z}$* está claro que nos referimos al supremo. En tal caso, se tiene que

$$f(0,1,1) = 0 \cdot 1 + 1 \cdot 0 = 0 + 0 = 0 \qquad f(1,1,0) = 1 \cdot 1 + 1 \cdot 1 = 1 + 1 = 1$$

**Definición 22.** *Dos expresiones booleanas son equivalentes si las correspondientes funciones booleanas son iguales. Si $e_1$ e $e_2$ son expresiones booleanas equivalentes emplearemos el símbolo $e_1 = e_2$.*

**Ejemplo 2.3.8.** *Las expresiones booleanas* $\overline{x}\,\overline{y}$ *y* $\overline{x+y}$ *son equivalentes. También lo son las expresiones* $x+y+\overline{x}\,\overline{y}$ *y* $1$*.*

A continuación vamos a dar una tabla de expresiones equivalentes.

**Proposición 2.3.2.** *Sean* $e_1$*,* $e_2$ *y* $e_3$ *tres expresiones booleanas en* $n$ *variables. Entonces:*

| | | |
|---|---|---|
| 1. | $e_1+(e_2+e_3)=(e_1+e_2)+e_3$ | $e_1\cdot(e_2\cdot e_3)=(e_1\cdot e_2)\cdot e_3$ |
| 2. | $e_1+e_2=e_2+e_1$ | $e_1\cdot e_2=e_2\cdot e_1$ |
| 3. | $e_1+e_1=e_1$ | $e_1\cdot e_1=e_1$ |
| 4. | $e_1\cdot(e_2+e_3)=e_1\cdot e_2+e_1\cdot e_3$ | $e_1+(e_2\cdot e_3)=(e_1+e_2)\cdot(e_1+e_3)$ |
| 5. | $\overline{e_1+e_2}=\overline{e_1}\cdot\overline{e_2}$ | $\overline{e_1\cdot e_2}=\overline{e_1}+\overline{e_2}$ |
| 6. | $e_1+\overline{e_1}=1$ | $e_1\cdot\overline{e_1}=0$ |
| 7. | $e_1+1=1$ | $e_1\cdot 0=0$ |
| 8. | $e_1+0=e_1$ | $e_1\cdot 1=e_1$ |
| 9. | $\overline{1}=0$ | $\overline{0}=1$ |

**Definición 23.** *Sea* $S=\{x_1,x_2,\ldots,x_n\}$*. Un* minterm *en* $n$ *variables es el producto de* $n$ *literales, cada uno con una variable diferente.*

**Ejemplo 2.3.9.** *Si* $S=\{x,y,z\}$*, entonces son minterm* $x\,y\,z$*,* $x\,\overline{y}\,\overline{z}$*,* $\overline{x}\,y\,z$*. No son minterm* $x\,y$*,* $x\,y\,\overline{y}$ *ni* $x\,z\,x$*.*

**Lema 2.3.2.** *Sea* $m$ *un minterm en* $n$ *variables. Entonces* $m$ *determina una función booleana* $f:\mathbb{B}^n\to\mathbb{B}$ *que vale* $1$ *en un elemento de* $\mathbb{B}^n$ *y* $0$ *en el resto.*

**Ejemplo 2.3.10.** *Sea* $f:\mathbb{B}^2\to\mathbb{B}$ *la función booleana dada por* $f(x,y)=x\,\overline{y}$*. Claramente* $x\,\overline{y}$ *es un minterm. Se tiene que* $f(1,0)=1$*, mientras que* $f(0,0)=f(0,1)=f(1,1)=0$*.*

**Corolario 2.3.1.** *Los minterm son los átomos del álgebra* $\mathcal{F}_n$*.*

**Corolario 2.3.2.** *Toda función booleana se expresa de forma única (salvo el orden) como suma (supremo) de minterm.*

La expresión de una función booleana como suma de minterm recibe el nombre de *forma normal disyuntiva*. Para hallar la forma normal disyuntiva de una función booleana podemos emplear dos métodos.

El primero consiste en evaluar la función en todos los elementos de $\mathbb{B}^n$, y observar en cuales de ellos toma el valor 1. Cada uno de esos elementos se corresponde con un minterm.

El segundo consiste en, a partir de una expresión booleana que nos defina a $f$, utilizar las equivalencias dadas en la proposición 2.3.2 para transformar la expresión en una suma de minterm.

**Ejemplo 2.3.11.** *Vamos a expresar como supremo de minterm la función booleana dada por* $f(x,y)=x+y$*.*

1. *Si queremos emplear el primer método, evaluamos la función en los cuatro elementos de* $\mathbb{B}^2$*. Nos queda:*

$$f(0,0)=0+0=0\qquad f(0,1)=0+1=1\qquad f(1,0)=1+0=1\qquad f(1,1)=1+1=1$$

*El elemento* $(0,1)$ *se corresponde con el minterm* $\overline{x}\,y$*, el* $(1,0)$ *con* $x\,\overline{y}$ *mientras que* $(1,1)$ *se corresponde con* $x\,y$*. Por tanto tenemos que* $f(x,y)=\overline{x}\,y+x\,\overline{y}+x\,y$*.*

*2. Empleamos ahora el segundo método. En este caso*

$$\begin{aligned} f(x,y) &= x+y \\ &= x\cdot 1 + 1\cdot y && \textit{(equivalencias 8 y 2)} \\ &= x(y+\overline{y}) + (x+\overline{x})y && \textit{(equivalencia 6)} \\ &= x\,y + x\,\overline{y} + x\,y + \overline{x}\,y && \textit{(equivalencias 4 y 2)} \\ &= x\,y + x\,y + x\,\overline{y} + \overline{x}\,y && \textit{(equivalencia 2)} \\ &= x\,y + x\,\overline{y} + \overline{x}\,y && \textit{(equivalencia 3).} \end{aligned}$$

Cada elemento de $\mathbb{B}^n$ es una secuencia de $n$ dígitos *ceros* o *unos*. Es por tanto, la expresión en binario de un número entre 0 y $2^n-1$. Por otra parte, a cada elemento de $\mathbb{B}^n$ le corresponde un minterm (aquél para el que toma el valor 1). Por tanto, cada minterm está determinado por un número comprendido entre 0 y $2^n-1$. Denotaremos por *el minterm* $a$, donde $0 \le a \le 2^{n-1}$, y lo representaremos como $m(a)$ o $m_a$, al minterm determinado por el número $a$ siguiendo el criterio anterior.

Por ejemplo, el minterm $x\,y\,\overline{z}\,\overline{t}$ toma el valor 1 en $(1,1,0,0)$. Puesto que $12 = (1100)_2$ tenemos que $x\,y\,\overline{z}\,\overline{t}$ es el minterm 12, o dicho de otra forma, $x\,y\,\overline{z}\,\overline{t} = m_{12} = m(12)$.

**Ejemplo 2.3.12.** *La función booleana del ejemplo anterior $f(x,y) = x+y$ hemos visto que se expresa como suma de minterm de la forma $f(x,y) = x\,y + x\,\overline{y} + \overline{x}\,y$. Empleando la notación recién introducida nos quedaría $f(x,y) = m_3 + m_2 + m_1$, o si preferimos $f(x,y) = m_1 + m_2 + m_3$.*

*También se suele emplear la notación $f(x,y) = \sum m(1,2,3)$.*

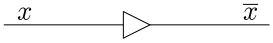
De la misma forma que toda función booleana se expresa de forma única como suma de minterm, se puede probar que toda función booleana se expresa de forma única como producto de maxterm. Una expresión de esta forma se denomina *forma canónica conjuntiva.*

Un maxtern es una suma de $n$ literales. Se corresponde con una función booleana que vale 1 en todos los elementos de $\mathbb{B}^n$ salvo en uno, en el que vale 0. Este elemento determina al maxterm.

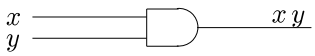
### 2.3.4. Puertas lógicas

En este apartado utilizaremos las funciones booleanas para el diseño de circuitos lógicos. Los elementos básicos de estos circuitos se llaman *puertas lógicas.* Aquí emplearemos tres tipos de puertas lógicas, cada una correspondiente a una operación booleana, y las combinaremos para diseñar circuitos que realicen una serie de tareas. Las puertas básicas a emplear son:

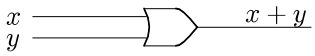
La puerta **NOT** que tiene como entrada el valor de una variable booleana y produce como salida el complementario de dicho valor. Para una puerta NOT emplearemos el siguiente símbolo.



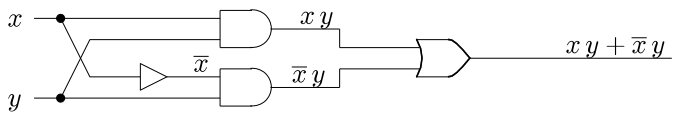

La puerta **AND** que tiene como entrada el valor de dos o más variables booleanas, y como salida el producto de éstas. Las entradas se muestran a la izquierda y la salida a la derecha. Emplearemos el siguiente símbolo para esta puerta.




La puerta **OR** tiene como entrada el valor de dos o más variables booleanas, y como salida la suma de éstas. La representaremos mediante el siguiente símbolo.



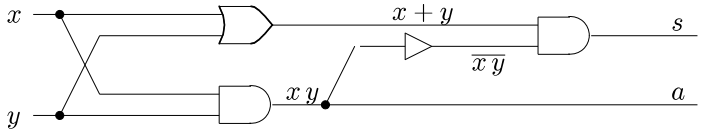

**Ejemplo 2.3.13.** *Vamos a diseñar un circuito con dos entradas y que produzca la salida $x\,y + \overline{x}\,y$.*




*Nótese que puesto que $x\,y + \overline{x}\,y = (x+\overline{x})y = 1\cdot y = y$ podría haberse diseñado un circuito mucho más simple que tuviera el mismo efecto.*

A continuación vamos a diseñar un circuito que, introducidos dos números en binario nos devuelve su suma.

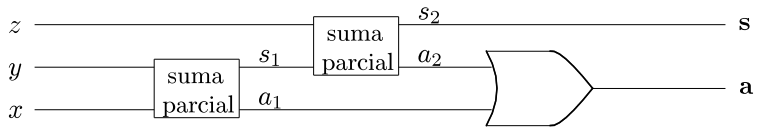
Para esto, comenzamos en primer lugar diseñando un circuito que, dados dos dígitos binarios nos devuelva la suma. Puesto que los posibles resultados de la suma son 0, 1 y 10 necesitamos un circuito que tenga dos salidas. Denotaremos el bit de la derecha como $s$ (suma) y el de la izquierda como $a$ (acarreo). Se tiene entonces que $s = \overline{x}\,y + x\,\overline{y} = (x+y)\overline{x\,y}$ mientras que $a = x\,y$. Un circuito podría ser entonces:




Denominaremos a este circuito como *suma parcial*.

Construyamos ahora un circuito que nos sume dos dígitos binarios más el posible acarreo de una suma anterior. Podemos ver fácilmente que esto es equivalente a sumar tres dígitos binarios $x$, $y$ y $z$. El resultado será, como antes una salida doble. A las dos salidas las denotaremos de la misma forma que en el caso anterior: $s$ y $a$.

Para obtener la salida $s$, obtenemos la suma de $x$ e $y$, y al resultado le sumamos $z$. Puede verse entonces que un circuito que nos da la suma de tres dígitos sería:

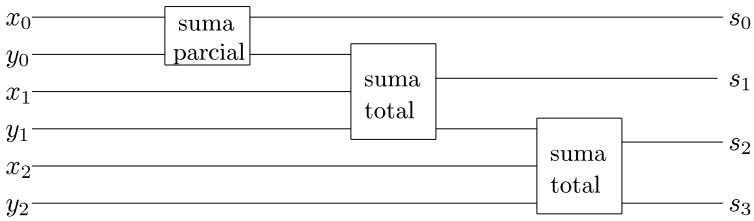



| $x$ | $y$ | $z$ | $s_1$ | $a_1$ | $s_2$ | $a_2$ | **s** | **a** | $a_1 + a_2$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |

pues como podemos apreciar, $\mathbf{s} = s_2$ y $\mathbf{a} = a_1 + a_2$.

Denotaremos a este circuito como *suma total*.

Veamos ahora como calcular la suma de dos números entre 0 y 7. Supongamos que estos números se escriben en binario como $x_2x_1x_0$ e $y_2y_1y_0$. Su suma, escrita en binario es $s_3s_2s_1s_0$.

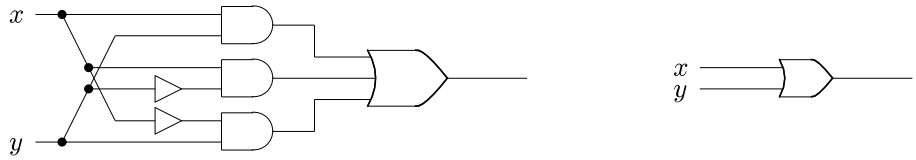



## 2.3.5. Optimización de funciones booleanas

Hemos visto en la subsección anterior como a partir de la representación de una función booleana en $n$ variables haciendo uso de una expresión booleana podemos diseñar un circuito que nos devuelva el resultado de aplicar la función a las $n$ variables.

Puesto que cualquier función booleana puede expresarse como suma de minterm, podemos diseñar cualquier circuito empleando las tres puertas NOT, OR y AND. Sin embargo, la expresión de una función como suma de minterm no es en general la más apropiada pues requiere de muchas operaciones, lo que se traduce en la necesidad de emplear gran cantidad de puertas.

Así, por ejemplo, los siguientes circuitos producen el mismo efecto sobre las entrada $x, y$.




pues el primer circuito responde a la función $x\,y + x\,\overline{y} + \overline{x}\,y$, mientras que el segundo a $x + y$, que vimos anteriormente que son iguales.

Lo que pretendemos es, a partir de una expresión de suma de minterm, transformarla en otra expresión equivalente con menos sumandos y menor productos en los sumandos. Vamos a estudiar dos métodos para este propósito. Por una parte, los mapas de Karnaugh, y por otra parte el método de Quine-McCluskey.

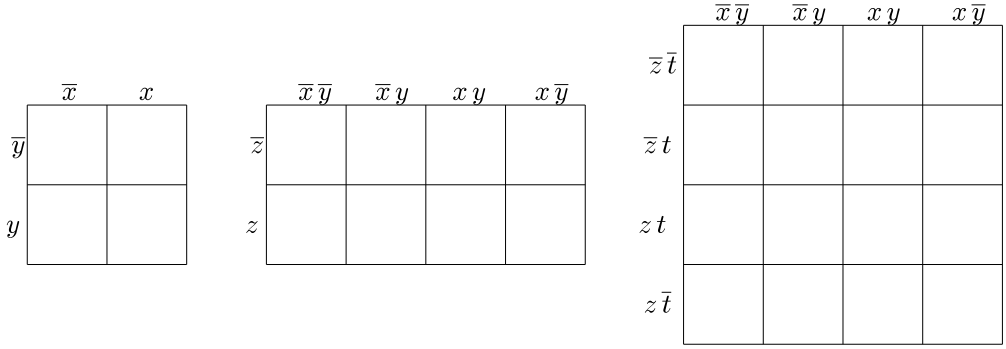
Referente al primero, decir que es un método eficiente para funciones de no más de cuatro variables, mientras que puede utilizarse hasta funciones de seis variables.

En cuanto al segundo, aunque realiza la optimización de forma automática, y podría implementarse como un programa informático, el algoritmo, para un número grande de variables booleanas, es computacionalmente muy costoso.

### Mapas de Karnaugh

En primer lugar veremos qué es un mapa de Karnaugh, y posteriormente veremos cómo utilizarlos para optimizar las expresiones booleanas.

Un mapa de Karnaugh para una función booleana de dos, tres o cuatro variables es una tabla con tantas celdas como posibles minterm (4 para dos variables, 8 para tres variables y 16 para cuatro variables). Cada celda va asociada a un minterm, y dos celdas adyacentes se diferencian únicamente en un literal, así como dos celdas opuestas en una fila o una columna.




Por ejemplo, en el mapa correspondiente a 4 variables, las cuatro celdas adyacentes a $\overline{x}\,y\,\overline{z}\,t$ son: por la derecha, $x\,y\,\overline{z}\,t$, por arriba, $\overline{x}\,y\,\overline{z}\,\overline{t}$, por la izquierda, $\overline{x}\,\overline{y}\,\overline{z}\,t$ y por abajo, $\overline{x}\,y\,z\,t$. Vemos como cada una de estas celdas se diferencia de $\overline{x}\,y\,\overline{z}\,t$ en sólo un literal ($\overline{x} - x$ en la primera, $t - \overline{t}$ en la segunda, $y - \overline{y}$ en la tercera y $\overline{z} - z$ en la cuarta).

Vemos también como las celdas opuestas de la misma fila se diferencian también en sólo un literal (en la segunda fila, estas celdas opuestas son $\overline{x}\,\overline{y}\,\overline{z}\,t$ y $x\,\overline{y}\,\overline{z}\,t$), así como las celdas opuestas de una columna.

Si ahora tenemos una función booleana en dos, tres o cuatro variables, su mapa de Karnaugh consiste en la tabla antes descrita, en la que se han destacado aquellas celdas correspondientes a los minterm que aparecen en la forma normal disyuntiva de la función. Nosotros aquí las marcaremos con un 1.

**Ejemplo 2.3.14.** *Vamos a dibujar los mapas de Karnaugh de las funciones booleanas:* $f(x,y) = x\,\overline{y} + \overline{x}\,\overline{y}$; $f(x,y,z) = (\overline{x} + \overline{y})(y\,\overline{z}) + \overline{y}\,\overline{z}$; $f(x,y,z,t) = x\,y\,\overline{z}\,\overline{t} + x\,\overline{y}\,z\,t + x\,y\,z\,\overline{t} + x\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t} + x\,\overline{y}\,z\,\overline{t} + x\,y\,\overline{z}\,t$.

| | $\overline{x}$ | $x$ |
|---|---|---|
| $\overline{y}$ | *1* | *1* |
| $y$ | | |

$x\,\overline{y} + \overline{x}\,\overline{y}$

| | $\overline{x}\,\overline{y}$ | $\overline{x}\,y$ | $x\,y$ | $x\,\overline{y}$ |
|---|---|---|---|---|
| $\overline{z}$ | 1 | | 1 | 1 |
| $z$ | 1 | 1 | 1 | 1 |

$(\overline{\overline{x} + \overline{y}})(y\,\overline{z}) + \overline{y}\,\overline{z}$

| | $\overline{x}\,\overline{y}$ | $\overline{x}\,y$ | $x\,y$ | $x\,\overline{y}$ |
|---|---|---|---|---|
| $\overline{z}\,\overline{t}$ | | | 1 | |
| $\overline{z}\,t$ | | | 1 | |
| $z\,t$ | | | 1 | 1 |
| $z\,\overline{t}$ | 1 | | 1 | 1 |

$x\,y\,\overline{z}\,\overline{t} + x\,\overline{y}\,z\,t + x\,y\,z\,\overline{t} + x\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t} + x\,\overline{y}\,z\,\overline{t} + x\,y\,\overline{z}\,t$

Una vez dibujado el mapa de Karnaugh de una función booleana, se buscan los 1 que aparezcan en celdas adyacentes (u opuestas en una misma fila o columna). Dos de estas celdas se transforman en un único producto en el que ha desaparecido el literal en que difieren. Así, en el ejemplo del mapa de Karnaugh para la función de dos variables, tenemos dos "unos" adyacentes, situados en las celdas $x\,\overline{y}$ y $\overline{x}\,\overline{y}$. Estas dos celdas dan lugar a un producto en el que desaparece el literal diferente ($x$, $\overline{x}$), quedando entonces la expresión booleana $\overline{y}$. Obviamente, lo único que estamos haciendo es la transformación $x\,\overline{y} + \overline{x}\,\overline{y} = (x + \overline{x})\overline{y} = 1 \cdot \overline{y} = \overline{y}$, donde se ha empleado la propiedad distributiva, la definición de complementario y de 1. Los mapas de Karnaugh constituyen una representación gráfica de una función booleana que ayuda a encontrar los minterm que podemos agrupar.

De la misma forma, si encontramos cuatro "unos" adyacentes, formando, bien un cuadrado, bien una línea (fila o columna), podemos sustituirlos por un solo producto en el que se eliminan los dos litereles que difieren en esas cuatro celdas.

El objetivo es tratar de agrupar los "unos" en el menor número posible de bloques, y de mayor tamaño.

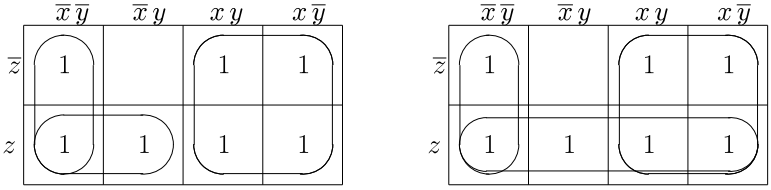
Vamos a optimizar las dos funciones que hemos representado mediante mapas de Karnaugh en el ejemplo anterior. En primer lugar consideramos la función $f : \mathbb{B}^3 \to \mathbb{B}$ dada por $f(x, y, z) = (\overline{\overline{x} + \overline{y}})(y\,\overline{z}) + \overline{y}\,\overline{z}$.

Su mapa de Karnaugh es:

| | $\overline{x}\,\overline{y}$ | $\overline{x}\,y$ | $x\,y$ | $x\,\overline{y}$ |
|---|---|---|---|---|
| $\overline{z}$ | 1 | | 1 | 1 |
| $z$ | 1 | 1 | 1 | 1 |

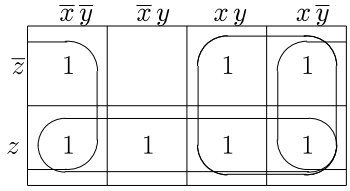
y vemos que podemos agrupar en 3 bloques, lo que da lugar a tres sumandos, que son $\overline{x}\,\overline{y}$, $\overline{x}\,y\,z$ y $x$. Es decir, $f(x, y, z) = \overline{x}\,\overline{y} + \overline{x}\,y\,z + x$.

Vemos también que podemos hacer otras agrupaciones en 3 bloques. Por ejemplo,




que dan lugar a las expresiones $f(x,y,z) = \overline{x}\,\overline{y} + \overline{x}\,z + x$ o a $f(x,y,z) = \overline{x}\,\overline{y} + z + x$.

Sin embargo, no olvidemos que también se consideran adyacentes las celdas opuestas de una misma fila. Podemos entonces agrupar en los siguientes bloques:



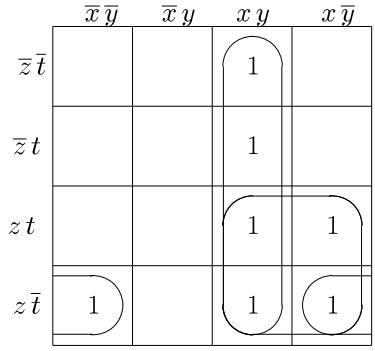

lo que da lugar a la expresión $f(x,y,z) = x + \overline{y} + z$.

Podemos apreciar como en todas las optimizaciones obtenidas hemos obtenido tres sumandos. Sin embargo, esta última parece mejor, pues es la que tiene menos productos en cada sumando. Esto viene de haber obtenido los bloques más grandes.

Por último, vamos a optimizar la función $f : \mathbb{B}^4 \to \mathbb{B}$ dada por

$$f(x,y,z,t) = x\,y\,\overline{z}\,\overline{t} + x\,\overline{y}\,z\,t + x\,y\,z\,\overline{t} + x\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t} + x\,\overline{y}\,z\,\overline{t} + x\,y\,\overline{z}\,t$$

Para esto, agrupamos los "unos" del mapa de Karnaugh por bloques:




lo que da lugar a la expresión $f(x,y,z,t) = x\,y + x\,z + \overline{y}\,z\,\overline{t}$.

**Método de Quine - McCluskey**

Acabamos de ver cómo los mapas de Karnaugh nos ayudan a minimizar el desarrollo de una función booleana como suma de productos. Sin embargo, este método se basa en la visualización de la función en un diagrama, y es poco eficiente para funciones de más de cuatro variables. Sería conveniente tener un proceso que pudiera automatizarse. El método de Quine-McCluskey se ajusta a esta condición. El método consta de dos partes. En una primera, se determinan que términos son candidatos a que aparezcan en un desarrollo minimal. En la segunda se seleccionan de estos candidatos los que intervienen en dicho desarrollo.

Describamos a continuación el método.

Sabemos que cada minterm en $n$ variables va unido a una secuencia de $n$ bits. En primer lugar, dada una función booleana como suma de minterm, ordenamos las cadenas de bits en una columna, agrupando aquellos en los que aparecen igual cantidad de "unos".

Comparamos las cadenas de un grupo con las del grupo inmediatamente inferior. Si encontramos dos cadenas que difieren únicamente en un bit, las marcamos y, en una columna situada a la derecha, representamos estas dos cadenas por una nueva en la que sustituimos el bit diferente por $-$. Si aparecieran dos cadenas iguales, se deja únicamente una.

Una vez realizadas todas las comparaciones posibles, en esta nueva columna repetimos el proceso.

Se continúa así hasta que no podamos obtener una nueva columna.

Se seleccionan aquellas cadenas que no hayan sido marcadas.

Veamos esto con un ejemplo.

**Ejemplo 2.3.15.** *Sea la expresión booleana* $x\,y\,z + \overline{x}\,y\,z + \overline{x}\,\overline{y}\,z + \overline{x}\,\overline{y}\,\overline{z} + x\,\overline{y}\,z$

*Cada minterm lo representamos mediante una cadena de tres dígitos binarios. Estos son* 111, 011, 001, 000 *y* 101. *Ordenamos las cadenas en una columna, situando en primer lugar la que tiene* 3 *"unos", a continuación las que tienen* 2 *"unos" y así sucesivamente.*

| |
|---|
| 111 |
| 011 |
| 101 |
| 001 |
| 000 |

*Comparamos la cadena del primer nivel con las de segundo. Resulta que hay* 2 *de las que se diferencia en un único dígito. Sustituimos este dígito por* $-$, *luego nos queda* $-11$ *y* $1-1$.

*Comparamos las cadenas del segundo y tercer nivel, y vemos que* 101 *y* 001 *se diferencian en un único dígito. Esto da lugar a la cadena* $-01$. *Por último, comparamos la del tercer nivel con el cuarto, lo que nos da* $00-$.

*Ordenamos todos estos datos en una nueva columna y todas las cadenas de esta columna que han intervenido en alguna de la segunda las marcamos.*

| | |
|---|---|
| $\sim 111$ | $-11$ |
| $\sim 011$ | $1-1$ |
| $\sim 101$ | $0-1$ |
| $\sim 001$ | $-01$ |
| $\sim 000$ | $00-$ |

*Repetimos aquí el proceso con la segunda columna*

| | | |
|---|---|---|
| $\sim 111$ | $\sim -11$ | $--1$ |
| $\sim 011$ | $\sim 1-1$ | |
| $\sim 101$ | $\sim 0-1$ | |
| $\sim 001$ | $\sim -01$ | |
| $\sim 000$ | $00-$ | |

*Las cadenas a seleccionar son entonces las no marcadas, es decir,* $--1$ *y* $00-$, *que se corresponden con los términos* $z$ *y* $\overline{x}\,\overline{y}$.

La segunda parte de este método consiste en encontrar, de todos los productos booleanos, el menor conjunto de ellos que represente a la expresión booleana dada. Para ello, hacemos una tabla en la que, en el eje horizontal situamos los minterm que nos definían la expresión booleana, mientras que en el eje vertical situamos los productos booleanos que hemos seleccionado en la primera parte. A continuación señalamos las celdas que se correspondan con un producto booleano y un minterm con la condición de que todos los literales que intervienen en el producto booleano también se encuentren en el minterm.

Una vez hecho esto, elegimos la menor cantidad de productos booleanos de forma que uniendo las celdas que están señaladas en sus filas podamos completar una fila completa de la tabla. De haber varias posibles elecciones, nos quedamos con aquellas en que los productos booleanos tengan la menor cantidad posible de literales.

**Ejemplo 2.3.16.** *En el ejemplo anterior, la tabla nos quedaría como sigue:*

| | $x\,y\,z$ | $x\,\overline{y}\,z$ | $\overline{x}\,y\,z$ | $\overline{x}\,\overline{y}\,z$ | $\overline{x}\,\overline{y}\,\overline{z}$ |
|---|---|---|---|---|---|
| $z$ | $X$ | $X$ | $X$ | $X$ | |
| $\overline{x}\,\overline{y}$ | | | | $X$ | $X$ |

*Vemos como aquí necesitamos los dos productos booleanos para rellenar una fila.*

*Después de todo esto deducimos que:*

$$x\,y\,z + \overline{x}\,y\,z + \overline{x}\,\overline{y}\,z + \overline{x}\,\overline{y}\,\overline{z} + x\,\overline{y}\,z = \overline{x}\,\overline{y} + z$$

Veamos a continuación un ejemplo completo.

**Ejemplo 2.3.17.** *Dada la expresión booleana* $x\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,y\,\overline{z}\,t + x\,\overline{y}\,z\,\overline{t} + \overline{x}\,\overline{y}\;z\,t + \overline{x}\,\overline{y}\,\overline{z}\,t + \overline{x}\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t}$ *vamos a tratar de encontrar una expresión óptima mediante el método de Quine-McCluskey.*

*Las cadenas de bits correspondientes a cada uno de los minterm son* 0111, 0101, 1010, 0011, 0001, 0111 *y* 0010. *A partir de ellas construimos la tabla:*

| | | | | |
|---|---|---|---|---|
| $a\ b$ | $\sim$ *0111* | $1$ | $\sim$ *01-1* | *0- -1* |
| $a\ c$ | $\sim$ *0101* | $2$ | $\sim$ *0-11* | |
| $d\ e$ | $\sim$ *1010* | $2$ | $\sim$ *0-01* | |
| $b\ f\ g$ | $\sim$ *0011* | | *10-0* | |
| $d$ | $\sim$ *1000* | | *-010* | |
| $c\ f$ | $\sim$ *0001* | $1$ | $\sim$ *00-1* | |
| $e\ g$ | $\sim$ *0010* | | *001-* | |

*A la izquierda de cada una de las cadenas marcadas hemos colocado unas letras (columna de la izquierda) o números (columna central) que nos indican cada cadena con cual se empareja para formar una cadena en la columna que tiene más a la derecha.*

*A partir de aquí seleccionamos las cadenas que no están marcadas, que se corresponden con los productos* $x\,\overline{y}\,\overline{t}$; $\overline{y}\,z\,\overline{t}$; $\overline{x}\,\overline{y}\,z$; $\overline{x}\,t$. *Esto nos da la siguiente tabla:*

| | $x\,\overline{y}\,\overline{z}\,\overline{t}$ | $\overline{x}\,y\,\overline{z}\,t$ | $x\,\overline{y}\,z\,\overline{t}$ | $\overline{x}\,\overline{y}\;z\,t$ | $\overline{x}\,\overline{y}\,\overline{z}\,t$ | $\overline{x}\,y\,z\,t$ | $\overline{x}\,\overline{y}\,z\,\overline{t}$ |
|---|---|---|---|---|---|---|---|
| $x\,\overline{y}\,\overline{t}$ | $X$ | | $X$ | | | | |
| $\overline{y}\,z\,\overline{t}$ | | | $X$ | | | | $X$ |
| $\overline{x}\,\overline{y}\,z$ | | | | $X$ | | | $X$ |
| $\overline{x}\,t$ | | $X$ | | $X$ | $X$ | $X$ | |

*Y a partir de la tabla se ve cómo los términos* $x\,\overline{y}\,\overline{t}$ *y* $\overline{x}\,t$ *tienen que aparecer en la expresión simplificada. Si el primero no lo pusiéramos, no quedaría cubierto el minterm* $x\,\overline{y}\,\overline{z}\,\overline{t}$, *mientras que si no lo hiciéramos con el segundo, sería el minterm* $\overline{x}\,y\,\overline{z}\,t$ *(y otros dos más) quien no quedaría cubierto. Aquellos términos que son los únicos que cubren a alguno de los minterms, se les llama* implicantes primos.

*En este caso, los implicantes primos son* $x\,\overline{y}\,\overline{t}$ *y* $\overline{x}\,t$.

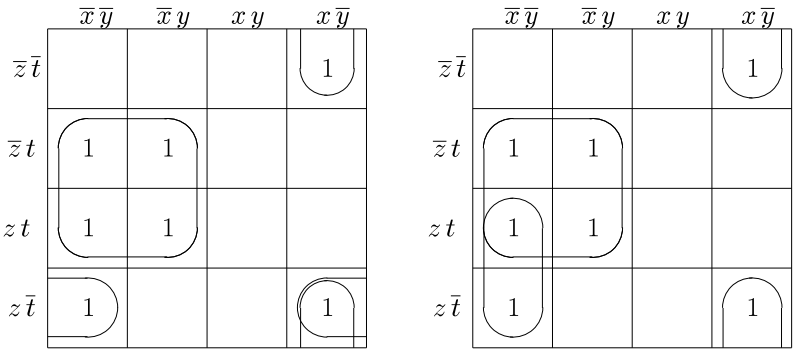
*Lo que hacemos ahora es, de la tabla anterior, eliminamos las filas donde están los implicantes primos, y las columnas donde están los minitérminos que quedan cubiertos por esos implicantes primos. Es decir, suprimimos las filas primera (correspondiente al término* $x\,\overline{y}\,\overline{t}$*) y cuarta (correspondiente al término* $\overline{x}\,t$*). También suprimimos las columnas primera, segunda, tercera, cuarta, quinta y sexta. Nos queda entonces:*

| | $\overline{x}\,\overline{y}\,z\,\overline{t}$ |
|---|---|
| $\overline{y}\,z\,\overline{t}$ | $X$ |
| $\overline{x}\,\overline{y}\,z$ | $X$ |

*y vemos que eligiendo cualquiera de los dos, podemos tener cubiertos todos los minterms. Por tanto,*

$$x\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,y\,\overline{z}\,t + x\,\overline{y}\,z\,\overline{t} + \overline{x}\,\overline{y}\;z\,t + \overline{x}\,\overline{y}\,\overline{z}\,t + \overline{x}\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t} = x\,\overline{y}\,\overline{t} + \overline{x}\,t + \overline{y}\,z\,\overline{t} = x\,\overline{y}\,\overline{t} + \overline{x}\,t + \overline{x}\,\overline{y}\,z$$

*Si para optimizar esta expresión booleana empleáramos los mapas de Karnaugh tendríamos dos formas diferentes de agrupar las celdas con "unos":*




*lo que nos da las dos expresiones que acabamos de ver.*

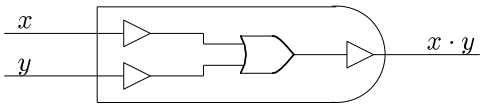
### 2.3.6. Conjuntos funcionalmente completos

En secciones precedentes hemos visto cómo a partir de tres puertas lógicas, las puertas AND, OR y NOT, podemos diseñar circuitos lógicos, y en la sección anterior hemos estudiado cómo minimizar el número de puertas necesarias para diseñar tales circuitos. Sin embargo, para construir tales circuitos es necesario emplear tres tipos de puertas lógicas diferentes. En esta sección vamos a intentar construir cualquier circuito lógico empleando menos puertas diferentes, aunque sea a costa de aumentar el número de éstas.

Comenzamos reduciendo el número de puertas distintas necesarias a 2.

**Proposición 2.3.3.** *Las puertas lógicas OR y NOT, o las puertas lógicas AND y NOT son suficientes para la construcción de cualquier circuito lógico.*

*Demostración:* Para ver que las puertas OR y NOT son suficientes, basta comprobar que $xy = \overline{\overline{x} + \overline{y}}$, lo que nos dice que podemos construir una puerta AND usando las puertas OR y NOT. Esta puerta podría quedar como sigue:




Y por tanto, usando únicamente puertas OR y NOT podemos construir cualquier circuito.

De la misma forma, y puesto que $x + y = \overline{\overline{x}\,\overline{y}}$ se puede ver que usando únicamente las puetas AND y NOT se puede diseñar cualquier circuito.

■

**Definición 24.** *Sean $x, y$ variables booleanas. Se definen las funciones booleanas $- \uparrow -$ y $- \downarrow -$ como sigue:*

$$x \uparrow y = \overline{x \cdot y}, \qquad x \downarrow y = \overline{x + y}.$$

Es decir:

$$0 \uparrow 0 = 1, \quad 0 \uparrow 1 = 1, \quad 1 \uparrow 0 = 1, \quad 1 \uparrow 1 = 0.$$
$$0 \downarrow 0 = 1, \quad 0 \downarrow 1 = 0, \quad 1 \downarrow 0 = 0, \quad 1 \downarrow 1 = 0.$$

Estos operadores se denotan como NAND (NOT AND) y NOR (NOT OR) respectivamente.

**Proposición 2.3.4.** *Cualquier función booleana se puede expresar usando únicamente el operador NAND (resp. NOR).*

*Demostración:*

Para comprobar esto, escribimos en primer lugar:

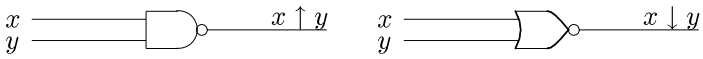
$\overline{x} = \overline{x \cdot x} = x \uparrow x$,

$x + y = \overline{\overline{x} \cdot \overline{y}} = \overline{x} \uparrow \overline{y} = (x \uparrow x) \uparrow (y \uparrow y)$,

es decir, los operadores NOT y OR pueden expresarse utilizando únicamente NAND. La Proposición 2.3.3 nos dice que cualquier funcíón booleana la podemos expresar únicamente con el operador NAND.

De la misma forma, puesto que $\overline{x} = x \downarrow x$ y $x \cdot y = (x \downarrow x) \downarrow (y \downarrow y)$ deducimos que el operador NOR es suficiente para expresar cualquier función booleana. ■.

Las puertas correspondientes NAND y NOR se suelen representar como sigue:




Cualquiera de los circuitos que vimos en la Sección 3.3.4, o cualquier otro que se nos ocurra podemos ahora diseñarlo usando únicamente la puerta NAND (o la puerta NOR). Esta puerta se construye de forma sencilla con transistores, tanto con la tecnología de semiconductores como con las técnicas más recientes de fabricación de microcircuitos.

# Capítulo 2

# Conjuntos ordenados. Retículos y álgebras de Boole.

## 2.1. Conjuntos ordenados.

En este capítulo vamos a estudiar el concepto de retículo. Hay dos caminos para llegar a esta estructura. Uno es mediante un conjunto con dos operaciones binarias que satisfacen una serie de axiomas. El otro es a partir del concepto de conjunto ordenado. Nosotros aquí hemos adoptado el segundo. Si enriquecemos la estructura de retículo con unos axiomas adicionales obtenemos lo que se conoce como *Álgebra de Boole.* Analizaremos su estructura, y llegaremos a que en el caso finito, las álgebras de Boole tiene una forma muy particular. Estudiaremos el álgebra de Boole de las funciones booleanas, y el teorema de estructura nos conducirá a las formas normales. Terminaremos viendo algunas aplicaciones de las álgebras de Boole al diseño de circuitos lógicos.

**Definición 5.** *Sea $X$ un conjunto, y $\leq$ una relación binaria en $X$. Se dice que $\leq$ es una relación de orden si se verifican las siguientes propiedades.*

*Reflexiva: $x \leq x$ para todo $x \in X$.*

*Antisimétrica: Si $x \leq y$ e $y \leq x$ entonces $x = y$.*

*Transitiva: Si $x \leq y$ e $y \leq z$ entonces $x \leq z$.*

*Si $X$ es un conjunto en el que tenemos definida una relación de orden $\leq$, se dice que $(X, \leq)$ es un conjunto ordenado (o, si está claro cual es la relación $\leq$ se dice simplemente que $X$ es un conjunto ordenado).*

*Si $\leq$ es una relación de orden en $X$ que satisface la propiedad adicional de que dados $x, y \in X$ entonces $x \leq y$ ó $y \leq x$, se dice entonces que $\leq$ es una relación de orden total, y que $(X, \leq)$ (o $X$) es un conjunto totalmente ordenado (en ocasiones, para destacar que $(X, \leq)$ es una relación de orden, pero que no es total se dice que $\leq$ es una relación de orden parcial y que $(X, \leq)$ es un conjunto parcialmente ordenado).*

**Ejemplo 2.1.1.**

1. *El conjunto de los números naturales, con el orden natural ($m \leq n$ si existe $k \in \mathbb{N}$ tal que $n = m+k$) es un conjunto totalmente ordenado. De la misma forma, también lo son $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ y $(\mathbb{R}, \leq)$.*

2. *Dado un conjunto $X$, entonces $\mathcal{P}(X)$, con el orden dado por la inclusión es un conjunto ordenado. Si $X$ tiene más de un elemento, este orden no es total, pues dados $x, y \in X$ distintos se tiene que $\{x\} \not\subseteq \{y\}$ y $\{y\} \not\subseteq \{x\}$.*

3. *En el conjunto de los números naturales, la relación de divisibilidad es una relación de orden que no es total. Esta relación viene dada por $a|b$ si existe $c \in \mathbb{N}$ tal que $b = a \cdot c$ (compara con la relación de orden natural). Sin embargo, en el conjunto de los números enteros esta relación no es de orden pues no es antisimétrica, ya que $2|-2$, $-2|2$ y sin embargo $2 \neq -2$.*

4. *Para cualquier número natural $n$ consideramos el conjunto*

$$D(n) = \{m \in \mathbb{N} : m|n\}$$

*Entonces $(D(n), |)$ es un conjunto (parcialmente) ordenado.*

5. *Sea $(X, \leq)$ es un conjunto ordenado, e $Y$ un subconjunto de $X$. Definimos en $Y$ el orden $x \preceq y$ si $x \leq y$ (vistos como elementos de $X$). Entonces, $(Y, \preceq)$ es un conjunto ordenado. De ahora en adelante, el orden en $Y$ lo denotaremos igual que en $X$.*

   *Un ejemplo de esto último podría ser el caso de los divisores de un número natural $n$.*

   *Si $(X, \leq)$ es un conjunto totalmente ordenado, entonces, para cualquier $Y \subseteq X$ se tiene que $(Y, \leq)$ es un conjunto totalmente ordenado.*

La definición de conjunto ordenado puede hacerse también a partir de la noción de *orden estricto*.

**Definición 6.** *Sea $X$ un conjunto, $y <$ una relación binaria en $X$. Se dice que $<$ es un orden estricto si se verifican las siguientes propiedades:*

*Antirreflexiva Para cualquier $x \in X$ se tiene que $x \not< x$.*

*Transitiva Si $x < y$ e $y < z$ entonces $x < z$.*

Es fácil comprobar que si $\leq$ es una relación de orden en un conjunto $X$, entonces si definimos

$$x < y \text{ si } x \leq y \text{ y } x \neq y$$

se tiene que $<$ es una relación de orden estricto en $X$.

De la misma forma, si $<$ es una relación de orden estricto en $X$ entonces la relación siguiente:

$$x \leq y \text{ si } x < y \text{ o } x = y$$

es una relación de orden en $X$.

Vemos entonces que los conceptos de *relación de orden* y *relación de orden estricto* son equivalentes, pues dada una relación de orden tenemos determinada una relación de orden estricto y viceversa. Además, los caminos para pasar de orden a orden estricto, y de orden estricto a orden, son uno el inverso del otro.

A continuación vamos a construir un grafo (dirigido) asociado a una relación de orden. Aún cuando los grafos serán estudiados con posterioridad, la representación de una relación de orden mediante este grafo ayuda a visualizar mejor el orden dado.

**Definición 7.** *El diagrama de Hasse de un conjunto ordenado $(X, \leq)$ es un grafo dirigido cuyos vértices son los elementos de $X$, y existe un lado de $x$ a $y$ si $x < y$ y no existe $z$ tal que $x < z < y$.*

El diagrama de Hasse está definido para cualquier conjunto ordenado. Sin embargo, en general dicho diagrama no permite recuperar el orden. Por ejemplo, en el caso del conjunto $(\mathbb{R}, \leq)$, dado cualquier $x \in \mathbb{R}$ no existe ningún $y \in \mathbb{R}$ que esté conectado a $x$ por algún lado.

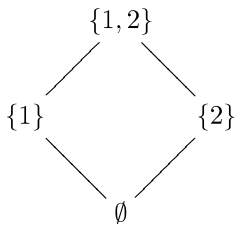
Sin embargo, si el conjunto $X$ es finito, entonces dados $x, y \in X$ se tiene que $x \leq y$ si $x = y$ o existe algún camino que parta de $x$ y termine en $y$.

Una forma habitual de representar el diagrama de Hasse es dibujar los lados como líneas ascendentes, lo que implica colocar los vértices de forma apropiada.

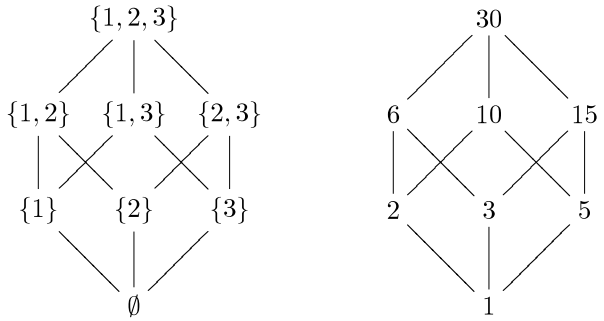
**Ejemplo 2.1.2.**

1. *El diagrama de Hasse del conjunto* $(\mathbb{N}, \leq)$ *sería*


2. *Consideramos el conjunto ordenado* $(\mathcal{P}(\{1,2\}, \subseteq)$. *Entonces el diagrama de Hasse sería:*

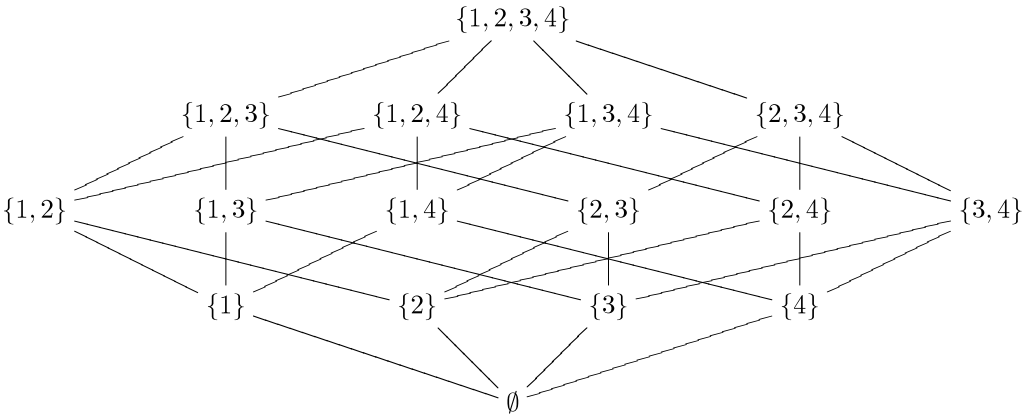



3. *Vamos a representar los diagramas de Hasse de los conjuntos ordenados* $\mathcal{P}(\{1,2,3\})$ *y* $D(30)$.



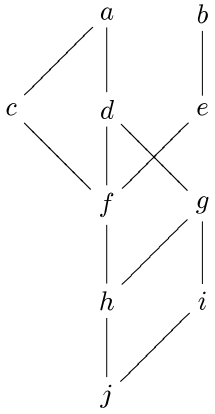

*Observa como la estructura de conjunto ordenado es igual en ambos casos.*

4. *Vamos a representar el diagrama de Hasse de* $\mathcal{P}(\{1,2,3,4\})$.




*Prueba a dibujar el diagrama de Hasse de los divisores de 210 y compáralo con este último.*

5. *Si tenemos un grafo dirigido que no contiene caminos cerrados, entonces podemos definir un orden en el conjunto de los vértices. $x \leq y$ si $x = y$ o existe un camino con inicio $x$ y fin $y$. Si en el grafo no hay caminos entre dos vértices adyacentes, entonces el grafo es el diagrama de Hasse de un conjunto ordenado.*




*tenemos definido un orden en el conjunto $X = \{a, b, c, d, e, f, g, h, i\}$. Con este orden se tiene, por ejemplo que,*

*$h \leq e$, pues tenemos un camino $h - f - e$ que empieza en $h$ y termina en $e$.*

*$i \leq a$, pues el camino $i - g - d - a$ empieza en $i$ y termina en $a$.*

*$i \not\leq e$, pues ningún camino empieza en $i$ y termina en $e$.*

**Definición 8.** *Sea $(X, \leq)$ un conjunto ordenado.*

1. *Un elemento $x \in X$ se dice que es maximal, si no existe $y \in X$ tal que $x \leq y$ y $x \neq y$.*
2. *Un elemento $x \in X$ se dice que es máximo, si para todo $y \in X$ se verifica que $y \leq x$.*

De la misma forma se puede definir lo que es un elemento minimal y lo que es un mínimo.

**Ejemplo 2.1.3.** *En el último conjunto ordenado del ejemplo anterior se tiene que $a$ y $b$ son elementos maximales, pues no hay ningún elemento que sea mayor que ellos. Sin embargo, el conjunto $X$ no tiene máximo.*

*El elemento $j$ es un elemento minimal, y además es mínimo.*

*En el conjunto de los divisores de 30 (ver ejemplo anterior) tenemos que 10 no es un elemento maximal, pues $10 \leq 30$. Sí se tiene que 30 es un elemento maximal, pues no hay ningún elemento que sea mayor que él. También se tiene que 30 es un máximo de ese conjunto.*

*En el conjunto $(\mathbb{N}, \leq)$, el cero es el mínimo y es el único elemento minimal. Este conjunto no tiene máximo ni elementos maximales.*

*Si $(X, \leq)$ es un conjunto ordenado finito, entonces $X$ tiene al menos un elemento maximal y un elemento minimal.*

Nótese, que si un conjunto tiene máximo, entonces este es único. Además, en el caso de que tenga máximo, entonces tiene sólo un elemento maximal, que coincide con el máximo.

Idéntica observación vale para mínimo y elemento minimal.

Denotaremos por máx$(X)$ al máximo del conjunto $X$, en el caso de que exista, y por mín$(X)$ al mínimo.

En el ejemplo que hemos estudiado anteriormente no existe máx$(X)$, mientras que mín$(X) = j$.

**Definición 9.** *Sea $(X, \leq)$ un conjunto ordenado, e $Y$ un subconjunto de $X$. Consideramos en $Y$ el orden inducido de $X$.*

1. *Un elemento $x \in X$ se dice que es* cota superior *de $Y$ si $x \geq y$ para todo $y \in Y$.*

2. *Un elemento $x \in X$ se dice que es* supremo *de $Y$ si es el mínimo del conjunto de las cotas superiores de $Y$.*

De la misma forma se define lo que es una cota inferior y un ínfimo.

**Ejemplo 2.1.4.** *Si $X = \{a, b, c, d, e, f, g, h, i, j\}$ con el orden dado anteriormente, e $Y = \{c, d, f, g, h\}$ entonces:*

*El conjunto de las cotas superiores de $Y$ es $\{a\}$.*

*Puesto que este conjunto tiene mínimo, que es a, entonces a es el supremo de $Y$.*

*Los elementos c y d son elementos maximales de $Y$.*

*El conjunto de las cotas inferiores es $\{h, j\}$.*

*De éstas, h es el máximo, luego h es el ínfimo de $Y$.*

*h es además el único elemento minimal y el mínimo de $Y$.*

Cuando un conjunto tiene supremo éste es único. Podemos entonces hablar de *el supremo de $Y$*, y lo representaremos mediante $\sup(Y)$.

De la misma forma, denotaremos por $\text{ínf}(Y)$ al ínfimo del conjunto $Y$ cuando exista.

Cuando un conjunto tiene máximo, entonces también tiene supremo, y coincide con él. En el último ejemplo vemos como el recíproco no es cierto, pues $Y$ tiene supremo pero no tiene máximo.

Cuando el supremo de un conjunto pertenezca al conjunto, entonces será también el máximo.

**Definición 10** (Buen orden)**.** *Sea $(X, \leq)$ un conjunto ordenado. Se dice que $\leq$ es un buen orden si todo subconjunto no vacío de $X$ tiene mínimo. En tal caso, se dice que $(X, \leq)$ (o $X$) es un conjunto bien ordenado.*

**Observación:** Todo conjunto bien ordenado es un conjunto totalmente ordenado, pues dados dos elementos $x, y \in X$ el subconjunto $\{x, y\}$ tiene mínimo. Si $\text{mín}(\{x, y\}) = x$ entonces $x \leq y$, mientras que si $\text{mín}(\{x, y\}) = y$ entonces $y \leq x$.

El recíproco no es cierto. Busca un ejemplo.

**Ejemplo 2.1.5.** *El conjunto de los números naturales, con el orden usual, es un conjunto bien ordenado, como demostramos en el Teorema 1.1.1.*

**Definición 11.** *Sean $(X_1, \leq_1)$ y $(X_2, \leq_2)$ dos conjuntos ordenados.*

*Se define el* orden producto *en $X_1 \times X_2$ como sigue:*

$$(x_1, x_2) \leq_{prod} (y_1, y_2) \text{ si } x_1 \leq_1 y_1 \text{ y } x_2 \leq_2 y_2.$$

*Se define el* orden lexicográfico *en $X_1 \times X_2$ como sigue:*

$$(x_1, x_2) \leq_{lex} (y_1, y_2) \overset{def}{\iff} \begin{cases} x_1 <_1 y_1 & \text{ó} \\ x_1 = y_1 \text{ y } x_2 \leq_2 y_2. \end{cases}$$

Claramente, si $(x_1, x_2) \leq_{prod} (y_1, y_2)$ entonces $(x_1, x_2) \leq_{lex} (y_1, y_2)$.

**Proposición 2.1.1.** *Si $(X_1, \leq_1)$ y $(X_2, \leq_2)$ son dos conjuntos ordenados, entonces $(X_1 \times X_2, \leq_{prod})$ y $(X_1 \times X_2, \leq_{lex})$ son conjuntos ordenados.*

*Además, si $\leq_1$ y $\leq_2$ son órdenes totales (resp. buenos órdenes) entonces $\leq_{lex}$ es un orden total (resp. buen orden).*

*Demostración:* La demostración de que el orden producto es una relación de orden es fácil, y se deja como ejercicio. Centrémonos pues en el orden lexicográfico.

Notemos en primer lugar que si $(x_1, x_2) \leq_{lex} (y_1, y_2)$ entonces $x_1 \leq_1 y_1$.

Veamos que la relación es de orden.

Reflexiva: Si $(x_1, x_2) \in X_1 \times X_2$ entonces $(x_1, x_2) \leq_{lex} (x_1, x_2)$, pues se da la segunda opción ($x_1 = x_1$ y $x_2 \leq x_2$).

Simétrica: Supongamos que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ y $(y_1, y_2) \leq_{lex} (x_1, x_2)$. Entonces se tiene que $x_1 \leq_1 y_1$ e $y_1 \leq_1 x_1$, de donde $x_1 = y_1$. Deducimos entonces que $x_2 \leq_2 y_2$ e $y_2 \leq_2 x_2$, lo que implica que $x_2 = y_2$.

Transitiva: Supongamos ahora que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ y $(y_1, y_2) \leq_{lex} (z_1, z_2)$. Pueden darse entonces tres opciones(no excluyentes):

- $x_1 <_1 y_1$, en cuyo caso $x_1 <_1 z_1$, luego $(x_1, x_2) \leq_{lex} (z_1, z_2)$.
- $y_1 <_1 z_1$, en cuyo caso $x_1 <_1 z_1$ y concluimos como en la opción anterior.
- $x_1 = y_1$ e $y_1 = z_1$. En tal caso, $x_2 \leq_2 y_2$ e $y_2 \leq_2 z_2$, de donde $x_1 = z_1$ y $x_2 \leq_2 z_2$, es decir, $(x_1, x_2) \leq_{lex} (z_1, z_2)$.

Supongamos ahora que $\leq_1$ y $\leq_2$ son órdenes totales. Sean $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$. Aquí pueden darse tres opciones (mutuamente excluyentes):

- $x_1 <_1 y_1$. En tal caso $(x_1, x_2) \leq_{lex} (y_1, y_2)$.
- $y_1 <_1 x_1$. En este caso $(y_1, y_2) \leq_{lex} (x_1, x_2)$.
- $x_1 = y_1$. Entonces dependiendo de que $x_2 \leq_2 y_2$ o $y_2 \leq_2 x_2$ se tendrá que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ o que $(y_1, y_2) \leq_{lex} (x_1, x_2)$.

Por último, supongamos que $\leq_1$ y $\leq_2$ son buenos órdenes, y sea $Y \subseteq X_1 \times X_2$ un subconjunto no vacío.

Nos quedamos con el conjunto de todas las primeras coordenadas de los elementos de $A$, es decir, tomamos

$$Y_1 = \{x_1 \in X_1 : (x_1, x_2) \in A \text{ para algún } x_2 \in X_2\}.$$

Sea $a = \text{mín}(Y_1)$. Tomamos entonces $Y_2 = \{x_2 \in X_2 : (a, x_2) \in A\}$. Como $Y_2 \neq \emptyset$, tiene mínimo. Sea éste $b$. Entonces $(a, b) = \text{mín}(A)$. ■

**Observación:** Si tenemos $n$ conjuntos ordenados $X_1, X_2, \ldots, X_n$, podemos definir recursivamente el orden producto y el orden lexicográfico en $X_1 \times X_2 \times \cdots \times X_n$.

Supuesto definido el orden producto $\leq_{prod}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{prod} (y_1, \ldots, y_{n-1}, y_n) \text{ } si \text{ } (x_1, \ldots, x_{n-1}) \leq_{prod} (y_1, \ldots, y_{n-1}) \text{ y } x_n \leq y_n,$$

es decir, definimos el orden producto en $(X_1 \times \cdots \times X_{n-1}) \times X_n$.

Supuesto definido el orden lexicográfico $\leq_{lex}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{lex} (y_1, \ldots, y_{n-1}, y_n) \overset{\text{def}}{\iff} \begin{cases} (x_1, \ldots, x_{n-1}) <_{lex} (y_1, \ldots, y_{n-1}) & \text{ó} \\ (x_1, \ldots, x_{n-1}) = (y_1, \ldots, y_{n-1}) \text{ y } x_n \leq y_n. \end{cases}$$

Sea el conjunto

$$\mathcal{A} = \{\ , a, b, c, d, e, f, g, h, i, j, l, l, m, n, \tilde{n}, o, p, q, r, s, t, u, v, w, x, y, z\},$$

es decir, las 27 letras del alfabeto junto con el espacio en blanco.

Claramente, $\mathcal{A}$ tiene un orden total de todos conocido.

Supongamos que $n$ es el número de letras de la palabra más larga de la lengua española. Entonces, cada palabra puede representarse como un elemento de $\mathcal{A}^n$ (poniendo tantos espacios al final como sea necesario).

Cuando ordenamos las palabras, tal y como vienen en un diccionario, nos fijamos en la primera letra, y es la que nos da el orden. Cuando ésta coincide, pasamos a la segunda, y es ésta entonces la que nos da el orden. De coincidir también, nos fijamos en la tercera, y así sucesivamente. Es decir, las palabras de la lengua están ordenadas siguiendo el orden lexicográfico.

**Ejemplo 2.1.6.**

*Consideramos en* $\mathbb{N}\times\mathbb{N}$ *los órdenes producto* ($\leq$) *y lexicográfico* $\leq_{lex}$ *deducidos a partir del orden usual en* $\mathbb{N}$. *Entonces:*

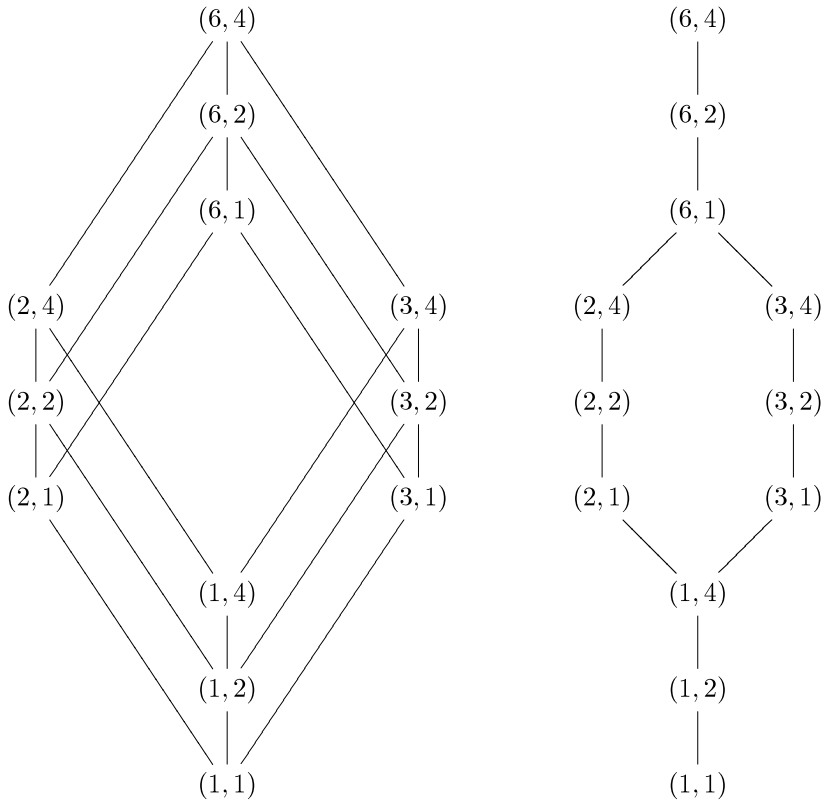
*Los elementos* $(0,n),(1,n-1),\ldots,(n-1,1),(n,0)$ *están ordenados según el orden lexicográfico, mientras que con el orden producto ninguna pareja de ellos es comparable.*

*Se puede ver entonces que la propiedad de ser orden total o buen orden no se mantiene al tomar el orden producto.*

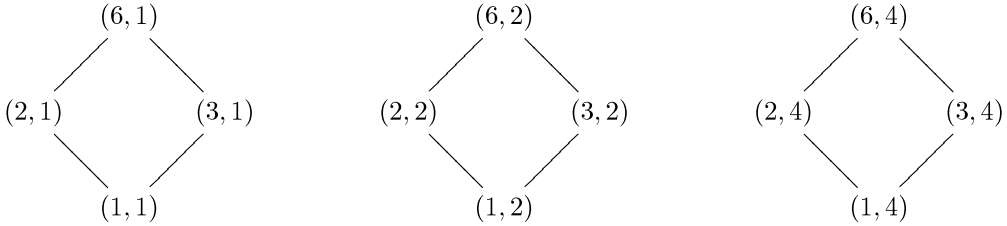
*Si* $X=\{(0,n),(1,n-1),\ldots,(n-1,1),(n,0)\}$ *entonces:*

- *El conjunto de cotas inferiores con respecto al orden lexicográfico es* $\{(0,0),(0,1),\ldots,(0,n)\}$, *mientras que con respecto al orden producto tiene una única cota inferior, que es* $(0,0)$.
- *El ínfimo, respecto al orden lexicográfico es* $(0,n)$, *que es también el mínimo. Con respecto al orden producto es* $(0,0)$, *y no tiene mínimo.*
- *Con respecto al orden lexicográfico tiene un elemento minimal, que es* $(0,n)$ *y un elemento maximal, que es* $(n,0)$. *Con respecto al orden producto, todos los elementos son maximales y minimales.*

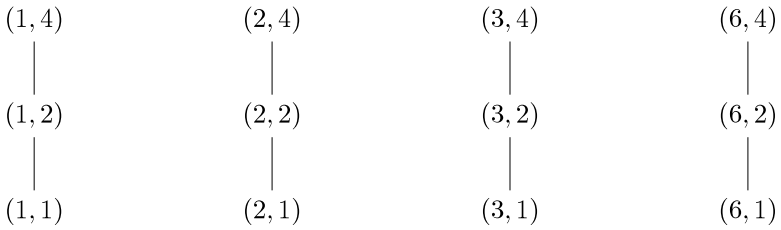
*Sean ahora los conjuntos ordenados* $(D(6),|)$ *y* $(D(4),|)$. *Entonces los diagramas de Hasse de* $D(6)\times D(4)$ *con el orden producto y el orden lexicográfico son respectivamente:*



*Nótese como el diagrama de Hasse de $D(6) \times D(4)$ con el orden producto consiste en "pegar" tres diagramas como el de $D(6)$*

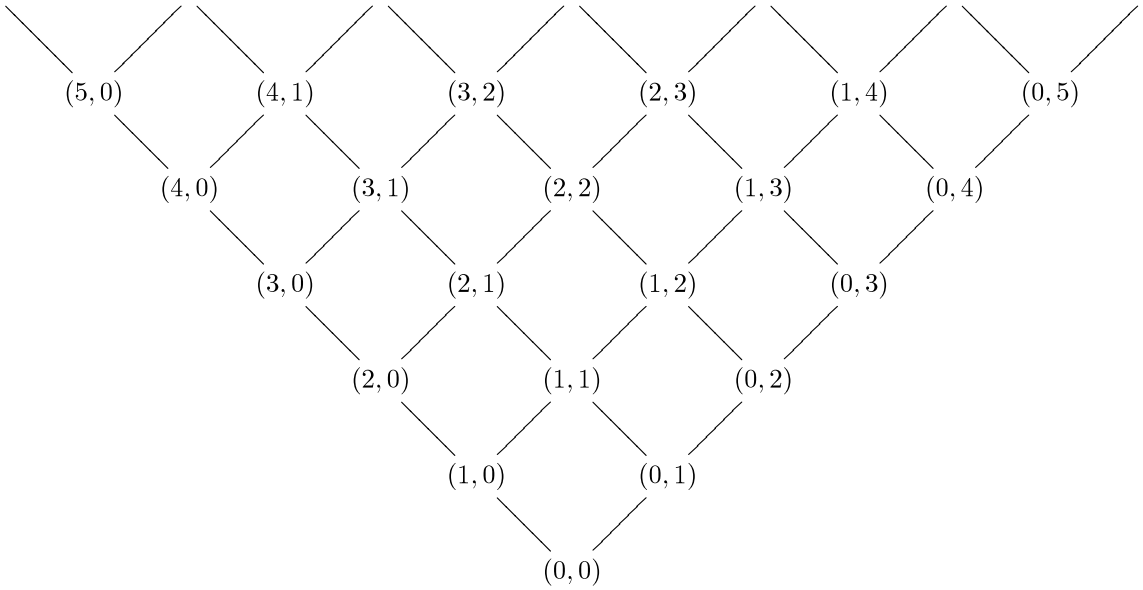



*y cuatro diagramas como el de $D(4)$*




*mientras que el diagrama de Hasse de $D(6) \times D(4)$ con el orden lexicográfico tiene la "misma forma" que el de $D(6)$, salvo que en cada vértice tenemos un diagrama de $D(4)$.*

*El diagrama de Hasse de $(\mathbb{N}^2, \leq_{prod})$ sería como sigue:*




## 2.2. Retículos.

**Definición 12.** *Un retículo es un conjunto ordenado, $(L, \leq)$ en el que cualquier conjunto finito tiene supremo e ínfimo.*

Si $(L, \leq)$ es un retículo y $x, y \in L$, denotaremos por $x \vee y$ al supremo del conjunto $\{x, y\}$ y por $x \wedge y$ al ínfimo del conjunto $\{x, y\}$.

Nótese que $x \vee y$ está definido por la propiedad:

$$x \leq x \vee y;\ y \leq x \vee y \qquad (x \leq z \text{ e } y \leq z) \Longrightarrow x \vee y \leq z$$

La primera parte dice que $x \vee y$ es una cota superior del conjunto $\{x, y\}$, mientras que la segunda dice que es la menor de las cotas superiores.

**Proposición 2.2.1.** *Si $(L, \leq)$ es un retículo, las operaciones $\vee$ y $\wedge$ satisfacen las siguienes propiedades:*

$$\begin{array}{rl} \textit{Conmutativa} & \left\{ \begin{array}{l} x \vee y = y \vee x \\ x \wedge y = y \wedge x. \end{array} \right. \\ \textit{Asociativa} & \left\{ \begin{array}{l} x \vee (y \vee z) = (x \vee y) \vee z \\ x \wedge (y \wedge z) = (x \wedge y) \wedge z. \end{array} \right. \\ \textit{Absorción} & \left\{ \begin{array}{l} x \vee (x \wedge y) = x \\ x \wedge (x \vee y) = x. \end{array} \right. \\ \textit{Idempotencia} & \left\{ \begin{array}{l} x \vee x = x \\ x \wedge x = x. \end{array} \right. \end{array}$$

*Demostración:* La demostración de la propiedad conmutativa, así como la de idempotencia es inmediata. Para demostrar la propiedad asociativa basta comprobar que tanto $x \vee (y \vee z)$ como $(x \vee y) \vee z$ representa el supremo del conjunto $\{x, y, z\}$, y lo mismo para el ínfimo. Veamos que $\sup(\{x, y, z\}) = x \vee (y \vee z)$.

Es claro que $x \leq x \vee (y \vee z)$, $y \leq x \vee (y \vee z)$ y $z \leq x \vee (y \vee z)$. Por otra parte,

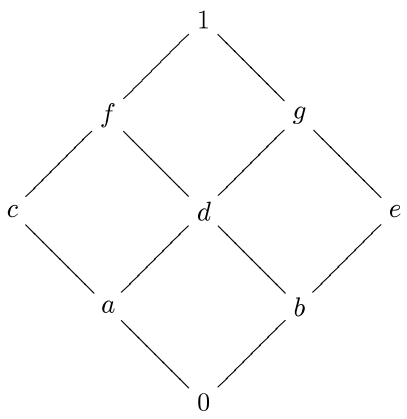
$$\left.\begin{array}{l} x \leq u \\ y \leq u \\ z \leq u \end{array}\right\} \Longrightarrow y \vee z \leq u \left.\right\} \Longrightarrow x \vee (y \vee z) \leq u.$$

Por tanto, $x \vee (y \vee z)$ es el supremo del conjunto $\{x, y, z\}$.

En cuanto a la absorción, la primera se deduce fácilmente del hecho de que $x \wedge y \leq x$ y la segunda de que $x \leq x \vee y$. ■

**Ejemplo 2.2.1.**

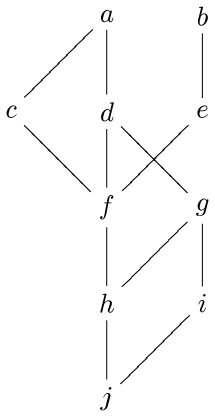
1. *Si $X$ es un conjunto totalmente ordenado, entonces $X$ es un retículo. Dados $x, y \in X$ se tiene que $x \vee y = \textit{máx}(\{x, y\})$ mientras que $x \wedge y = \textit{mín}(\{x, y\})$.*
2. *El conjunto ordenado $(\mathbb{N}, |)$ es un retículo. En este caso se tiene que $x \vee y = mcm(x, y)$ mientras que $x \wedge y = mcd(x, y)$. De la misma forma, si $n \in \mathbb{N}$ entonces $D(n)$, con el orden dado por la divisibilidad es un retículo. Supremo e ínfimo vienen dado por el mínimo común múltiplo y el máximo común divisor respectivamente.*
3. *Si $X$ es un conjunto, entonces $\mathcal{P}(X)$ es un retículo. En este caso supremo e ínfimo vienen dados por la unión y la intersección respectivamente; es decir, $A \vee B = A \cup B$ y $A \wedge B = A \cap B$.*
4. *Si $V$ es un $K$-espacio vectorial, el conjunto de los subespacios vectoriales de $V$ es un retículo, con el orden dado por la inclusión. Aquí, dado dos subespacios vectoriales $V_1$ y $V_2$ se tiene que $V_1 \vee V_2 = V_1 + V_2$ mientras que $V_1 \wedge V_2 = V_1 \cap V_2$.*
5. *El conjunto ordenado cuyo diagrama de Hasse es*



*es un retículo.*

*Se tiene, por ejemplo:* $c \vee d = f$, $c \wedge d = a$, $b \vee c = f$, $b \wedge c = 0$, $c \vee e = 1$, $c \wedge e = 0$.

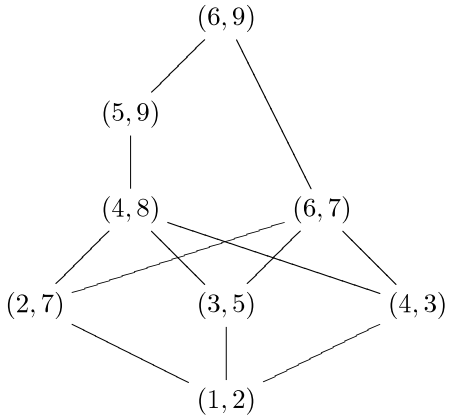
6. *El conjunto ordenado cuyo diagrama de Hasse es*




*no es un retículo, pues por ejemplo, no existe el supremo del conjunto* $\{a, e\}$. *Sin embargo, el conjunto* $\{f, i\}$ *sí tiene supremo (d) e ínfimo (j).*

7. *Dado el conjunto* $A = \{(1,2);\ (4,3);\ (3,5);\ (2,7);\ (4,8);\ (6,9);\ (6,7);(5,9)\} \subseteq \mathbb{N}^2$, *consideramos en A el orden inducido del orden producto en* $\mathbb{N}^2$.

*El diagrama de Hasse de A sería:*




*Este conjunto no es un retículo. Por ejemplo, tomamos* $x = (2,7)$ *e* $y = (3,5)$. *El conjunto de las cotas superiores de x e y es* $\{(4,8);\ (6,7);\ (5,9);\ (6,9)\}$. *Y ese conjunto no tiene mínimo. Por tanto, no existe la menor de las cotas superiores, luego no existe el supremo de x e y.*

Nótese que si $(L, \leq)$ es un retículo, entonces dados $x, y \in L$ se verifica que $x \leq y$ si, y sólo si, $x \vee y = y$, o si queremos, $x \leq y$ si, y sólo si, $x \wedge y = x$. Es decir, podemos recuperar el orden dentro del retículo a partir del conocimiento de las operaciones supremo o ínfimo.

La siguiente proposición nos da condiciones suficientes para que dos operaciones definidas en un conjunto puedan ser el supremo y el ínfimo de alguna relación de orden en ese conjunto.

**Proposición 2.2.2.** *Sea L un conjunto en el que tenemos definidas dos operaciones* $\vee$ *y* $\wedge$ *que satisfacen las propiedades conmutativa, asociativa, idempotencia y de absorción. Supongamos que en L definimos la relación*

$$x \leq y \quad \text{si } x \vee y = y.$$

*Entonces,* $(L, \leq)$ *es un retículo donde las operaciones supremo e ínfimo vienen dadas por* $\vee$ *y* $\wedge$ *respectivamente.*

*Demostración:*

1. Veamos en primer lugar que $(L, \leq)$ es un conjunto ordenado. Para esto, comprobemos que la relación $\leq$ es reflexiva, antisimétrica y transitiva.

   Reflexiva. Puesto que $x \vee x = x$ se tiene que $x \leq x$ para cualquier $x \in L$.

   Antisimétrica. Supongamos que $x \leq y$ e $y \leq x$. Esto implica que $x \vee y = y$ y que $y \vee x = x$. Puesto que $\vee$ es conmutativa deducimos que $x = y (= x \vee y)$.

   Transitiva. Supongamos ahora que $x \leq y$ y que $y \leq z$, es decir, $x \vee y = y$ e $y \vee z = z$. Entonces:

   $$x \vee z = x \vee (y \vee z) = (x \vee y) \vee z = y \vee z = z$$

   luego $x \leq z$.

2. Comprobemos ahora que dados $x, y \in L$ se verifica que $\sup(\{x, y\}) = x \vee y$.

   Puesto que $x \vee (x \vee y) = (x \vee x) \vee y = x \vee y$ se tiene que $x \leq x \vee y$. De la misma forma se comprueba que $y \leq x \vee y$.

   Si $x \leq u$ e $y \leq u$ (es decir, $x \vee u = u$ e $y \vee u = u$). Entonces:

   $$(x \vee y) \vee u = x \vee (y \vee u) = x \vee u = u,$$

   de donde se deduce que $x \vee y \leq u$.

3. Por último, veamos que $\text{ínf}(\{x, y\}) = x \wedge y$.

   $(x \wedge y) \vee x = x \vee (x \wedge y) = x$ luego $x \wedge y \leq x$.

   De la misma forma se comprueba que $x \wedge y \leq y$.

   Si $u \leq x$ y $u \leq y$ (es decir, $u \vee x = x$ y $u \vee y = y$) se tiene que:

   $$u \wedge x = u \wedge (u \vee x) = u \qquad u \wedge y = u \wedge (u \vee y) = u,$$

   $$u \wedge (x \wedge y) = (u \wedge x) \wedge y = u \wedge y = u,$$

   $$u \vee (x \wedge y) = (u \wedge (x \wedge y)) \vee (x \wedge y) = (x \wedge y) \vee ((x \wedge y) \wedge u) = x \wedge y,$$

   luego $u \leq x \wedge y$.

■

Nótese que se tiene que $x \vee y = y$ si, y sólo si, $x \wedge y = x$, luego podría haberse hecho la demostración definiendo la relación

$$x \leq y \quad \text{si } x \wedge y = x.$$

Nótese también que la propiedad de idempotencia se puede deducir a partir de la de absorción, pues

$$x \vee x = x \vee [x \wedge (x \vee x)] = x,$$

luego podemos demostrar la proposición anterior partiendo de que las operaciones $\vee$ y $\wedge$ satisfacen las propiedades asociativa, conmutativa y de absorción.

Esta proposición permite definir un retículo, bien dando la relación de orden, bien dando las operaciones $\vee$ y $\wedge$.

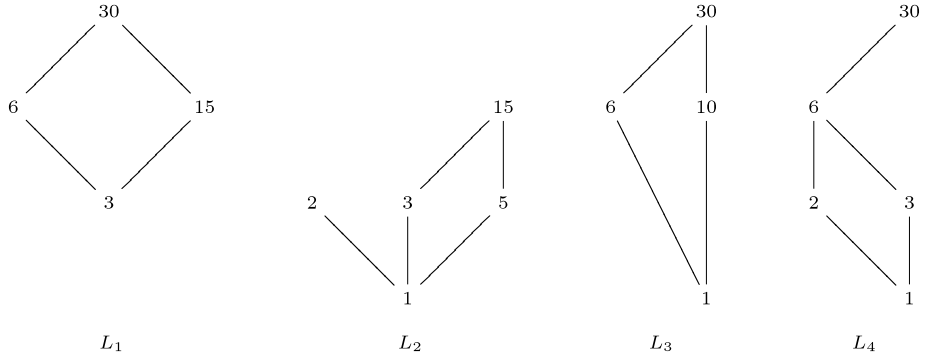
Si $(L, \leq)$ es un retículo y $L$ tiene máximo, denotaremos a éste por 1, mientras que si tiene mínimo lo denotaremos por 0. Se tiene entonces, $x \vee 1 = 1$, $x \wedge 1 = x$, $x \vee 0 = x$ y $x \wedge 0 = 0$.

Un retículo finito siempre tiene máximo y mínimo. Si el retículo es infinito, puede tenerlo o no. Así, por ejemplo, $(\mathbb{N}, \leq)$ tiene mínimo pero no tiene máximo; $(\mathbb{Z}, \leq)$ no tiene ni mínimo ni máximo. El retículo $(\mathbb{N}, |)$ es infinito y tiene máximo y mínimo. En este caso, el máximo es 0 mientras que el mínimo es 1.

**Definición 13.** *Sea $(L, \leq)$ un retículo, y $L' \subseteq L$ un subconjunto de $L$. Entonces $L'$ es un subrretículo si para cualesquiera $x, y \in L'$ se verifica que $x \vee y \in L'$ y $x \wedge y \in L'$.*

**Ejemplo 2.2.2.** *Consideramos el retículo $D(30)$.*

*Sean $L_1 = \{3, 6, 15, 30\}$, $L_2 = \{1, 2, 3, 5, 15\}$, $L_3 = \{1, 6, 10, 30\}$ y $L_4 = \{1, 2, 3, 6, 30\}$. Sus diagramas de Hasse son:*




$L_1$ $L_2$ $L_3$ $L_4$

*Entonces $L_1$ y $L_4$ son subrretículos de $D(30)$, mientras que $L_2$ y $L_3$ no lo son. $L_2$ no es subrretículo porque el supremo de 2 y 3 es 6, que no pertenece a $L_2$. $L_3$ no es subrretículo porque el ínfimo de 6 y 10 vale 2, que no pertenece a $L_3$. Nótese que $L_3$, con el orden que hereda de $D(30)$, es un retículo, pero no es subrretículo de $L_3$.*

**Definición 14.** *Sea $L$ un retículo. Se dice que $L$ es distributivo si para cualesquiera $x, y, z \in L$ se verifica que*

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad y \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

En general, si $L$ es un retículo se tiene que $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$.

$$\left.\begin{array}{l} \left.\begin{array}{l} x \leq x \vee y \\ x \leq x \vee z \end{array}\right\} \implies x \leq (x \vee y) \wedge (x \vee z) \\ \left.\begin{array}{l} y \wedge z \leq x \vee y \\ y \wedge z \leq x \vee z \end{array}\right\} \implies y \wedge z \leq (x \vee y) \wedge (x \vee z) \end{array}\right\} \implies x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z),$$

y de la misma forma se tiene que $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$. Por tanto, se tiene que un retículo es distributivo si $(x \vee y) \wedge (x \vee z) \leq x \vee (y \wedge z)$ y $(x \wedge (y \vee z) \leq x \wedge y) \vee (x \wedge z)$.

Por otra parte, si $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ para cualesquiera $x, y, z \in L$ se tiene que

$$\begin{array}{rcll} (x \wedge y) \vee (x \wedge z) & = & [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z] & \text{propiedad distributiva} \\ & = & [x \vee (x \wedge y)] \wedge [z \vee (x \wedge y)] & \text{pues } \vee \text{ es conmutativa} \\ & = & [(x \vee x) \wedge (x \vee y)] \wedge [(z \vee x) \wedge (z \vee y)] & \text{propiedad distributiva} \\ & = & (x \vee x) \wedge (x \vee y) \wedge (x \vee z) \wedge (y \vee z) & \text{propiedad asociativa y conmutativa} \\ & = & [x \wedge (x \vee y) \wedge (x \vee z)] \wedge (y \vee z) & \text{idempotencia y propiedad asociativa} \\ & = & x \wedge (y \vee z) & \text{Absorción} \end{array}$$

mientras que si $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ para cualesquiera $x, y, z \in L$ entonces se verifica que $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ también para cualesquiera $x, y, z \in L$.

Es decir, basta con que se dé una de las dos posibles propiedades distributivas para que se dé la otra.

**Ejemplo 2.2.3.**

1. *Si $L$ es un conjunto totalmente ordenado, entonces $L$ es un retículo distributivo. Basta comprobar que para cualesquiera $x, y, z \in L$ se verifica que*

$$máx\{x, mín\{y, z\}\} = mín\{máx\{x, y\}, máx\{x, z\}\},$$

*lo cual puede hacerse fácilmente comprobando que se da la igualdad en cualquiera de los seis casos siguientes:*

$$x \leq y \leq z; \quad x \leq z \leq y; \quad y \leq x \leq z; \quad y \leq z \leq x; \quad z \leq x \leq y; \quad z \leq y \leq x,$$

*y puesto que en la igualdad el papel que juegan $y$ y $z$ es el mismo, bastaría con comprobarlo en los casos*

$$x \leq y \leq z; \qquad y \leq x \leq z; \qquad y \leq z \leq x.$$

2. *El retículo $(\mathbb{N}, |)$ es un retículo distributivo. Basta ver que en este caso, el cálculo del supremo y el ínfimo se reduce al cálculo del máximo y el mínimo de los exponentes, y entonces reducirse al caso anterior.*

   *Por el mismo motivo, para cada número natural $n \in \mathbb{N}$ el retículo $D(n)$ es distributivo.*

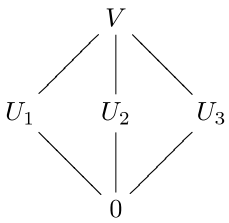
3. *Si $X$ es un conjunto, entonces $(\mathcal{P}(X), \subseteq)$ es un retículo distributivo, pues la unión y la intersección de conjuntos son distributivas la una con respecto de la otra.*

4. *Si $V$ es un $K$-espacio de dimensión mayor que $1$, entonces el retículo de los subespacios vectoriales de $V$ es un retículo que no es distributivo.*

   *Como ejemplo, sea $K = \mathbb{Z}_2$ y $V = \mathbb{Z}_2^2$. Entonces $V$ tiene $5$ subespacios vectoriales que son:*

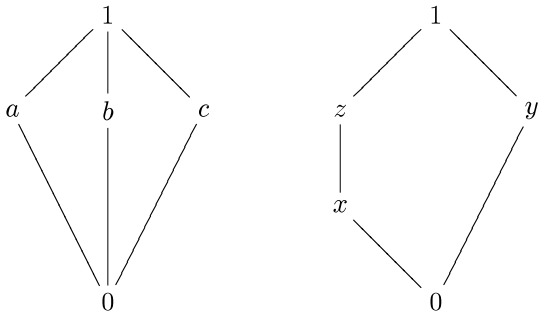
$$V; \quad U_1 = \{(0,0),(1,0)\}; \quad U_2 = \{(0,0),(0,1)\}; \quad U_3 = \{(0,0),(1,1)\}; \quad 0.$$

   *y se tiene que $U_2 \cap U_3 = 0$, luego $U_1 + (U_2 \cap U_3) = U_1$, mientras que $(U_1 + U_2) \cap (U_1 + U_3) = V \cap V = V$. El diagrama de Hasse de este retículo es:*




   *En general, si $V$ es un $K$-espacio de dimensión mayor o igual que $2$, y $u, v$ son dos vectores linealmente independientes, consideramos $U_1 = L\{u\}$, $U_2 = L\{v\}$ y $U_3 = L\{u+v\}$ y se verifica que $U_1 + (U_2 \cap U_3) = U_1$, mientras que $(U_1 + U_2) \cap (U_1 + U_3) = L\{u, v\}$.*

5. *Consideramos los siguientes retículos:*




   *denominados respectivamente* diamante *y* pentágono. *En el ejemplo anterior hemos visto que el diamente no es distributivo. En cuanto al pentágono, se tiene que*

$$x \vee (y \wedge z) = x \vee 0 = x, \qquad (x \vee y) \wedge (x \vee z) = 1 \wedge z = z.$$

*luego tampoco es distributivo.*

*En general, se tiene que un retículo es distributivo si no contiene como subrretículos ni al pentágono ni al diamante. En el apartado anterior hemos visto como el retículo de subespacios vectoriales de un espacio vectorial tiene al diamante como subrretículo.*

**Proposición 2.2.3.** *Sea $L$ un retículo distributivo, y sen $x, y, z \in L$ tales que $x \vee y = x \vee z$ y $x \wedge y = x \wedge z$. Entonces $y = z$.*

*Demostración:* Se tiene que

$$y = y \vee (x \wedge y) = y \vee (x \wedge z) = (y \vee x) \wedge (y \vee z) = (z \vee x) \wedge (z \vee y) = z \vee (x \wedge y) = z \vee (x \wedge z) = z.$$

■

**Ejemplo 2.2.4.** *En el diamante se tiene que $a \vee b = a \vee c = 1$, y $a \wedge b = a \wedge c = 0$, y sin embargo, $b \neq c$.*
*En el pentágono, $y \vee x = y \vee z = 1$ e $y \wedge x = y \wedge z = 0$, y sin embargo, $x \neq z$.*

**Definición 15.** *Sea $L$ un retículo que tiene máximo y mínimo (a los que denotaremos por 1 y 0 respectivamente), y $x \in L$. Se dice que $y \in L$ es un complemento de $x$ si $x \vee y = 1$ y $x \wedge y = 0$.*
*Un reticulo en el que todo elemento tiene complemento se dice complementado.*

Obviamente, si $y$ es un complemento de $x$ entonces $x$ es un complemento de $y$.

Por otra parte, si $L$ es un retículo distributivo y $x$ un elemento de $L$ que tiene complemento, entonces el complemento es único (ver Proposicion 2.2.3).

Si $L$ es un retículo distributivo y $x$ es un elemento que tiene complemento, denotaremos por $x'$ o $\overline{x}$ al único complemento de $x$.

**Ejemplo 2.2.5.**

1. *Si $L$ tiene máximo (1) y mínimo (0), entonces 0 es un complemento de 1.*
2. *El retículo $(\mathcal{P}(X), \subseteq)$ es un retículo complementado. Dado $A \in \mathcal{P}(X)$ se verifica que $A \cup (X \setminus A) = X$ y $A \cap (X \setminus A) = \emptyset$. Por ser un retículo distributivo, el complemento de cada elemento es único.*
3. *El pentágono y el diamente son retículos complementados. Vemos sin embargo, que los complementos de algunos elementos no son únicos.*

   *Así, en el diamante, tanto b como c son complementos de a; tanto a como c son complementos de b y tanto a como b son complementos de c.*

   *En el pentágono, tanto $x$ como $z$ son complementos de $y$. Sin embargo, $x$ tiene un único complemento, que es $y$, al igual que $z$.*
4. *Si $L$ es un conjunto totalmente ordenado con más de dos elementos, entonces es un retículo distributivo, pero no es complementado.*
5. *Si $V$ es un $K$-espacio vectorial de dimensión finita (esto último no es necesario) entonces el retículo de los subespacios vectoriales de $V$ es un retículo complementado.*

   *Para ver esto, tomamos $U$ un subespacio vectorial de $V$. Supongamos que $\mathcal{B}_U = \{u_1, \ldots, u_m\}$ es una base de $U$. Esta base puede ser ampliada hasta una base de $V$. Si dicha base ampliada es $\mathcal{B} = \{u_1, \ldots, u_m, u_{m+1}, \ldots, u_n\}$ entonces el subespacio generado por $\{u_{m+1}, \ldots, u_n\}$ es un complemento de $U$.*

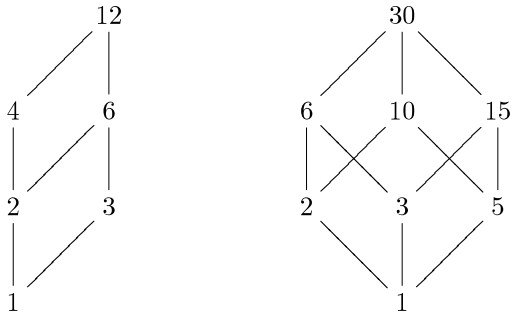
   *Puesto que en general hay muchas formas de completar una base de $V$ a partir de una base de $U$, el subespacio $U$ puede tener muchos complementos.*

   *Así, si tomamos $U = \mathbb{R}^2$ y $U = L[(1, 0)]$ (es decir, el eje $OX$) entonces cualquier recta que pase por el origen distinta del eje $OX$ es un complemento de $U$.*

6. *Dado un número natural $D(n)$, el retículo $D(n)$ no tiene por qué ser un retículo complementado. Por ejemplo, $D(4)$ no es complementado (es un conjunto totalmente ordenado con 3 elementos), mientras que $D(6)$ sí lo es.*

   *Se pide, determinar qué elementos de $D(n)$ tienen complemento, y a partir de ahí, determinar para qué valores de $n$ es $D(n)$ un retículo complementado.*

   *Así, por ejemplo, en $D(12)$ tienen complemento $1, 3, 4, 12$ mientras que no tienen $2, 6$. En $D(30)$ todos los elementos tienen complemento.*




$D(12)$ $D(30)$

**Proposición 2.2.4.** *Sean $(L_1, \leq)$ y $(L_2, \leq)$ dos conjuntos ordenados. Consideramos en $L_1 \times L_2$ el orden producto. Entonces:*

- *Si $L_1$ y $L_2$ son retículos, también lo es $L_1 \times L_2$. Las operaciones supremo e ínfimo en $L_1 \times L_2$ vienen dadas por*

$$(x_1, x_2) \vee (y_1, y_2) = (x_1 \vee y_1, x_2 \vee y_2) \qquad (x_1, x_2) \wedge (y_1, y_2) = (x_1 \wedge y_1, x_2 \wedge y_2)$$

- *Si $L_1$ y $L_2$ son retículos distributivos, también lo es $L_1 \times L_2$.*
- *Si $L_1$ y $L_2$ son retículos complementados, también lo es $L_1 \times L_2$.*

## 2.3. Álgebras de Boole

### 2.3.1. Generalidades sobre álgebras de Boole

**Definición 16.** *Un* álgebra de Boole *es un retículo distributivo y complementado.*

**Ejemplo 2.3.1.**

1. *Dado un conjunto $X$, el conjunto $\mathcal{P}(X)$, con el orden dado por la inclusión es un álgebra de Boole.*
2. *$D(6)$, o $D(30)$ son álgebras de Boole. No es álgebra de Boole $D(4)$ o $D(12)$.*

Al igual que los retículos se pueden definir sin mencionar el orden, sino únicamente las operaciones supremo e ínfimo, con las respectivas propiedades, un álgebra de Boole puede definirse también a partir de las operaciones $\vee$ y $\wedge$.

**Definición 17** (Segunda definición de álgebra de Boole)**.** *Sea $B$ un conjunto. Supongamos que en $B$ tenemos definidas dos operaciones, $\vee$ y $\wedge$ tales que:*

1. $x \vee (y \vee z) = (x \vee y) \vee z, \qquad x \wedge (y \wedge z) = (x \wedge y) \wedge z.$
2. $x \vee y = y \vee x, \qquad x \wedge y = y \wedge z.$

3. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), \qquad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$

4. $x \vee (x \wedge y) = x, \qquad x \wedge (x \vee y) = x.$

5. *Existen* $0, 1 \in B$ *tales que* $x \vee 0 = x, \quad x \wedge 0 = 0, \quad x \vee 1 = 1, \quad x \wedge 1 = x.$

6. *Para cada* $x \in B$ *existe* $\overline{x} \in B$ *tal que* $x \vee \overline{x} = 1$ *y* $x \wedge \overline{x} = 0.$

Es fácil comprobar que las definiciones 16 y 17 son equivalentes.

**Proposición 2.3.1** (Leyes de De Morgan)**.** *Sea* $B$ *un álgebra de Boole, y* $x, y \in B$*. Entonces:*

$$\overline{x \vee y} = \overline{x} \wedge \overline{y}, \qquad \overline{x \wedge y} = \overline{x} \vee \overline{y}.$$

*Demostración:* Se verifica que:

$$(x \vee y) \vee (\overline{x} \wedge \overline{y}) = [(x \vee y) \vee \overline{x}] \wedge [(x \vee y) \vee \overline{y}] = (x \vee \overline{x} \vee y) \wedge (x \vee y \vee \overline{y}) = (1 \vee y) \wedge (x \vee 1) = 1 \wedge 1 = 1,$$

$$(x \vee y) \wedge (\overline{x} \wedge \overline{y}) = [x \wedge (\overline{x} \wedge \overline{y})] \vee [y \wedge (\overline{x} \wedge \overline{y})] = (0 \wedge \overline{y}) \vee (\overline{x} \wedge 0) = 0 \vee 0 = 0.$$

■

**Ejemplo 2.3.2.**

1. *Consideremos el conjunto* $\mathbb{Z}_2$*. En él, consideramos las operaciones*

$$x \wedge y = xy, \qquad x \vee y = x + y + xy.$$

*Entonces* $\mathbb{Z}_2$*, con estas operaciones es un álgebra de Boole. De hecho, es el álgebra de Boole más simple (a excepción de un álgebra de Boole con un elemento). Representaremos a este álgebra de Boole como* $\mathbb{B}$*.*

*Nótese que este álgebra de Boole se corresponde con el orden* $0 \leq 1$*.*

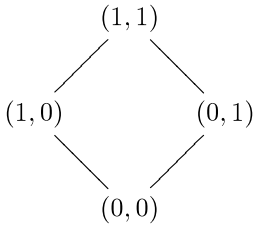
2. *Puesto que el producto de álgebras de Boole es un álgebra de Boole, tenemos, para cada número natural* $n$ *el álgebra de Boole* $\mathbb{B}^n$ *que tiene* $2^n$ *elementos. En este caso, las operaciones del álgebra de Boole vienen dadas por:*

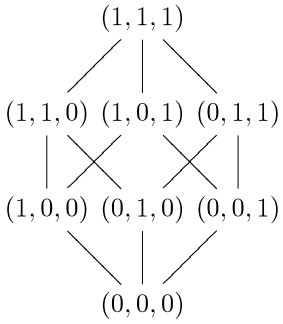
$$(x_1, x_2, \ldots, x_n) \vee (y_1, y_2, \ldots, y_n) = (x_1 \vee y_1, x_2 \vee y_2, \ldots, x_n \vee y_n),$$

$$(x_1, x_2, \ldots, x_n) \wedge (y_1, y_2, \ldots, y_n) = (x_1 \wedge y_1, x_2 \wedge y_2, \ldots, x_n \wedge y_n),$$

$$\overline{(x_1, x_2, \ldots x_n)} = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}).$$

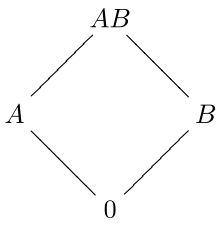
*Veamos los diagramas de Hasse de* $\mathbb{B}^2$ *y* $\mathbb{B}^3$*.*



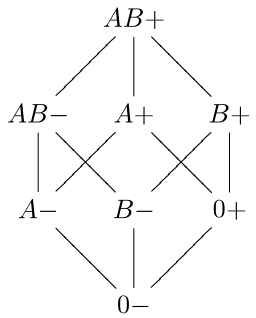

*Podemos comparar las estructuras de álgebra de Boole de* $\mathbb{B}^2$ *y* $\mathbb{B}^3$ *con las de* $\mathcal{P}(\{a, b\})$ *y* $\mathcal{P}(\{a, b, c\})$*.*

*3. Consideramos las álgebras de Boole siguientes:*





*que como podemos ver tienen una estructura semejante a $\mathbb{B}^2$ y $\mathbb{B}$ respectivamente. Su producto, tendrá entonces la misma estructura que $\mathbb{B}^3$. El diagrama de Hasse de dicho álgebra sería*




*y vemos que los elementos que la forman son los ocho grupos sanguíneos. En este caso, ser* menor o igual *significa* puede donar*. Así, el grupo* 0− *es el donante universal, mientras que el grupo* $AB+$ *es el receptor universal.*

**Definición 18.** *Sea $B$ un álgebra de Boole y $x \in B$. Se dice que $x$ es un átomo si $x$ es un elemento minimal de $B \setminus \{0\}$.*

**Nota:** Si $(X, \leq)$ es un conjunto ordenado que tiene mínimo (que llamaremos 0), podemos también definir los átomos de $X$ como los elementos minimales del conjunto $X \setminus \{0\}$.

**Ejemplo 2.3.3.** *Si $X$ es un conjunto, los átomos del álgebra de Boole $\mathcal{P}(X)$ son los subconjuntos unitarios.*

*Los átomos del álgebra de Boole $\mathbb{B}^n$ son aquellos que tienen todas las coordenadas nulas salvo una.*

*En el álgebra de Boole $D(30)$ los átomos son los divisores primos de* 30.

**Teorema 2.3.1.** *Sea $B$ un álgebra de Boole finita, y $x \in B \setminus \{0\}$. Entonces, $x$ se expresa de forma única como supremo de átomos.*

Antes de demostrar el teorema, veamos el siguiente lema:

**Lema 2.3.1.** *Sea $B$ un álgebra de Boole finita y $x \in B \setminus \{0\}$. Entonces existe $a \in B$, átomo, y tal que $a \leq x$.*

*Demostración:* Basta tomar el conjunto $A_x = \{y \in B : 0 < y \leq x\}$, que es distinto del vacío (pues $x$ es un elemento suyo). Se tiene que un elemento minimal de $A_x$ (que existe por ser $A_x$ finito) es un átomo de $B$. ■

Dado cualquier elemento $x \in B \setminus \{0\}$, denotaremos por $\mathcal{A}_x$ al conjunto de todos los átomos de $B$ que son menores o iguales que $x$.

*Demostración:*(teorema 2.3.1)

Supongamos que $\mathcal{A}_x = \{a_1, a_2, \ldots, a_m\}$. Sea entonces $z = a_1 \vee a_2 \vee \ldots \vee a_m$. Comprobemos que $z = x$.

Puesto que $a_i \leq x$ se tiene que $z \leq x$. Supongamos que $z \neq x$.

Consideramos $\overline{z}$. Se tiene entonces que $1 = z \vee \overline{z} \leq x \vee \overline{z}$ de donde $x \vee \overline{z} = 1$. Por tanto, $x \wedge \overline{z} \neq 0$ (si valiera 0 tendríamos que $\overline{z} = \overline{x}$, lo que implicaría que $z = x$).

Sea $a$ un átomo menor o igual que $x \wedge \overline{z}$. Entonces, $a \leq x$, luego $a = a_i$ para algún $i$. Supongamos que $a = a_1$. En ese caso, se tiene que:

$$0 = \overline{z} \wedge z = \overline{z} \wedge (a_1 \vee \cdots \vee a_m) \geq a \wedge (a_1 \vee \cdots \vee a_m) = (a \wedge a_1) \vee (a \wedge a_2) \vee \cdots \vee (a \wedge a_m) = a_1,$$

lo cual no es posible.

Deducimos por tanto que $z = x$, es decir, $x$ se expresa como supremo de átomos.

Supongamos ahora que podemos expresar $x$ como supremo de átomos de la forma $x = b_1 \vee \cdots \vee b_k$. Entonces:

$$b_i = b_i \wedge x = b_i \wedge (a_1 \vee \cdots \vee a_m) = (b_i \wedge a_1) \vee (b_i \wedge a_2) \vee \cdots \vee (b_i \wedge a_m),$$

y puesto que el ínfimo de dos átomos vale cero salvo que los dos átomos coincidan deducimos que $b_i = a_j$ para algún $j$. Por tanto, se tiene que

$$\{b_1, \ldots, b_k\} \subseteq \{a_1, \ldots, a_m\}.$$

De forma análoga se demuestra la otra inclusión. ■

Este teorema nos dice que si $B$ es un álgebra de Boole finita, y $X = \{a_1, \ldots, a_n\}$ son sus átomos (es decir, $X = \mathcal{A}_1$) entonces los elementos de $B$ son:

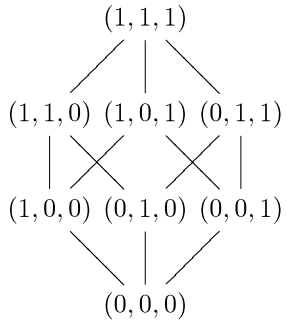
$$B = \left\{ \bigvee_{x \in A} x : \ A \in \mathcal{P}(X) \right\},$$

donde se ha empleado la notación $0 = \bigvee_{x \in \emptyset} x$.

Vemos entonces que $B$ tiene tantos elementos como $\mathcal{P}(X)$. Por tanto, el número de elementos de $B$ es $2^n$, donde $n$ es el número de átomos. Es más, tenemos que las álgebras de Boole $B$, $\mathbb{B}^n$ y $\mathcal{P}(X)$ con $X = \{1, 2, \ldots, n\}$ son isomorfas.

**Ejemplo 2.3.4.**

1. *Consideramos el álgebra de Boole* $\mathbb{B}^3$.

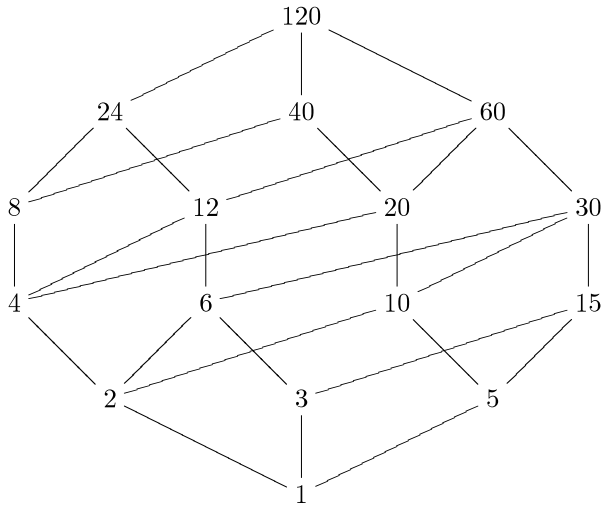



*Vemos que los átomos son* $(1, 0, 0)$, $(0, 1, 0)$ *y* $(0, 0, 1)$. *Si tomamos cualquier elemento distinto de* $(0, 0, 0)$, *por ejemplo,* $(1, 0, 1)$ *podemos comprobar fácilmente que se puede expresar como supremo de átomos. En este caso,* $(1, 0, 1) = (1, 0, 0) \vee (0, 0, 1)$.

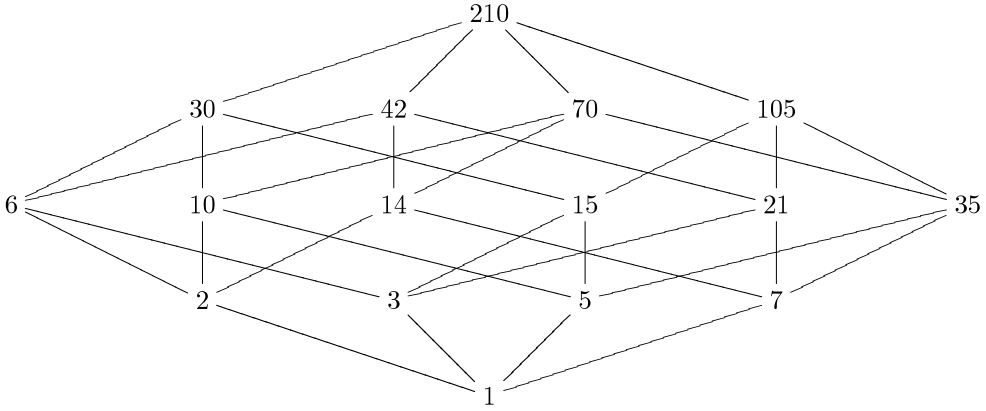
*Con cualquier otro elemento podríamos hacer lo mismo.*

2. *Sean ahora los conjuntos ordenados $D(120)$ y $D(210)$, cuyos diagramas de Hasse son:*

$D(120)$




$D(210)$



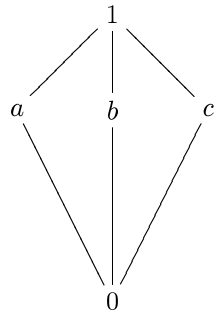

*Los átomos del primer conjunto ordenado serían los elementos $2, 3, 5$. Si tomamos por ejemplo el elemento $30$ vemos que podemos ponerlo como supremo de átomos, pues $30 = 2 \vee 3 \vee 5$. Pero, por ejemplo, si tomamos $x = 20$ vemos que no podemos ponerlo como supremo de átomos. Los átomos que son menores que 20 son 2 y 5, y como podemos comprobar, $2 \vee 5 = 10 \neq 20$.*

*Por tanto, aquí hay elementos que no se pueden poner como supremo de átomos. Esto nos dice que $D(120)$ no es un álgebra de Boole.*

*Los átomos del segundo conjunto son $2, 3, 5, 7$. Podemos tomar cualquier elemento distinto de 1, y comprobar que puede expresarse como supremo de átomos. Por ejemplo: $42 = 2 \vee 3 \vee 7$, $35 = 5 \vee 7$, $105 = 3 \vee 5 \vee 7$.*

*El conjunto de los divisores de 210 es un álgebra de Boole.*

3. *Consideramos el diamante, que sabemos que no es un álgebra de Boole, pues es distributivo.*



*Los átomos aquí serían a, b, c. La situación aquí es que todo elemento (salvo 0) se expresa como supremo de átomos. Pero la forma no es única, pues* $1 = a \vee b = a \vee c = b \vee c = a \vee b \vee c$.

### 2.3.2. Funciones y expresiones booleanas

**Definición 19.** *Una función booleana con n variables es una aplicación* $f : \mathbb{B}^n \to \mathbb{B}$.
*Denotaremos por* $\mathcal{F}_n$ *al conjunto de las funciones booleanas con n variables. Es decir:*

$$\mathcal{F}_n = \{f : \mathbb{B}^n \to \mathbb{B} \quad f \text{ es aplicación}\}.$$

**Ejemplo 2.3.5.**

1. *La aplicación* $f : \mathbb{B} \to \mathbb{B}$ *dada por* $f(0) = 1$; $f(1) = 0$ *es una función booleana en* 1 *variable (es decir, un elemento de* $\mathcal{F}_1$. *Esta aplicación responde a la expresión* $f(x) = \overline{x}$.

2. *Sea* $f : \mathbb{B}^2 \to \mathbb{B}$ *la aplicación* $f(x, y) = x \vee y$. *Entonces f es una aplicación booleana en* 2 *variables* ($f \in \mathcal{F}_2$). *Esta aplicación, elemento a elemento es:*

$$(0,0) \mapsto 0, \qquad (1,0) \mapsto 1, \qquad (0,1) \mapsto 1, \qquad (1,1) \mapsto 1.$$

**Definición 20.** *Dadas* $f, g : \mathbb{B}^n \to \mathbb{B}$ *se dice que* $f \leq g$ *si* $f(x_1, x_2, \ldots, x_n) \leq g(x_1, x_2, \ldots x_n)$ *para todo* $(x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$.

Es fácil comprobar que esta relación convierte a $\mathcal{F}_n$ en un álgebra de Boole. Las operaciones *supremo* e *ínfimo*, así como el complementario vienen dador por

$$f \vee g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \vee g(x_1, \ldots x_n),$$

$$f \wedge g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \wedge g(x_1, \ldots x_n),$$

$$\overline{f}(x_1, \ldots, x_n) = \overline{f(x_1, \ldots, x_n)},$$

mientras que el máximo y el mínimo son las aplicaciones constantes 1 y 0 respectivamente.

Los átomos de este álgebra de Boole son las aplicaciones que valen 1 en un elemento de $\mathbb{B}^n$, y 0 en el resto. Puesto que en $\mathbb{B}^n$ hay $2^n$ elementos, tenemos que $\mathcal{F}_n$ tiene $2^n$ átomos, lo que nos dice que $\mathcal{F}_n$ tiene $2^{2^n}$ elementos.

**Ejemplo 2.3.6.**

1. *El álgebra* $\mathcal{F}_1$ *tiene* $2^2 = 4$ *elementos. Éstos son:*

$$\begin{array}{cccc} 0 \mapsto 0 & 0 \mapsto 0 & 0 \mapsto 1 & 0 \mapsto 1 \\ 1 \mapsto 0 & 1 \mapsto 1 & 1 \mapsto 0 & 1 \mapsto 1. \end{array}$$

   *Los átomos son las aplicaciones segunda y tercera.*

2. *El álgebra* $\mathcal{F}_2$ *tiene* 4 *átomos, y por tanto* 16 *elementos. Los átomos son:*

$$\begin{array}{cccc} (0,0) \mapsto 1 & (0,0) \mapsto 0 & (0,0) \mapsto 0 & (0,0) \mapsto 0 \\ (1,0) \mapsto 0 & (1,0) \mapsto 1 & (1,0) \mapsto 0 & (1,0) \mapsto 0 \\ (0,1) \mapsto 0 & (0,1) \mapsto 0 & (0,1) \mapsto 1 & (0,1) \mapsto 0 \\ (1,1) \mapsto 0 & (1,1) \mapsto 0 & (1,1) \mapsto 0 & (1,1) \mapsto 1. \end{array}$$

### 2.3.3. Expresiones booleanas

**Definición 21.** *Sea $S$ un conjunto. Se definen las expresiones booleanas sobre el conjunto $S$ de forma recursiva como sigue:*

1. *Si $x \in S \cup \{0,1\}$ entonces $x$ es una expresión booleana.*
2. *Si $e_1, e_2$ son expresiones booleanas, entonces también lo son $e_1 \vee e_2$, $e_1 \wedge e_2$ y $\overline{e_1}$.*

*A las expresiones booleanas que sean elementos de $S$, o complementos suyos, los denominaremos* literales.

**Ejemplo 2.3.7.** *Si $S = \{x, y, z\}$ son expresiones booleanas $x$, $x \vee z$, $\overline{x \wedge \overline{y}}$, $1$.*
*Son literales, $x$, $\overline{z}$, $z$.*

A la hora de representar las expresiones booleanas, emplearemos la notación $x\,y$ o $x{\cdot}y$ para la expresión $x \wedge y$, mientras que usaremos la notación $x + y$ para la expresión $x \vee y$.
Así, la expresión booleana $x \vee (y \wedge \overline{z})$ la representaremos como $x + (y\,\overline{z})$.

Supongamos que tenemos un conjunto $S$ con $n$ elementos, es decir, $S = \{x_1, x_2, \ldots, x_n\}$. A cada elemento de $S$ le vamos a asignar un elemento de $\mathcal{F}_n$. Concretamente, al elemento $x_i$ le asignamos la función $x_i : \mathbb{B}^n \to \mathbb{B}$ dada por $x_i(a_1, \ldots, a_i, \ldots, a_n) = a_i$. De esta forma, a cada expresión booleana sobre el conjunto $S$ le podemos hacer corresponder una función $\mathbb{B}^n \to \mathbb{B}$.
Por ejemplo, si $S = \{x, y, z\}$ y consideramos la expresión booleana $x \vee (\overline{y} \wedge z)$, le corresponde la función booleana

$$\begin{array}{ll} (0,0,0) \mapsto 0 \vee (1 \wedge 0) = 0, & (0,0,1) \mapsto 0 \vee (1 \wedge 1) = 1, \\ (0,1,0) \mapsto 0 \vee (0 \wedge 0) = 0, & (0,1,1) \mapsto 0 \vee (0 \wedge 1) = 0, \\ (1,0,0) \mapsto 1 \vee (1 \wedge 0) = 1, & (1,0,1) \mapsto 1 \vee (1 \wedge 1) = 1, \\ (1,1,0) \mapsto 1 \vee (0 \wedge 0) = 1, & (1,1,1) \mapsto 1 \vee (0 \wedge 1) = 1. \end{array}$$

Puesto que cada expresión booleana determina una función booleana, podremos referirnos a las funciones mencionando las expresiones que las representan. Así, la función que acabamos de ver podría definirse como $f(x, y, z) = x \vee (\overline{y} \wedge z)$. Ahora, para calcular la imagen de un elemento de $\mathbb{B}^3$ basta sustituir en la expresión booleana $x$, $y$ y $z$ por los valores en los que queremos evaluar, y efectuar las operaciones en el álgebra de Boole $\mathbb{B}$. Por ejemplo

$$f(0,0,1) = 0 \vee (\overline{0} \wedge 1) = 0 \vee (1 \wedge 1) = 0 \vee 1 = 1.$$

Nótese que en el Ejemplo 2.3.5 ya se ha empleado esta forma de definir una función booleana.
Si ahora quisiéramos emplear la notación introducida anteriormente, la función $f$ adoptaría la forma $f(x, y, z) = x + (\overline{y}\,z)$.
A la hora de emplear esta notación hemos de tener cuidado en no confundir con las operaciones suma y producto hecho en $\mathbb{Z}_2$. En relación al producto no hay problema, pues vimos como la operación $\wedge$ se corresponde con el producto en $\mathbb{Z}_2$. Sin embargo, en $\mathbb{Z}_2$ se tiene que $x \vee y = x + y + x\,y$, lo cual hace que la operación $+$ difiera de la operación $\vee$, pues $1 + 1 = 0$ mientras que $1 \vee 1 = 1$. Para el resto de parejas, ambas operaciones coinciden ($0 + 0 = 0 \vee 0$; $0 + 1 = 0 \vee 1$; $1 + 0 = 1 \vee 0$). El contexto nos aclarará en cada caso si al emplear el símbolo $+$ nos estamos refiriendo a la suma (en $\mathbb{Z}_2$) o al supremo (en $\mathbb{B}$).
Por ejemplo, si decimos *sea $f$ la función booleana dada por $f(x, y, z) = x\,y + y\,\overline{z}$* está claro que nos referimos al supremo. En tal caso, se tiene que

$$f(0,1,1) = 0 \cdot 1 + 1 \cdot 0 = 0 + 0 = 0 \qquad f(1,1,0) = 1 \cdot 1 + 1 \cdot 1 = 1 + 1 = 1$$

**Definición 22.** *Dos expresiones booleanas son equivalentes si las correspondientes funciones booleanas son iguales. Si $e_1$ e $e_2$ son expresiones booleanas equivalentes emplearemos el símbolo $e_1 = e_2$.*

**Ejemplo 2.3.8.** *Las expresiones booleanas* $\overline{x}\,\overline{y}$ *y* $\overline{x+y}$ *son equivalentes. También lo son las expresiones* $x+y+\overline{x}\,\overline{y}$ *y* $1$*.*

A continuación vamos a dar una tabla de expresiones equivalentes.

**Proposición 2.3.2.** *Sean* $e_1$*,* $e_2$ *y* $e_3$ *tres expresiones booleanas en* $n$ *variables. Entonces:*

| | | |
|---|---|---|
| 1. | $e_1+(e_2+e_3)=(e_1+e_2)+e_3$ | $e_1\cdot(e_2\cdot e_3)=(e_1\cdot e_2)\cdot e_3$ |
| 2. | $e_1+e_2=e_2+e_1$ | $e_1\cdot e_2=e_2\cdot e_1$ |
| 3. | $e_1+e_1=e_1$ | $e_1\cdot e_1=e_1$ |
| 4. | $e_1\cdot(e_2+e_3)=e_1\cdot e_2+e_1\cdot e_3$ | $e_1+(e_2\cdot e_3)=(e_1+e_2)\cdot(e_1+e_3)$ |
| 5. | $\overline{e_1+e_2}=\overline{e_1}\cdot\overline{e_2}$ | $\overline{e_1\cdot e_2}=\overline{e_1}+\overline{e_2}$ |
| 6. | $e_1+\overline{e_1}=1$ | $e_1\cdot\overline{e_1}=0$ |
| 7. | $e_1+1=1$ | $e_1\cdot 0=0$ |
| 8. | $e_1+0=e_1$ | $e_1\cdot 1=e_1$ |
| 9. | $\overline{1}=0$ | $\overline{0}=1$ |

**Definición 23.** *Sea* $S=\{x_1,x_2,\ldots,x_n\}$*. Un* minterm *en* $n$ *variables es el producto de* $n$ *literales, cada uno con una variable diferente.*

**Ejemplo 2.3.9.** *Si* $S=\{x,y,z\}$*, entonces son minterm* $x\,y\,z$*,* $x\,\overline{y}\,\overline{z}$*,* $\overline{x}\,y\,z$*. No son minterm* $x\,y$*,* $x\,y\,\overline{y}$ *ni* $x\,z\,x$*.*

**Lema 2.3.2.** *Sea* $m$ *un minterm en* $n$ *variables. Entonces* $m$ *determina una función booleana* $f:\mathbb{B}^n\to\mathbb{B}$ *que vale* $1$ *en un elemento de* $\mathbb{B}^n$ *y* $0$ *en el resto.*

**Ejemplo 2.3.10.** *Sea* $f:\mathbb{B}^2\to\mathbb{B}$ *la función booleana dada por* $f(x,y)=x\,\overline{y}$*. Claramente* $x\,\overline{y}$ *es un minterm. Se tiene que* $f(1,0)=1$*, mientras que* $f(0,0)=f(0,1)=f(1,1)=0$*.*

**Corolario 2.3.1.** *Los minterm son los átomos del álgebra* $\mathcal{F}_n$*.*

**Corolario 2.3.2.** *Toda función booleana se expresa de forma única (salvo el orden) como suma (supremo) de minterm.*

La expresión de una función booleana como suma de minterm recibe el nombre de *forma normal disyuntiva*. Para hallar la forma normal disyuntiva de una función booleana podemos emplear dos métodos.

El primero consiste en evaluar la función en todos los elementos de $\mathbb{B}^n$, y observar en cuales de ellos toma el valor 1. Cada uno de esos elementos se corresponde con un minterm.

El segundo consiste en, a partir de una expresión booleana que nos defina a $f$, utilizar las equivalencias dadas en la proposición 2.3.2 para transformar la expresión en una suma de minterm.

**Ejemplo 2.3.11.** *Vamos a expresar como supremo de minterm la función booleana dada por* $f(x,y)=x+y$*.*

1. *Si queremos emplear el primer método, evaluamos la función en los cuatro elementos de* $\mathbb{B}^2$*. Nos queda:*

$$f(0,0)=0+0=0\qquad f(0,1)=0+1=1\qquad f(1,0)=1+0=1\qquad f(1,1)=1+1=1$$

*El elemento* $(0,1)$ *se corresponde con el minterm* $\overline{x}\,y$*, el* $(1,0)$ *con* $x\,\overline{y}$ *mientras que* $(1,1)$ *se corresponde con* $x\,y$*. Por tanto tenemos que* $f(x,y)=\overline{x}\,y+x\,\overline{y}+x\,y$*.*

*2. Empleamos ahora el segundo método. En este caso*

$$\begin{aligned} f(x,y) &= x+y \\ &= x\cdot 1 + 1\cdot y && \textit{(equivalencias 8 y 2)} \\ &= x(y+\overline{y}) + (x+\overline{x})y && \textit{(equivalencia 6)} \\ &= x\,y + x\,\overline{y} + x\,y + \overline{x}\,y && \textit{(equivalencias 4 y 2)} \\ &= x\,y + x\,y + x\,\overline{y} + \overline{x}\,y && \textit{(equivalencia 2)} \\ &= x\,y + x\,\overline{y} + \overline{x}\,y && \textit{(equivalencia 3).} \end{aligned}$$

Cada elemento de $\mathbb{B}^n$ es una secuencia de $n$ dígitos *ceros* o *unos*. Es por tanto, la expresión en binario de un número entre 0 y $2^n-1$. Por otra parte, a cada elemento de $\mathbb{B}^n$ le corresponde un minterm (aquél para el que toma el valor 1). Por tanto, cada minterm está determinado por un número comprendido entre 0 y $2^n-1$. Denotaremos por *el minterm* $a$, donde $0 \le a \le 2^{n-1}$, y lo representaremos como $m(a)$ o $m_a$, al minterm determinado por el número $a$ siguiendo el criterio anterior.

Por ejemplo, el minterm $x\,y\,\overline{z}\,\overline{t}$ toma el valor 1 en $(1,1,0,0)$. Puesto que $12 = (1100)_2$ tenemos que $x\,y\,\overline{z}\,\overline{t}$ es el minterm 12, o dicho de otra forma, $x\,y\,\overline{z}\,\overline{t} = m_{12} = m(12)$.

**Ejemplo 2.3.12.** *La función booleana del ejemplo anterior $f(x,y) = x+y$ hemos visto que se expresa como suma de minterm de la forma $f(x,y) = x\,y + x\,\overline{y} + \overline{x}\,y$. Empleando la notación recién introducida nos quedaría $f(x,y) = m_3 + m_2 + m_1$, o si preferimos $f(x,y) = m_1 + m_2 + m_3$.*

*También se suele emplear la notación $f(x,y) = \sum m(1,2,3)$.*

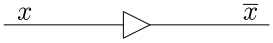
De la misma forma que toda función booleana se expresa de forma única como suma de minterm, se puede probar que toda función booleana se expresa de forma única como producto de maxterm. Una expresión de esta forma se denomina *forma canónica conjuntiva.*

Un maxtern es una suma de $n$ literales. Se corresponde con una función booleana que vale 1 en todos los elementos de $\mathbb{B}^n$ salvo en uno, en el que vale 0. Este elemento determina al maxterm.

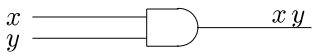
### 2.3.4. Puertas lógicas

En este apartado utilizaremos las funciones booleanas para el diseño de circuitos lógicos. Los elementos básicos de estos circuitos se llaman *puertas lógicas.* Aquí emplearemos tres tipos de puertas lógicas, cada una correspondiente a una operación booleana, y las combinaremos para diseñar circuitos que realicen una serie de tareas. Las puertas básicas a emplear son:

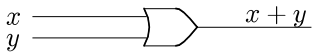
La puerta **NOT** que tiene como entrada el valor de una variable booleana y produce como salida el complementario de dicho valor. Para una puerta NOT emplearemos el siguiente símbolo.



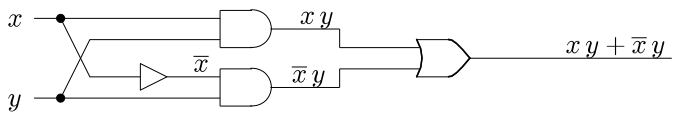

La puerta **AND** que tiene como entrada el valor de dos o más variables booleanas, y como salida el producto de éstas. Las entradas se muestran a la izquierda y la salida a la derecha. Emplearemos el siguiente símbolo para esta puerta.




La puerta **OR** tiene como entrada el valor de dos o más variables booleanas, y como salida la suma de éstas. La representaremos mediante el siguiente símbolo.



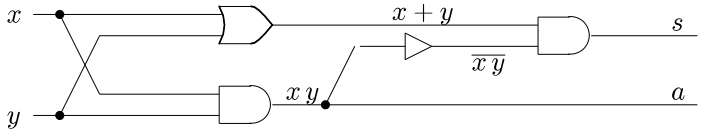

**Ejemplo 2.3.13.** *Vamos a diseñar un circuito con dos entradas y que produzca la salida $x\,y + \overline{x}\,y$.*




*Nótese que puesto que $x\,y + \overline{x}\,y = (x+\overline{x})y = 1\cdot y = y$ podría haberse diseñado un circuito mucho más simple que tuviera el mismo efecto.*

A continuación vamos a diseñar un circuito que, introducidos dos números en binario nos devuelve su suma.

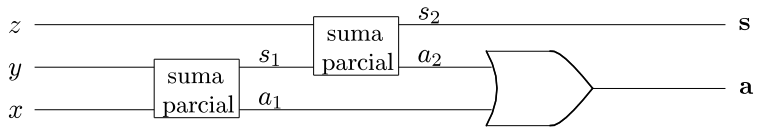
Para esto, comenzamos en primer lugar diseñando un circuito que, dados dos dígitos binarios nos devuelva la suma. Puesto que los posibles resultados de la suma son 0, 1 y 10 necesitamos un circuito que tenga dos salidas. Denotaremos el bit de la derecha como $s$ (suma) y el de la izquierda como $a$ (acarreo). Se tiene entonces que $s = \overline{x}\,y + x\,\overline{y} = (x+y)\overline{x\,y}$ mientras que $a = x\,y$. Un circuito podría ser entonces:




Denominaremos a este circuito como *suma parcial*.

Construyamos ahora un circuito que nos sume dos dígitos binarios más el posible acarreo de una suma anterior. Podemos ver fácilmente que esto es equivalente a sumar tres dígitos binarios $x$, $y$ y $z$. El resultado será, como antes una salida doble. A las dos salidas las denotaremos de la misma forma que en el caso anterior: $s$ y $a$.

Para obtener la salida $s$, obtenemos la suma de $x$ e $y$, y al resultado le sumamos $z$. Puede verse entonces que un circuito que nos da la suma de tres dígitos sería:

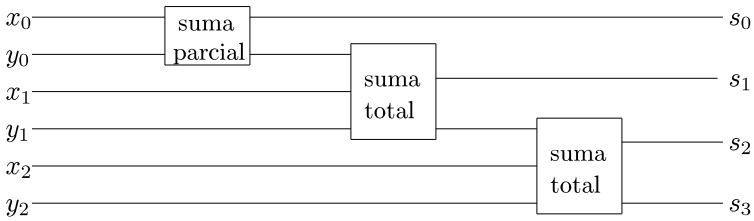



| $x$ | $y$ | $z$ | $s_1$ | $a_1$ | $s_2$ | $a_2$ | **s** | **a** | $a_1 + a_2$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |

pues como podemos apreciar, $\mathbf{s} = s_2$ y $\mathbf{a} = a_1 + a_2$.

Denotaremos a este circuito como *suma total*.

Veamos ahora como calcular la suma de dos números entre 0 y 7. Supongamos que estos números se escriben en binario como $x_2x_1x_0$ e $y_2y_1y_0$. Su suma, escrita en binario es $s_3s_2s_1s_0$.

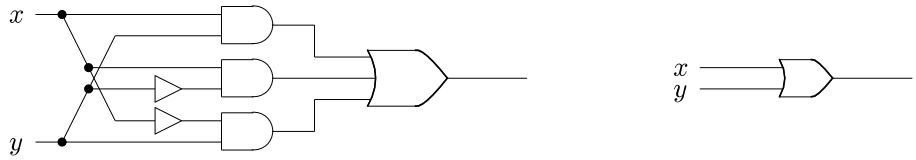



## 2.3.5. Optimización de funciones booleanas

Hemos visto en la subsección anterior como a partir de la representación de una función booleana en $n$ variables haciendo uso de una expresión booleana podemos diseñar un circuito que nos devuelva el resultado de aplicar la función a las $n$ variables.

Puesto que cualquier función booleana puede expresarse como suma de minterm, podemos diseñar cualquier circuito empleando las tres puertas NOT, OR y AND. Sin embargo, la expresión de una función como suma de minterm no es en general la más apropiada pues requiere de muchas operaciones, lo que se traduce en la necesidad de emplear gran cantidad de puertas.

Así, por ejemplo, los siguientes circuitos producen el mismo efecto sobre las entrada $x, y$.




pues el primer circuito responde a la función $x\,y + x\,\overline{y} + \overline{x}\,y$, mientras que el segundo a $x + y$, que vimos anteriormente que son iguales.

Lo que pretendemos es, a partir de una expresión de suma de minterm, transformarla en otra expresión equivalente con menos sumandos y menor productos en los sumandos. Vamos a estudiar dos métodos para este propósito. Por una parte, los mapas de Karnaugh, y por otra parte el método de Quine-McCluskey.

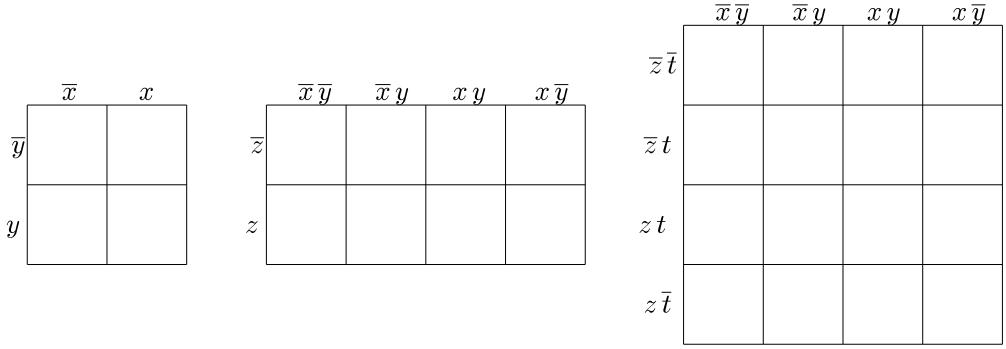
Referente al primero, decir que es un método eficiente para funciones de no más de cuatro variables, mientras que puede utilizarse hasta funciones de seis variables.

En cuanto al segundo, aunque realiza la optimización de forma automática, y podría implementarse como un programa informático, el algoritmo, para un número grande de variables booleanas, es computacionalmente muy costoso.

### Mapas de Karnaugh

En primer lugar veremos qué es un mapa de Karnaugh, y posteriormente veremos cómo utilizarlos para optimizar las expresiones booleanas.

Un mapa de Karnaugh para una función booleana de dos, tres o cuatro variables es una tabla con tantas celdas como posibles minterm (4 para dos variables, 8 para tres variables y 16 para cuatro variables). Cada celda va asociada a un minterm, y dos celdas adyacentes se diferencian únicamente en un literal, así como dos celdas opuestas en una fila o una columna.




Por ejemplo, en el mapa correspondiente a 4 variables, las cuatro celdas adyacentes a $\overline{x}\,y\,\overline{z}\,t$ son: por la derecha, $x\,y\,\overline{z}\,t$, por arriba, $\overline{x}\,y\,\overline{z}\,\overline{t}$, por la izquierda, $\overline{x}\,\overline{y}\,\overline{z}\,t$ y por abajo, $\overline{x}\,y\,z\,t$. Vemos como cada una de estas celdas se diferencia de $\overline{x}\,y\,\overline{z}\,t$ en sólo un literal ($\overline{x} - x$ en la primera, $t - \overline{t}$ en la segunda, $y - \overline{y}$ en la tercera y $\overline{z} - z$ en la cuarta).

Vemos también como las celdas opuestas de la misma fila se diferencian también en sólo un literal (en la segunda fila, estas celdas opuestas son $\overline{x}\,\overline{y}\,\overline{z}\,t$ y $x\,\overline{y}\,\overline{z}\,t$), así como las celdas opuestas de una columna.

Si ahora tenemos una función booleana en dos, tres o cuatro variables, su mapa de Karnaugh consiste en la tabla antes descrita, en la que se han destacado aquellas celdas correspondientes a los minterm que aparecen en la forma normal disyuntiva de la función. Nosotros aquí las marcaremos con un 1.

**Ejemplo 2.3.14.** *Vamos a dibujar los mapas de Karnaugh de las funciones booleanas:* $f(x,y) = x\,\overline{y} + \overline{x}\,\overline{y}$; $f(x,y,z) = (\overline{x} + \overline{y})(y\,\overline{z}) + \overline{y}\,\overline{z}$; $f(x,y,z,t) = x\,y\,\overline{z}\,\overline{t} + x\,\overline{y}\,z\,t + x\,y\,z\,\overline{t} + x\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t} + x\,\overline{y}\,z\,\overline{t} + x\,y\,\overline{z}\,t$.

| | $\overline{x}$ | $x$ |
|---|---|---|
| $\overline{y}$ | *1* | *1* |
| $y$ | | |

$x\,\overline{y} + \overline{x}\,\overline{y}$

| | $\overline{x}\,\overline{y}$ | $\overline{x}\,y$ | $x\,y$ | $x\,\overline{y}$ |
|---|---|---|---|---|
| $\overline{z}$ | 1 | | 1 | 1 |
| $z$ | 1 | 1 | 1 | 1 |

$(\overline{\overline{x} + \overline{y}})(y\,\overline{z}) + \overline{y}\,\overline{z}$

| | $\overline{x}\,\overline{y}$ | $\overline{x}\,y$ | $x\,y$ | $x\,\overline{y}$ |
|---|---|---|---|---|
| $\overline{z}\,\overline{t}$ | | | 1 | |
| $\overline{z}\,t$ | | | 1 | |
| $z\,t$ | | | 1 | 1 |
| $z\,\overline{t}$ | 1 | | 1 | 1 |

$x\,y\,\overline{z}\,\overline{t} + x\,\overline{y}\,z\,t + x\,y\,z\,\overline{t} + x\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t} + x\,\overline{y}\,z\,\overline{t} + x\,y\,\overline{z}\,t$

Una vez dibujado el mapa de Karnaugh de una función booleana, se buscan los 1 que aparezcan en celdas adyacentes (u opuestas en una misma fila o columna). Dos de estas celdas se transforman en un único producto en el que ha desaparecido el literal en que difieren. Así, en el ejemplo del mapa de Karnaugh para la función de dos variables, tenemos dos "unos" adyacentes, situados en las celdas $x\,\overline{y}$ y $\overline{x}\,\overline{y}$. Estas dos celdas dan lugar a un producto en el que desaparece el literal diferente ($x$, $\overline{x}$), quedando entonces la expresión booleana $\overline{y}$. Obviamente, lo único que estamos haciendo es la transformación $x\,\overline{y} + \overline{x}\,\overline{y} = (x + \overline{x})\overline{y} = 1 \cdot \overline{y} = \overline{y}$, donde se ha empleado la propiedad distributiva, la definición de complementario y de 1. Los mapas de Karnaugh constituyen una representación gráfica de una función booleana que ayuda a encontrar los minterm que podemos agrupar.

De la misma forma, si encontramos cuatro "unos" adyacentes, formando, bien un cuadrado, bien una línea (fila o columna), podemos sustituirlos por un solo producto en el que se eliminan los dos litereles que difieren en esas cuatro celdas.

El objetivo es tratar de agrupar los "unos" en el menor número posible de bloques, y de mayor tamaño.

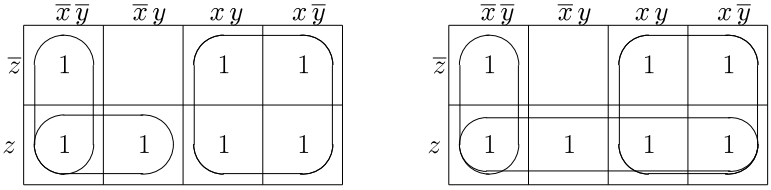
Vamos a optimizar las dos funciones que hemos representado mediante mapas de Karnaugh en el ejemplo anterior. En primer lugar consideramos la función $f : \mathbb{B}^3 \to \mathbb{B}$ dada por $f(x, y, z) = (\overline{\overline{x} + \overline{y}})(y\,\overline{z}) + \overline{y}\,\overline{z}$.

Su mapa de Karnaugh es:

| | $\overline{x}\,\overline{y}$ | $\overline{x}\,y$ | $x\,y$ | $x\,\overline{y}$ |
|---|---|---|---|---|
| $\overline{z}$ | 1 | | 1 | 1 |
| $z$ | 1 | 1 | 1 | 1 |

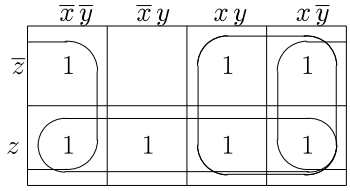
y vemos que podemos agrupar en 3 bloques, lo que da lugar a tres sumandos, que son $\overline{x}\,\overline{y}$, $\overline{x}\,y\,z$ y $x$. Es decir, $f(x, y, z) = \overline{x}\,\overline{y} + \overline{x}\,y\,z + x$.

Vemos también que podemos hacer otras agrupaciones en 3 bloques. Por ejemplo,




que dan lugar a las expresiones $f(x,y,z) = \overline{x}\,\overline{y} + \overline{x}\,z + x$ o a $f(x,y,z) = \overline{x}\,\overline{y} + z + x$.

Sin embargo, no olvidemos que también se consideran adyacentes las celdas opuestas de una misma fila. Podemos entonces agrupar en los siguientes bloques:



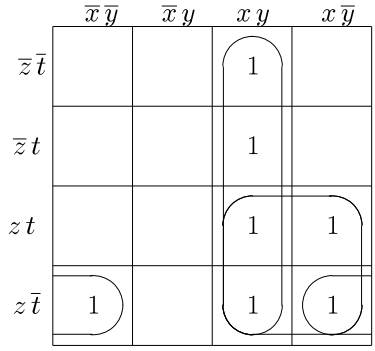

lo que da lugar a la expresión $f(x,y,z) = x + \overline{y} + z$.

Podemos apreciar como en todas las optimizaciones obtenidas hemos obtenido tres sumandos. Sin embargo, esta última parece mejor, pues es la que tiene menos productos en cada sumando. Esto viene de haber obtenido los bloques más grandes.

Por último, vamos a optimizar la función $f : \mathbb{B}^4 \to \mathbb{B}$ dada por

$$f(x,y,z,t) = x\,y\,\overline{z}\,\overline{t} + x\,\overline{y}\,z\,t + x\,y\,z\,\overline{t} + x\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t} + x\,\overline{y}\,z\,\overline{t} + x\,y\,\overline{z}\,t$$

Para esto, agrupamos los "unos" del mapa de Karnaugh por bloques:




lo que da lugar a la expresión $f(x,y,z,t) = x\,y + x\,z + \overline{y}\,z\,\overline{t}$.

**Método de Quine - McCluskey**

Acabamos de ver cómo los mapas de Karnaugh nos ayudan a minimizar el desarrollo de una función booleana como suma de productos. Sin embargo, este método se basa en la visualización de la función en un diagrama, y es poco eficiente para funciones de más de cuatro variables. Sería conveniente tener un proceso que pudiera automatizarse. El método de Quine-McCluskey se ajusta a esta condición. El método consta de dos partes. En una primera, se determinan que términos son candidatos a que aparezcan en un desarrollo minimal. En la segunda se seleccionan de estos candidatos los que intervienen en dicho desarrollo.

Describamos a continuación el método.

Sabemos que cada minterm en $n$ variables va unido a una secuencia de $n$ bits. En primer lugar, dada una función booleana como suma de minterm, ordenamos las cadenas de bits en una columna, agrupando aquellos en los que aparecen igual cantidad de "unos".

Comparamos las cadenas de un grupo con las del grupo inmediatamente inferior. Si encontramos dos cadenas que difieren únicamente en un bit, las marcamos y, en una columna situada a la derecha, representamos estas dos cadenas por una nueva en la que sustituimos el bit diferente por $-$. Si aparecieran dos cadenas iguales, se deja únicamente una.

Una vez realizadas todas las comparaciones posibles, en esta nueva columna repetimos el proceso.

Se continúa así hasta que no podamos obtener una nueva columna.

Se seleccionan aquellas cadenas que no hayan sido marcadas.

Veamos esto con un ejemplo.

**Ejemplo 2.3.15.** *Sea la expresión booleana* $x\,y\,z + \overline{x}\,y\,z + \overline{x}\,\overline{y}\,z + \overline{x}\,\overline{y}\,\overline{z} + x\,\overline{y}\,z$

*Cada minterm lo representamos mediante una cadena de tres dígitos binarios. Estos son* 111, 011, 001, 000 *y* 101. *Ordenamos las cadenas en una columna, situando en primer lugar la que tiene* 3 *"unos", a continuación las que tienen* 2 *"unos" y así sucesivamente.*

| |
|---|
| 111 |
| 011 |
| 101 |
| 001 |
| 000 |

*Comparamos la cadena del primer nivel con las de segundo. Resulta que hay* 2 *de las que se diferencia en un único dígito. Sustituimos este dígito por* $-$, *luego nos queda* $-11$ *y* $1-1$.

*Comparamos las cadenas del segundo y tercer nivel, y vemos que* 101 *y* 001 *se diferencian en un único dígito. Esto da lugar a la cadena* $-01$. *Por último, comparamos la del tercer nivel con el cuarto, lo que nos da* $00-$.

*Ordenamos todos estos datos en una nueva columna y todas las cadenas de esta columna que han intervenido en alguna de la segunda las marcamos.*

| | |
|---|---|
| $\sim 111$ | $-11$ |
| $\sim 011$ | $1-1$ |
| $\sim 101$ | $0-1$ |
| $\sim 001$ | $-01$ |
| $\sim 000$ | $00-$ |

*Repetimos aquí el proceso con la segunda columna*

| | | |
|---|---|---|
| $\sim 111$ | $\sim -11$ | $--1$ |
| $\sim 011$ | $\sim 1-1$ | |
| $\sim 101$ | $\sim 0-1$ | |
| $\sim 001$ | $\sim -01$ | |
| $\sim 000$ | $00-$ | |

*Las cadenas a seleccionar son entonces las no marcadas, es decir,* $--1$ *y* $00-$, *que se corresponden con los términos* $z$ *y* $\overline{x}\,\overline{y}$.

La segunda parte de este método consiste en encontrar, de todos los productos booleanos, el menor conjunto de ellos que represente a la expresión booleana dada. Para ello, hacemos una tabla en la que, en el eje horizontal situamos los minterm que nos definían la expresión booleana, mientras que en el eje vertical situamos los productos booleanos que hemos seleccionado en la primera parte. A continuación señalamos las celdas que se correspondan con un producto booleano y un minterm con la condición de que todos los literales que intervienen en el producto booleano también se encuentren en el minterm.

Una vez hecho esto, elegimos la menor cantidad de productos booleanos de forma que uniendo las celdas que están señaladas en sus filas podamos completar una fila completa de la tabla. De haber varias posibles elecciones, nos quedamos con aquellas en que los productos booleanos tengan la menor cantidad posible de literales.

**Ejemplo 2.3.16.** *En el ejemplo anterior, la tabla nos quedaría como sigue:*

| | $x\,y\,z$ | $x\,\overline{y}\,z$ | $\overline{x}\,y\,z$ | $\overline{x}\,\overline{y}\,z$ | $\overline{x}\,\overline{y}\,\overline{z}$ |
|---|---|---|---|---|---|
| $z$ | $X$ | $X$ | $X$ | $X$ | |
| $\overline{x}\,\overline{y}$ | | | | $X$ | $X$ |

*Vemos como aquí necesitamos los dos productos booleanos para rellenar una fila.*

*Después de todo esto deducimos que:*

$$x\,y\,z + \overline{x}\,y\,z + \overline{x}\,\overline{y}\,z + \overline{x}\,\overline{y}\,\overline{z} + x\,\overline{y}\,z = \overline{x}\,\overline{y} + z$$

Veamos a continuación un ejemplo completo.

**Ejemplo 2.3.17.** *Dada la expresión booleana* $x\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,y\,\overline{z}\,t + x\,\overline{y}\,z\,\overline{t} + \overline{x}\,\overline{y}\;z\,t + \overline{x}\,\overline{y}\,\overline{z}\,t + \overline{x}\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t}$ *vamos a tratar de encontrar una expresión óptima mediante el método de Quine-McCluskey.*

*Las cadenas de bits correspondientes a cada uno de los minterm son* 0111, 0101, 1010, 0011, 0001, 0111 *y* 0010. *A partir de ellas construimos la tabla:*

| | | | | |
|---|---|---|---|---|
| $a\ b$ | $\sim$ *0111* | $1$ | $\sim$ *01-1* | *0- -1* |
| $a\ c$ | $\sim$ *0101* | $2$ | $\sim$ *0-11* | |
| $d\ e$ | $\sim$ *1010* | $2$ | $\sim$ *0-01* | |
| $b\ f\ g$ | $\sim$ *0011* | | *10-0* | |
| $d$ | $\sim$ *1000* | | *-010* | |
| $c\ f$ | $\sim$ *0001* | $1$ | $\sim$ *00-1* | |
| $e\ g$ | $\sim$ *0010* | | *001-* | |

*A la izquierda de cada una de las cadenas marcadas hemos colocado unas letras (columna de la izquierda) o números (columna central) que nos indican cada cadena con cual se empareja para formar una cadena en la columna que tiene más a la derecha.*

*A partir de aquí seleccionamos las cadenas que no están marcadas, que se corresponden con los productos* $x\,\overline{y}\,\overline{t}$; $\overline{y}\,z\,\overline{t}$; $\overline{x}\,\overline{y}\,z$; $\overline{x}\,t$. *Esto nos da la siguiente tabla:*

| | $x\,\overline{y}\,\overline{z}\,\overline{t}$ | $\overline{x}\,y\,\overline{z}\,t$ | $x\,\overline{y}\,z\,\overline{t}$ | $\overline{x}\,\overline{y}\;z\,t$ | $\overline{x}\,\overline{y}\,\overline{z}\,t$ | $\overline{x}\,y\,z\,t$ | $\overline{x}\,\overline{y}\,z\,\overline{t}$ |
|---|---|---|---|---|---|---|---|
| $x\,\overline{y}\,\overline{t}$ | $X$ | | $X$ | | | | |
| $\overline{y}\,z\,\overline{t}$ | | | $X$ | | | | $X$ |
| $\overline{x}\,\overline{y}\,z$ | | | | $X$ | | | $X$ |
| $\overline{x}\,t$ | | $X$ | | $X$ | $X$ | $X$ | |

*Y a partir de la tabla se ve cómo los términos* $x\,\overline{y}\,\overline{t}$ *y* $\overline{x}\,t$ *tienen que aparecer en la expresión simplificada. Si el primero no lo pusiéramos, no quedaría cubierto el minterm* $x\,\overline{y}\,\overline{z}\,\overline{t}$, *mientras que si no lo hiciéramos con el segundo, sería el minterm* $\overline{x}\,y\,\overline{z}\,t$ *(y otros dos más) quien no quedaría cubierto. Aquellos términos que son los únicos que cubren a alguno de los minterms, se les llama* implicantes primos.

*En este caso, los implicantes primos son* $x\,\overline{y}\,\overline{t}$ *y* $\overline{x}\,t$.

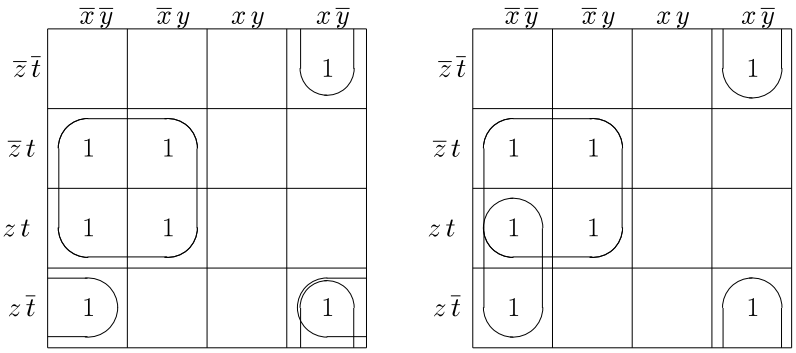
*Lo que hacemos ahora es, de la tabla anterior, eliminamos las filas donde están los implicantes primos, y las columnas donde están los minitérminos que quedan cubiertos por esos implicantes primos. Es decir, suprimimos las filas primera (correspondiente al término* $x\,\overline{y}\,\overline{t}$*) y cuarta (correspondiente al término* $\overline{x}\,t$*). También suprimimos las columnas primera, segunda, tercera, cuarta, quinta y sexta. Nos queda entonces:*

| | $\overline{x}\,\overline{y}\,z\,\overline{t}$ |
|---|---|
| $\overline{y}\,z\,\overline{t}$ | $X$ |
| $\overline{x}\,\overline{y}\,z$ | $X$ |

*y vemos que eligiendo cualquiera de los dos, podemos tener cubiertos todos los minterms. Por tanto,*

$$x\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,y\,\overline{z}\,t + x\,\overline{y}\,z\,\overline{t} + \overline{x}\,\overline{y}\;z\,t + \overline{x}\,\overline{y}\,\overline{z}\,t + \overline{x}\,y\,z\,t + \overline{x}\,\overline{y}\,z\,\overline{t} = x\,\overline{y}\,\overline{t} + \overline{x}\,t + \overline{y}\,z\,\overline{t} = x\,\overline{y}\,\overline{t} + \overline{x}\,t + \overline{x}\,\overline{y}\,z$$

*Si para optimizar esta expresión booleana empleáramos los mapas de Karnaugh tendríamos dos formas diferentes de agrupar las celdas con "unos":*




*lo que nos da las dos expresiones que acabamos de ver.*

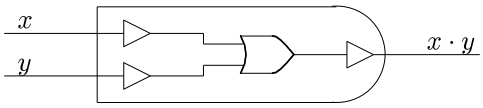
### 2.3.6. Conjuntos funcionalmente completos

En secciones precedentes hemos visto cómo a partir de tres puertas lógicas, las puertas AND, OR y NOT, podemos diseñar circuitos lógicos, y en la sección anterior hemos estudiado cómo minimizar el número de puertas necesarias para diseñar tales circuitos. Sin embargo, para construir tales circuitos es necesario emplear tres tipos de puertas lógicas diferentes. En esta sección vamos a intentar construir cualquier circuito lógico empleando menos puertas diferentes, aunque sea a costa de aumentar el número de éstas.

Comenzamos reduciendo el número de puertas distintas necesarias a 2.

**Proposición 2.3.3.** *Las puertas lógicas OR y NOT, o las puertas lógicas AND y NOT son suficientes para la construcción de cualquier circuito lógico.*

*Demostración:* Para ver que las puertas OR y NOT son suficientes, basta comprobar que $xy = \overline{\overline{x} + \overline{y}}$, lo que nos dice que podemos construir una puerta AND usando las puertas OR y NOT. Esta puerta podría quedar como sigue:




Y por tanto, usando únicamente puertas OR y NOT podemos construir cualquier circuito.

De la misma forma, y puesto que $x + y = \overline{\overline{x}\,\overline{y}}$ se puede ver que usando únicamente las puetas AND y NOT se puede diseñar cualquier circuito.

■

**Definición 24.** *Sean $x, y$ variables booleanas. Se definen las funciones booleanas $- \uparrow -$ y $- \downarrow -$ como sigue:*

$$x \uparrow y = \overline{x \cdot y}, \qquad x \downarrow y = \overline{x + y}.$$

Es decir:

$$0 \uparrow 0 = 1, \quad 0 \uparrow 1 = 1, \quad 1 \uparrow 0 = 1, \quad 1 \uparrow 1 = 0.$$
$$0 \downarrow 0 = 1, \quad 0 \downarrow 1 = 0, \quad 1 \downarrow 0 = 0, \quad 1 \downarrow 1 = 0.$$

Estos operadores se denotan como NAND (NOT AND) y NOR (NOT OR) respectivamente.

**Proposición 2.3.4.** *Cualquier función booleana se puede expresar usando únicamente el operador NAND (resp. NOR).*

*Demostración:*

Para comprobar esto, escribimos en primer lugar:

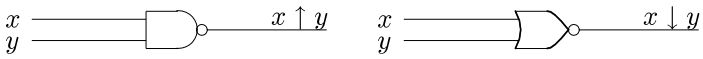
$\overline{x} = \overline{x \cdot x} = x \uparrow x$,

$x + y = \overline{\overline{x} \cdot \overline{y}} = \overline{x} \uparrow \overline{y} = (x \uparrow x) \uparrow (y \uparrow y)$,

es decir, los operadores NOT y OR pueden expresarse utilizando únicamente NAND. La Proposición 2.3.3 nos dice que cualquier funcíón booleana la podemos expresar únicamente con el operador NAND.

De la misma forma, puesto que $\overline{x} = x \downarrow x$ y $x \cdot y = (x \downarrow x) \downarrow (y \downarrow y)$ deducimos que el operador NOR es suficiente para expresar cualquier función booleana. ■.

Las puertas correspondientes NAND y NOR se suelen representar como sigue:




Cualquiera de los circuitos que vimos en la Sección 3.3.4, o cualquier otro que se nos ocurra podemos ahora diseñarlo usando únicamente la puerta NAND (o la puerta NOR). Esta puerta se construye de forma sencilla con transistores, tanto con la tecnología de semiconductores como con las técnicas más recientes de fabricación de microcircuitos.

# Capítulo 3

# Combinatoria

La combinatoria trata del estudio de las posibles agrupaciones de objetos. Contar el número de objetos que verifican ciertas propiedades es uno de los objetivos de la combinatoria. Problemas muy diversos, como determinar el número posible de apuestas diferentes en una quiniela, el número posible de posiciones en que unos corredores pueden terminar una carrera, el número posible de matrículas de los coches de un país o las diferentes formas de distribuir una serie de objetos en cajas son problemas que se abordan mediante las técnicas de conteo que veremos en este capítulo.

Lo que pretendemos es por tanto, contar los elementos de un conjunto, o más precisamente, determinar su cardinal. Dado un conjunto $A$ denotaremos por $|A|$ a su cardinal. Nosotros aquí trataremos únicamente con conjuntos que tienen un número finito de elementos. En tal caso, se dice que un conjunto $A$ tiene cardinal $n$ si existe una biyección entre el conjunto $A$ y el conjunto $\{0, 1, \cdots, n-1\}$. Es claro que si dos conjuntos son biyectivos tienen el mismo cardinal.

A la hora de contar ciertos objetos, lo que haremos será identificar estos objetos con los elementos de algún conjunto del cual sepamos determinar su cardinal (es decir, estableceremos una biyección entre el conjunto de objetos que queremos contar y otro conjunto del cual hallaremos su cardinal).

Para comenzar, estudiaremos en primer lugar cómo determinar el cardinal de algunos conjuntos.

## 3.1. Métodos elementales de conteo

### 3.1.1. Principio de inclusión-exclusión

**Proposición 3.1.1** (Principio de la suma)**.** *Sean $A_1$ y $A_2$ dos conjuntos disjuntos (es decir, $A_1 \cap A_2 = \emptyset$). Entonces $|A_1 \cup A_2| = |A_1| + |A_2|$.*

Intuitivamente está claro lo que significa este principio. No obstante, si quisiéramos una demostración, ésta se basaría en que los conjuntos $\{0, 1, \cdots, m-1\}$ y $\{n, n+1, \cdots, n+m-1\}$ son biyectivos.

El principio puede extenderse a tres o más conjuntos. En tal caso, dice que si $A_1, A_2, \cdots, A_n$ son conjuntos disjuntos dos a dos (es decir, $A_i \cap A_j = \emptyset$ para $i \neq j$) entonces

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

El principio de la suma podría enunciarse también como sigue:

*Si una primera tarea se puede realizar de $n_1$ formas, y una segunda tarea se puede realizar de $n_2$ formas, y las dos tareas son incompatibles, entonces hay $n_1 + n_2$ formas de realizar una de las dos tareas.*

Este principio de la suma es muy restrictivo, pues requiere que los conjuntos sean disjuntos, o que las tareas sean incompatibles. Sin embargo, en general, la situación es que los conjuntos no sean disjuntos. En este caso se tiene:

**Proposición 3.1.2.** *Sean $A_1$ y $A_2$ dos conjuntos. Entonces $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.*

La idea de este resultado está clara. Si queremos contar los elementos que están en $A_1 \cup A_2$, contamos por una parte los que están en $A_1$ y por otra parte los que están en $A_2$, lo que nos da $|A_1| + |A_2|$. Sin

embargo, los que se encuentran en $A_1 \cap A_2$ los hemos contado dos veces, luego hemos de restar $|A_1 \cap A_2|$ a la suma anterior.

Una demostración algo más rigurosa podría ser:

*Demostración:* Es claro que $A_1 = (A_1 \setminus A_2) \cup (A_1 \cap A_2)$. Además, $(A_1 \setminus A_2) \cap (A_1 \cap A_2) = \emptyset$, luego $|A_1| = |A_1 \setminus A_2| + |A_1 \cap A_2|$, luego

$$|A_1 \setminus A_2| = |A_1| - |A_1 \cap A_2|$$

De la misma forma se obtiene que $|A_2 \setminus A_1| = |A_2| - |A_1 \cap A_2|$.

Dado que $A_1 \cup A_2 = (A_1 \setminus A_2) \cup (A_1 \cap A_2) \cup (A_2 \setminus A_1)$ y que estos conjuntos son disjuntos se tiene que:

$$|A_1 \cup A_2| = |A_1 \setminus A_2| + |A_1 \cap A_2| + |A_2 \setminus A_1| = |A_1| - |A_1 \cap A_2| + |A_1 \cap A_2| + |A_2| - |A_1 \cap A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

■

**Ejemplo 3.1.1.** *Vamos a determinar, cuantos números entre* 1 *y* 100 *son, bien divisibles por* 2*, bien divisibles por* 3*.*

*Sean* $A_1$ *y* $A_2$ *los números que son múltiplos de* 2 *y* 3 *respectivamente.* $A_1$ *tiene cincuenta elementos (desde* $2 \cdot 1$ *hasta* $2 \cdot 50$*), mientras que* $A_3$ *tiene* 33 *(desde* $3 \cdot 1$ *hasta* $3 \cdot 33$*). Por otra parte,* $A_1 \cap A_2$ *son los múltiplos de* 6*, luego tiene* 16 *elementos (desde* $6 \cdot 1$ *hasta* $6 \cdot 16$*). Por tanto*

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 50 + 33 - 16 = 67$$

Esta proposición tiene una generalización a la unión de tres o más conjuntos. El resultado se conoce como *principio de inclusión exclusión*

**Proposición 3.1.3** (Principio de inclusión-exclusión)**.** *Sean* $A_1, A_2, \cdots, A_n$ *conjuntos. Entonces:*

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap \cdots \cap A_{i_k}| + \cdots \\ &\quad + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n| \end{aligned}$$

La demostración del principio de inclusión-exclusión se haría por inducción. Para $n = 1$ el resultado es trivialmente cierto, y supuesto cierto para $n$ conjuntos se demostraría para $n+1$ conjuntos poniendo $A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1} = (A_1 \cup A_2 \cup \cdots \cup A_n) \cup A_{n+1}$. La demostración es bastante engorrosa. Veamos aquí como se haría el paso de 2 a 3.

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| = \\ &= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - |(A_1 \cap A_3) \cup (A_2 \cap A_3)| = \\ &= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - \left[|A_1 \cap A_3| + |A_2 \cap A_3| - |(A_1 \cap A_3) \cap (A_2 \cap A_3)|\right] = \\ &= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| = \\ &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

**Ejemplo 3.1.2.** *Vamos a ver cuantos números entre* 1 *y* 111 *son compuestos (lo que nos dará inmediatamente cuántos números primos hay menores que* 111*.*

*Dado que* $\sqrt{111} < 11$*, se tiene que si un número menor o igual que* 111 *es compuesto, tiene un divisor primo menor que* 11*. Por tanto, será múltiplo de* 2*, múltiplo de* 3*, múltiplo de* 5 *o múltiplo de* 7*. Consideramos entonces:*

$A_1 = \{$*Números compuestos múltiplos de* 2$\} = \{2 \cdot x : \ 2 \le x \le 55\}$*. Por tanto* $|A_1| = 54$*.*

$A_2 = \{$*Números compuestos múltiplos de* 3$\} = \{3 \cdot x : \ 2 \le x \le 37\}$*. Por tanto* $|A_2| = 36$*.*

$A_3 = \{$*Números compuestos múltiplos de* 5$\} = \{5 \cdot x : \ 5 \le x \le 22\}$*. Por tanto* $|A_3| = 21$*.*

$A_4 = \{$*Números compuestos múltiplos de* $7\} = \{7 \cdot x : \ 2 \leq x \leq 15\}$. *Por tanto* $|A_4| = 14$.
*Luego* $A_1 \cap A_2 = \{6 \cdot x : \ 1 \leq x \leq 18\}$, *que tiene cardinal* 18. *De la misma forma, obtenemos:*
$|A_1 \cap A_3| = 11$; $|A_1 \cap A_4| = 7$; $|A_2 \cap A_3| = 7$; $|A_2 \cap A_4| = 5$; $|A_3 \cap A_4| = 3$.
$|A_1 \cap A_2 \cap A_3| = 3$; $|A_1 \cap A_2 \cap A_4| = 2$; $|A_1 \cap A_3 \cap A_4| = 1$; $|A_2 \cap A_3 \cap A_4| = 1$; $A_1 \cap A_2 \cap A_3 \cap A_4 = \emptyset$.
*Por tanto, deducimos que*

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = (54+36+21+14) - (18+11+7+7+5+3) + (3+2+1+1) - 0 = 125 - 51 + 7 = 81$$

*Es decir, entre* 1 *y* 111 *hay* 81 *números compuestos, de donde deducimos que hay* 29 *números primos (el* 1 *no es ni primo ni compuesto).*

### 3.1.2. Principio del producto. Variaciones

**Proposición 3.1.4** (Principio del producto)**.** *Sean* $A_1, A_2$ *dos conjuntos. Entonces,* $|A_1 \times A_2| = |A_1| \cdot |A_2|$.

Aquí también el principio es intuitivamente muy claro. No obstante, si quisiéramos hacer una demostración de este hecho, deberíamos encontrar una biyección entre $\{0, 1, \cdots, mn-1\}$ y $\{0, 1, \cdots, m-1\} \times \{0, 1, \cdots, n-1\}$. Esta biyección vendría dada por $a \mapsto (a \text{ mód } m, a \text{ div } m)$
Este principio puede generalizarse a tres o más conjuntos, teniéndose en dicho caso:

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdots |A_m|$$

El principio del producto podría enunciarse también como sigue:
*Si una tarea podemos dividirla en dos (o más) tareas consecutivas, de forma que hay* $n_1$ *formas de realizar la primera tarea, y* $n_2$ *formas de realizar la segunda tarea, entonces hay* $n_1 n_2$ *formas de completar la tarea.*

**Ejemplo 3.1.3.**

1. *Vamos a ver cuantas apuestas diferentes de una quiniela pueden hacerse. La tarea de elegir una combinación la podemos dividir en catorce pasos. En cada uno de ellos hacemos una elección entre tres posibilidades (*1, $X$, 2*). Por tanto, el número de apuestas es* $3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^{14} = 4782969$.

   *Nótese que si* $A = \{1, X, 2\}$ *una combinación es simplemente un elemento del conjunto*

   $$A \times A \times A \times A \times A \times A \times A \times A \times A \times A \times A \times A \times A \times A$$

   *cuyo cardinal es* $3^{14}$.

2. *En el sistema de matriculación vigente cada matrícula se compone de cuatro dígitos y tres consonantes (salvo la "*$\tilde{N}$*"). Si consideramos los conjuntos*

   $$\mathcal{D} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \qquad \mathcal{C} = \{B, C, D, F, G, H, J, K, L, M, N, P, Q, R, S, T, V, W, X, Y, Z\}$$

   *cada matrícula puede identificarse entonces con un elemento de* $\mathcal{D} \times \mathcal{D} \times \mathcal{D} \times \mathcal{D} \times \mathcal{C} \times \mathcal{C} \times \mathcal{C}$ *cuyo cardinal es* $10^4 \cdot 21^3 = 92610000$ *(existe una biyección entre el conjunto de posibles matrículas y* $\mathcal{D} \times \mathcal{D} \times \mathcal{D} \times \mathcal{D} \times \mathcal{C} \times \mathcal{C} \times \mathcal{C}$*)*

3. *Vamos a calcular cuantos números de* 6 *cifras, escritos en binario, contienen la secuencia* 00. *Los números con estas características pueden adquirir una de las cuatro formas siguientes:*

   $$100\_\_\_ \qquad 1\_00\_\_ \qquad 1\_\_00\_ \qquad 1\_\_\_00$$

   *Llamemos* $A_1$ *al conjunto de los números de la forma* $100\_\_\_$, $A_2$ *al conjunto de los números de la forma* $1\_00\_\_$ *y así hasta* $A_4$.

*Por el principio del producto cada uno de estos conjuntos tiene* 8 *elementos, pues para elegir un elemento de uno de estos conjuntos hemos de hacer tres elecciones con dos opciones para cada una. Razonando de forma análoga se tiene que*

$|A_1 \cap A_2| = |A_2 \cap A_3| = |A_3 \cap A_4| = 4$ *(un elemento de* $A_1 \cap A_2$ *es de la forma* $1000\_\_$*).*

$|A_1 \cap A_3| = |A_1 \cap A_4| = |A_2 \cap A_4| = 2$ *(un elemento de* $A_1 \cap A_3$ *es de la forma* $10000\_$*).*

$|A_1 \cap A_2 \cap A_3| = |A_2 \cap A_3 \cap A_4| = 2.$

$|A_1 \cap A_2 \cap A_4| = |A_1 \cap A_3 \cap A_4| = |A_1 \cap A_2 \cap A_3 \cap A_4| = 1.$

*Y ahora, el principio de inclusión-exclusión nos dice que*

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = (8+8+8+8) - (4+4+4+2+2+2) + (2+2+1+1) - 1 = 32 - 18 + 6 - 1 = 19$$

*de donde deducimos que hay* 19 *números de seis cifras en binario que contienen la secuencia* 00*.*

*Estos 19 números son:*

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 100000 | 100001 | 100010 | 100011 | 100100 | 100101 | 100110 | 100111 | 101000 | 101001 |
| 101100 | 110000 | 110001 | 110010 | 110011 | 110100 | 111000 | 111001 | 111100 | |

*Estos números, escritos en decimal, son 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 44, 48, 49, 50, 51, 52, 56, 57 y 60. En la siguiente tabla, los clasificamos según pertenezcan a* $A_1$*,* $A_2$*, etc.*

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A_1$ : | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | | | | | | | | | | |
| $A_2$ : | 32 | 33 | 34 | 35 | | | | | | | | 48 | 49 | 50 | 51 | | | |
| $A_3$ : | 32 | 33 | | | | | | | 40 | 41 | | 48 | 49 | | | | 56 | 57 | |
| $A_4$ : | 32 | | | | 36 | | | | 40 | | 44 | 48 | | | | 52 | 56 | | 60 |
| $A_1 \cap A_2$ : | 32 | 33 | 34 | 35 | | | | | | | | | | | | | | | |
| $A_1 \cap A_3$ : | 32 | | | | | | | | | | | | | | | | | | |
| $A_1 \cap A_4$ : | 32 | | | | 36 | | | | | | | | | | | | | | |
| $A_2 \cap A_3$ : | 32 | 33 | | | | | | | | | | 48 | 49 | | | | | | |
| $A_2 \cap A_4$ : | 32 | | | | | | | | | | | 48 | | | | | | | |
| $A_3 \cap A_4$ : | 32 | | | | | | | | 40 | | | 48 | | | | | 56 | | |
| $A_1 \cap A_2 \cap A_3$ : | 32 | 33 | | | | | | | | | | | | | | | | | |
| $A_1 \cap A_2 \cap A_4$ : | 32 | | | | | | | | | | | | | | | | | | |
| $A_1 \cap A_3 \cap A_4$ : | 32 | | | | | | | | | | | | | | | | | | |
| $A_2 \cap A_3 \cap A_4$ : | 32 | | | | | | | | | | | 48 | | | | | | | |
| $A_1 \cap A_2 \cap A_3 \cap A_4$ : | 32 | | | | | | | | | | | | | | | | | | |

Como consecuencia del principio del producto se tiene:

**Proposición 3.1.5.** *Sean* $A$ *y* $B$ *dos conjuntos finitos. Entonces el número de aplicaciones de* $A$ *en* $B$ *es* $|B|^{|A|}$*.*

*Demostración:* Supongamos que $|A| = m$ y $|B| = n$. Podría hacerse una demostración a partir de la representación de un número menor que $n^m$ en base $n$.

Nosotros aquí emplearemos el principio del producto.

La elección de una aplicación $f : A \to B$ podemos dividirla en $m$ etapas. Cada etapa consiste en definir la imagen de cada uno de los elementos de $A$, para lo cual tenemos $n$ posibilidades (una por cada elemento de $B$). Por tanto, el número posible de aplicaciones es $n^m$.

De hecho, si $A = \{a_1, a_2, \cdots, a_m\}$, dar una aplicación $f : A \to B$ es equivalente a dar un elemento de $B \times B \times \cdots \times B$ (en concreto, el elemento $(f(a_1), f(a_2), \cdots, f(a_m))$. ■

**Notación:** En ocasiones se representa al conjunto de aplicaciones de $A$ en $B$ como $B^A$, es decir:

$$B^A = \{f : A \to B;\ f \text{ es aplicación}\}$$

Con esta notación se tiene que $\left|B^A\right| = |B|^{|A|}$.

**Ejemplo 3.1.4.** *Una apuesta quinielística puede ser identificada con una aplicación*

$$f : \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\} \longrightarrow \{1, X, 2\}$$

*por tanto, el número posible de aplicaciones es* $3^{14}$*, como ya habíamos visto antes.*

Vamos a ver también cuantas aplicaciones inyectivas podemos definir de un conjunto a otro.

**Proposición 3.1.6.** *Sea* $A$ *un conjunto con* $m$ *elementos y* $B$ *un conjunto con* $n$ *elementos. El número de aplicaciones inyectivas de* $A$ *en* $B$ *es* $n(n-1)\cdots(n-m+1)$*.*

*Demostración:* Nótese que si $m < n$ no existe ninguna aplicación inyectiva $f : A \to B$. Por tanto, supondremos que $m \geq n$.

Supongamos que $A = \{a_1, a_2, \cdots, a_m\}$. Para dar una aplicación inyectiva $f : A \to B$ necesitamos dar $f(a_1),\ f(a_2), \cdots, f(a_m)$.

Para elegir $f(a_1)$ tenemos un total de $n$ posibilidades. Al ser $f$ inyectiva, para elegir $f(a_2)$ tenemos $n-1$ posibilidades (pues no podemos hacer la misma elección que para $f(a_1)$). De la misma forma, para $f(a_3)$ tenemos $(n-2)$ posibilidades. Continuando con este razonamiento, llegamos a que para elegir $f(a_m)$ tenemos $n-m+1$ posibilidades. Por tanto, el número de aplicaciones inyectivas es $n(n-1)\cdots(n-m+1)$.

Notemos que en el caso de que $m < n$ la expresión anterior es también válida, pues uno de los factores es $n - n = 0$. ■

**Definición 25.**

1. *Se llaman* variaciones con repetición *de* $n$ *elementos, tomados de* $m$ *en* $m$ *a cada una de las posibles elecciones de* $m$ *elementos, dentro de un conjunto de* $n$ *elementos, pudiéndose tomar elementos repetidos. Dos posibles elecciones se diferencian, bien en la naturaleza de los elementos elegidos, bien en el orden en que se han elegido.*

2. *Se llaman* variaciones sin repetición *de* $n$ *elementos, tomados de* $m$ *en* $m$ *a cada una de las posibles elecciones de* $m$ *elementos, dentro de un conjunto de* $n$ *elementos, no pudiendo aparecer un elemento más de una vez. Dos posibles elecciones se diferencian, bien en la naturaleza de los elementos elegidos, bien en el orden en que se han elegido.*

El número de variaciones con repetición de $n$ elementos, tomados de $m$ en $m$ es igual a $n^m$. El número de variaciones sin repetición de $n$ elementos, tomados de $m$ en $m$ es $n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!}$.

**Ejemplo 3.1.5.**

1. *Para hacer una quiniela, debemos elegir una lista de* 14 *elementos entre los elementos de un conjunto con* 3 *(*1*,* $X$*,* 2*). Son por tanto, variaciones con repetición de* 3 *elementos tomados de* 14 *en* 14*. El número total de posibles apuestas es por tanto* $3^{14}$*.*

2. *En una carrera participan* 35 *personas. El ganador recibe una medalla de oro, el segundo clasificado una medalla de plata y el tercer clasificado una medalla de bronce.*

   *El número de formas diferentes en que se pueden repartir las medallas corresponde al número de variaciones sin repetición de* 35 *elementos, tomados de* 3 *en* 3*. Por tanto es* $35 \cdot 34 \cdot 33 = 39270$*.*

### 3.1.3. El principio del palomar

Aunque su enunciado pueda parecer trivial, es conveniente recordarlo, pues de él deduciremos algunas consecuencias.

**Proposición 3.1.7** (Principio del palomar)**.** *Si queremos repartir* $n$ *objetos en* $m$ *cajas, y* $n > m$ *entonces al menos una caja ha de contener* 2 *o más objetos.*

Nótese que repartir objetos en cajas es equivalente a definir una aplicación del conjunto de objetos en el conjunto de las cajas (la imagen de un elemento nos dice en que caja se coloca). Decir que una caja tiene dos o más objetos se traduce en que la aplicación no es inyectiva (pues esos dos elementos tendrían la misma imagen). El principio del palomar se enunciaría entonces:

*Si $n > m$ no existen aplicaciones inyectivas de un conjunto de cardinal $n$ en un conjunto de cardinal $m$.*

**Ejemplo 3.1.6.**

1. *Si tenemos un grupo de 500 personas (bastaría con tener 367) debe haber dos que celebren el cumpleaños el mismo día (siempre y cuando todas celebren su cumpleaños).*

   *En este caso las cajas serían cada uno de los días del año, mientras que los objetos a repartir son las personas.*

2. *Vamos a comprobar que cualquier número natural tiene un múltiplo suyo que escrito en el sistema decimal está formado únicamente por ceros y unos.*

   *Para esto, sea $n \in \mathbb{N}$ y consideramos los $n+1$ números naturales siguientes:*

   $x_1 = 1,\ x_2 = 10+1,\ x_3 = 10^2+10+1,\ \cdots x_{n+1} = 10^n + \cdots + 10 + 1$

   *cuya expresión en base decimal está formada únicamente por unos.*

   *Reducimos estos elementos módulos $n$ (es decir, consideramos estos números en $\mathbb{Z}_n$). Debe haber al menos dos que coincidan (es decir, $x_k \equiv x_l (\text{mód } m)$) si $k < l$ se tiene que $10^k + 10^{k+1} + \cdots + 10^{l-1}$ es múltiplo de $n$. La expresión decimal de este número está formada por $k$ ceros y $l-k$ unos.*

   *Vamos a realizar los cálculos para $n = 6$. Tomamos los números:*

   $$1 \quad 11 \quad 111 \quad 1111 \quad 11111 \quad 111111 \quad 1111111$$

   *Reducimos módulo 6.*

   $$1 \quad 5 \quad 3 \quad 1 \quad 5 \quad 3 \quad 1$$

   *de donde deducimos que $1111 - 1 = 1110$ es múltiplo de 6.*

   *Lo mismo, vamos a hacerlo con $n = 17$. En este caso, la lista de los números $1,\ 11,\ 111, \cdots$ reducida módulo 17 es:*

   $$1 \quad 11 \quad 9 \quad 6 \quad 10 \quad 16 \quad 8 \quad 13 \quad 12 \quad 2 \quad 4 \quad 7 \quad 3 \quad 14 \quad 5 \quad 0$$

   *Y vemos como el número 1111111111111111 es múltiplo de 17. De hecho, se tiene que $1111111111111111 = 17 \cdot 65359477124183$.*

   *También podemos ver, dado que 16-6+11 es múltiplo de 17, que $111111 - 11111 + 11 = 100011$ es múltiplo de 17. De la misma forma, $11111 - 11 + 1$ también lo es.*

3. *Un razonamiento semejante a este permite probar que dado un conjunto formado por $n$ números enteros, podemos encontrar un subconjunto suyo cuya suma sea múltiplo de $n$.*

   *Sea el conjunto de partida $\{x_1, x_2, \cdots, x_n\}$, y construimos:*

   $y_1 = x_1$
   $y_2 = x_1 + x_2$
   $\cdots\cdots\cdots$
   $y_n = x_1 + x_2 + \cdots + x_n$

   *reducimos módulo $n$, y obtenemos $n$ elementos de $\mathbb{Z}_n$.*

   *Si alguno de estos elementos es cero, digamos $y_k$, tenemos que $x_1 + \cdots + x_k$ es múltiplo de $n$.*

*Si ninguno de ellos vale cero, entonces $n$ elementos de $\mathbb{Z}_n \setminus \{0\}$. Por tanto, dos de estos elementos son iguales. Si estos son $y_k$ e $y_l$ se tiene que $y_l - y_k = x_{k+1} + \cdots + x_l$ es múltiplo de $n$.*

*Nótese que en el ejemplo anterior se ha empleado el mismo razonamiento, tomando los elementos $x_1 = 1,\ x_2 = 10, \cdots x_k = 10^{k-1}$.*

**Proposición 3.1.8** (Principio del palomar generalizado)**.** *Si queremos repartir $n$ objetos en $m$ cajas, al menos una caja ha de contener al menos $n/m$ elementos.*

Obviamente, si $n/m$ no es entero, se toma el número entero inmediatamente superior.

**Ejemplo 3.1.7.**
*Si tenemos un grupo de 200 personas, dado que hay 12 signos zodiacales y $200/12 = 16,3...$ sabemos que debe haber al menos 17 personas con el mismo signo del Zodíaco.*

## 3.2. Combinaciones

En secciones anteriores estudiamos cómo, de un conjunto de $n$ elementos podíamos extraer $m$, de forma que el orden en que se extraían los elementos fuera significativo. En esta trataremos de encontrar cómo extraer $m$ elementos de un conjunto que tiene $n$, pero ahora no importa el orden en que se elijan, sino únicamente la naturaleza de estos elementos.

En términos de conjuntos, nos preguntamos cuántos subconjuntos de cardinal $m$ tiene un conjunto con $n$ elementos. Vamos a denotar por $\binom{n}{m}$ a tal cantidad.

Es fácil ver que $\binom{n}{0} = 1$, pues cada conjunto de cardinal $n$ tiene un único subconjunto con 0 elementos, a saber, el conjunto vacío. De la misma forma se tiene que $\binom{n}{n} = 1$ (pues el único subconjunto de cardinal $n$ de un conjunto de $n$ elementos es el propio conjunto).

También es fácil ver que $\binom{n}{m} = \binom{n}{n-m}$ pues cada subconjunto de $m$ elementos determina de forma única un subconjunto de $n - m$ elementos (concretamente, el de los elementos que no pertenecen a él) y viceversa.

Por último, una tercera propiedad referente a estos números nos dice que $\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$. Razonemos esto último.

Supongamos que $A = \{a_1, a_2, \cdots, a_n, a_{n+1}\}$ es un conjunto de cardinal $n+1$, y queremos ver cuántos subconjuntos de $m$ elementos tiene.

Si queremos elegir un subconjunto $X$ de $A$ con $m$ elementos, tenemos dos opciones, mutuamente excluyentes: que $a_{n+1} \in X$ o que $a_{n+1} \notin X$. En el primer caso, está determinado por los $m-1$ elementos de $\{a_1, a_2, \cdots, a_n\}$ que pertenecen a $X$. Podemos entonces elegir un total de $\binom{n}{m-1}$ subconjuntos con estas condiciones. En el segundo caso, está determinado por los $m$ elementos que pertenecen a él, y que sabemos con seguridad que están en el conjunto $\{a_1, a_2, \cdots, a_n\}$. Podemos por tanto hacer la elección de $\binom{n}{m}$ formas. El principio de la suma nos asegura entonces que $\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$, como queríamos.

Estas tres propiedades nos permiten demostrar la siguiente proposición.

**Proposición 3.2.1.** *Sean $m, n \in \mathbb{N}$ con $m \leq n$. Entonces*

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

*Demostración:* Haremos la demostración por inducción.

Para $n = 0$, y para $m = n$ el resultado es cierto (lo que nos dice que es cierto para $n = 1$)

Supongamos que $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ para cualquier $k$ tal que $0 \leq k \leq n$. Sea $m$ comprendido entre 1 y $n$. En ese caso se tiene que

$$\begin{aligned}
\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m} &= \frac{n!}{(m-1)!(n-m+1)!} + \frac{n!}{m!(n-m)!} \\
&= \frac{n!m}{m!(n-m+1)!} + \frac{n!(n-m+1)}{m!(n-m+1)!} \\
&= \frac{n!(m+n-m+1)}{m!(n-m+1)!} \\
&= \frac{(n+1)!}{m!(n+1-m)!}
\end{aligned}$$

y para $m = 0$ o $m = n+1$ sabemos que el resultado es cierto. ■

**Ejemplo 3.2.1.**

1. *El número de subconjuntos con* 2 *elementos del conjunto* $\{a, b, c, d, e\}$ *es*

$$\binom{5}{2} = \frac{5!}{2!3!} = \frac{5 \cdot 4}{2!} = 10$$

*Éstos son:*

$$\{a,b\} \quad \{a,c\} \quad \{a,d\} \quad \{a,e\} \quad \{b,c\} \quad \{b,d\} \quad \{b,e\} \quad \{c,d\} \quad \{c,e\} \quad \{d,e\}$$

*Nótese que de estos* 10 *sobconjuntos hay* $\binom{4}{1} = 4$ *que contienen al elemento* $e$

$$\{a,e\} \quad \{b,e\} \quad \{c,e\} \quad \{d,e\}$$

*y* $\binom{4}{2} = 6$ *que no contienen al elemento* $e$

$$\{a,b\} \quad \{a,c\} \quad \{a,d\} \quad \{b,c\} \quad \{b,d\} \quad \{c,d\}$$

2. *El número de cadenas de* $n$ *bits que contienen exactamente* $m$ *unos (y por tanto* $n-m$ *ceros) es* $\binom{n}{m}$. *Para justificar esta afirmación numeramos los* $n$ *bits desde* 1 *hasta* $n$. *Elegir una cadena en estas condiciones es equivalente a tomar un subconjunto del conjunto* $\{1, 2, \cdots, n\}$ *con* $m$ *elementos.*

3. *Sabemos que si* $X$ *es un conjunto con* $n$ *elementos, entonces* $X$ *tiene* $2^n$ *subconjuntos (las álgebras de Boole* $\mathbb{B}^n$ *y* $\mathcal{P}(X)$ *son isomorfas). Deducimos entonces que, para cualquier* $n \in \mathbb{N}$ *se verifica que*

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$$

4. *Supongamos que un departamento está formado por* 7 *mujeres y* 9 *hombres, y se quiere formar una comisión con cinco miembros, de forma que haya al menos un hombre y una mujer en la comisión. Vamos a determinar cuantas posibles comisiones pueden formarse con esas condiciones. Para esto, vemos en primer lugar que pueden formarse* $\binom{16}{5} = 4368$ *posibles comisiones con* 5 *miembros. De ellas,* $\binom{9}{5} = 126$ *no contienen ninguna mujer (están formadas únicamente por hombres), mientras que* $\binom{7}{5} = 21$ *no contienen ningún hombre. Por tanto, el número posible de comisiones es* $4368 - 126 - 21 = 4221$.

   *Nótese que para realizar esta operación se han considerado los conjuntos:*

   *- Conjunto de todas las comisiones con* 5 *miembros:* $X$.

   *- Conjunto de las comisiones con al menos un hombre:* $A$.

   *- Conjunto de las comisiones con al menos una mujer:* $B$.

   *Lo que queremos calcular es* $|A \cap B|$, *y sabemos que:*

   $|X| = 4368$, $|A'| = |X \setminus A| = 21$, $|B'| = 126$, $A' \cap B' = \emptyset$.

   *Por tanto, se tiene:*

$$|A \cap B| = |X| - |(A \cap B)'| = |X| - |A' \cup B'| = |X| - (|A'| + |B'|) = 4368 - (21 + 126) = 4221$$

**Teorema 3.2.1** (Teorema del binomio)**.** *Sea* $A$ *un anillo conmutativo, y* $a, b \in A$. *Entonces, para cualquier* $n \in \mathbb{N}$ *se verifica que:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n} b^n$$

*Demostración:* La demostración la haremos por inducción en $n$.

Para $n = 0$ o $n = 1$ el resultado es trivialmente cierto.

Supongamos que se verifica que $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$. Entonces:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = a\cdot(a+b)^n + b\cdot(a+b)^n \\
&= a\left[\binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{k}a^{n-k}b^k + \cdots + \binom{n}{n}b^n\right] \\
&\quad + b\left[\binom{n}{0}a^n + \cdots + \binom{n}{k-1}a^{n-k+1}b^{k-1} + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n\right] \\
&= \binom{n}{0}a^{n+1} + \binom{n}{1}a^n b + \cdots + \binom{n}{k}a^{n-k+1}b^k + \cdots + \binom{n}{n}ab^n \\
&\quad + \binom{n}{0}a^n b + \cdots + \binom{n}{k-1}a^{n-k+1}b^k + \cdots + \binom{n}{n-1}ab^n + \binom{n}{n}b^{n+1} \\
&= \binom{n}{0}a^{n+1} + \left[\binom{n}{1} + \binom{n}{0}\right]a^n b + \cdots + \left[\binom{n}{k} + \binom{n}{k-1}\right]a^{n-k+1}b^k + \cdots + \left[\binom{n}{n} + \binom{n}{n-1}\right]ab^n + \binom{n}{n}b^{n+1} \\
&= \binom{n+1}{0}a^{n+1} + \binom{n+1}{1}a^n b + \cdots + \binom{n+1}{k}a^{n+1-k}b^k + \cdots + \binom{n+1}{n}ab^n + \binom{n+1}{n+1}b^{n+1}
\end{aligned}$$

que es la expresión que buscábamos. ■

**Ejemplo 3.2.2.**

1. *Sabemos que* $(a+b)^2 = a^2+2ab+b^2$. *Esta igualdad puede obtenerse a partir del teorema del binomio teniendo en cuenta que* $\binom{2}{0} = \binom{2}{2} = 1$, *mientras que* $\binom{2}{1} = 2$.
2. *Para exponente* 5 *se tiene que:*

$$(a+b)^5 = \binom{5}{0}a^5 + \binom{5}{1}a^4b + \binom{5}{2}a^3b^2 + \binom{5}{3}a^2b^3 + \binom{5}{4}ab^4 + \binom{5}{5}b^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$

3. *El coeficiente de* $a^7b^3$ *en* $(a+b)^{10}$ *es* $\binom{7}{3} = 35$.
4. *Usando el teorema del binomio se tiene que:*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = (1+1)^n = 2^n$$

*algo que ya habíamos obtenido anteriormente.*

Hasta ahora hemos estudiado, como de un conjunto de $n$ elementos podemos elegir $m$, sin que influya el orden en que se pueden elegir los elementos, y sin que puedan repetirse los elementos. Es lo que se llama *combinaciones (sin repetición) de n elementos tomados de m en m*. Nos planteamos a continuación el caso en el que los elementos puedan repetirse. Por ejemplo, tenemos en una caja bolas rojas, negras y blancas, y extraemos 4 bolas. ¿Cuántas extracciones distintas podemos realizar?.

Se trata, de un conjunto de tres elementos ($\{R, N, B\}$) elegir cuatro, pudiéndose repetir los elementos, y sin que influya el orden en que los elegimos. Da igual la extracción $RNBN$ que $RNNB$. Lo único que importa es que se han elegido una bola roja, dos bolas negras y una blanca.

En este caso, las posibles extracciones son (suponemos que tenemos al menos cuatro bolas de cada color):

$$RRRR \quad RRRN \quad RRRB \quad RRNN \quad RRNB \quad RRBB \quad RNNN \quad RNNB$$
$$RNBB \quad RBBB \quad NNNN \quad NNNB \quad NNBB \quad NBBB \quad BBBB$$

es decir, un total de 15.

Para encontrar una forma de generalizar esto, vamos a escribir las quince posibles extracciones como sigue:

$$RRRRxx \quad RRRxNx \quad RRRxxB \quad RRxNNx \quad RRxNxB \quad RRxxBB \quad RxNNNx \quad RxNNxB$$

$$RxNxBB \quad RxxBBB \quad xNNNNx \quad xNNNxB \quad xNNxBB \quad xNxBBB \quad xxBBBB$$

y vemos que cada extracción está determinada por la posición que ocupan las dos $x$ en la cadena $\_\_\_\_\_$ El número de posiciones que quedan a la izquierda de las dos equis nos indican la cantidad de bolas rojas; el número de posiciones que quedan entre las dos equis nos indican el número de bolas negras mientras que el número de posiciones a la derecha de las dos equis nos indican la cantidad de bolas blancas. Así, colocando las equis en las posiciones 2 y 4 nos queda $\_x\_x\_\_$, lo que nos da una bola roja, una bola negra y dos bolas blancas.

Puesto que entre las seis posiciones podemos colocar las dos equis de $\binom{6}{2} = 15$ formas diferentes obtenemos que se pueden hacer un total de 15 extracciones diferentes.

Situémonos en el caso general. Supongamos que tenemos un conjunto con $n$ elementos, que podrían ser bolas de $n$ colores diferentes, y extraemos $m$ elementos (se supone que de cada color hay al menos $m$ bolas). Esto es lo que se llama *combinaciones con repetición de $n$ elementos tomados de $m$ en $m$*. Para determinar cuantas combinaciones con repetición hay, identificamos cada combinación con la elección de la posición de $m-1$ equis de un total de $n+m-1$ posibles posiciones. El número de combinaciones con repetición de $n$ elementos, tomados de $m$ en $m$ resulta ser entonces $\binom{n+m-1}{m} = \binom{n+m-1}{n-1}$.

**Ejemplo 3.2.3.**

1. *Vamos a determinar cuantas soluciones naturales tiene la ecuación $x+y+z+t = 13$. Para resolverlo, planteamos el problema de otra forma. Supongamos que tenemos cuatro tipos de bolas (rojas, negras, blancas y azules), y extraemos trece bolas. Cada extracción la podemos identificar con una solución de la ecuación anterior, donde $x$ es el número de bolas rojas, $y$ es el número de bolas negras, $z$ es el número de bolas blancas y $t$ es el número de bolas azules.*

   *El número de posibles extracciones es el número de combinaciones con repetición de 4 elementos tomados de 13 en 13. Su valor es $\binom{16}{3} = 560$.*

   *Supongamos ahora que queremos resolver la misma ecuación, pero queremos que las variables tomen valores mayores o iguales que 1. En ese caso, llamamos $x' = x-1$, $y' = y-1$, $z' = z-1$, $t' = t-1$, con lo que la ecuación se transforma en $x'+y'+z'+t' = 9$, y están permitidas todas las soluciones naturales. El número de soluciones es $\binom{9+4-1}{4-1} = 84$.*

   *Por tanto, de las 560 soluciones de la ecuación $x+y+z+t = 13$ hay 476 $(560-84)$ en las que alguna de las variables toma el valor cero.*

2. *Supongamos que tenemos 15 caramelos (iguales) y los queremos repartir entre 5 niños. Podemos ver que el número de posibles repartos es el de combinaciones con repetición de 5 elementos tomados de 15 en 15, que resulta ser $\binom{19}{4} = 3876$.*

3. *Vamos a calcular cuantas soluciones naturales tiene la inecuación $x+y+z \leq 9$.*

   *Vamos a utilizar dos formas para resolverlo:*

   - *Lo que tenemos que contar es el número de soluciones de la ecuación $x+y+z = 0$, el número de soluciones de la ecuación $x+y+z = 1$, y así hasta $x+y+z = 9$, y sumar los resultados. El número de soluciones de $x+y+z = 0$ es $\binom{0+3-1}{0} = \binom{2}{0} = 1$; el número de soluciones de la ecuación $x+y+z = 1$ es $\binom{1+3-1}{1} = \binom{3}{1} = 3$; el número de soluciones de la ecuación $x+y+z = 2$ es $\binom{2+3-1}{2} = \binom{4}{2} = 6$, y así hasta llegar a la ecuación $x+y+z = 9$, que tiene $\binom{9+3-1}{9} = \binom{11}{9} = 55$ soluciones naturales. Entonces, el número de soluciones naturales de la inecuación $x+y+z \leq 9$ son*

     $$\binom{2}{0} + \binom{3}{1} + \binom{4}{2} + \binom{5}{3} + \binom{6}{4} + \binom{7}{5} + \binom{8}{6} + \binom{9}{7} + \binom{10}{8} + \binom{11}{9} =$$

     $$1+3+6+10+15+21+28+36+45+55 = 220$$

   - *Vamos a llamar $t$ a $9-x-y-z$. Entonces, $t \geq 0$, y cada solución de la inecuación $x+y+z \leq 9$ se corresponde con una solución de la ecuación $x+y+z+t = 9$. Y recíprocamente, cada solución de la ecuación $x+y+z+t = 9$ nos da una solución de la inecuación $x+y+z \leq 9$.*

*Por ejemplo, $x = 2$, $y = 3$, $z = 1$ es una solución natural de la inecuación $x + y + z \leq 9$, que se corresponde con la solución $x = 2$, $y = 3$, $z = 1$, $t = 3$, de la ecuación $x + y + z + t = 9$. Recíprocamente, si tomamos una solución de la ecuación $x+y+z+t = 9$ (por ejemplo, $x = 1$, $y = 1$, $z = 5$, $t = 2$), esa solución se corresponde con una de la inecuación $x + y + z \leq 9$ (en este caso, $x = 1$, $y = 1$, $z = 5$).*

*Por tanto, lo que tenemos que hacer es contar el número de soluciones naturales de la ecuación $x + y + z + t = 9$. Este número es:*

$$\binom{9+4-1}{9} = \binom{12}{9} = \frac{12!}{9! \cdot 3!} = \frac{12 \cdot 11 \cdot 10 \cdot 9!}{3 \cdot 2 \cdot 9!} = \frac{12 \cdot 11 \cdot 10}{3 \cdot 2} = 2 \cdot 11 \cdot 10 = 220$$

*Y como vemos obtenemos el mismo resultado que antes.*

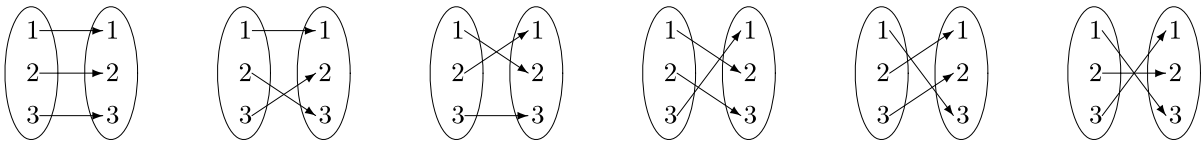
## 3.3. Permutaciones

En esta sección estudiaremos las formas diferentes de ordenar los elementos de un conjunto. Dado un conjunto $X$ con $n$ elementos, una permutación en $X$ es una ordenación de los elementos de $X$. Otra forma de definir una permutación en $X$ es como una aplicación biyectiva $X \to X$.

Por ejemplo, si $X = \{1, 2, 3\}$, hay seis permutaciones en $X$ que se corresponden con las seis formas de ordenar los elementos de $X$. Éstas son:

123 132 213 231 312 321

Las seis biyecciones de $X$ en $X$ son:




Y vemos como cada biyección se corresponde con una ordenación de los elementos de $X$ y viceversa.

En general, si $X$ es un conjunto con $n$ elementos, el número de permutaciones en $X$ es igual al número de aplicaciones inyectivas $X \to X$, pues toda aplicación inyectiva $X \to X$ es biyectiva. Este número fue calculado en la sección dedicada a las variaciones, y sabemos que vale $n \cdot (n-1) \cdots 2 \cdot 1 = n!$.

Algo más complicado es ordenar los elementos de un conjunto cuando alguno de sus elementos aparece repetido. Por ejemplo, nos preguntamos de cuántas formas podemos ordenar las letras de la palabra *cara*. Para ordenarlas, supongamos que distinguimos las dos aes que aparecen en la palabra, escribiendo una de ellas en negrita, y realizamos las 24 ordenaciones posibles:

| | | | | | |
|---|---|---|---|---|---|
| car**a** | ca**a**r | cra**a** | rca**a** | rac**a** | ra**a**c |
| c**a**ra | c**a**ar | cr**a**a | rc**a**a | r**a**ca | r**a**ac |
| | | | | | |
| acr**a** | ac**a**r | arc**a** | ar**a**c | a**a**cr | a**a**rc |
| **a**cra | **a**car | **a**rca | **a**rac | **a**acr | **a**arc |

Vemos que cada 2 ordenaciones de las letras de car**a** da lugar a la misma ordenación de las letras de cara (la que resulta de intercambiar "a" con "**a**"). Por tanto, las letras de cara se pueden ordenar de $\frac{24}{2} = 12$ formas distintas.

Si quisiéramos ahora estudiar de cuantas formas podemos ordenar las letras de la palabra rara, tendríamos, si distinguimos las dos letras "r" un total de 12 ordenaciones diferentes. Sin embargo, cada dos de ellas da lugar a una sola ordenación de las letras de *rara*. Tenemos entonces un total de $\frac{12}{2} = 6$ ordenaciones diferentes.

Otra forma de razonar este resultado es como sigue:

Para ordenar las letras de *cara*, situamos en primer lugar las dos "aes". Esto podemos hacerlo de $\binom{4}{2}$ formas diferentes. Una vez situadas las dos "aes", colocamos la "c", para la que tenemos dos posibilidades. Por tanto, hay $\binom{4}{2} \cdot 2 = 12$ formas diferentes de colocarla. La posición de la "r" queda determinada por la de la "c" y las "aes".

Para ordenar las letras de *rara*, situamos en primer lugar las dos "aes", cosa que podemos hacer de $\binom{4}{2}$ formas diferentes. Puesto que esto determina el lugar en que van las letras "r", concluimos que hay seis maneras de ordenar las letras de *rara*.

Situémonos en el caso general.

**Proposición 3.3.1.** *Supongamos que tenemos una lista de $n$ objetos, de $r$ tipos diferentes. Del tipo 1 hay un total de $n_1$ objetos, todos ellos indistinguibles. Del tipo 2 hay $n_2$ objetos, y así hasta el tipo $r$, del que hay $n_r$ objetos. Entonces el número total de ordenaciones de estos objetos es*

$$\frac{n!}{n_1!n_2!\cdots n_r!}$$

*Demostración:* Igual que hemos hecho antes, podemos razonarlo de dos formas diferentes.

1. Supongamos que todos los objetos sean distinguibles. Entonces, podemos ordenarlos de $n!$ formas diferentes. Sin embargo, de todas estas, cada $n_1!$ ordenaciones resulta ser la misma salvo en los $n_1$ objetos del tipo 1 que están reordenados entre sí. Por tanto, si consideramos los $n_1$ objetos del tipo 1 indistinguibles tenemos un total de $\frac{n!}{n_1!}$.

   Razonando de la misma forma, cada $n_2!$ ordenaciones de las obtenidas resulta ser la misma salvo en los $n_2$ objetos del tipo 2 que están intercambiados entre ellos. Por tanto, considerando también los $n_2$ objetos del tipo 2 indistinguibles tenemos un total de $\frac{n!}{n_1!n_2!}$.

   Repitiendo el razonamiento, llegamos a que el número de ordenaciones diferentes es $\frac{n!}{n_1!n_2!\cdots n_r!}$.

2. Para situar los $n$ objetos, situamos en primer lugar los $n_1$ objetos del tipo 1. Para esto, únicamente hay que elegir el lugar en que van a situarse estos objetos, y eso puede hacerse de $\binom{n}{n_1}$ formas diferentes.

   Una vez hecho esto, situamos los $n_2$ objetos del tipo 2. Ahora tenemos únicamente $n - n_1$ lugares donde colocarlos, luego podemos colocarlos de $\binom{n-n_1}{n_2}$.

   Razonando de esta forma, el número total de ordenaciones posibles es:

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-\cdots n_{r-1}}{n_r}$$

   Desarrollando se obtiene

$$\frac{n!}{n_1!(n-n_1)!}\cdot\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdot\frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!}\cdots\frac{(n-n_1-\cdots-n_{r-1})!}{n_r!0!} = \frac{n!}{n_1!n_2!\cdots n_r!}$$

Como vemos, de las dos formas se obtiene el mismo resultado. ■

Este problema es equivalente al de repartir objetos distinguibles en cajas distinguibles. Supongamos que tenemos $n$ objetos, y queremos repartirlos en $r$ cajas, de forma que en la primera caja haya $n_1$ objetos, en la segunda carta haya $n_2$ objetos, y así, hasta la $r$-ésima caja, en la que debe haber $n_r$ objetos.

Los $n_1$ objetos que van a la primera caja se pueden elegir de $\binom{n}{n_1}$ formas. Nos quedan entonces $n - n_1$ objetos, y de estos elegimos $n_2$ para la segunda caja, lo cual podemos hacerlo de $\binom{n-n_1}{n_2}$ formas. Repitiendo el razonamiento, y usando el principio del producto llegamos a que las formas distintas en que podemos repartir los objetos en las cajas es

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\cdots-n_{r-1}}{n_r} = \frac{n!}{n_1!n_2!\cdots n_r!}$$

Se deja como ejercicio encontrar una biyección entre las distintas ordenaciones de $n$ objetos donde $r$ tipos de objetos, y del tipo $k$-ésimo hay $n_k$ objetos, y las distribuciones de $n$ objetos distinguibles en $r$ cajas distinguibles, de forma que en la caja $k$-ésima haya $n_k$-objetos.

**Ejemplo 3.3.1.** *Tenemos cuatro jugadores, y repartimos cinco cartas a cada uno de una baraja de 40 cartas. Vamos a calcular de cuantas formas distintas se pueden repartir. Para esto, consideramos las cartas como las bolas, a las que hay que distribuir en* 5 *cajas: 4 por cada uno de los jugadores, y una quinta por las* 20 *cartas que quedan sin repartir.*

*Se trata entonces de distribuir 40 objetos distinguibles en cinco cajas también distinguibles, de forma que en las cuatro primeras haya* 5 *objetos y en la última haya* 20*. El número de formas de hacerlo es*

$$\frac{40!}{5!5!5!5!20!} = 161731817508852759168 0$$

**Definición 26.** *Sea $n \in \mathbb{N}$, y $n_1, n_2, \cdots, n_r \in \mathbb{N}$ tales que $n_1 + n_2 + \cdots + n_r = n$. Se define el coeficiente multinomial $\binom{n}{n_1\ n_2\ \cdots\ n_r}$ como*

$$\binom{n}{n_1\ n_2\ \cdots\ n_r} = \frac{n!}{n_1!n_2!\cdots n_r!}$$

En el caso $r = 2$ se tiene que $\binom{n}{n_1\ n_2} = \binom{n}{n_1} = \binom{n}{n_2}$. En este caso se denominan *coeficientes binomiales.*

El teorema del binomio tiene ahora una generalización. Para ello, necesitamos el siguiente lema:

**Lema 3.3.1.** *Sea $n \in \mathbb{N}$, y $n_1, n_2, \cdots, n_r$ tales que $n_1 + n_2 + \cdots + n_r = n + 1$. Entonces*

$$\sum_{k=1}^{r} \binom{n}{n_1\ n_2\ \cdots\ n_k - 1\ \cdots\ n_r} = \binom{n+1}{n_1\ n_2\ \cdots\ n_r}$$

*(si para algún $i$ entre 1 y $r$, $n_i$ fuera igual a cero, el sumando para $k = i$ valdría igualmente cero).*

*Demostración:* Se tiene que

$$\begin{aligned}
&\tbinom{n}{n_1-1\ n_2\ \cdots\ n_r} + \tbinom{n}{n_1\ n_2-1\ \cdots\ n_r} + \cdots + \tbinom{n}{n_1\ n_2\ \cdots\ n_r-1} = \\
= \ &\tfrac{n!}{(n_1-1)!n_2!\cdots n_r!} + \tfrac{n!}{n_1!(n_2-1)!\cdots n_r!} + \cdots + \tfrac{n!}{n_1!n_2!\cdots(n_r-1)!} = \\
= \ &\tfrac{n_1 n!}{n_1!n_2!\cdots n_r!} + \tfrac{n_2 n!}{n_1!n_2!\cdots n_r!} + \cdots + \tfrac{n_r n!}{n_1!n_2!\cdots n_r!} = \\
= \ &\tfrac{(n_1+n_2+\cdots+n_r)n!}{n_1!n_2!\cdots n_r!} = \tfrac{(n+1)!}{n_1!n_2!\cdots n_r!} = \\
= \ &\tbinom{n+1}{n_1\ n_2\ \cdots\ n_r}
\end{aligned}$$

■

**Teorema 3.3.1** (Teorema Multinomial)**.** *Sea $A$ un anillo conmutativo, y $x_1, x_2, \cdots x_r \in A$. Entonces, para cada $n \in \mathbb{N}$ se verifica que:*

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{n_1+n_2+\cdots+n_r=n} \binom{n}{n_1\ n_2\ \cdots\ n_r} x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}$$

*Demostración:* La demostración la haremos por inducción. Para $n = 1$ el resultado es cierto, pues dice simplemente que

$$(x_1 + x_2 + \cdots + x_n)^1 = x_1 + x_2 + \cdots + x_n$$

pues las únicas formas de poner 1 como suma de $r$ números naturales es $1 + 0 + \cdots + 0$ (que da lugar al sumando $x_1$), $0 + 1 + \cdots + 0$ (que da lugar al sumando $x_2$) y así sucesivamente.

Supongamos que el resultado es cierto para un exponente $n$ y vamos a demostrarlo para $n+1$. Entonces se tiene que

$$(x_1 + x_2 + \cdots + x_r)^{n+1} = (x_1 + x_2 + \cdots + x_r)^n (x_1 + x_2 + \cdots + x_r) = a \cdot (x_1 + x_2 + \cdots + x_r)$$

donde $a = (x_1 + x_2 + \cdots + x_r)^n$.

Dados $n_1, n_2, \cdots n_r \in \mathbb{N}$ tales que $n_1 + n_2 + \cdots + n_r = n + 1$, el coeficiente de $x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}$ en $(x_1+x_2+\cdots+x_r)^{n+1}$ se obtendrá sumando los coeficientes de $x_1^{n_1-1} x_2^{n_2} \cdots x_r^{n_r}$, $x_1^{n_1} x_2^{n_2-1} \cdots x_r^{n_r}$ y así hasta $x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r-1}$ en $a$. Por hipótesis de inducción, estos coeficientes valen $\binom{n}{n_1-1\ n_2\ \cdots\ n_r}$, $\binom{n}{n_1\ n_2-1\ \cdots\ n_r}$ y $\binom{n}{n_1\ n_2\ \cdots\ n_r-1}$, y su suma, según el lema precedente es $\binom{n+1}{n_1\ n_2\ \cdots\ n_r}$. ■

**Ejemplo 3.3.2.** *El número* 3 *se puede expresar de* $\binom{3+3-1}{3-1} = 10$ *formas diferentes como suma de* 3 *números naturales. Éstas son:*

$$3+0+0 \quad 2+1+0 \quad 2+0+1 \quad 1+2+0 \quad 1+1+1 \quad 1+0+2 \quad 0+3+0 \quad 0+2+1 \quad 0+1+2 \quad 0+0+3$$

*Por tanto, en el desarrollo de* $(x+y+z)^3$ *aparecen* 10 *sumandos. El desarrollo es:*

$$\frac{3!}{3!0!0!}x^3y^0z^0 + \frac{3!}{2!1!0!}x^2y^1z^0 + \frac{3!}{2!0!1!}x^2y^0z^1 + \frac{3!}{1!2!0!}x^1y^2z^0 + \frac{3!}{1!1!1!}x^1y^1z^1 +$$
$$+\frac{3!}{1!0!2!}x^1y^0z^2 + \frac{3!}{0!3!0!}x^0y^3z^0 + \frac{3!}{0!2!1!}x^0y^2z^1 + \frac{3!}{0!1!2!}x^0y^1z^2 + \frac{3!}{0!0!3!}x^0y^0z^3$$

*es decir,*

$$(x+y+z)^3 = x^3 + 3x^2y + 3x^2z + 3xy^2 + 6xyz + 3xz^2 + y^3 + 3y^2z + 3yz^2 + z^3$$

El teorema multinomial tiene también una demostración combinatoria.

$$(x_1 + x_2 + \cdots + x_r)^n = \underbrace{(x_1 + x_2 + \cdots + x_r)}_{c_1}\underbrace{(x_1 + x_2 + \cdots + x_r)}_{c_2} \cdots \underbrace{(x_1 + x_2 + \cdots + x_r)}_{c_n}$$

Cada término de $(x_1+x_2+\cdots+x_r)^n$ se obtiene multiplicando un sumando de $c_1$, con un sumando de $c_2$ y así hasta $c_n$. El coeficiente de $x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}$ en $(x_1 + x_2 + \cdots + x_r)^n$ se obtendrá contando cuantos términos (obtenidos como acabamos de decir) hay en los que ha elegido $n_1$ veces el sumando $x_1$, $n_2$ veces el sumando $x_2$ y así sucesivamente.

En definitiva, lo que hay que hacer es ver de cuantas maneras diferentes se pueden distribuir los "objetos" $c_1, c_2, \cdots, c_n$ en $r$ cajas distinguibles $(x_1, x_2, \cdots, x_r)$; y esto sabemos que se puede hacer de $\binom{n}{n_1\ n_2\ \cdots\ n_r}$ formas diferentes.

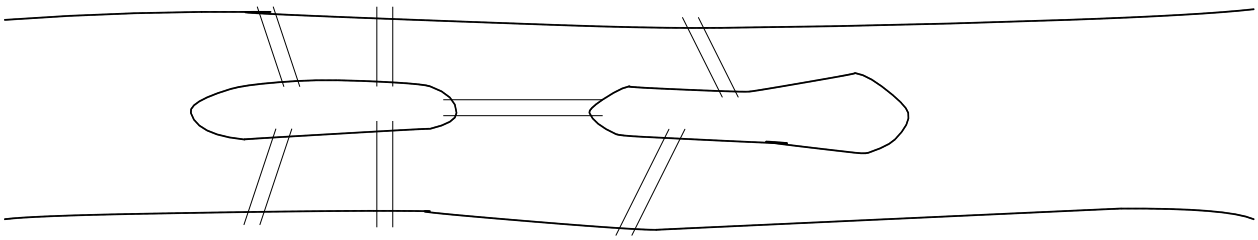
# Capítulo 4

# Introducción a la teoría de grafos

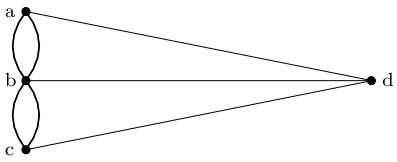
## 4.1. Generalidades sobre grafos

En esta sección vamos a comenzar el estudio de la teoría de Grafos. El inicio de esta teoría tuvo lugar en 1736, en un artículo de Leonhard Euler. El trabajo surgió de un problema conocido como el *problema de los puentes de Königsberg.*

> Durante el Siglo XVIII, la ciudad de Königsberg, en Prusia Oriental estaba dividida en cuatro zonas por el río Pregel. Había siete puentes que comunicaban estas regiones, tal y como se muestra en el dibujo. Los habitantes de la ciudad hacían paseos dominicales tratando de encontrar una forma de caminar por la ciudad, cruzando cada puente una sola vez, y regresando al lugar de partida.



Para resolver este problema, Euler representó las cuatro zonas como cuatro puntos, y los puentes como aristas que unen los puntos, tal y como se muestra en la figura.




Más adelante veremos cómo resolver el problema.

Por ahora nos quedamos con la representación que hizo Euler. En ella intervienen cuatro puntos (a los que denominaremos vértices), a saber, $a, b, c, d$ y siete aristas o lados que conectan algunos de los vértices. Esto da pie a la siguiente definición de grafo.

**Definición 27.** *Un grafo $G$ es un par $(V, E)$, donde $V$ y $E$ son conjuntos, junto con una aplicación*

$$\gamma_G : E \to \{\{u, v\} : u, v \in V\}.$$

*Al conjunto $V$ se le llama conjunto de vértices; al conjunto $E$ conjunto de lados o aristas, y a la aplicación $\gamma_G$ (o simplemente $\gamma$) aplicación de incidencia.*

**Ejemplo 4.1.1.** *En el caso de los puentes de Königsberg, el grafo correspondiente tiene como conjunto de vértices al conjunto* $V = \{a, b, c, d\}$*, como conjunto de lados el conjunto* $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ *y la aplicación de incidencia es la dada por:*

$$\gamma_G(e_1) = \gamma_G(e_2) = \{a, b\} \quad \gamma_G(e_3) = \gamma_G(e_4) = \{b, c\} \quad \gamma_G(e_5) = \{a, d\} \quad \gamma_G(e_6) = \{b, d\} \quad \gamma_G(e_7) = \{c, d\}.$$

Si $e_1$ y $e_2$ son dos lados tales que $\gamma_G(e_1) = \gamma_G(e_2)$, se dice que son *lados paralelos.*

Un lado tal que $\gamma_G(e) = \{v\}$ se dice *un lazo.*

Algunos autores, al definir un grafo, no incluyen la posibilidad de que tenga lados paralelos ni lazos. En tal caso, lo que aquí hemos definido como un grafo lo denominan como *multigrafo.*

**Definición 28.** *Un grafo dirigido u orientado es un par* $(V, E)$*, donde* $V$ *y* $E$ *son conjuntos, junto con dos aplicaciones* $s, t : E \to V$*.*

*Al conjunto* $V$ *se le llama conjunto de vértices, al conjunto* $E$ *conjunto de lados, y a las aplicaciones* $s$ *y* $t$ *aplicaciones dominio y codominio ("source" y "target").*

**Definición 29.** *Sea* $G = (V, E)$ *un grafo con aplicación de incidencia* $\gamma_G$*. Un subgrafo de* $G$ *es un nuevo grafo* $G' = (V', E')$ *donde* $V' \subseteq V$*,* $E' \subseteq E$ *y se verifica que* $\gamma_{G'}(e) = \gamma_G(e)$ *para cualquier* $e \in E'$*.*

*Si* $G' = (V', E')$ *es un subgrafo de un grafo* $G = (V, E)$*, se dice que es un subgrafo completo si dado* $e \in E$ *tal que* $\gamma_G(e) \subseteq V'$*, se verifica que* $e \in E'$*. Dicho de otra forma, si tiene todos los lados que tenía* $G$ *y que unen vértices de* $V'$*.*

**Observación:**

Un subgrafo completo está completamente determinado por el conjunto de vértices. Así, para determinar un subgrafo de un grafo $G$ en ocasiones explicitaremos únicamente el conjunto de vértices de dicho subgrafo, sobreentendiendo que se trata del subgrafo completo con dicho conjunto de vértices.

**Definición 30.** *Sea* $G$ *un grafo. Un camino de longitud* $n$ *es una sucesión de lados* $e_1 e_2 \cdots e_n$*, junto con una sucesión de vértices* $v_0 v_1 \cdots v_n$ *tales que* $\gamma_G(e_i) = \{v_{i-1}, v_i\}$*.*

*En tal caso se dice que el camino* $e_1 e_2 \cdots e_n$ *es un camino del vértice* $v_0$ *al vértice* $v_n$*.*

Se considera un camino de longitud cero de $v$ a $v$ a aquel cuya sucesión de vértices es $v$ y cuya sucesión de lados es vacía.

Para dar un camino en un grafo, en ocasiones daremos únicamente la sucesión de vértices, y en ocasiones daremos únicamente la sucesión de lados.

Nótese que si $e_1 e_2 \cdots e_n$ es un camino de $u$ a $v$, entonces $e_n e_{n-1} \cdots e_2 e_1$ es un camino de $v$ a $u$.

Un camino en el que no aparecen lados repetidos se llama *recorrido.*

Un recorrido en el que no hay vértices repetidos (salvo eventualmente el primero y el último) se llama *camino simple.*

Un camino en el que coinciden el primer y el último vértice se llama *camino cerrado.*

Un recorrido que es a la vez camino cerrado se llama *circuito.*

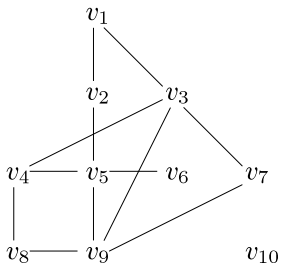
Un circuito que a su vez es camino simple es un *ciclo.*

La siguiente tabla puede ayudar a aclarar estas definiciones.

| Vértices repetidos | Aristas repetidas | Abierto | Nombre |
|---|---|---|---|
| | | | Camino |
| | | No | Camino cerrado |
| | No | | Recorrido |
| | No | No | Circuito |
| No | No | | Camino simple |
| No | No | No | Ciclo |

Por tanto, en un circuito puede haber o puede no haber vértices repetidos. Sin embargo, no puede haber aristas repetidas. Se tiene entonces, por ejemplo, que todo ciclo es un circuito, es un camino cerrado y es un camino.

**Ejemplo 4.1.2.** *Consideramos el siguiente grafo:*




*La sucesión $v_7v_3v_9v_5v_4v_8v_9v_3$ es un camino de longitud 7 que une $v_7$ con $v_6$. No es recorrido, pues el lado que une $v_3$ con $v_9$ aparece dos veces en el camino.*

*La sucesión $v_1v_3v_9v_8v_4v_3v_7$ es un camino de longitud 6 que une $v_1$ con $v_7$. Es un recorrido, pues ningún lado se repite. Sin embargo, el camino pasa dos veces por el vértice $v_3$. No es por tanto un camino simple.*

*$v_3v_4v_8v_9$ es un camino simple de longitud 3.*

*La sucesión $v_1v_3v_7v_9v_3v_4v_5v_2v_1$ es un camino cerrado de longitud 8. Es además un circuito, pues ningún lado se encuentra repetido. No es un ciclo, ya que el vértice $v_3$ se repite.*

*Un ejemplo de ciclo podría ser $v_1v_2v_5v_9v_7v_3v_1$.*

**Proposición 4.1.1.** *Sea $G$ un grafo. Supongamos que existe un camino de $u$ a $v$. Entonces existe un camino simple de $u$ a $v$.*

*Demostración:* Supongamos que el camino es $u = v_1v_2\cdots v_n = v$. Si el camino no es simple, debe haber dos vértices repetidos. Sean estos $v_i$ y $v_j$, con $i < j$. En tal caso, se tiene que $v_1\cdots v_iv_{j+1}\cdots v_n$ es un camino de $u$ a $v$. Si este camino no fuera simple, repetiríamos el proceso, hasta llegar a un camino simple. ■

**Proposición 4.1.2.** *Sea $G$ un grafo, y sean $u$ y $v$ dos vértices distintos. Supongamos que tenemos dos caminos simples distintos de $u$ a $v$. Entonces existe un ciclo en $G$.*

**Ejemplo 4.1.3.** *En el Ejemplo 4.1.2 teníamos un camino de longitud 6 que une $v_1$ con $v_7$ ($v_1v_3v_9v_8v_4v_3v_7$). Este camino no es simple, pues el vértice $v_3$ está repetido. Eliminamos los vértices que se encuentran entre las dos apariciones de $v_3$ y obtenemos el camino $v_1v_3v_7$, que es un camino simple que une $v_1$ con $v_7$.*

*Por otra parte, tenemos dos caminos simples que unen $v_3$ con $v_8$, como son $v_3v_4v_8$ y $v_3v_9v_8$. A partir de estos dos caminos podemos obtener el ciclo $v_3v_4v_8v_9v_3$, recorriendo en primer lugar uno de los caminos que une $v_3$ con $v_8$, y recorriendo a continuación el otro en sentido contrario.*

*Nótese que si partimos de los caminos simple $v_3v_4v_8$ y $v_3v_1v_2v_5v_4v_8$ y repetimos lo hecho en el párrafo precedente obtenemos el camino cerrado $v_3v_4v_8v_4v_5v_2v_1v_3$ que no es un ciclo, pues el vértice $v_4$ está repetido (o el lado $v_4v_8$). Sin embargo, la existencia de los dos caminos simples sí nos da la existencia de un ciclo, a saber, $v_3v_4v_5v_2v_1v_3$.*

*A la luz de estos dos ejemplos se deja como ejercicio demostrar la proposición 4.1.2.*

**Definición 31.** *Sea $G$ un grafo. Se dice que $G$ es conexo, si dados $u$ y $v$ dos vértices de $G$ existe al menos un camino de $u$ a $v$.*

En general, si $G$ es un grafo, podemos definir en el conjunto de vértices la relación:

$$uRv \text{ si existe un camino de } u \text{ a } v.$$

Esta relación es de equivalencia, pues:

Es reflexiva ya que todo vértice está unido con él mismo por un camino de longitud cero.

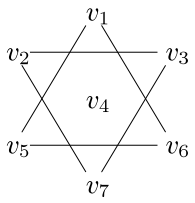
Es simétrica pues si $e_1e_2\cdots e_n$ es un camino de $u$ a $v$ entonces $e_ne_{n-1}\cdots e_1$ es un camino de $v$ a $u$.

Es transitiva pues si $e_1e_2\cdots e_n$ es un camino de $u$ a $v$ y $e'_1e'_2\cdots e'_m$ es un camino de $v$ a $w$, entonces $e_1e_2\cdots e_ne'_1e'_2\cdots e'_m$ es un camino de $u$ a $w$.

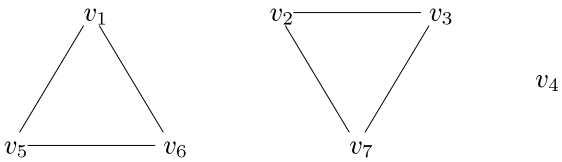
Se tiene entonces que un grafo es conexo si el conjunto cociente por la relación que acabamos de definir tiene un solo elemento.

A partir de esta relación, podemos considerar, para cada clase de equivalencia, el subgrafo (completo) determinado por los vértices de dicha clase de equivalencia. Cada uno de estos grafos es lo que se denomina una *componente conexa de* $G$.

**Ejemplo 4.1.4.** *Consideramos el siguiente grafo:*




*tiene tres componentes conexas. Éstas son*




## 4.2. Matrices asociadas a grafos

En esta sección vamos a ver cómo podemos representar los grafos finitos mediante matrices. A partir de estas matrices podremos obtener propiedades sobre los grafos.

**Definición 32.** *Sea $G$ un grafo cuyo conjunto de vértices es $V = \{v_1, v_2, \cdots, v_n\}$. Se define su* matriz de adyacencia *como la matriz $A \in \mathcal{M}_n(\mathbb{N})$ cuyo coeficiente $(i, j)$ es igual al número de lados e que unen $v_i$ con $v_j$ (es decir, que verifican que $f(e) = \{v_i, v_j\}$).*

**Observaciones:**

1. La matriz de adyacencia de un grafo es una matriz simétrica, pues cada lado que une $v_i$ con $v_j$ une también $v_j$ con $v_i$.
2. Si tomáramos otra ordenación de los vértices, la matriz de adyacencia es diferente. Por tanto, un grafo puede tener varias matrices de adyacencia. En general, si $A$ y $C$ son dos matrices de adyacencia de un mismo grafo, entonces existe una matriz de permutación $P$ tal que $P^{-1}CP = A$ (una matriz de permutación es una matriz que tiene en cada fila y en cada columna un coeficiente que vale "uno" y el resto toman el valor "cero". Es una matriz que se obtiene a partir de la matriz identidad realizando intercambio de filas y/o columnas).

3. La existencia de lados paralelos se traduce en la matriz de adyacencia en la existencia de coeficientes mayores que 1. De la misma forma, la existencia de lazos se traduce en que algún elemento de la diagonal principal de la matriz de adyacencia es distinto de cero.

4. Si tenemos un grafo dirigido, también podemos definir su matriz de adyacencia. En este caso, el coeficiente $a_{ij}$ es el número de lados que verifican que $s(e) = v_i$ y $t(e) = v_j$. En este caso, la matriz no tiene porqué ser simétrica.

5. La matriz de adyacencia de un grafo determina a éste. Además, toda matriz cuadrada con coeficientes en $\mathbb{N}$ es la matriz de adyacencia de un grafo (dirigido o no) finito. Podríamos entonces tomar como definición de grafo la de una matriz cuadrada con coeficientes en $\mathbb{N}$.

El siguiente resultado nos muestra la importancia de las matrices de adyacencia.

**Proposición 4.2.1.** *Sea $G$ un grafo cuyo conjunto de vértices es $\{v_1, v_2, \cdots, v_n\}$ y sea $A$ su matriz de adyacencia. Entonces el coeficiente $(i, j)$ de la matriz $A^n$ es igual al número de caminos de longitud $n$ que unen $v_i$ con $v_j$.*

*Demostración:* Hagamos la demostración por inducción. Para $n = 1$ el resultado no es más que la definición de la matriz de adyacencia.

Supongamos que el resultado es cierto para $n - 1$ y demostrémoslo para $n$.

Sea entonces $B = A^{n-1}$ y $C = A^n$. Queremos probar que $c_{ij}$ es el número de caminos de longitud $n$ que unen $v_i$ con $v_j$. Es claro que $c_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}$.

Todos los caminos de longitud $n$ entre $v_i$ y $v_j$ se obtienen añadiendo a un camino de longitud $n - 1$ entre $v_i$ y $v$ el vértice $v_j$; y esto podremos hacerlo únicamente cuando tengamos un lado que incide en los vértices $v$ y $v_j$. Por tanto, para contar los caminos de longitud $n$ entre $v_i$ y $v_j$ necesitamos, para cada vértice $v_k : k = 1, 2, \cdots, n$ contar los caminos de longitud $n - 1$ entre $v_i$ y $v_k$, y por cada uno de estos, contar los lados (caminos de longitud 1) entre $v_k$ y $v_j$. Luego, realizar la suma de los resultados obtenidos para cada $k$. Es decir, estamos diciendo que el número de caminos de longitud $n$ entre $v_i$ y $v_j$ es:

$$b_{i1}a_{1j} + b_{i2}a_{2j} + \cdots + b_{in}a_{nj} = c_{ij}$$

como queríamos.

Nótese que este razonamiento vale tanto si el grafo $G$ es dirigido como si no lo es. ■

**Definición 33.** *Sea $G$ un grafo cuyo conjunto de vértices es $V = \{v_1, v_2, \cdots, v_n\}$ y cuyo conjunto de lados es $E = \{e_1, e_2, \cdots, e_m\}$. Se define la* matriz de incidencia *del grafo $G$ como una matriz $n \times m$ que tiene en la posición $(i, j)$ un 1 si $v_i \in \gamma_G(e_j)$ y 0 en otro caso.*

**Observación:**

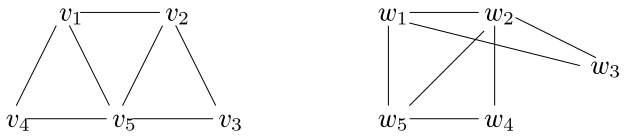
1. Si tomamos otra ordenación de los vértices y/o lados, la matriz de incidencia puede ser diferente. En este caso, dos matrices de incidencia corresponden al mismo grafo si se puede pasar de una a otra mediante operaciones elementales por filas y/o columnas Tipo I (intercambio de filas y/o columnas).

2. El que un grafo tenga lados paralelos se traduce en que tenga dos columnas iguales en la matriz de incidencia, mientras que los lazos se traducen en filas con un único coeficiente "uno".

3. Si el grafo es dirigido, se puede definir también la matriz de incidencia. En este caso, el coeficiente $(i, j)$ puede también tomar el valor $-1$ (si el lado $e_j$ parte del vértice $v_i$). En tal caso, el grafo no podría tener lazos.

## 4.3. Isomorfismo de grafos

Consideremos los siguientes grafos

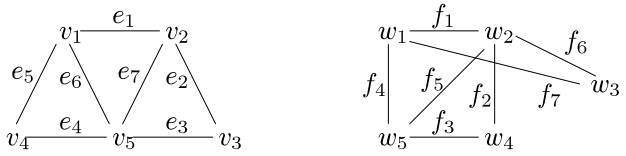



En una primera observación apreciamos dos grafos diferentes. Sin embargo, si profundizamos algo más encontramos muchas semejanzas entre ellos. Por ejemplo, ambos tienen igual número de vértices e igual número de lados. Existe un vértice en cada uno de ellos ($v_5$ en el primero y $w_2$ en el segundo) que está unidos al resto de vértices.

Siguiendo en esta línea, vemos que podemos renombrar los vértices del segundo grafo $w_1 \mapsto v'_1$, $w_2 \mapsto v'_5$, $w_3 \mapsto v'_4$, $w_4 \mapsto v'_3$ y $w_5 \mapsto v'_2$, y tenemos que por cada lado que une dos vértices $v_i$ y $v_j$ en el primer grafo tenemos un lado que une los vértices $v'_i$ y $v'_j$ en el segundo.

Vemos entonces que ambos grafos podemos considerarlos iguales. Lo único que los diferencia es el nombre que le hemos dado a los vértices (y a los lados) y la forma en que los hemos representado. Pero todo lo que digamos sobre un grafo es válido para el otro.

Para precisar un poco más lo que hemos hecho, vamos a ponerle nombre a los lados:




Entonces, lo que tenemos son dos biyecciones $h_V : V_G \to V_{G'}$ y $h_E : E_G \to E_{G'}$, que en este caso serían:

| $h_V$ | $h_E$ |
|---|---|
| $v_1 \mapsto w_1$ | $e_1 \mapsto f_4$ |
| $v_2 \mapsto w_5$ | $e_2 \mapsto f_3$ |
| $v_3 \mapsto w_4$ | $e_3 \mapsto f_2$ |
| $v_4 \mapsto w_3$ | $e_4 \mapsto f_6$ |
| $v_5 \mapsto w_2$ | $e_5 \mapsto f_7$ |
| | $e_6 \mapsto f_1$ |
| | $e_7 \mapsto f_5$ |

verificando que si $\gamma_G(e) = \{u, v\}$ entonces $\gamma_{G'}(h_E(e)) = \{h_V(u), h_V(v)\}$.

Nótese que en este caso, la aplicación $h_V$ determina totalmente a la aplicación $h_E$.

Esto da pie a la siguiente definición:

**Definición 34.** *Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos con aplicaciones de incidencia $\gamma_G$ y $\gamma_{G'}$. Se dice que $G$ y $G'$ son isomorfos si existen dos biyecciones $h_V : V \to V'$ y $h_E : E \to E'$ tales que para cada lado $e \in E$ se verifica que $\gamma_{G'}(h_E(e)) = \{h_V(u), h_V(v)\}$ donde $\{u, v\} = \gamma_G(e)$.*

*En tal caso, diremos que las aplicaciones $h_V$ y $h_E$ forman un* isomorfismo *de $G$ a $G'$.*

**Observación:**

1. Si los grafos no tienen lados paralelos, entonces la aplicación $h_V$ determina de forma única a la aplicación $h_E$. De ahí, que normalmente, para dar un isomorfismo de grafos se de únicamente como actúa sobre los vértices.

2. Si $h = (h_V, h_E)$ es un isomorfismo de $G$ a $G'$ entonces $((h_V)^{-1}, (h_E)^{-1})$ es un isomorfismo de $G'$ a $G$.

En general, no es fácil determinar cuando dos grafos son isomorfos o no lo son. Claramente, si dos grafos son isomorfos deben tener igual número de vértices e igual número de lados. Sin embargo, esto no es suficiente, como pone de manifiesto el siguiente ejemplo.

pues ambos tiene cuatro vértices y cuatro lados, y sin embargo no son isomorfos (¿por qué?).

Vemos que tenemos dos números asociados a cada grafo (número de vértices y número de lados) que deben coincidir para que los grafos sean isomorfos. Es lo que se llama *invariante por isomorfismo*. Obviamente, la coincidencia de estos números no implica que los grafos sean isomorfos.

**Definición 35.** *Una propiedad se dice invariante por isomorfismo si dados dos grafos isomorfos $G$ y $G'$, uno satisface la propiedad si, y sólo si, la satisface el otro.*

**Definición 36.** *Sea $G$ un grafo y $v$ un vértice de $G$. Se define el grado de $v$, y lo denotaremos como $gr(v)$, como el número de lados (no lazos) de $G$ que son incidentes en $v$ más 2 veces el número de lazos incidentes en $v$.*

*Denotaremos por $D_k(G)$ como el número de vértices de $V$ que tienen grado igual a $k$. A partir de esto, podemos construir la sucesión*

$$D_0(G), D_1(G), D_2(G), \ldots, D_k(G), \ldots$$

*que llamaremos* sucesión de grados.

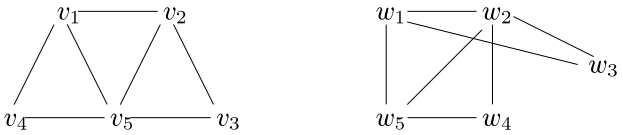
Nótese que si $G$ es un grafo con $n$ vértices $v_1, v_2, \ldots, v_n$ y $l$ lados entonces

$$gr(v_1) + gr(v_2) + \cdots + gr(v_n) = 2l,$$

pues al contar todos los lados que inciden en todos los vértices (el miembro de la izquierda) estamos contando cada lado 2 veces (por cada uno de los vértices en los que incide)

**Ejemplo 4.3.1.**

1. *En los grafos siguientes*




*se tiene que $gr(v_3) = gr(v_4) = 2$, $gr(v_1) = gr(v_2) = 3$, $gr(v_5) = 4$. Por tanto, $D_0(G) = D_1(G) = 0$, $D_2(G) = 2$, $D_3(G) = 2$, $D_4(G) = 1$. La sucesión de grados es por tanto*

$$0, 0, 2, 2, 1, 0, 0, \ldots$$

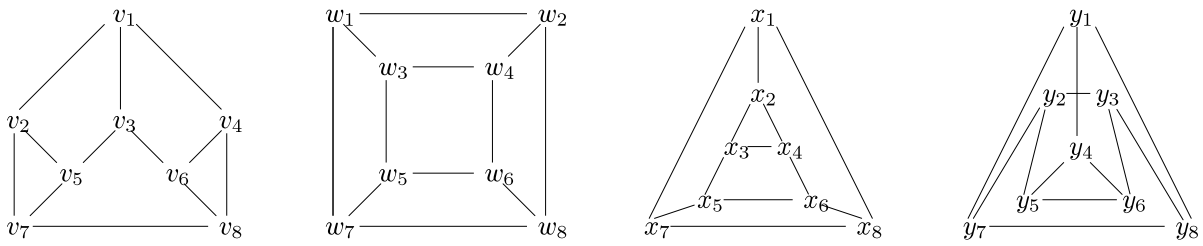
*Para el otro grafo se tiene que $gr(w_3) = gr(w_4) = 2$, $gr(w_1) = gr(w_5) = 3$, $gr(w_2) = 4$. La sucesión de grados resulta ser la misma que en el grafo anterior.*

2. *Las sucesiones de grados de los grafos*

*son respectivamente* $0, 0, 4, 0, 0, \ldots$ *y* $0, 1, 2, 1, 0, \ldots$

Es fácil comprobar que si $(h_V, h_E) : G \to G'$ es un isomorfismo de grafos y $v \in V$ entonces $gr(v) = gr(h_V(v))$, de donde deducimos que las sucesiones de grados de dos grafos isomorfos son iguales. El recíproco no es cierto, como podemos ver en el siguente ejemplo.

**Ejemplo 4.3.2.** *Consideramos los siguientes grafos:*




*En los cuatro grafos la sucesión de grados es la misma, pues todos los vértices tienen grado* 3 *(es decir, la sucesión de grados es en los cuatro casos* $0, 0, 0, 8, 0, \ldots$*). Sin embargo, el primero, tercero y cuarto son isomorfos y los isomorfismos vienen dados por*

$$\begin{array}{lllll} v_1 & \mapsto & x_5 & \mapsto & y_2 \\ v_2 & \mapsto & x_7 & \mapsto & y_7 \\ v_3 & \mapsto & x_6 & \mapsto & y_3 \\ v_4 & \mapsto & x_3 & \mapsto & y_5 \\ v_5 & \mapsto & x_8 & \mapsto & y_8 \\ v_6 & \mapsto & x_4 & \mapsto & y_6 \\ v_7 & \mapsto & x_1 & \mapsto & y_1 \\ v_8 & \mapsto & x_2 & \mapsto & y_4 \end{array}$$

*mientras que el segundo no es isomorfo a ninguno de los otros tres, ya que en este segundo no hay ciclos de longitud* 3*, mientras que en los otros sí los hay (*$v_2v_5v_7$ *por ejemplo).*

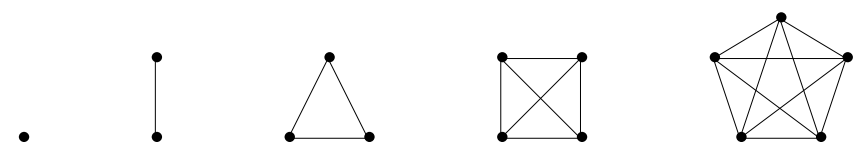
Los cuatro grafos que intervienen en este ejemplo tienen una peculiaridad, y es que todos los vértices tienen el mismo grado. Estos grafos reciben el nombre de *grafos regulares* de grado $n$ (si $n$ es el grado común de todos los vértices). En el ejemplo precedente, los cuatro grafos son grafos regulares de grado 3. Un ejemplo importante de grafos regulares son los grafos completos.

**Definición 37.** *Se llama grafo completo de* $n$ *vértices al grafo (con* $n$ *vértices) que no tiene vértices ni lados paralelos, y dados dos vértices hay un lado que los une. Dicho de otra forma, su matriz de adyacencia toma el valor "cero" en todos los elementos de la diagonal y el valor "uno" en el resto.*

*Dicho grafo se suele denotar como* $K_n$*.*

**Ejemplo 4.3.3.**

*Veamos cuales son los cinco primeros grafos completos:*



## 4.4. Sucesiones gráficas.

Sea $G$ un grafo sin lazos ni lados paralelos, cuyo conjunto de vértices es $\{v_1, v_2, \cdots, v_n\}$. Para cada $i$ entre 1 y $n$, sea $d_i = gr(v_i)$. Tenemos de esta forma una secuencia $d_1, d_2, \cdots, d_n$, que se corresponde con los grados de los vértices del grafo $G$.

Nos planteamos si dada una lista de $n$ números naturales $d_1, d_2, \cdots, d_n$, existe algún grafo (sin lazos ni lados paralelos) con $n$ vértices tal que los grados de esos vértices sean estos números naturales. Y en caso de que exista, cómo podríamos dar un grafo con tales características.

Antes de responder a estas cuestiones, vamos a introducir un poco de nomenclatura.

**Definición 38.** *Sean $d_1, d_2, \cdots, d_n \in \mathbb{N}$. Decimos que la sucesión $d_1, d_2, \cdots, d_n$ es una* sucesión gráfica *si existe un grafo $G$ sin lazos ni lados paralelos, con conjunto de vértices $V = \{v_1, v_2, \cdots, v_n\}$ y tal que $d_i = gr(v_i)$.*

*Si $d_1, d_2, \cdots, d_n$ es una sucesión gráfica, y $G$ es un grafo con $n$ vértices cuyos grados son los términos de la sucesión, diremos que $G$ es una* realización *de la sucesión $d_1, d_2, \cdots, d_n$.*

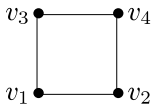
**Ejemplo 4.4.1.**

1. *La sucesión de $n$ términos $0, 0, \cdots, 0$ es una sucesión gráfica. Podemos considerar un grafo cuyo conjunto de vértices tiene $n$ elementos, y cuyo conjunto de lados es el conjunto vacío.*

2. *La sucesión $1, 1, 1, 1, 1, 1$ es una sucesión gráfica. Podemos verlo con el siguiente grafo.*


   *En general, cualquier sucesión con un número par de unos es una sucesión gráfica.*

3. *La sucesión $2, 2, 2, 2$ es una sucesión gráfica. El siguiente grafo es una realización de dicha sucesión.*




4. *La sucesión $4, 3, 3, 2, 2, 1$ no es una sucesión gráfica. Si esos fueran los grados de los vértices de un grafo, tendríamos que la suma de los grados de los vértices valdría 15, y eso es imposible, pues sabemos que esa suma es igual al doble del número de lados (lo que supondría que el grafo tiene siete lados y medio).*

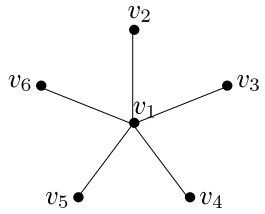
5. *La sucesión $5, 4, 3, 2, 2$ no es una sucesión gráfica. De serlo, tendríamos un grafo (sin lazos ni lados paralelos) con cinco vértices, y un vértice de grado 5. Pero el grado de un vértice no puede ser mayor que 4, pues como mucho, un vértice puede estar unido a los cuatro restantes.*

Los dos últimos ejemplos nos dan dos condiciones necesarias para que una sucesión sea gráfica. Por una parte, la suma de los elementos de la sucesión debe ser un número par, y por otra, cualquier elemento de la sucesión debe ser menor que el número de términos.

Sin embargo, estas dos condiciones no son suficientes. Por ejemplo, consideramos la sucesión 5, 4, 4, 2, 2, 1. Vamos a ver que no es una sucesión gráfica.

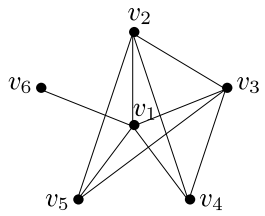
Vemos que la suma de los términos de la sucesión es 18, que es un número par. Además, hay seis términos y el mayor de ellos vale 5. Por tanto, las dos condiciones que hemos visto son satisfechas por esta sucesión.

Supongamos que hubiera un grafo con seis vértices cuyos grados fueran los elementos de la sucesión. Sean estos vértices $v_1, v_2, v_3, v_4, v_5, v_6$. Hay uno de los vértices cuyo grado es cinco, luego este vértice debe estar unido a los cinco restantes. Suponemos que dicho vértice es $v_1$. Es decir, tendríamos:




También tiene que haber un vértice de grado 1. Supongamos que es, por ejemplo, $v_6$. Este vértice está unido a $v_1$, luego ya no puede unirse a ninguno más.

Por último, tenemos dos vértices de grado 4. Por ejemplo, $v_2$ y $v_3$. Entonces, estos deben unirse a 3 vértices más. Como no pueden unirse a $v_6$, las únicas posibilidades son, que $v_2$ esté unido a $v_3$, $v_4$ y $v_5$ y que $v_3$ esté unido a $v_2$, $v_4$ y $v_5$. Tenemos entonces:




Y vemos que los vértices $v_4$ y $v_5$ tienen grado 3, cuando deberían tener grado 2.

De esta forma hemos visto que la sucesión $5, 4, 4, 2, 2, 1$ no es gráfica. Pero esta forma de ir probando a ver si encontramos o no un grafo con las condiciones requeridas parece no ser muy práctica.

Lo que vamos a hacer es dar un método más preciso para determinar si una sucesión dada es una sucesión gráfica. Para esto, necesitamos el siguiente resultado.

**Teorema 4.4.1** (Havel-Hakimi). *Sea $d_1, d_2, \cdots, d_n$ una sucesión de números naturales. Supongamos que están ordenados en orden decreciente, es decir, $d_1 \geq d_2 \geq \cdots \geq d_n$ y que $d_1 < n$.*

*Entonces esta sucesión es gráfica si, y sólo si, lo es la sucesión $d_2 - 1, \cdots, d_{d_1+1} - 1, d_{d_1+2}, \cdots, d_n$.*

**Observación:**

La condición $d_1 < n$ lo que nos dice es que no puede haber un vértice cuyo grado sea mayor o igual al número de vértices. Sabemos que si esto no se da, la sucesión no es gráfica, luego esto no supone ninguna restricción.

Podríamos comprobar en un principio si la suma $d_1 + \cdots + d_n$ es un número par, pues sabemos que si esa suma es impar la sucesión no es gráfica. Pero no es necesario realizar esa comprobación, pues en el proceso que vamos a dar, detectaremos esa circunstancia.

*Demostración:*

Demostremos en primer lugar que si existe un grafo $G$ tal que los grados de sus vértices son $d_2 - 1, \cdots, d_{d_1+1} - 1, d_{d_1+2}, \cdots, d_n$, entonces existe un grafo $G'$ tal que los grados de sus vértices son $d_1, d_2, \cdots, d_n$.

Sea $G$ un tal grafo, y supongamos que el conjunto de vértices de $G$ es $\{v_1, v_2, \cdots, v_{d_1}, v_{d_1+1}, \cdots v_{n-1}\}$, y que

$$gr(v_i) = \begin{cases} d_{i+1} - 1 & \text{si } 1 \leq i \leq d_1 \\ d_{i+1} & \text{si } d_1 < i \leq n-1 \end{cases}$$

es decir,

$$gr(v_1) = d_2 - 1; \quad gr(v_2) = d_3 - 1; \quad \cdots \quad gr(v_{d_1}) = d_{d_1+1} - 1; \quad gr(v_{d_1+1}) = d_{d_1+2}; \quad \cdots \quad gr(v_{n-1}) = d_n$$

Formamos entonces el grafo $G'$ añadiendo un nuevo vértice $v_0$ al grafo $G$, y los lados $\{v_0, v_1\}$, $\{v_0, v_2\}$, $\cdots \{v_0, v_{d_1}\}$.

Entonces:

$gr(v_0) = d_1$, pues $v_0$ está unido a los vértices $v_1, v_2, \cdots, v_{d_1}$.

El grado de los vértices $v_1, v_2, \cdots, v_{d_1}$ ha aumentado en uno, pues cada uno de ellos se ha unido al vértice $v_0$. Por tanto, $gr(v_1) = d_2,\ gr(v_2) = d_3, \cdots, gr(v_{d_1}) = d_{d_1+1}$.

El grado de los vértices $v_{d_1+1}, \cdots, v_{n-1}$ no ha variado.

Por tanto, tenemos:

| Vértice | $v_0$ | $v_1$ | $\cdots$ | $v_{d_1}$ | $v_{d_1+1}$ | $\cdots$ | $v_{n-1}$ |
|---|---|---|---|---|---|---|---|
| Grado | $d_1$ | $d_2$ | $\cdots$ | $d_{d_1+1}$ | $d_{d_1+2}$ | $\cdots$ | $d_n$ |

Es decir, hemos encontrado un grafo para el que los grados de sus vértices son los términos de la sucesión $d_1, d_2, \cdots, d_n$.

Recíprocamente, supongamos que tenemos un grafo $G$ con conjunto de vértices $\{v_1, v_2, \cdots, v_n\}$ tal que $gr(v_i) = d_i$.

Esto significa que el vértice $v_1$ está unido a $d_1$ vértices. Vamos a analizar en primer lugar el caso en que estos vértices son $v_2, v_3, \cdots, v_{d_1+1}$.

Entonces, si eliminamos del grafo $G$ el vértice $v_1$ y todos los lados que inciden en $v_1$, obtenemos un nuevo grafo cuyo conjunto de vértices es $\{v_2, \cdots, v_n\}$, y en el que el grado de los vértices $v_2, \cdots, v_{d_1+1}$ ha disminuido en uno (pues se ha eliminado el lado que lo une a $v_1$), y el grado de los vértices restantes se mantiene igual. Por tanto, hemos construido un grafo $G'$, con $n-1$ vértices, y cuyos grados son $d_2 - 1, \cdots, d_{d_1+1} - 1, d_{d_1+2}, \cdots, d_n$.

Nos situamos ahora en el caso de que el conjunto de vértices a los que está unido el vértice $v_1$ no es el conjunto $\{v_2, \cdots, v_{d_1+1}\}$. En este caso, no podemos repetir el razonamiento que acabamos de hacer.

Lo que vamos a hacer es transformar el grafo $G$ en otro grafo con los mismos vértices, con los mismos grados de cada vértice, pero que los vértices a los que está unido el grafo $v_1$ sean los vértices $v_2, \cdots, v_{d_1+1}$.

Puesto que el conjunto de vértices a los que está unido $v_1$ no es el conjunto $\{v_2, \cdots, v_{d_1+1}\}$, debe haber algún vértice de ese conjunto al que no está unido $v_1$, y debe haber algún vértice del conjunto $\{v_{d_1+2}, \cdots, v_n\}$ al que sí esté unido $v_1$.

Sean estos vértices $v_i$ y $v_j$ respectivamente. Tenemos:

- Un vértice $v_i$, con $2 \leq i \leq d_1 + 1$ que no está unido por un lado al vértice $v_1$ (no existe el lado $\{v_1, v_i\}$).
- Un vértice $v_j$, con $d_1 + 2 \leq j \leq n$ que está unido al vértice $v_1$ (tenemos el lado $\{v_1, v_j\}$).
- El grado de $v_i$ es mayor o igual que el grado de $v_j$.

Por lo que acabamos de decir, debe haber un vértice $v$ que esté unido a $v_i$ pero que no esté unido a $v_j$ (de no ser así, es decir, si todo vértice al que está unido $v_i$ estuviera unido también a $v_j$, y puesto que además $v_j$ está unido a $v_1$, el grado de $v_j$ sería mayor que el de $v_i$).

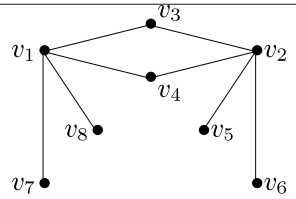
Tenemos entonces en nuestro grafo $G$ los lados $\{v_1, v_j\}$ y $\{v_i, v\}$, mientras que no están los lados $\{v_1, v_i\}$ ni $\{v_j, v\}$.

Eliminamos estos dos lados ($\{v_1, v_j\}$ y $\{v_i, v\}$) del grafo $G$, y le añadimos los lados $\{v_1, v_i\}$ $\{v_j, v\}$. De esta forma, conseguimos un nuevo grafo $G'$ con los mismos vértices que el grafo $G$, estos vértices tienen los mismos grados que en el grafo $G$, y ahora, el vértice $v_1$ está unido en $G'$ a todos los vértices del conjunto $\{v_2, \cdots, v_{d_1+1}\}$ que estaban unidos en el grafo $G$ a $v_1$, y además está unido al vértice $v_i$ (que está en ese mismo conjunto).

Esto que hemos hecho lo repetimos mientras queden vértices del conjunto $\{v_2, v_3, \cdots, v_{d_1+1}\}$ que no están unidos a $v_1$. Cuando esto ya no ocurra, procedemos a eliminar el vértice $v_1$ y todos los lados que inciden en él.

■

**Ejemplo 4.4.2.** *Vamos a ilustrar con un ejemplo el razonamiento que hemos seguido en la demostración anterior. Partimos del grafo $G$*




*Y vemos que* $gr(v_1) = gr(v_2) = 4$, $gr(v_3) = gr(v_4) = 2$, $gr(v_5) = gr(v_6) = gr(v_7) = gr(v_8) = 1$. *Por tanto, la sucesión* $4, 4, 2, 2, 1, 1, 1, 1$ *es una sucesión gráfica.*

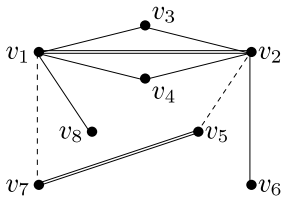
*Vamos a dar un grafo con siete vértices, cuyos grados serán* $3, 1, 1, 0, 1, 1, 1$.

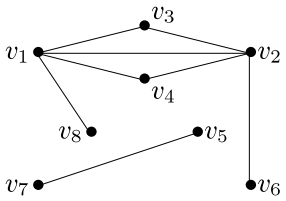
*Vemos en primer lugar que el vértice* $v_1$ *está unido a los vértices* $v_3$, $v_4$, $v_7$ *y* $v_8$. *Transformamos este grafo en otro con el mismo conjunto de vértices, y los mismos grados, pero de forma que los vértices adyacentes a* $v_1$ *sean* $v_2$, $v_3$, $v_4$ *y* $v_5$.

*De los vértices adyacentes a* $v_1$ *sólo hay dos del conjunto* $\{v_2, v_3, v_4, v_5\}$. *Tomamos un vértice de este conjunto que no esté unido por un lado a* $v_1$ *(por ejemplo, tomamos* $v_2$*), y un vértice que no esté en ese conjunto y que sea adyacente a* $v_1$, *por ejemplo* $v_7$ *(es decir, siguiendo la notación que hemos usado en la demostración,* $i = 2$ *y* $j = 7$*).*

*Buscamos un vértice* $v$ *que sea adyacente a* $v_2$ *y no lo sea a* $v_7$. *Por ejemplo,* $v = v_5$.

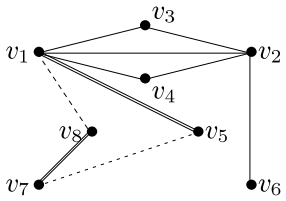
*Eliminamos los lados* $\{v_1, v_7\}$ *y* $\{v_2, v_5\}$, *y añadimos* $\{v_1, v_2\}$ *y* $\{v_5, v_7\}$. *En el dibujo siguiente representamos los lados que eliminamos con línea discontinua, y los lados que añadimos con trazo doble.*

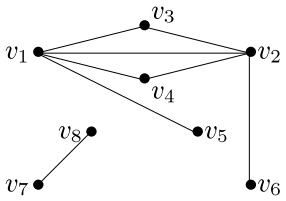



*Y ahora tenemos un grafo con los mismos vértices que el de partida, cada vértice tiene el mismo grado, pero el vértice* $v_1$ *está unido a tres vértices del conjunto* $\{v_2, v_3, v_4, v_5\}$. *Concretamente, a* $v_2$, $v_3$ *y* $v_4$. *Y está unido a un vértice de fuera de ese conjunto* ($v_8$). *Como el vértice que falta del conjunto* $\{v_2, v_3, v_4, v_5\}$ *tiene el mismo grado que el vértice* $v_8$ *ahora no sería necesario realizar ningún cambio (sólo intercambiar los vértices* $v_8$ *y* $v_5$*). Pero vamos a proceder tal y como hemos dicho en la demostración.*

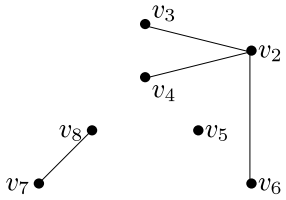
*Entonces, eliminamos los lados* $\{v_1, v_8\}$ *y* $\{v_5, v_7\}$, *y añadimos dos lados nuevos, a saber,* $\{v_1, v_5\}$ *y* $\{v_7, v_8\}$.




*Y así hemos conseguido un grafo con el mismo conjunto de vértices que le vértice* $G$, *cada vértice tiene el mismo grado que en el grafo* $G$, *pero ahora, el vértice* $v_1$ *está unido a los vértices* $v_2$, $v_3$, $v_4$ *y* $v_5$.

*Si ahora suprimimos del grafo* $G$ *el vértice* $v_1$, *y todos los lados que inciden en* $v_1$ *nos queda el grafo*



*Y obtenemos un grafo con un vértice menos, y los grados de los vértices son* $3, 1, 1, 0, 1, 1, 1$

Basándonos en el teorema, podemos determinar fácilmente si una sucesión es o no gráfica.

Para esto, partimos de una sucesión $d_1, d_2, \cdots, d_n$. Si sus elementos no están ordenados, los ordenamos de mayor a menor, así que supondremos que se tiene que $d_1 \geq d_2 \geq \cdots \geq d_n$.

A partir de esta sucesión formamos la sucesión $d_2 - 1, \cdots, d_{d_1+1} - 1, d_{d_1+2}, \cdots, d_n$. Esta sucesión se obtiene en dos etapas: En primer lugar, eliminamos el primer término. En segundo lugar, a los $d_1$ términos siguientes le restamos 1.

Si la respuesta a si esta sucesión es o no gráfica la conocemos, entonces sabremos si $d_1, \cdots, d_n$ es gráfica. Caso de no conocerla, repetimos el proceso para esta nueva sucesión.

Como en cada paso vamos disminuyendo, tanto el tamaño de la sucesión como el valor de sus términos, en un número finito de pasos terminaremos.

**Ejemplo 4.4.3.**

1. *Consideramos la sucesión* $2, 2, 2, 2$*, que sabemos que es gráfica. Vamos a comprobarlo usando el método aquí descrito.*

   *Como están ordenados los elementos, formamos la nueva sucesión eliminando el primer* $2$*, y restando* $1$ *a los dos términos siguientes. Tenemos entonces la sucesión* $(2-1), (2-1), 2$*, es decir,* $1, 1, 2$*. Esta es la nueva sucesión que tenemos que estudiar si es gráfica.*

   *La ordenamos (nos queda* $2, 1, 1$*). Eliminamos el primer término (tenemos así* $1, 1$*) y a los dos términos siguientes, le restamos uno (y llegamos a la sucesión* $0, 0$*).*

   *Esta sucesión sabemos que es gráfica, como ya hemos visto anteriormente.*

2. *Tomamos ahora la sucesión* $5, 4, 4, 2, 2, 1$*, que sabemos que no es gráfica. Vamos a comprobarlo usando el método que acabamos de describir.*

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 4 | 4 | 2 | 2 | 1 | *Eliminamos el* 5 *y restamos uno a los* 5 *términos siguientes.* |
| | 3 | 3 | 1 | 1 | 0 | *Están ordenados. Eliminamos el* 3 *y restamos uno a los* 3 *términos siguientes.* |
| | | 2 | 0 | 0 | 0 | *Eliminamos el* 2 *y restamos uno a los* 2 *términos siguientes.* |
| | | | $-1$ | $-1$ | 0 | |

   *Y hemos llegado a una sucesión que no es gráfica, pues no puede haber vértices con grado igual a -1. Por tanto, la sucesión de partida no puede ser gráfica.*

3. *Sea ahora la sucesión* $4, 3, 3, 2, 2, 1$*, que sabemos que no es gráfica pues la suma de sus términos es un número impar. Vamos a comprobarlo ahora basándonos en el teorema 4.4.1.*

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | 3 | 3 | 2 | 2 | 1 | *Eliminamos el* 4 *y restamos uno a los* 4 *términos siguientes.* |
| | 2 | 2 | 1 | 1 | 1 | *Eliminamos el* 2 *y restamos uno a los* 2 *términos siguientes.* |
| | | 1 | 0 | 1 | 1 | *Reordenamos.* |
| | | 1 | 1 | 1 | 0 | *Eliminamos el primer* 1 *y restamos uno al siguiente término.* |
| | | | 0 | 1 | 0 | *Reordenamos.* |
| | | | 1 | 0 | 0 | *Eliminamos el* 1 *y restamos uno al siguiente término.* |
| | | | | $-1$ | 0 | |

*Y vemos como nos ha vuelto a aparecer un* $-1$*.*

*Consideramos la sucesión* $4, 4, 3, 2, 2, 2, 1$*. Nos planteamos si es o no una sucesión gráfica.*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 4 | 3 | 2 | 2 | 2 | 1 | *Eliminamos el* 4 *y restamos uno a los* 4 *términos siguientes.* |
| | 3 | 2 | 1 | 1 | 2 | 1 | *Reordenamos.* |
| | 3 | 2 | 2 | 1 | 1 | 1 | *Eliminamos el* 3 *y restamos uno a los* 3 *términos siguientes.* |
| | | 1 | 1 | 0 | 1 | 1 | *Reordenamos.* |
| | | 1 | 1 | 1 | 1 | 0 | *Eliminamos el* 1 *y restamos uno al términos siguiente.* |
| | | | 0 | 1 | 1 | 0 | *Reordenamos.* |
| | | | 1 | 1 | 0 | 0 | *Eliminamos el* 1 *y restamos uno al siguiente término.* |
| | | | | 0 | 0 | 0 | |

*Y al llegar a una sucesión de ceros, deducimos que la sucesión de partida es una sucesión gráfica.*

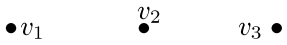
Supongamos que tenemos una sucesión, a la que le hemos aplicado el proceso anterior, y hemos llegado a una sucesión de ceros. Sabemos por tanto que la sucesión es gráfica. Nos planteamos encontrar un grafo de forma que los grados de sus vértices sean los términos de la sucesión.

La idea es ir recorriendo las distintas sucesiones que nos han ido apareciendo al revés, y en casa paso ir construyendo un grafo en el que se materialice la sucesión correspondiente.

Para esto, en cada paso, lo que hacemos es añadir un vértice que lo uniremos a tantos vértices como nos indica su grado.

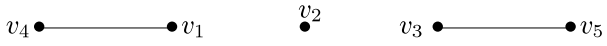
**Ejemplo 4.4.4.** *Tenemos la sucesión* $4,4,3,2,2,2,1$*, que sabemos que es gráfica pues lo hemos visto en el ejemplo precedente, ya que hemos llegado a la sucesión* $0,0,0$*.*

*Comenzamos con la sucesión 0, 0, 0, y formamos un grafo con tres vértices y cuyos grados sean estos, es decir, un grafo sin lados.*

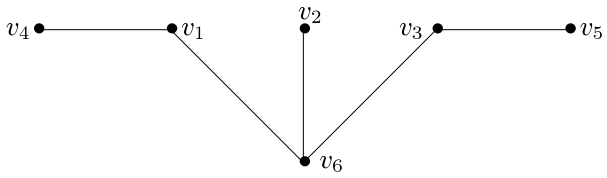



*Ahora pasamos a la sucesión* $1,1,0,0$*. Para esto, añadimos un vértice de grado 1, y lo unimos a uno de los que tenía grado cero (que pasa de grado cero a grado uno), por ejemplo, a* $v_1$*.*

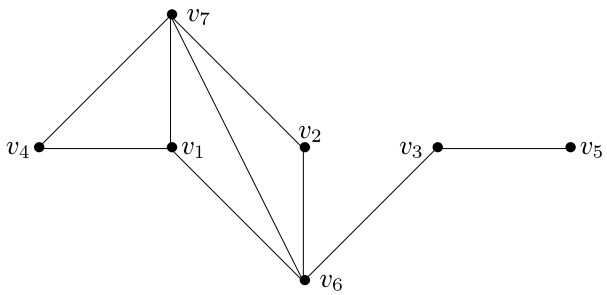

*La siguiente sucesión es* $1,1,1,1,0$*, que proviene de* $\mathbf{0},1,1,0$ *(donde hemos marcado en negrita el término de la sucesión que aumenta en uno). Por tanto, hemos de añadir un vértice nuevo (*$v_5$*) de grado uno, y unirlo a uno de grado cero (por ejemplo, a* $v_3$*).*




*De esta sucesión reordenada (*$\mathbf{1},\mathbf{1},\mathbf{0},1,1$*) pasamos a* $3,2,2,1,1,1$*. Por tanto, hemos de añadir un vértice (*$v_6$*), de grado 3, y unirlo a tres vértices de grados 1, 1 y 0 respectivamente. Tomamos entonces, por ejemplo,* $v_1$*,* $v_3$ *y* $v_2$*.*




*Y por último, llegamos a la sucesión* $4,4,3,2,2,2,1$*, que proviene de* $\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},2,1$ *añadiendo un 4, y sumando 1 a los términos que están en negrita. Por tanto, añadimos un vértice (*$v_7$*), de grado 4, y que estará unido a un vértice de grado 3 (*$v_6$*), uno de grado 2 (por ejemplo,* $v_1$*) y dos vértices de grado 1 (por ejemplo,* $v_4$ *y* $v_2$*).*




*Y de esta forma, ya hemos encontrado un grafo con 7 vértices, y cuyos grados son* $4,4,3,2,2,2,1$*.*

## 4.5. Grafos de Euler

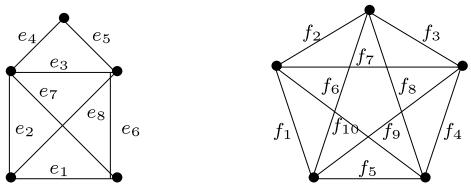
**Definición 39.** *Sea $G$ un grafo conexo. Un camino de Euler es un recorrido en el que aparecen todos los lados.*

*Un circuito de Euler es un camino de Euler que es cerrado.*

*Un grafo con un circuito de Euler es un grafo de Euler.*

**Ejemplo 4.5.1.**

*Consideramos los grafos*




*La sucesión $e_2e_4e_5e_8e_1e_7e_3e_6$ es un camino de Euler en el primer grafo, mientras que $f_1f_2f_3f_4f_5f_6f_8f_{10}f_7f_9$ es un circuito de Euler en el segundo.*

**Proposición 4.5.1.** *Sea $G$ un grafo. Entonces si $G$ tiene un circuito de Euler, el grado de cada vértice es par, mientras que si $G$ tiene un camino de Euler, $G$ tiene exactamente dos vértices de grado impar (exactamente los vértices donde empieza y termina el camino).*

*Demostración:*

Sea $G$ un grafo en el que tenemos un circuito de Euler. Supongamos que queremos ver cual es el grado de un vértice $v$, es decir, vamos a contar cuantos lados inciden en dicho vértice. Para esto, tomamos el circuito de Euler, y lo recorremos empezando en un vértice que no sea el que estamos considerando. Conforme lo recorremos vamos contando los lados que son incidentes en $v$. Ahora bien, cada vez que pasemos por $v$ nos encontramos con dos lados incidentes en él, por el que llegamos a $v$ y por el que salimos de $v$. Por tanto, el número total de lados incidentes en $v$ será el doble del número de veces que el circuito pase por el vértice $v$.

Si lo que tenemos es un camino de Euler que empieza en $u$ y termina en $v$, añadimos al grafo un lado que une los vértices $u$ y $v$. Tenemos entonces, con este nuevo lado, un circuito de Euler en el nuevo grafo. El grado de cada vértice es entonces par.

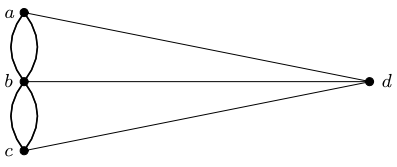
Al eliminar el lado que hemos añadido, el grado de todos los vértices se mantiene igual, salvo el de los vértices $u$ y $v$ que disminuye en 1. Por tanto, estos dos vértices tendrán grado impar, y el resto tendrán grado par. ■

**Ejemplo 4.5.2.**

1. *En el primer grafo del ejemplo anterior, tenemos que hay dos vértices de grado 3, un vértice de grado 2 y dos vértices de grado 4. Podemos ver cómo el camino de Euler que teníamos empezaba en uno de los vértices de grado tres y terminaba en el otro.*

   *En el segundo grafo del ejemplo se tiene que todos los vértices tienen grado 4.*

2. *Si consideramos el grafo que representaba el problema de los puentes de Königsberg*



*vemos que a, c y d tiene grado* 3*, mientras que b tiene grado* 5*. Como todos los vértices tienen grado impar, deducimos que no existe ningún circuito de Euler. Por tanto, el problema de los puentes de Königsberg no tiene solución.*

Hemos visto una condición necesaria para que un grafo tenga un circuito o un camino de Euler. Veamos a continuación que esta condición es también suficiente.

**Teorema 4.5.1.** *Sea $G$ un grafo conexo. Entonces $G$ es un grafo de Euler si, y sólo si, el grado de cada vértice es par.*

Antes de pasar a la demostración del teorema, veamos el siguiente lema.

**Lema 4.5.1.** *Sea $G$ un grafo en el que cada vértice tiene grado mayor que* 1*. Entonces $G$ contiene un circuito (y por tanto un ciclo).*

*Demostración:* Elegimos un vértice cualquiera $v = v_0$. Puesto que el grado de $v$ es mayor que 1, tomamos un lado que incida en $v_0$. Sea éste $e_0$, y $v_1$ el otro vértice sobre el que incide $e_0$. Podría darse el caso de que $v_0 = v_1$, en cuyo caso ya tendríamos el recorrido.

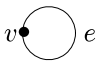
Puesto que $v_1$ tiene grado mayor que 1, debe haber otro lado incidente con $v_1$. Sea éste $e_1$, y $v_2$ el otro vértice sobre el que incide. Tenemos entonces el camino dado por la sucesión de vértices $v_0v_1v_2$ y la sucesión de lados $e_0e_1$.

Continuamos el proceso ahora con $v_2$ hasta que se repita algún vértice (sin repetir ningún lado). En cuanto esto ocurra, ya habremos encontrado el circuito que buscábamos (obviamente, estamos hablando de grafos con un número finito de vértices y de lados). ■

*Demostración:*(Teorema 4.5.1)

Haremos la demostración por inducción sobre el número de lados.

El primer caso es para grafos con un solo lado. Si el grafo es conexo, tiene un solo lado, y el grado del único vértice es par, la única posibilidad es que el grafo sea




en cuyo cado, el circuito de Euler es el camino $vv$.

Supongamos que ahora que tenemos un grafo conexo, con $n$ lados, y en el que el grado de cada vértice es par, y supongamos también que el resultado es cierto para cualquier grafo conexo con menor número de lados.

Por el lema precedente, puesto que el grado de cada vértice es mayor o igual que 2 deducimos que existe en $G$ un circuito $c$.

Eliminamos de $G$ todos los lados que intervienen en el circuito, y nos queda un grafo en el que todos los vértices tienen grado par (pues de cada vértice se han eliminado un número par de lados que inciden en él). El grafo resultante no tiene que ser conexo, pero cada una de sus componentes conexas sí lo es. Además, cada componente conexa debe tener al menos un vértice por el que se pasa en el circuito $c$.

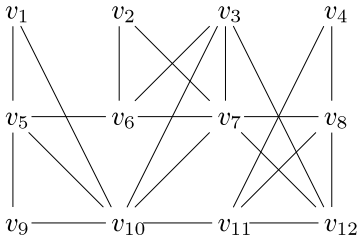
Para cada una de ellas que tenga al menos un lado, tenemos un circuito de Euler. Sean estos circuitos $c_1, c_2, \ldots, c_r$. Para cada uno de estos circuitos $c_i$, tenemos un vértice $v_i$ que también está en el circuito $c$.

Recorremos entonces el circuito $c$. En cuanto lleguemos a algún vértice $v_i$, insertamos el circuito $c_i$, y continuamos con el circuito $c$. De esta forma, al cerrar el circuito $c$ habremos recorrido todos los lados del grafo $G$ una sola vez, es decir, tendremos un circuito de Euler. ■

**Corolario 4.5.1.** *Sea $G$ un grafo conexo. Entonces $G$ tiene un camino de Euler si, y sólo si, $G$ tiene exactamente dos vértices de grado impar.*

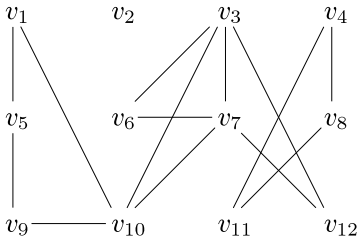
**Ejemplo 4.5.3.**

*Consideramos el siguiente grafo*

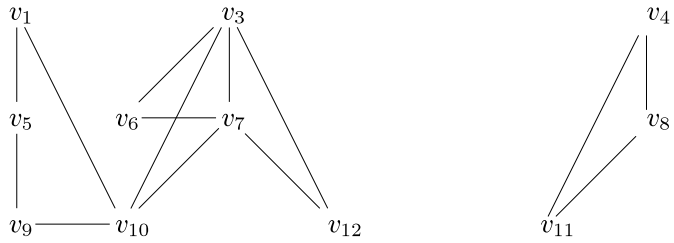



*en el que vemos que los vértices $v_1$, $v_2$, $v_4$ y $v_9$ tienen grado 2; los vértices $v_3$, $v_5$, $v_6$, $v_8$, $v_{11}$ y $v_{12}$ tienen grado 4, mientras que los vértices $v_7$ y $v_{10}$ tienen grado 6. Como todos los vértices tienen grado par, sabemos que existe un circuito de Euler. Vamos a encontrarlo.*

*Para esto, buscamos un circuito cualquiera, por ejemplo, $v_2v_6v_5v_{10}v_{11}v_{12}v_8v_7v_2$, y eliminamos los lados que intervienen en este circuito. Nos queda entonces el grafo*



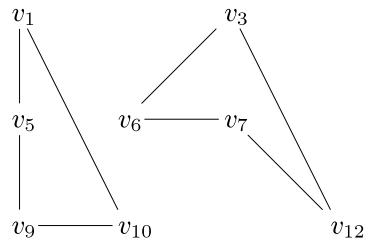

*que tiene (aparte del vértice $v_2$) dos componentes conexas que son las siguientes:*




*de los cuales hemos de encontrar un circuito de Euler. En el segundo grafo, este circuito sería $v_4v_8v_{11}v_4$.*

*Vamos a encontrarlo en el primero. Para ello, hacemos como hicimos al principio.*

*Buscamos un circuito en dicho grafo, que podría ser $v_3v_7v_{10}v_3$; eliminamos los lados que intervienen, y nos queda entonces el grafo*




*que tiene dos componentes conexas. Para cada una de ellas es fácil encontrar un circuito de Euler. El circuito de la primera componente es $v_1v_5v_9v_{10}v_1$, mientras que el de la segunda es $v_3v_6v_7v_{12}v_3$.*

*Un vértice común entre los circuitos $v_3v_7v_{10}v_3$ y $v_1v_5v_9v_{10}v_1$ es $v_{10}$, mientras que un vértice común entre los circuitos $v_3v_7v_{10}v_3$ y $v_3v_6v_7v_{12}v_3$ podría ser $v_3$ (o $v_7$).*

*Recorremos entonces el circuito $v_3v_7v_{10}v_3$, y al llegar a los vértices que hemos elegido insertamos los circuitos de cada una de las componentes conexas.*

$$v_3 \underbrace{v_6v_7v_{12}v_3} v_7v_{10} \underbrace{v_1v_5v_9v_{10}} v_3$$

*Volvemos ya al grafo de partida. En él elegimos un circuito ($v_2v_6v_5v_{10}v_{11}v_{12}v_8v_7v_2$), que al eliminarlo dividía al grafo en dos componentes conexas. De cada una de éstas tomamos ahora un vértice común con*

*el circuito. Sean éstos $v_6$ y $v_{11}$. Recorremos el circuito elegido, y al llegar a estos vértices insertamos los circuitos de Euler para cada una de las componentes. Tenemos entonces:*

$$v_2v_6\underbrace{v_7v_{12}v_3v_7v_{10}v_1v_5v_9v_{10}v_3v_6}v_5v_{10}v_{11}\underbrace{v_4v_8v_{11}}v_{12}v_8v_7v_2$$

*que es un circuito de Euler para el grafo del que partíamos.*

A continuación veremos un algoritmo que calcula, dado un grafo del que sabemos que tiene un camino o circuito de Euler, un tal camino.

**Algoritmo de Fleury**
Como entrada, tenemos un grafo $G$. Como salida, dos sucesiones $S_V$ y $S_E$, que son las sucesiones de vértices y lados del camino buscado.

1. Si todos los vértices son de grado par, elegimos un vértice cualquiera $v$. Si $G$ tiene dos vértices de grado impar elegimos uno de estos vértices.
2. Hacemos $S_V = v$ y $S_E = []$.
3. Si $G$ tiene sólo a $v$, devuelve $S_V$ y $S_E$, y termina.
4. Si hay un único lado $e$ que incida en $v$, llamamos $w$ al otro vértice donde incida el lado $e$; quitamos de $G$ el vértice $v$ y el lado $e$ y vamos al paso 6.
5. Si hay más de un lado $e$ que incida en $v$, elegimos uno de estos de forma que al quitarlo el grafo $G$ siga siendo conexo. Llamamos $e$ a dicho lado y $w$ al otro vértice en el que incide $e$.
6. Añadimos $w$ al final de $S_V$ y $e$ al final de $S_E$.
7. Cambiamos $v$ por $w$ y volvemos al paso 3.

## 4.6. Grafos de Hamilton

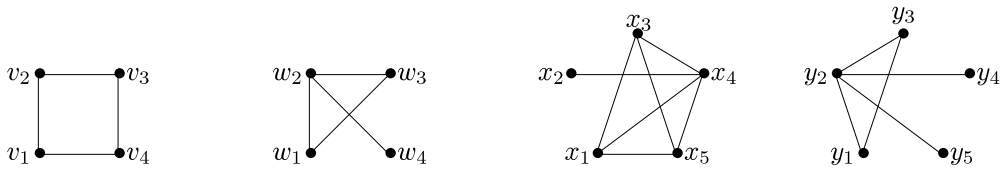
En la sección anterior estudiamos cuándo en un grafo podíamos encontrar un camino que recorriera todos los lados una sola vez. En esta, pretendemos estudiar como recorrer todos los vértices una sola vez.

**Definición 40.** *Sea $G$ un grafo. Un* camino de Hamilton *es un camino que recorre todos los vértices una sola vez.*

*Un* circuito de Hamilton *es un camino cerrado que recorre todos los vértices una sola vez (salvo los extremos).*

*Un grafo con un circuito de Hamilton se denomina* grafo de Hamilton *o* grafo hamiltoniano.

**Ejemplo 4.6.1.** *Consideramos los siguientes grafos:*




*Entonces, el primer grafo es un grafo de Hamilton. Un circuito de Hamilton es $v_1v_2v_3v_4v_1$. Obviamente, al tener un circuito de Hammilton, podemos encontrar también un camino de Hamilton ($v_1v_2v_3v_4$).*

*En el segundo grafo tenemos un camino de Hamilton ($w_1w_3w_2w_4$). Podemos ver como no existe ningún circuito de Hamilton, pues debería tener al menos dos lados incidentes en $w_4$ (el lado entrante y el lado saliente).*

*El mismo razonamiento sirve para ver que en el tercer grafo no es hamiltoniano. En este también podemos encontrar caminos de Hamilton. Por ejemplo* $x_1x_3x_5x_4x_2$.

*Por último, en el último grafo no hay caminos de Hamilton. Fácilmente, podemos ver que de haberlo debería empezar en* $y_4$ *y terminar en* $y_5$ *(o al revés). En ese caso, el camino debería empezar* $y_4y_2$*, y debería terminar* $y_2y_5$*, luego el vértice* $v_2$ *aparecería repetido.*

*Nótese que en los grafos segundo y cuarto existen caminos de Euler, mientras que en el tercero no. Por tanto, no existe ninguna relación entre tener caminos de Hamilton y caminos de Euler.*

**Observaciones:**

Puesto que a la hora de buscar un camino o circuito de Hamilton no podemos pasar dos veces por un mismo vértice, no es posible que el camino contenga dos lados paralelos, ni que contenga lazos. Supondremos por tanto en esta sección que todos los grafos que intervienen no tienen ni lazos ni lados paralelos.

Hemos visto en el ejemplo anterior, que si hay un vértice de grado 1, entonces el grafo no es de Hamilton.

Por otra parte, si un grafo con $n$ vértices es de Hamilton, en el circuito de Hamilton intervienen $n$ lados. Por tanto, un grafo de Hamilton con $n$ vértices tiene al menos $n$ lados.

Intuitivamente, cuantos más lados tenga un grafo con un número de vértices fijado, más fácil será poder encontrar un circuito de Hamilton. Veremos a continuación que si tenemos el número suficiente de lados, entonces tenemos garantizada la existencia de circuitos de Hamilton.

**Teorema 4.6.1.** *Sea* $G$ *un grafo con* $n$ *vértices.*

1. *Si el número de lados es mayor o igual que* $\frac{1}{2}(n-1)(n-2)+2$*, entonces el grafo es hamiltoniano.*
2. *Si* $n \geq 3$ *y para cada par de vértices no adyacentes se verifica que* $gr(v)+gr(w) \geq n$*, entonces* $G$ *es un grafo de Hamilton.*

*Demostración:*

Hagamos en primer lugar la demostración de la segunda parte. Probemos que si $G$ no es un grafo de Hamilton, hay al menos dos vértices no adyacentes tales que la suma de sus grados es menor que $n$.

Supongamos entonces que $G$ es un grafo que no es de Hamilton. Añadimos un lado al grafo. Si sigue sin ser de Hamilton, volvemos a añadir un lado, y así sucesivamente, hasta que encontremos un grafo de Hamilton. Sea $ab = v_1v_2$ el último lado que hemos añadido. El grafo obtenido es un grafo de Hamilton, y el ciclo de Hamilton debe contener al lado $ab$. Sea entonces dicho ciclo $abv_3v_4\cdots v_na$.

Llamemos $H$ al grafo que hemos obtenido justo antes de añadir el lado $ab$.

Para cada $i$ entre 3 y $n$, vamos a ver que no pueden estar simultáneamente los lados $av_{i-1}$ y $bv_i$ en el grafo $H$.

Si $i = 3$, entonces $av_{i-1} = av_2 = ab$, que no está en $H$.

Si $i \geq 4$, en caso de que estuvieran ambos lados, podríamos construir el circuito de Hamilton

$$bv_iv_{i+1}\cdots v_nav_{i-1}v_{i-2}\cdots v_3b$$

que no contiene al lado $ab$, lo cual no es posible, pues el grafo $H$ no es de Hamilton.

Tenemos entonces que en el grafo $H$, se verifica que $gr(a)+gr(b) < n$, y como $G$ es un subgrafo de $H$, entonces en $G$ se verifica la misma propiedad. Hemos encontrado entonces dos vértices no adyacentes tales que la suma de sus grados es menor que $n$, como queríamos.

Demostremos ahora la primera parte.

Sean $u$ y $v$ dos vértices no adyacentes. Vamos a probar que $gr(u)+gr(v) \geq n$.

Sea $G' = (V', E')$ el subgrafo completo (ver definición 29) de $G$ formado por todos los vértices de $G$ salvo $u$ y $v$. Este grafo es un subgrafo de $K_{n-2}$, por tanto el número de lados de $G'$ es menor o igual que $\frac{(n-2)(n-3)}{2}$.

Por otra parte, $|E| = |E'| + gr(u) + gr(v)$ (pues el lado $uv$ no está en $E$), luego

$$\frac{(n-1)(n-2)}{2} + 2 \leq |E| = |E'| + gr(u) + gr(v) \leq \frac{(n-2)(n-3)}{2} + gr(u) + gr(v)$$

por tanto,

$$\begin{aligned} gr(u)+gr(v) &\geq \tfrac{(n-1)(n-2)}{2}+2-\tfrac{(n-2)(n-3)}{2} \\ &= \tfrac{(n-2)[n-1-(n-3)]+4}{2} \\ &= \tfrac{(n-2)(n-1-n+3)+4}{2} \\ &= \tfrac{(n-2)2+4}{2} \\ &= \tfrac{2n-4+4}{2} = n \end{aligned}$$

■

Sabemos que si el número de lados de un grafo de $n$ vértices es menor que $n$ no es un grafo hamiltoniano. Si el número de lados está comprendido entre $n$ y $\frac{1}{2}(n-1)(n-2)+1$, en principio no podemos asegurar nada.

**Ejemplo 4.6.2.**

1. *Dado $n$ un número natural mayor o igual que 2. Construimos el grafo $K_{n-1}$. El número de lados de este grafo es $\frac{1}{2}(n-1)(n-2)$.*

   *Tomamos un vértice más y lo unimos a un lado cualquiera de $K_{n-1}$. El grafo resultante no es de Hamilton, pues hay un vértice de grado 1. Tenemos entonces un grafo con $n$ vértices, $\frac{1}{2}(n-1)(n-2)+1$ lados, y que no es hamiltoniano.*

   *Por tanto, la mejor cota sobre el número de lados para asegurar que un grafo es de Hamilton es la dada en el teorema.*

2. *Sea $V=\{v_1,v_2,\ldots,v_n\}$, $E=\{e_1,e_2,\ldots,e_n\}$ y $\gamma: E\to\{\{u,v\}: u,v\in V\}$ dada por $\gamma(e_n)=\{v_1,v_n\}$ y $\gamma(e_i)=\{v_i,v_{i+1}\}$ para $1\leq i\leq n-1$.*

   *Tenemos así un grafo de Hamilton con $n$ vértices y $n$ lados.*

3. *Sea $G$ un grafo regular de grado 4 y 8 vértices. Dicho grafo tiene un total de 16 lados. Para 8 vértices, la cota para el número de lados es $\frac{7\cdot 6}{2}+2=23$.*

   *Sin embargo, en tal caso podemos ver que la suma de los grados de cualquier pareja de vértices es 8. Por tanto, podemos asegurar que dicho grafo es hamiltoniano.*

## 4.7. Grafos bipartidos

**Definición 41.** *Sea $G=(V,E)$ un grafo. Se dice que $G$ es bipartido si podemos descomponer $V$ en dos subconjuntos disjuntos $V_1$ y $V_2$ de forma que todo lado incide en un vértice de $V_1$ y en un vértice de $V_2$.*

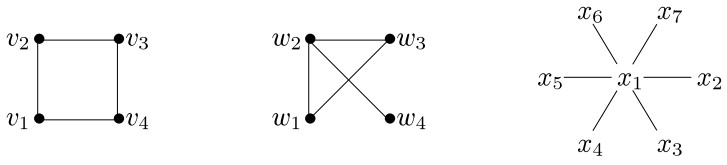
*Un grafo $G=(V,E)$ se dice bipartido completo si es bipartido, y para cada $v_1\in V_1$ y $v_2\in V_2$ existe un único lado $e\in E$ tal que $\gamma_G(e)=\{v_1,v_2\}$.*

Un grafo bipartido completo está completamente determinado por el cardinal de $V_1$ y $V_2$.

Si $G$ es un grafo bipartido completo en el que $V_1$ tiene cardinal $m$ y $V_2$ tiene cardinal $n$, entonces denotaremos a $G$ como $K_{m,n}$.

**Ejemplo 4.7.1.**

1. *Consideramos los siguientes grafos*



*Entonces el primer y el tercer grafos son bipartidos.*

*En el primero, se tiene que $V_1 = \{v_1, v_3\}$ y $V_2 = \{v_2, v_4\}$. Además, podemos ver que cualquier para cualquier pareja formada por un vértice de $V_1$ y un vértice de $V_2$ hay un lado y sólo uno que los une. Por tanto, es un grafo bipartido completo. Dado que $V_1$ y $V_2$ tienen dos elementos, dicho grafo es $K_{2,2}$.*

*En el tercero tenemos $V_1 = \{x_1\}$ y $V_2 = \{x_2, x_3, x_4, x_5, x_6, x_7\}$. Vemos también que este es un grafo bipartido completo, es decir, este grafo es $K_{1,6}$.*

*El segundo grafo no es bipartido. Para comprobarlo, supongamos que tenemos una división del conjunto de vértices de la forma $\{w_1, w_2, w_3, w_4\} = V_1 \cup V_2$. Entonces $w_1$ pertenecerá a uno de los dos conjuntos. Supongamos que a $V_1$. En tal caso, se tiene que $w_2 \in V_2$ (pues $w_1$ y $w_2$ están unidos por un lado) y $w_3 \in V_2$ (por el mismo motivo). Tenemos entonces dos vértices en el mismo subconjunto de la partición, y unidos por un lado.*

El siguiente teorema nos da una caracterización de los grafos bipartidos.

**Teorema 4.7.1.** *Sea $G = (V, E)$ un grafo. Entonces $G$ es bipartido si, y sólo si, $G$ no contiene ciclos de longitud impar.*

Antes de demostrar el teorema veamos el siguiente lema, cuya demostración se deja como ejercicio.

**Lema 4.7.1.** *Sea $G$ un grafo bipartido con partición del conjunto de vértices $V = V_1 \cup V_2$. Supongamos que $v_1 v_2 \cdots v_m$ es un camino en $G$ y que $v_1 \in V_1$. Entonces $\{v_1, v_3, v_5, \ldots\} \subseteq V_1$ y $\{v_2, v_4, \ldots\} \subseteq V_2$.*

*Demostración:* (Teorema)

Veamos en primer lugar que si $G$ contiene ciclos de longitud impar entonces $G$ no es bipartido.

Supongamos que $v_1 v_2 \cdots v_{m-1} v_m v_1$ es un ciclo de longitud impar, es decir, $m = 2k + 1$ para algún $k \in \mathbb{N}$.

Si $G$ fuera bipartido, tendríamos que $v_1, v_3, \cdots, v_{2k+1}$ están en el mismo subconjunto de la partición, mientras que $v_2, v_4, \cdots, v_{2m}, v_1$ están en el otro subconjunto de la partición.

Encontramos entonces un vértice ($v_1$) que está simultáneamente en los dos subconjuntos, lo cual no es posible.

Hagamos la demostración del recíproco. Es decir, supongamos que el grafo no tiene ciclos de longitud impar, y veamos que entonces $G$ es bipartido.

Vamos a hacer la demostración en el caso de que el grafo sea conexo. Caso de no serlo, se deja como ejercicio adaptar la demostración.

Sean $u$ y $v$ dos vértices de $G$. Definimos el número $d(u, v)$ como la menor longitud posible de los caminos que unen $u$ con $v$. Claramente, si $d(u, v) = r$ entonces existe un camino simple que une $u$ con $v$.

Elegimos un vértice $v_0 \in V$, y definimos los conjuntos:

$$V_1 = \{v \in V : d(v_0, v) \text{ es par}\}, \qquad V_2 = \{v \in V : d(v_0, v) \text{ es impar}\}.$$

Es claro que $V = V_1 \cup V_2$ y que $V_1 \cap V_2 = \emptyset$. Veamos que cualquier lado de $G$ une un vértice de $V_1$ con un vértice de $V_2$.

Sea $e$ un lado incidente con los vértices $w$ y $w'$, y sean $r = d(v_0, w)$ y $s = d(v_0, w')$. Entonces pueden darse tres posibilidades:

- $r = s + 1$. En tal caso, uno es par y el otro es impar. Por tanto, el lado considerado une un vértice de $V_1$ con un vértice de $V_2$.
- $s = r + 1$. Vale lo mismo a lo dicho en el caso anterior.

- $r = s$. Vamos a ver que esta situación no puede darse, pues de ser así tendríamos un ciclo de longitud impar.

  Para comprobarlo, tomamos los dos caminos simples de longitud $r$

  $v_0v_1v_2\cdots v_r = w$; $v_0v_1'\cdots v_r' = w'$.

  Y a partir de ellos vamos a buscar un un ciclo de longitud impar.

  En principio, pueden ahora darse también dos situaciones:

  1. $\{v_1, v_2, \cdots, v_r\} \cap \{v_1'v_2', \cdots, v_r'\} = \emptyset$.
     Y aquí tenemos un ciclo $v_0v_1\cdots v_rv_r'v_{r-1}'\cdots v_1'v_0$ de longitud $2r+1$, que tiene longitud impar.
  2. $\{v_1, v_2, \cdots, v_r\} \cap \{v_1'v_2', \cdots, v_r'\} \neq \emptyset$.
     La idea aquí es la misma, sólo que para obtener un ciclo hemos de eliminar los vértices repetidos.
     En primer lugar, veamos que si $v_i \in \{v_1, v_2, \cdots, v_r\} \cap \{v_1'v_2', \cdots, v_r'\}$ entonces $v_i = v_i'$. Esto es cierto pues si $v_i = v_j'$ con $j \neq i$ entonces, bien $j < i$ o bien $i < j$. En el primer caso tenemos que $v_0v_1'\cdots v_j'v_{i+1}\cdots v_r$ es un camino que une $v_0$ con $v_r = w$ de longitud menor que $r$, lo cual no es posible. En el segundo se razona de la misma forma.
     Tomamos ahora el mayor $i$ tal que $v_i \in \{v_1, v_2, \cdots, v_r\} \cap \{v_1'v_2', \cdots, v_r'\}$. En tal caso, podemos tomar el ciclo $v_iv_{i+1}\cdots v_rv_r'v_{r-1}'\cdots v_i' = v_i$, que tiene longitud $2(r-i)+1$, es decir, un número impar.

■

**Proposición 4.7.1.** *Sea $G$ un grafo bipartido con partición $V_1$ y $V_2$. Supongamos que $|V_1| = n$ y $|V_2| = m$. Entonces:*
*Si $G$ tiene un camino de Hamilton, entonces $|n - m| \leq 1$.*
*Si $G$ es un grafo de Hamilton, entonces $n = m$.*
*Si $G$ es completo y $|n - m| \leq 1$, entonces $G$ tiene un camino de Hamilton.*
*Si $G$ es completo y $n = m$, entonces $G$ es un grafo de Hamilton.*

La demostración se deja como ejercicio.

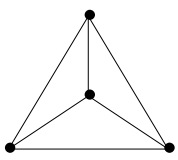
## 4.8. Grafos planos

En esta sección vamos a estudiar los grafos que pueden ser representados en el plano.

**Definición 42.** *Sea $G$ un grafo. Una representación de $G$ se dice plana si los vértices y los lados se encuentran todos en un plano, y las líneas que representan dos lados distintos no se cortan.*
*Un grafo se dice plano si admite una representación plana.*

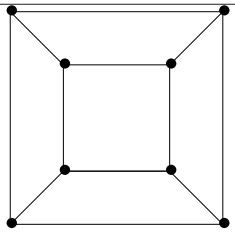
**Ejemplo 4.8.1.**

1. *El grafo $K_4$ es plano, pues admite una representación plana.*



2. *Cualquier poliedro tiene asociado un grafo. Los vértices son los vértices del poliedro, y los lados sus aristas. Este grafo es siempre plano.*

   *Por ejemplo, el grafo correspondiente al tetraedro es $K_4$. El grafo correspondiente al cubo es*



Una representación plana de un grafo divide al plano en que se encuentra en varias regiones, que denominaremos *caras*.

**Teorema 4.8.1** (Característica de Euler)**.** *Sea $G$ un grafo plano y conexo. Llamemos $v$ al número de vértices, $l$ al número de lados y $c$ al número de caras de una representación plana. Entonces $v-l+c=2$.*

*En general, si $G$ es un grafo plano, y $\chi$ es el número de componentes conexas entonces $v-l+c=1+\chi$.*

*Demostración:* Hagamos la demostración por inducción en el número de lados.

Para grafos (conexos) con un único lado el resultado es cierto, pues únicamente hay dos posibilidades, que son

y en el primer caso $v=1$, $l=1$ y $c=2$, mientras que en el segundo $v=2$, $l=1$ y $c=1$. Fácilmente se ve como en ambos casos se da la igualdad.

Supongamos que el resultado es cierto para todos los grafos planos, conexos y con $n$ lados, y sea $G$ un grafo plano, conexo con $n+1$ lados. Sean $v$, $l$ y $c$ el número de vértices, lados y caras respectivamente de $G$.

Pueden ocurrir dos cosas:

- Que $G$ contenga un ciclo.

  En tal caso, sea $G'$ el grafo que resulta de quitar de $G$ un lado que formaba parte de un ciclo. Entonces $G'$ sigue siendo conexo. Llamemos $v'$, $l'$ y $c'$ al número de vértices, lados y caras de este nuevo grafo. Se tiene que $v'=v$ (no hemos eliminado ningún vértice); $l'=l-1=n$ (hemos eliminado un lado) y $c'=c-1$ (al quitar un lado de un ciclo, las dos caras que separaba ese lado se convierten en una).

  Por tanto, se tiene que

  $$v-l+c=v'-(l'+1)+(c'+1)=v'-l'-1+c'+1=v'-l'+c'=2$$

  pues, por hipótesis de inducción, para dicho grafo sí era cierta la tesis del teorema.

- Que $G$ no contenga ningún ciclo.

  En este caso, por el lema 4.5.1 $G$ debe tener algún vértice de grado 1.

  Sea $G'$ el grafo que resulta de eliminar este vértice y el lado que en él incide. Para el grafo resultante se tiene que $v'=v-1$, $l'=l-1$ y $c'=c$ (pues el lado eliminado no separaba ninguna región).

  Razonando igual que antes se tiene que $v-l+c=2$.

La demostración del caso general (no conexo) se deja como ejercicio. ■

**Corolario 4.8.1.** *En un poliedro, si $v$ es el número de vértices; $l$ es el número de aristas y $c$ es el número de caras entonces $v-l+c=2$.*

**Ejemplo 4.8.2.**

1. *En la representación plana que hicimos de $K_4$ se tienen un total de 4 caras. Como en $K_4$ se verifica que $v = 4$ y $l = 6$ entonces $v - l + c = 4 - 6 + 4 = 2$.*

2. *El cubo tiene 8 vértices, 12 aristas y 6 caras. Obviamente se ve que $v - l + c = 2$.*

3. *Vamos a demostrar aquí que sólo existen 5 sólidos regulares. Es decir, poliedros en donde todas las caras son polígonos regulares iguales.*

   *Supongamos que tenemos un poliedro regular, y sea $G$ el grafo asociado a dicho poliedro. Sabemos que se verifica que*

   $$v - l + c = 2$$

   *Sabemos además que este grafo es regular de grado $r$ ($r$ es el número de aristas que inciden en cada vértice) y que $r \geq 3$. Por tanto, se verifica que*

   $$rv = 2l.$$

   *Por otra parte, todas las caras son polígonos regulares de $n$ lados. Si contamos el número de caras, y lo multiplicamos por $n$ estamos contando el número de aristas dos veces, pues cada arista es arista común de dos caras. Por tanto, se tiene también que*

   $$nc = 2l.$$

   *Sustituyendo en la expresión $v - l + c = 2$ obtenemos que*

   $$\frac{2l}{r} - l + \frac{2l}{n} = 2 \Longrightarrow \frac{1}{r} + \frac{1}{n} = \frac{1}{2} + \frac{1}{l}$$

   *Sabemos que $r \geq 3$ y $n \geq 3$ (pues el polígono regular más simple es el triángulo). Si tanto $n$ como $r$ fueran simultáneamente mayores que 3, es decir, $n \geq 4$ y $r \geq 4$ tendríamos que $\frac{1}{n} \leq \frac{1}{4}$ y $\frac{1}{r} \leq \frac{1}{4}$, luego*

   $$\frac{1}{2} + \frac{1}{l} = \frac{1}{r} + \frac{1}{n} \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \Longrightarrow \frac{1}{l} \leq 0,$$

   *lo cual es imposible.*

   *Por tanto, tenemos dos posibilidades:*

   - *$n = 3$. Las caras del sólido son triángulos.*

     *En este caso tenemos*

     $$\frac{1}{3} + \frac{1}{r} = \frac{1}{2} + \frac{1}{l} \Longrightarrow \frac{1}{l} = \frac{1}{r} - \frac{1}{6} \Longrightarrow l = \frac{6r}{6 - r}.$$

     *Por tanto, $r < 6$, lo que nos da sólo tres posibilidades para $r$.*

     a) *$r = 3$. Entonces $l = \frac{6 \cdot 3}{6-3} = 6$. Puesto que $nc = 2l$ deducimos que $c = 4$, y dado que $rv = 2l$ también tenemos que $v = 4$. El sólido regular resulta ser el tetraedro.*

     b) *$r = 4$. Aquí $l = \frac{24}{2} = 12$, y de aquí deducimos que $c = 8$ y $v = 6$. El sólido regular es el octaedro.*

     c) *$r = 5$. Ahora, $l = 30$, y por tanto $c = 20$ y $v = 12$. El sólido es el icosaedro.*

   - *$r = 3$. Razonando igual que antes, pero intercambiando el papel de $r$ y $n$ tenemos tres posibilidades para $n$.*

     a) *$n = 3$. Este caso ya lo hemos analizado. Es el tetraedro.*

     b) *$n = 4$. Ahora las caras son cuadrados. Ahora $l = 12$, lo que implica que $c = 6$ y $v = 8$. Estamos hablando del cubo.*

     c) *$n = 5$. Las caras son pentágonos. Aquí $l = 30$, de donde $c = 12$ y $v = 20$. El sólido es en este caso el dodecaedro.*

**Corolario 4.8.2.** *Sea $G$ un grafo plano, conexo, sin lazos ni lados paralelos. Entonces $3c \leq 2l$ y $l \leq 3v-6$.*

*Demostración:* Vamos a llamar grado de una cara al número de lados que delimitan dicha cara, o mejor dicho, al número de aristas que son frontera de la cara.

Es claro que al no tener lazos ni lados paralelos, el grado de cualquier cara es mayor o igual que 3. La suma de los grados de todas las caras será entonces mayor o igual que $3c$.

Por otra parte, al sumar los grados de todas las caras estamos contando dos veces el número de lados, pues cada lado es frontera común de dos caras. Tenemos entonces que $3c \leq 2l$.

La otra desigualdad es consecuencia del Teorema 4.8.1, pues

$$2 = v - l + c \leq v - l + \frac{2l}{3} = v - \frac{l}{3} \quad \Longrightarrow \quad 6 \leq 3v - l \quad \Longrightarrow \quad l \leq 3v - 6.$$

■

En la demostración del corolario se han utilizado dos hechos: que toda cara tiene al menos tres lados que son frontera y el Teorema 4.8.1. Si de un grafo pudiéramos asegurar que cada cara tiene al menos $r$ lados que son frontera, entonces las dos desigualdades se transformarían en

$$rc \leq 2l, \qquad (r-2)l \leq r(v-2).$$

**Ejemplo 4.8.3.** *Vamos a comprobar que los grafos $K_5$ y $K_{3,3}$ no son planos.*

*En el grafo $K_5$ tenemos que $v = 5$. De ser plano, se tendría que $l \leq 3 \cdot 5 - 6 = 9$. Sabemos, sin embargo que $l = 10$. Por tanto, $K_5$ no puede ser plano.*

*Si utilizamos la misma expresión para $K_{3,3}$, y puesto que $v = 6$, obtendríamos que $l \leq 3 \cdot 6 - 6 = 12$, lo cual no supone contradicción alguna, ya que $K_{3,3}$ tiene 9 lados.*

*Sin embargo, por ser $K_{3,3}$ bipartido, no tiene ciclos de longitud impar, luego no puede haber caras que estén delimitadas por 3 lados. Como mínimo, hay cuatro lados fronterizos con cada cara. En este caso, tenemos que si fuera plano se verificaría que*

$$(4-2)l \leq 4(6-2) \quad \Longrightarrow \quad 2l \leq 16$$

*que sabemos que no es cierto.*

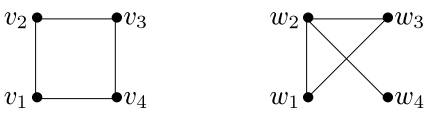
*Deducimos por tanto que $K_{3,3}$ no es plano.*

Vamos a continuaión a dar un teorema que viene a decirnos que, esencialmente, los únicos grafos no planos son los vistos en este ejmplo, es decir, $K_5$ y $K_{3,3}$. Antes, hemos de introducir las contracciones en grafos.

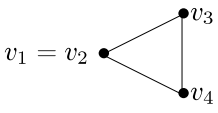
**Definición 43.** *Sea $G$ un grafo. Una* contracción simple *de $G$ es el resultado de indentificar en $G$ dos vértices adyacentes.*

*Una* contracción *de $G$ es una cadena de contracciones simples.*

**Ejemplo 4.8.4.** *Consideramos los grafos*




*Si en el primer grafo identificamos los vértices $v_1$ y $v_2$ obtenemos el grafo*



*luego dicho grafo es una contracción del "cuadrado".*

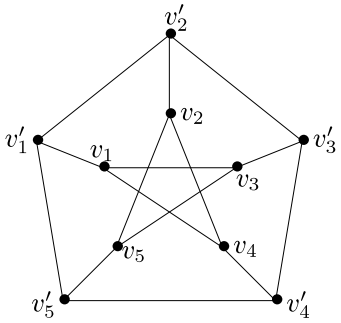
*En el segundo grafo vamos a realizar una contracción simple identificando los vértices $w_1$ y $w_2$, y otra identificando $w_2$ y $w_4$. Los grafos que obtenemos son*


Es muy intuitivo ver que cualquier contracción de un grafo plano sigue siendo un grafo plano.

Estamos ya en condiciones de dar el siguiente teorema.

**Teorema 4.8.2** (Kuratowski)**.** *Sea $G$ un grafo. Entonces $G$ es plano si, y sólo si, ningún subgrafo suyo puede contraerse a $K_5$ ni a $K_{3,3}$.*

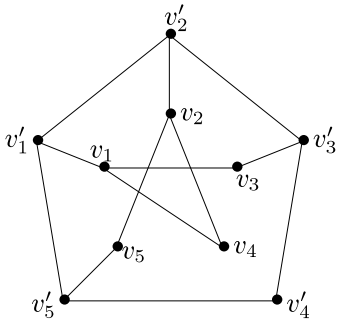
**Ejemplo 4.8.5.** *Consideramos el siguiente grafo $G$:*



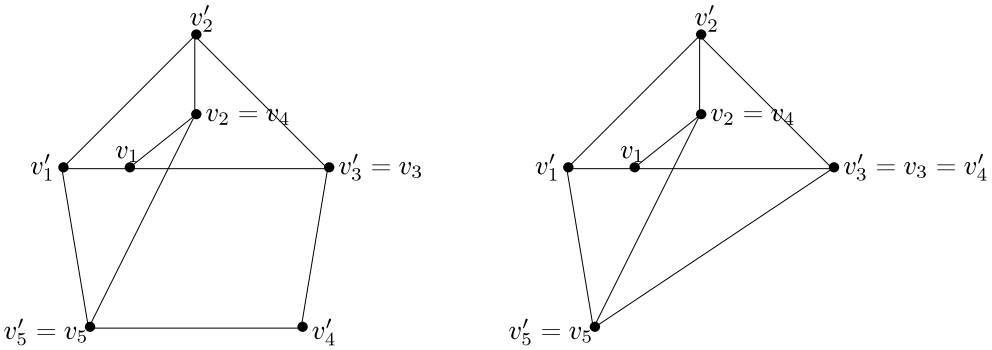

*Entonces, si identificamos cada vértice $v_i$ con $v_i'$ (es decir, realizamos cinco contracciones) obtenemos el grafo $K_5$, que sabemos que no es plano. Deducimos por tanto que este grafo no es plano.*

*También podemos ver que este grafo no es plano como sigue:*

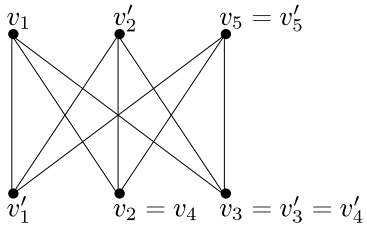
*Tomamos el subgrafo de $G$ con los mismos vértices, y del que se eliminan los lados que unen $v_3$ con $v_5$, y $v_4$ con $v_4'$. El grafo que obtenemos es*




*Identificamos los vértices $v_2$ con $v_4$, $v_3$ con $v_3'$ y $v_5$ con $v_5'$, y a continuación $v_4'$ con $v_3 = v_3'$. El grafo resultante es:*



*que podemos representar como*



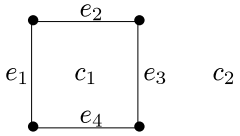

*Es decir, hemos encontrado un subgrafo de $G$ que puede contraerse hasta $K_{3,3}$.*

*La representación que hemos obtenido de $K_{3,3}$ (no esta última) puede servirnos para comprobar que si en $K_{3,3}$ se suprime algún lado, el grafo resultante es plano (basta suprimir el lado $v_2v_5$ o el lado $v_1v_3$).*

Por último, para acabar esta sección introducimos el concepto de grafo dual.

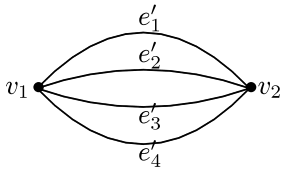
**Definición 44.** *Sea $G$ un grafo plano. Supongamos que tenemos una representación plana con caras $c_1, c_2, \ldots, c_r$. Definimos el grafo dual para la representación dada como el grafo cuyo conjunto de vértices es igual al conjunto de caras (o tiene un vértice $v_i'$ para cada cara $c_i$), y cuyo conjunto de lados coincide (o es biyectivo) con el conjunto de lados de $G$. En el grafo dual, un lado une dos vértices si en la representación plana de $G$ dicho lado es frontera común de las dos caras.*

**Ejemplo 4.8.6.** *Consideramos el grafo*




*que divide al plano en dos regiones $c_1$ y $c_2$. El grafo dual, tendrá entonces dos vértices $v_1$ y $v_2$ (uno por cada cara), y cuatro lados (uno por cada lado de $G$). Puesto que cada lado tiene frontera común con $c_1$ y $c_2$, cada lado del dual unirá los vértices $v_1$ y $v_2$.*

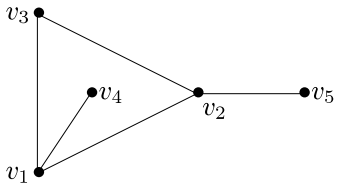
*El grafo dual es entonces:*

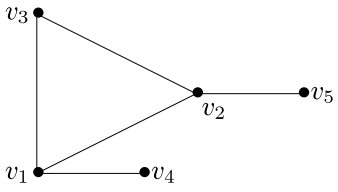



*Podemos ver que si hacemos el dual de este grafo obtenemos el grafo inicial.*

Cuando hablamos de dual de un grafo, hacemos referencia a su representación plana. Esto es así porque el dual de un grafo depende de la representación plana que tomemos, como podemos ver en el siguiente ejemplo.

**Ejemplo 4.8.7.** *Vamos a considerar dos representaciones planas de un mismo grafo, y vamos a hallar el dual para cada una de las representaciones. El grafo tiene 5 vértices ($v_1, v_2, v_3, v_4$ y $v_5$) y 5 lados, de los que damos los dos vértices que unen ($v_1v_2$, $v_1v_3$, $v_1v_4$, $v_2v_3$ y $v_2v_5$). Dos representaciones planas del mismo grafo podrían ser:*



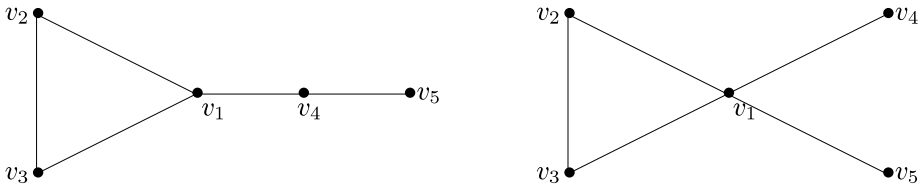



*Calculamos el dual de cada una de las dos representaciones. Vemos que en ambos casos tenemos dos caras, lo que da lugar a 2 vértices en el grafo dual. Los grafos duales son entonces:*

*que podemos ver que no son isomorfos. Mientras el primer grafo tiene dos vértices de grado* 5*, el segundo tiene un vértice de grado* 7 *y uno de grado* 3*.*

*Del segundo grafo que hemos obtenido, podemos hacer varias representaciones planas. Por ejemplo,*


*y cada una de ellas tiene un dual diferente. En estos casos serían:*




*que no son isomorfos entre sí, ni isomorfos al grafo original (basta estudiar en cada caso la sucesión de grados).*

*Si quisiéramos obtener el grafo inicial, deberíamos tomar otra representación, aquella en la que uno de los lazos estaría "dentro" de la región* $c_2$*.*

## 4.9. Coloración de grafos

**Definición 45.** *Sea* $G = (V, E)$ *un grafo. Una coloración* $G$ *es una aplicación* $f : V \to C$*, donde* $C$ *es un conjunto, de tal forma que para cualquier* $e \in E$*, si* $\gamma_G(e) = \{v, w\}$ *con* $v \neq w$ *entonces* $f(u) \neq f(v)$*.*

Cuando el conjunto $C$ sea un conjunto de colores, la aplicación $f$ lo que hace es asignar un color a cada vértice de $G$, de forma que dos vértices adyacentes no tienen el mismo color.

Se llama número cromático de $G$, y lo representaremos como $\chi(G)$ al cardinal del menor conjunto $C$ para el que existe una coloración de $G$.

**Ejemplo 4.9.1.**

1. *El grafo*  *necesita al menos dos colores para colorearlo, ya que los dos vértices no pueden ser coloreados con el mismo color al ser adyacentes. Su número cromático es por tanto* 2*.*

2. *En general, el número cromático del grafo* $K_n$ *es* $n$*, pues todos los vértices deben tener colores distintos, ya que dos vértices cualesquiera son adyacentes.*

3. *Una definición alternativa de grafo bipartido es la de un grafo cuyo número cromático es* 2*, pues se tiene que un grafo es bipartido si, y sólo si, su número cromático vale* 2*.*

   *Si el grafo es bipartido, con partición* $V = V_1 \cup V_2$*, entonces podemos colorear todos los vértices de* $V_1$ *de un color, y todos los vértices de* $V_2$ *de otro color. Es claro entonces que dos vértices adyacentes tienen distinta coloración.*

4. *Si $G_1$ es un subgrafo de $G_2$, entonces $\chi(G_1) \leq \chi(G_2)$.*

5. *Si un grafo es plano, su número cromático es menor o igual que 4. Éste es un problema que se planteó por primera vez a mitad del siglo XIX, cuando se intentaba colorear los condados de un mapa de Inglaterra de forma que dos condados con frontera común tuvieran distinto color. El problema estuvo abierto durante más de un siglo, hasta que en 1976, Appel y Haken probaron el resultado basándose en un complicado análisis computacional.*

   *El recíproco de este resultado no es cierto. $K_{3,3}$ tiene número cromático igual a 2, y sin embargo no es plano.*

En general, determinar el número cromático de un grafo es complicado. Para ello, vamos a valernos del polinomio cromático.

**Definición 46.** *Sea $G$ un grafo y $x \in \mathbb{N}$. Vamos a denotar por $p(G, x)$ al número de coloraciones distintas, con $x$ colores, que tiene el grafo $G$.*

**Ejemplo 4.9.2.**

1. *Si $G$ es un grafo que tiene al menos un lado (que no es lazo) entonces $p(G, 1) = 0$.*

2. *Si queremos colorear el grafo $K_2$ y disponemos de $x$ colores, entonces para uno de los vértices podemos elegir cualquiera de los $x$ colores, mientras que para el otro podemos elegir entre los $x - 1$ restantes. El principio del producto nos dice entonces que $p(K_2, x) = x(x - 1)$.*

3. *En general, se tiene que $p(K_n, x) = x(x - 1) \cdots (x - n + 1)$. De aquí se deduce que si $m \leq n$, $p(K_n, m) = 0$, mientras que $p(K_n, n) = n!$. Por tanto, el número cromatico de $K_n$ es $n$.*

4. *Si $G$ es un grafo cuyas componentes conexas son $G_1, G_2, \ldots, G_m$ entonces $p(G, x) = p(G_1, x) \cdot p(G_2, x) \cdots p(G_m, x)$.*

   *Por tanto, nos limitaremos a estudiar las coloraciones de los grafos conexos.*

5. *Si $G$ es un grafo con $n$ vértices, que es un camino simple, entonces $p(G, x) = x(x - 1)^{n-1}$.*

   *Es decir, $G = (V, E)$ donde $V = \{v_1, v_2, \ldots, v_n\}$ y $E = \{e_1, e_2, \ldots, e_{n-1}\}$ y $\gamma_G(e_i) = \{v_i, v_{i+1}\}$.*

   *En este caso, para elegir una coloración de $G$ con $x$ colores, podemos elegir el que queramos para $v_1$, y para el resto de los vértices tenemos $x - 1$ posibilidades (todas menos la que hayamos elegido para $v_{i-1}$). El principio del producto nos dice que $p(G, x) = x(x - 1)^{n-1}$.*

Antes de ver cómo calcular el polinomio cromático de un grafo, realizamos la siguiente construcción.

Dado un grafo $G$, tomamos un lado $e$ (que no sea un lazo) que una los vértices $u$ y $v$. Entonces el grafo $G_e$ es el grafo con los mismos vértices que $G$, pero al que se le ha quitado el lado $e$, y el grafo $G'_e$ es el grafo que resulta de identificar en $G_e$ los vértices $u$ y $v$.

**Teorema 4.9.1.** *Sea $G$ un grafo, y $u$ y $v$ dos vértices adyacentes. Sea $e$ el lado que los une. Entonces $p(G_e, x) = p(G, x) + p(G'_e, x)$.*

*Demostración:* Vamos a descomponer el conjunto de las posibles coloraciones de $G_e$ con $x$ colores en dos subconjuntos, los cuales los identificaremos con las coloraciones de $G$ y las de $G'_e$ respectivamente (con $x$ colores). Esto, junto con el principio de la suma, nos dará la relación que buscamos.

Puesto que en $G_e$ los vértices $u$ y $v$ no son adyacentes, una coloración de $G_e$ puede tener en los vértices $u$ y $v$ del mismo color o de distinto color.

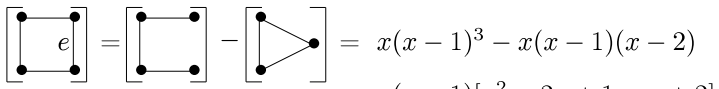
Si tienen distinto color, lo que tenemos es una coloración del grafo $G$ (obviamente, toda coloración de $G$ es una coloración de $G_e$). Por tanto, las coloraciones en las que $u$ y $v$ tienen distinto color pueden identificarse con las coloraciones de $G$.

Si $u$ y $v$ tienen el mismo color, entonces lo que tenemos es una coloración de $G'_e$. Recíprocamente, cualquier coloración de $G'_e$ nos da lugar a una coloración de $G_e$ en la que $u$ y $v$ tienen el mismo color. ■

Esta expresión podemos verla como $p(G,x) = p(G_e,x) - p(G'_e,x)$, lo cual nos permite reducir el cálculo del polinomio cromático de un grafo al cálculo de polinomios cromáticos de grafos más pequeños (con menos lados o con menos vértices). Veamos algún ejemplo.

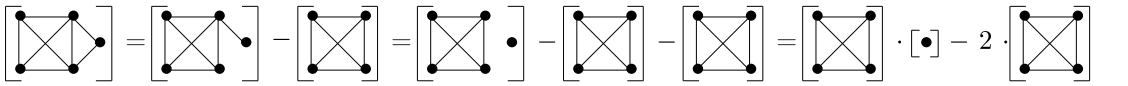
**Ejemplo 4.9.3.** *Para simplificar la notación, vamos a representar el polinomio cromático de un grafo encerrando el grafo entre corchetes.*

1. *Vamos a calcular el polinomio cromático de un ciclo de longitud* 4.




$$= x(x-1)^3 - x(x-1)(x-2)$$
$$= x(x-1)[x^2 - 2x + 1 - x + 2]$$
$$= x(x-1)(x^2 - 3x + 3).$$

2. *Vamos a calcular otro polinomio cromático.*



$$= x(x-1)(x-2)(x-3) \cdot x \; - 2 \cdot x(x-1)(x-2)(x-3) \;=\; x(x-1)(x-2)^2(x-3).$$

## 4.10. Árboles

Comenzamos en esta sección el estudio de un tipo especial de grafos, los llamados árboles. Éstos fueron estudiados por vez primera por Kirchhoff, en 1847, en su trabajo de redes eléctricas. Sin embargo, estas estructuras son hoy día muy importantes en el estudio de las estructuras de datos, las ordenaciones, etc.

**Definición 47.** *Un* árbol *es un grafo conexo que no tiene ciclos.*
*Un grafo que no tenga ciclos se denomina* bosque.
*Dado un grafo conexo, un subgrafo suyo se dice* árbol generador *si tiene todos los vértices y es un árbol.*

Nótese que un árbol no puede tener lazos ni lados paralelos.
Un primer resultado sobre árboles, muy intuitivo, es el siguiente:

**Proposición 4.10.1.** *Todo grafo conexo tiene un árbol generador.*

Este resultado es consecuencia inmediata del siguiente lema, cuya demostración se deja como ejercicio.

**Lema 4.10.1.** *Sea $G$ un grafo conexo que contiene un ciclo. Entonces, si quitamos uno de los lados del ciclo el grafo sigue siendo conexo.*

Otro resultado, también muy intuitivo es:

**Proposición 4.10.2.** *Todo árbol es un grafo plano.*

*Demostración:* Usando el teorema de Kuratowski el resultado es trivial, pues al no tener ciclos no puede tener ningún subgrafo que pueda contraerse hasta $K_5$ o $K_{3,3}$. No obstante, puede darse también una demostración sin hacer uso de este teorema, por inducción.

En realidad, lo que vamos a probar es que *todo grafo con n lados y que no tenga ciclos es un grafo plano*, y esto lo haremos por inducción en $n$.

Para $n = 0$ el resultado es trivialmente cierto, pues al no haber lados no pueden cruzarse.

Supuesto el resultado cierto para $n$ lo demostramos para $n + 1$.

Si tenemos un grafo sin ciclos con $n+1$ lados, le quitamos un lado y nos resulta un grafo plano (pues no tiene ciclos y tiene $n$ lados). Al no tener ciclos no divide al plano en regiones, por lo que dos puntos cualesquiera pueden unirse por una línea. Por tanto, el lado que añadimos podemos dibujarlo sin que corte a ninguno de los ya existentes. ■

**Corolario 4.10.1.** *Sea $G$ un grafo conexo con $n$ vértices. Entonces $G$ es un árbol si, y sólo si, $G$ tiene $n-1$ lados.*

*Demostración:* Supongamos que $G$ es un árbol. Entonces es un grafo plano, y el número de regiones en que se divide el plano es 1. Por el teorema 4.8.1 se tiene que $n-l+1 = 2$, lo que implica que $l = n-1$.

Recíprocamente, supongamos que tenemos un grafo conexo con $n$ vértices y $n-1$ lados. Si no fuera un árbol, podríamos obtener un árbol generador quitando lados, lo que nos daría un árbol con $n$ vértices y menos de $n-1$ lados, lo cual no es posible. ■

El siguiente teorema nos da una caracterización de los árboles.

**Teorema 4.10.1.** *Sea $G$ un grafo con $n$ vértices, sin lados paralelos ni lazos. Entonces son equivalentes:*

1. *$G$ es un árbol.*
2. *Dos vértices cualesquiera están unidos por un único camino simple.*
3. *$G$ es conexo, pero si le quitamos un lado deja de serlo.*
4. *$G$ no tiene ciclos, pero si le añadimos un lado tendrá algún ciclo.*
5. *$G$ tiene $n-1$ lados.*

Es decir, los árboles son los menores grafos conexos, o los mayores grafos sin ciclos.

Nótese también que para las caracterizaciones segunda, tercera y cuarta no es necesario suponer que el grafo no tiene lazos ni lados paralelos, pues de ellas se deduce.

*Demostración:* La equivalencia entre 1 y 5 ya la hemos visto. Vamos a ver que los enunciados 1,2,3,4 son equivalentes.

$1 \Longrightarrow 2$

Supongamos que $G$ es un árbol. Entonces es conexo, luego dados dos vértices cualesquiera hay un camino que los une. Por la proposición 4.1.1, hay un camino simple entre ambos vértices. Si hubiera más de uno, entonces el grafo contendría un ciclo (ver proposición 4.1.2), y esto no es posible, pues $G$ es un árbol.

$2 \Longrightarrow 3$

Puesto que dados dos vértices cualesquiera hay un camino (simple) que los une, el grafo es conexo.

Eliminamos del grafo $G$ un lado cualquiera. Supongamos que este lado une los vértices $u$ y $v$. Entonces, en el grafo resultante (que llamaremos $G'$) no hay ningún camino que una $u$ y $v$.

Esto es así porque de haber un camino que uniera $u$ y $v$ tendríamos un camino simple que uniría $u$ con $v$ en $G'$, lo que nos daría dos caminos simples que unen $u$ con $v$ en $G$: el que hemos encontrado

en $G'$ y el camino de longitud 1 $uv$. Pero por hipótesis, entre dos vértices había un único camino simple.

Por tanto, al eliminar un lado cualquiera el grafo resultante no es conexo, como queríamos.

$3 \Longrightarrow 4$

Supongamos que $G$ tuviera un ciclo. Entonces, por el lema 4.10.1, podríamos quitarle un lado a $G$ y el grafo seguiría siendo conexo. Por tanto, $G$ no tiene ciclos.

Le añadimos a $G$ un lado. Por ejemplo, el lado $uv$. Entonces, entre los vértices $u$ y $v$ hay al menos dos caminos simples. Uno, el camino $uv$, y otro, que podemos tomar en el grafo $G$ por ser éste conexo.

Al haber dos caminos simples entre dos vértices, el grafo resultante contiene un ciclo (proposición 4.1.2).

$4 \Longrightarrow 1$

Hay que demostrar que $G$ es conexo, en cuyo caso será un árbol (por no contener ciclos).

Pero si $G$ no fuera conexo, habría dos vértices $u$ y $v$ que no están unidos por ningún camino. Podríamos entonces añadir a $G$ el lado $uv$, y el grafo no contendría ningún ciclo, en contra de nuestra hipótesis.

Por tanto, el grafo $G$ es conexo.

■

# Capítulo 5

# Lógica proposicional

## 5.1. Lenguaje Proposicional

### 5.1.1. Introducción

El primer objetivo de la lógica es simbolizar el razonamiento humano. Es decir, producir un lenguaje en el que al menos parte del razonamiento humano (matemático o no) pueda ser expresado. La Lógica proposicional es la aproximación más sencilla a este objetivo. Los elementos del lenguaje humano que vamos a manejar son sentencias declarativas que pueden ser ciertas o falsas (pero no ambas cosas o ninguna de las dos). Cada una de esas sentencias es lo que llamaremos *proposición* o *fórmula bien formada* (f.b.f.). El método de trabajo consiste en partir de sentencias simples y combinarlas para formar otras más elaboradas. Las sentencias más simples se denominan *fórmulas atómicas* y se combinan mediante lo que llamamos *conectivas* (o también *operadores lógicos*) y las *reglas de sintaxis* correspondientes.

Un ejemplo sencillo de la necesidad de las conectivas y las reglas de sintaxis puede ser el de un niño que escribiera: Hoy es mi cumpleaños. No voy al parque. Estoy enfadado. Todos añadiríamos a esta secuencia de fórmulas atómicas unas conectivas gramaticales para indicar la relación entre ellas; por ejemplo: *Estoy enfadado porque hoy es mi cumpleaños y no voy al parque.* Pero también podríamos componer: *Hoy es mi cumpleaños pero no voy al parque porque estoy enfadado.* Cada una de ellas tiene un significado diferente, así que el discurso del niño puede ser interpretado de distintas formas porque carece de elementos de ligadura entre las distintas sentencias. Además el enlace entre los distintos elementos del discurso debe seguir unas reglas de sintaxis; no sería correcto decir: *Pero hoy es mi cumpleaños o no voy al parque o estoy enfadado.*

### 5.1.2. Elementos del lenguaje proposicional:

Como ya hemos adelantado, necesitamos los siguientes tipos de elementos para construir el lenguaje:

Las proposiciones básicas

Operadores lógicos o Conectivas

Sintaxis del cálculo proposicional

#### Las proposiciones básicas

En el lenguaje humano las proposiciones básicas pueden ser

Los enunciados de acción,

los enunciados de propiedades de sujetos,

los enunciados de relación entre sujetos.

**Ejemplo 5.1.1.** *Hace calor, Llueve, Enrique conduce autobuses, La lluvia se lleva la contaminación.*

*Mi coche está sucio, Belén es una chica, La ciudad está contaminada*

*El autobús contamina menos que los coches, Belén es la mujer de Enrique*

En el cálculo proposicional (o lógica proposicional) *las proposiciones básicas son los elementos de un conjunto predeterminado (finito o infinito numerable).* No se trata por tanto de elementos con un significado asignado.

**Ejemplo 5.1.2.** $\{HC, L, ECA, LLSLLA, MCES, BEUC, LCEC, EACMQLC, BELMDE\}$

$\{H, L1, E, L2, M, B, L3, E, B\}$

$\{a, b, g, d, e, j, r, w\}$

$\{a, b, c, d\}$

*El conjunto de todas las proposiciones básicas en el lenguaje humano.*

**Operadores lógicos o Conectivas:**

En el lenguaje humano la conexión entre distintos enunciados se hace mediante partículas como las conjunciones; en el lenguaje proposicional consideraremos unos símbolos que nos permitirán construir elementos complejos a partir de los más simples, estos son:

$$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$$

$\neg$ se lee **no** (negación)

$\wedge$ se lee **y** (conjunción)

$\vee$ se lee **o** (disyunción)

$\rightarrow$ se lee **implica** (implicación)

$\leftrightarrow$ se lee **equivale** (equivalencia o doble implicación)

**Sintaxis del cálculo proposicional (Reglas para la formación de nuevas proposiciones a partir de las básicas):**

Son consideradas *proposiciones o fórmulas bien formadas (fbfs)* del cálculo proposicional:

Las proposiciones básicas, a las que llamamos *proposiciones atómicas*

Si $\alpha$ y $\beta$ son fbfs, también lo son:

$$\alpha \wedge \beta; \quad \alpha \vee \beta; \quad \neg\alpha; \quad \alpha \rightarrow \beta; \quad \alpha \leftrightarrow \beta$$

**Ejemplo 5.1.3.** *Para el conjunto de proposiciones atómicas*

$$X = \{\alpha, \beta, \gamma, \varphi\}$$

*son fórmulas bien formadas:*

$(\alpha \wedge \neg\beta) \rightarrow ((\gamma \vee \varphi) \vee \alpha)$

$\gamma \wedge (\alpha \vee \beta) \rightarrow (\neg\alpha \vee \beta)$

$(\gamma \vee \neg\alpha) \vee (\neg\alpha \rightarrow \beta)$

*y* no *son fbfs:*

$\alpha\neg\beta$

$\gamma(\alpha \vee \beta) \rightarrow \beta$

En resumen, tenemos:

**Definición 48.** *Sea $X$ un conjunto finito o infinito numerable. Definimos el conjunto de las proposiciones (o fórmulas proposicionales o fórmulas bien formadas, o simplemente, fórmulas) sobre $X$ como el conjunto $Form(X)$ como sigue:*

1. *Todo elemento de $X$ es una proposición (es decir, $X \subseteq Form(X)$).*
2. *Si $\alpha$ y $\beta$ son proposiciones, también lo son $\alpha \vee \beta$, $\alpha \wedge \beta$, $\alpha \to \beta$, $\alpha \leftrightarrow \beta$ y $\neg\alpha$.*
3. *Todo elemento de $Form(X)$, o bien pertenece a $X$, o bien se ha obtenido como hemos indicado en el apartado anterior.*

*A los elementos de $X$ se les conoce como proposiciones atómicas o fórmulas atómicas.*

### 5.1.3. Uso de las reglas de prioridad en la escritura de fórmulas:

Al igual que en las fórmulas algebraicas o aritméticas, los paréntesis se usan para anteponer el uso de una conectiva al de otras. Pero existen aquí también unas reglas de escritura que permiten prescindir de los paréntesis en determinados casos. Para ello tendremos en cuenta que:

1. Cualquier conectiva dentro de un paréntesis tiene prioridad sobre las demás.

2. $\neg$ tiene prioridad sobre todos las otras, es decir,
$$\begin{aligned} \neg a \wedge b &\text{ sustituye a } (\neg a) \wedge b \text{ y es diferente de } \neg(a \wedge b),\\ \neg a \vee b &\text{ sustituye a } (\neg a) \vee b \text{ y es diferente de } \neg(a \vee b),\\ \neg a \to b &\text{ sustituye a } (\neg a) \to b \text{ y es diferente de } \neg(a \to b),\\ \neg a \leftrightarrow b &\text{ sustituye a } (\neg a) \leftrightarrow b \text{ y es diferente de } \neg(a \leftrightarrow b). \end{aligned}$$

3. $\wedge$ y $\vee$ tienen el mismo rango de prioridad, pero ambas tienen mayor prioridad que $\to$ y $\leftrightarrow$, por tanto,
$$\begin{aligned} a \wedge b \to c &\text{ sustituye a } (a \wedge b) \to c \text{ y es diferente de } a \wedge (b \to c),\\ a \to b \vee c &\text{ sustituye a } a \to (b \vee c) \text{ y es diferente de } (a \to b) \vee c. \end{aligned}$$

   No es conveniente escribir

$$a \wedge b \vee c$$

   De hecho, con la definición que hemos dado, esto no sería una fórmula. Habría que distinguir entre $(a \wedge b) \vee c$ y $a \wedge (b \vee c)$. En $(a \wedge b) \vee c$, primero se construye la fórmula $a \wedge b$ y después se utiliza la conectiva $\vee$ entre ella y la proposición atómica $c$, mientras que en $a \wedge (b \vee c)$ en primer lugar se forma $b \vee c$ para luego obtener la fórmula con la proposición atómica $a$, la conectiva $\wedge$ y la proposición $b \vee c$.

   Por el mismo motivo, no se debería escribir $a \vee b \vee c$, pues habría que distinguir entre $(a \vee b) \vee c$ y $a \vee (b \vee c)$. Sin embargo, más adelante veremos que las fórmulas $(a \vee b) \vee c$ y $a \vee (b \vee c)$ son equivalentes (que no iguales), por lo que en casos así prescindiremos de los paréntesis.

   La misma situación se da para $a \wedge b \wedge c$.

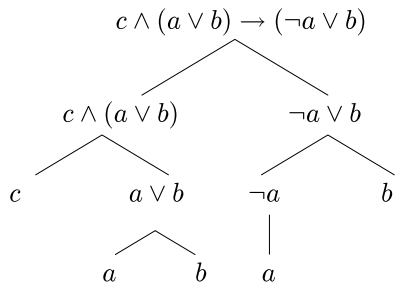
   Sin embargo, esta situación no se da para $a \to b \to c$. Por tanto, en tal caso habría que indicar la prioridad con los paréntesis (bien $a \to (b \to c)$, bien $(a \to b) \to c$).

4. Es frecuente usar $\to$ con preferencia sobre $\leftrightarrow$, aunque somos partidarios de utilizar paréntesis para priorizar la conectiva que se desee entre estas dos.

5. *En caso de duda siempre es preferible abusar de los paréntesis.*

**Árbol de formación de una fórmula y subfórmulas**

Para practicar sobre las reglas de uso de paréntesis en las construcciones de fórmulas y familizarizarnos con ellas podríamos realizar un sencillo ejercicio; se trata de desglosar una fórmula construyendo un árbol que tiene por raíz a la fórmula dada, y las ramas que salen de cada nodo nos llevan a las fórmulas que junto con la correspondiente conectiva formaban ese nodo. Las hojas del árbol serán las proposiciones atómicas. Por ejemplo: $c \wedge (a \vee b) \to (\neg a \vee b)$ tendría asociado el árbol:




El recorrido del árbol partiendo de las hojas hacia la raíz nos da el procedimiento de construcción de la f.b.f. a partir de las proposiciones atómicas $a, b$ y $c$.

Así, de las fórmulas atómicas $a$ y $b$, y la conectiva $\vee$ formamos la fórmula $\alpha_1 = a \vee b$. Esta fórmula, junto con la fórmula (atómica) $c$ y la conectiva $\wedge$ nos da la fórmula $\alpha_2 = c \wedge (a \vee b)$.

Por otra parte, la fórmula $a$ junto con la conectiva $\neg$ nos da la fórmula $\beta_1 = \neg a$, que junto con la conectiva $\vee$ y la fórmula $b$ nos da la fórmula $\beta_2 = \neg a \vee b$.

Por último, la fórmula que hemos desglosado es $\alpha_2 \to \beta_2$. De acuerdo con las reglas que hemos dado, podríamos haber escrito esta fórmula como $c \wedge (a \vee b) \to \neg a \vee b$.

**Ejercicio 5.1.1.** *Dadas las siguientes fórmulas, construye su árbol de desglose.*

1. $a \wedge \neg b \to c \vee (e \wedge a)$
2. $c \wedge (a \vee b) \to \neg a \vee b$
3. $\neg(a \to b) \to a \wedge \neg(a \wedge b)$
4. $a \wedge (a \vee b \to d) \wedge (d \to \neg a)$
5. $(a \wedge c) \vee b \to d \wedge (d \to \neg a)$
6. $\neg a \to (b \to a) \wedge \neg(a \wedge b)$
7. $(a \wedge \neg(b \to c \vee e)) \vee a$
8. $b \wedge (a \vee b) \to d \wedge \neg(d \to \neg a)$
9. $b \wedge a(\neg b \to d \wedge \neg(d \to \neg a))$
10. $\neg(b \to a) \wedge \neg(a \wedge b) \to \neg a \vee b$

Dada una fórmula $\alpha$, una subfórmula suya es una fórmula que aparece en algún nodo de su árbol de formación.

Más precisamente, podemos definirlo como sigue:

**Definición 49.** *Sea $\alpha$ una fórmula. Definimos el conjunto $Sub(\alpha)$ como sigue:*

1. *Si* $\alpha$ *es una fórmula atómica,* $Sub(\alpha) = \{\alpha\}$.
2. *Si* $\alpha$ *es de la forma* $\alpha_1 \vee \alpha_2$, $Sub(\alpha) = \{\alpha\} \cup Sub(\alpha_1) \cup Sub(\alpha_2)$.
3. *Si* $\alpha$ *es de la forma* $\alpha_1 \wedge \alpha_2$, $Sub(\alpha) = \{\alpha\} \cup Sub(\alpha_1) \cup Sub(\alpha_2)$.
4. *Si* $\alpha$ *es de la forma* $\alpha_1 \rightarrow \alpha_2$, $Sub(\alpha) = \{\alpha\} \cup Sub(\alpha_1) \cup Sub(\alpha_2)$.
5. *Si* $\alpha$ *es de la forma* $\alpha_1 \leftrightarrow \alpha_2$, $Sub(\alpha) = \{\alpha\} \cup Sub(\alpha_1) \cup Sub(\alpha_2)$.
6. *Si* $\alpha$ *es de la forma* $\neg\alpha_1$, $Sub(\alpha) = \{\alpha\} \cup Sub(\alpha_1)$.

Por ejemplo, vamos a calcular el conjunto de subfórmulas de $\alpha = c \wedge (a \vee b) \rightarrow (\neg a \vee b)$. Entonces: $Sub(\alpha) = \{c \wedge (a \vee b) \rightarrow (\neg a \vee b)\} \ \cup \ Sub(c \wedge (a \vee b)) \ \cup \ Sub(\neg a \vee b)$.

- $Sub(c \wedge (a \vee b)) = \{c \wedge (a \vee b)\} \cup Sub(c) \cup Sub(a \vee b)$.
  - $Sub(c) = \{c\}$.
  - $Sub(a \vee b) = \{a \vee b\} \cup Sub(a) \cup Sub(b) = \{a \vee b\} \cup \{a\} \cup \{b\} = \{a, b, a \vee b\}$.

  Por tanto,
  $Sub(c \wedge (a \vee b)) = \{c \wedge (a \vee b)\} \cup \{c\} \cup \{a, b, a \vee b\} = \{a, b, c, a \vee b, c \wedge (a \vee b)\}$.
- $Sub(\neg a \vee b) = \{\neg a \vee b\} \cup Sub(\neg a) \cup Sub(b)$.
  - $Sub(\neg a) = \{\neg a\} \cup Sub(a) = \{\neg a\} \cup \{a\} = \{a, \neg a\}$.
  - $Sub(b) = \{b\}$.

  Luego $Sub(\neg a \vee b) = \{\neg a \vee b\} \cup \{a, \neg a\} \cup \{b\} = \{a, b, \neg a, \neg a \vee b\}$.

Y volviendo a la fórmula $\alpha$ se tiene que:

$$\begin{aligned} Sub(\alpha) &= \{c \wedge (a \vee b) \rightarrow (\neg a \vee b)\} \cup \{a, b, c, a \vee b, c \wedge (a \vee b)\} \cup \{a, b, \neg a, \neg a \vee b\} \\ &= \{a,\ b,\ c,\ \neg a,\ a \vee b,\ \neg a \vee b,\ c \wedge (a \vee b),\ c \wedge (a \vee b) \rightarrow (\neg a \vee b)\} \end{aligned}$$

que vemos que son exactamente las que aparecían en el árbol de formación de la fórmula.

**Traducción del lenguaje humano a la lógica proposicional:**

No es de nuestro interés profundizar en la interpretación del lenguaje humano en términos de la lógica proposicional, pero nos permitimos escribir un ejemplo sencillo que relaciona ambos lenguajes.

Consideremos el razonamiento:

*Si estudio quizás pueda o no aprobar el examen, pero si no lo hago seguro que no aprobaré el examen*

Podemos extaer unas sentencias básicas que serían:

$P =$ Yo estudio $Q =$ Yo apruebo el examen

a partir de las cuales podemos construir el enunciado completo:

$$(P \rightarrow Q \vee \neg Q) \wedge (\neg P \rightarrow \neg Q)$$

## 5.2. Semántica de la lógica proposicional

Nuestro objetivo final en este curso es obtener métodos que nos permitan decidir si un determiando razonamiento es correcto. Para ello introducimos ahora una forma de asignar un cierto *significado* a un conjunto de proposiciones.

### 5.2.1. Interpretaciones o valoraciones

Si $X$ es un conjunto de proposiciones atómicas, una **interpretación** para las proposiciones que se obtienen de $X$ es una aplicación

$$I : X \to \{0, 1\}$$

que se extiende a todas las fórmulas bien formadas mediante las reglas:

$$\begin{array}{l} I(\neg a) = 1 + I(a) \\ I(a \vee b) = I(a) + I(b) + I(a)I(b) \\ I(a \wedge b) = I(a)I(b) \\ I(a \to b) = 1 + I(a) + I(a)I(b) \\ I(a \leftrightarrow b) = 1 + I(a) + I(b) \end{array}$$

Cuadro 5.1: Interpretaciones y conectivas

donde las operaciones se efectúan en $\mathbb{Z}_2$. El valor $I(\alpha)$ se llama **el valor de verdad de la fórmula** $\alpha$ bajo la interpretación $I$, y frecuentemente usaremos los términos *verdadera* o *falsa* para afirmar que el valor de verdad de una fórmula es 1 o 0 respectivamente.

En otros textos las interpretaciones son nombradas como "valoraciones" y para designarlas se usa la letra "v".

Hay que observar que si el conjunto de proposiciones atómicas de partida tiene $n$ elementos, entonces podemos elegir $2^n$ interpretaciones distintas para él.

**Ejemplo 5.2.1.** *Consideremos el conjunto de fórmulas atómicas $X = \{a, b\}$ y para él la interpretación que asigna*

$$I_1(a) = 0; \quad I_1(b) = 1$$

*entonces, para calcular el valor de verdad de la fórmula*

$$a \wedge b \to \neg a$$

*calculamos en primer lugar $I_1(a \wedge b) = I_1(a)I_1(b) = 0 \cdot 1 = 0$ así como $I_1(\neg a) = 1 + I_1(a) = 1 + 0 = 1$; ahora podemos determinar*

$$I_1((a \wedge b) \to \neg a) = 1 + I_1(a \wedge b) + I_1(a \wedge b)I_1(\neg a) = 1 + 0 + 0 \cdot 1 = 1$$

*Por tanto la fórmula es verdadera bajo la interpretación $I_1$. Tomemos ahora otra interpretación que asigne*

$$I_2(a) = 1; \quad I_2(b) = 1$$

*y volvemos a calcular en la misma secuencia que antes el valor de verdad para la misma fórmula*

$$a \wedge b \to \neg a$$

*Tenemos ahora $I_2(a \wedge b) = I_2(a)I_2(b) = 1 \cdot 1 = 1$; $I_2(\neg a) = 1 + I_2(a) = 1 + 1 = 0$; entonces*

$$I_2((a \wedge b) \to \neg a) = 1 + I_2(a \wedge b) + I_2(a \wedge b)I_2(\neg a) = 1 + 1 + 1 \cdot 0 = 0$$

*Por tanto la fórmula es falsa bajo la interpretación $I_2$.*

*En este ejemplo observamos que el cálculo del valor de una interpretación para una fórmula puede hacerse a través del árbol de descomposición de la fórmula que aprendimos en la sección anterior, partiendo de las hojas y aplicando la tabla 5.1 en cada nodo.*

**Ejemplo 5.2.2.** *Consideremos la fórmula*

$$\alpha = \neg(a \to b) \to (\neg a \to \neg b)$$

*Tratamos de calcular a continuación el valor de una interpretación de esta fórmula en función de las fórmulas atómicas que intervienen. LLamemos*

$$\beta = a \to b; \qquad \delta = \neg a \to \neg b$$

*entonces*

$$I(\alpha) = 1 + I(\neg\beta) + I(\neg\beta)I(\delta) = 1 + (1 + I(\beta)) + (1 + I(\beta))I(\delta)$$

*como* $1 + 1 = 0$ *en* $\mathbb{Z}_2$

$$I(\alpha) = I(\beta) + (1 + I(\beta))I(\delta)$$

*calculamos primero*

$$I(\beta) = 1 + I(a) + I(a)I(b)$$

$$I(\delta) = 1 + I(\neg a) + I(\neg a)I(\neg b) = 1 + (1 + I(a)) + (1 + I(a))(1 + I(b))$$

*simplificando y desarrollando los productos*

$$I(\delta) = I(a) + 1 + I(a) + I(b) + I(a)I(b)$$

*como en cualquier caso* $I(a) + I(a) = 0$*, queda*

$$I(\delta) = 1 + I(b) + I(a)I(b)$$

*y sustituyendo*

$$I(\alpha) = 1 + I(a) + I(a)I(b) + (1 + 1 + I(a) + I(a)I(b))(1 + I(b) + I(a)I(b))$$

*de nuevo simplificando* $1 + 1 = 0$ *y desarrollando el producto*

$$= 1 + I(a) + I(a)I(b) + (I(a) + I(a)I(b) + I(a)I(b) + I(a)I(b)^2 + I(a)^2I(b) + (I(a)I(b))^2)$$

*tendremos en cuenta ahora que en* $\mathbb{Z}_2$ *el cuadrado de cualquier elemento es el propio elemento (*$0^2 = 0$ *y* $1^2 = 1$*) y de nuevo que* $I(a)I(b) + I(a)I(b) = 0$ *con lo que resulta*

$$= 1 + I(a) + I(a)I(b) + I(a) + I(a)I(b) + I(a)I(b) + I(a)I(b) + I(a)I(b) + I(a)I(b) = 1$$

*Es decir, se obtiene que bajo cualquier interpretación de las proposiciones atómicas el valor de verdad de la fórmula es* 1*. A las fórmulas que verifican esta propiedad las llamaremos* **tautologías**.

### 5.2.2. Tabla de verdad para una fórmula

Un método alternativo al cálculo de interpretaciones en $\mathbb{Z}_2$ es tener en cuenta la siguiente tabla:

| $a$ | $b$ | $a \wedge b$ | $a \vee b$ | $\neg a$ | $a \to b$ | $a \leftrightarrow b$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |

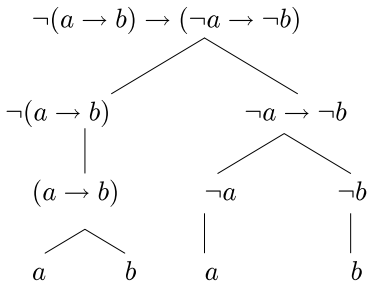
Cuadro 5.2: Tabla de verdad

en la que se han recogido todas las posibilidades para los valores de verdad de una fórmula en la que sólo aparece una conectiva. A partir de esta tabla (que hay que memorizar), se pueden calcular los valores de verdad de una fórmula para **todas las interpretaciones** posibles del conjunto de fórmulas atómicas que intervengan; es lo que se llama **la tabla de verdad** de una fórmula.

**Ejemplo 5.2.3.** *Consideremos la fbf*

$$\alpha = \neg(a \to b) \to (\neg a \to \neg b)$$

*Podemos obtener la* **tabla de verdad de la fórmula** *en la que aparecen todas las interpretaciones posibles, es decir, todas las asignaciones a las proposiciones atómicas y el resultado de extenderlas a la fórmula completa. Para ello se dibuja una tabla de doble entrada en la que en las columnas de la primera fila se escriben las subfórmulas que intervienen en la expresión, es decir, los nodos distintos del árbol que resulta al desglosar la fórmula.*




*En este caso la primera línea sería*

| $a$ | $b$ | $a \to b$ | $\neg(a \to b)$ | $\neg a$ | $\neg b$ | $\neg a \to \neg b$ | $\neg(a \to b) \to (\neg a \to \neg b)$ |
|---|---|---|---|---|---|---|---|

*Ahora se añaden tantas filas como interpretaciones distintas se puedan asignar al conjunto de proposiciones atómicas que intervienen, en este caso son dos $a$ y $b$ y por tanto son $2^2$ posibilidades:*

| $a$ | $b$ |
|---|---|
| 0 | 0 |
| 0 | 1 |
| 1 | 0 |
| 1 | 1 |

| $a$ | $b$ | $a \to b$ | $\neg(a \to b)$ | $\neg a$ | $\neg b$ | $\neg a \to \neg b$ | $\neg(a \to b) \to (\neg a \to \neg b)$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | | | 1 | 1 | 1 | |
| 0 | 1 | | | 1 | 0 | 0 | |
| 1 | 0 | | | 0 | 1 | 1 | |
| 1 | 1 | | | 0 | 0 | 1 | |

*Sólo queda calcular cada una de las columnas en blanco haciendo uso de las tablas conocidas para las conectivas y las columnas que corresponden a subfórmulas hijas en el árbol de desglose. Así, para calcular la columna de $\neg a \to \neg b$ tendremos en cuenta las de $\neg a$ y de $\neg b$.*

*Si completas la tabla anterior correctamente debes obtener como última columna los valores $(1, 1, 1, 1)$. Es decir, tendrás de nuevo que es una* **tautología**.

**Ejemplo 5.2.4.** *La siguiente es la tabla de verdad de la fórmula:*

$$\varphi = (a \wedge b \to c) \wedge (\neg(a \wedge b) \to d)$$

| $a$ | $b$ | $c$ | $d$ | $a \wedge b$ | $a \wedge b \to c$ | $\neg(a \wedge b)$ | $\neg(a \wedge b) \to d$ | $\varphi$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |

### 5.2.3. Clasificación de fórmulas

Hemos visto en la sección precedente que hay fórmulas que son ciertas para cualquier interpretación. Es lo que hemos llamado una tautología. Vamos a continuación a clasificar las fórmulas según los valores de verdad que pueden tomar:

**Definición 50.** *Sea $\alpha$ una fórmula de un lenguaje proposicional:*

1. *$\alpha$ es una* **tautología** *si para cualquier interpretación $I$ se tiene que $I(\alpha) = 1$.*
2. *$\alpha$ es* **satisfacible** *si existe al menos una interpretación $I$ para la que $I(\alpha) = 1$.*
3. *$\alpha$ es* **refutable** *si existe al menos una interpretación $I$ para la que $I(\alpha) = 0$.*
4. *$\alpha$ es* **contradicción** *si para cualquier interpretación $I$ se tiene que $I(\alpha) = 0$.*
5. *$\alpha$ es* **contingente** *si es satisfacible y refutable.*

Veamos algunos ejemplos:

**Ejemplo 5.2.5.**

- *La fórmula* $\alpha = p \to (q \to p)$ *es una tautología. Para comprobarlo, construyamos su tabla de verdad:*

| $p$ | $q$ | $q \to p$ | $p \to (q \to p)$ |
|---|---|---|---|
| *0* | *0* | *1* | *1* |
| *0* | *1* | *0* | *1* |
| *1* | *0* | *1* | *1* |
| *1* | *1* | *1* | *1* |

  *y vemos que la fórmula es cierta para cualquier interpretación.*

  *La fórmula también es satisfacible, pues hay una interpretación (en este caso todas) para la que la fórmula es cierta.*

- *La fórmula* $\alpha = p \vee \neg q \to (\neg r \wedge (q \to p))$ *es satisfacible, pues si tomamos la interpretación* $I(p) = I(q) = 1, I(r) = 0$ *se tiene que* $I(\alpha) = 1$*, ya que:*

  $I(p \vee \neg q) = 1$*;* $I(q \to p) = 1$*;* $I(\neg r) = 1$*;* $I(\neg r \wedge (q \to p)) = 1$ *y por tanto,* $I(\alpha) = 1$*.*

  *También es refutable, pues si para la interpretación* $I(p) = I(q) = I(r) = 1$ *la fórmula es falsa.*

  $I(p \vee \neg q) = 1$*;* $I(q \to p) = 1$*;* $I(\neg r) = 0$*;* $I(\neg r \wedge (q \to p)) = 0$ *y por tanto,* $I(\alpha) = 0$*.*

  *La fórmula* $\alpha$ *es entonces contingente.*

- *La fórmula* $\alpha = (p \to \neg q) \wedge (p \wedge q)$ *es una contradicción, pues su tabla de verdad es*

| $p$ | $q$ | $\neg q$ | $p \to \neg q$ | $p \wedge q$ | $(p \to \neg q) \wedge (p \wedge q)$ |
|---|---|---|---|---|---|
| *0* | *0* | *1* | *1* | *0* | *0* |
| *0* | *1* | *0* | *1* | *0* | *0* |
| *1* | *0* | *1* | *1* | *0* | *0* |
| *1* | *1* | *0* | *0* | *1* | *0* |

**Observación:**

1. Podemos considerar las fórmulas divididas en cuatro grupos: tautologías, satisfacibles, refutables y contradicciones.

   En tal caso, cada fórmula pertenece exactamente a dos de estos grupos. Puede ser tautología y satisfacible, puede ser satisfacible y refutable, o puede ser refutable y contradicción.

2. Si en lugar de dividirlas en los cuatro grupos anteriores lo hacemos en los tres siguientes: tautologías, contingentes y contradicciones; entonces cada fórmula pertenece a uno (y sólo uno) de esos tres grupos.

3. Si $\alpha$ es una fórmula, no significa lo mismo decir $\alpha$ *no es tautología* que decir $\neg\alpha$ *es tautología.*

   En el primer caso estamos diciendo que $\alpha$ es refutable, mientras que en el segundo que $\alpha$ es contradicción.

   Es decir, $\alpha$ es refutable si, y sólo si, $\alpha$ no es tautología; y $\alpha$ es contradicción si, y sólo si, $\neg\alpha$ es tautología.

A continuación vamos a enumerar algunas fórmulas que son tautologías. Tanto $\alpha$, $\beta$ como $\gamma$ representan fórmulas cualesquiera de un lenguaje proposicional (no necesariamente fórmulas atómicas).

1. $\alpha \to \alpha$.
2. $\neg\neg\alpha \to \alpha$.
3. $\alpha \to \neg\neg\alpha$.

4. $\alpha \vee \beta \rightarrow \beta \vee \alpha$.
5. $\alpha \wedge \beta \rightarrow \beta \wedge \alpha$.
6. $\alpha \rightarrow (\beta \rightarrow \alpha)$.
7. $\alpha \rightarrow \alpha \vee \beta$.
8. $\alpha \wedge \beta \rightarrow \alpha$.
9. $\alpha \vee \neg\alpha$.
10. $\neg(\alpha \wedge \neg\alpha)$.
11. $((\alpha \rightarrow \beta) \wedge \alpha) \rightarrow \beta$.
12. $((\alpha \rightarrow \beta) \wedge \neg\beta) \rightarrow \neg\alpha$.
13. $((\alpha \vee \beta) \wedge \neg\alpha) \rightarrow \beta$.
14. $(\neg\alpha \rightarrow \alpha) \rightarrow \alpha$.
15. $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$.
16. $(\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha)$.
17. $(\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \neg\alpha)$.
18. $(\alpha \rightarrow \beta) \rightarrow ((\gamma \rightarrow \beta) \rightarrow (\alpha \vee \gamma \rightarrow \beta))$.
19. $(\alpha \rightarrow \beta) \rightarrow ((\alpha \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta \wedge \gamma))$.

**Definición 51.** *Sea $\Gamma = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ un conjunto de fórmulas de un lenguaje proposicional. Se dice que $\Gamma$ es* **satisfacible** *si existe una interpretación $I$ para la que $I(\gamma_1) = I(\gamma_2) = \cdots = I(\gamma_n) = 1$.*
*Si $\Gamma = \emptyset$ entonces $\Gamma$ es satisfacible.*
*Un conjunto de fórmulas es insatisfacible si no es satisfacible.*

Es decir, un conjunto es satisfacible si existe una iterpretación para la que todas las fórmulas son ciertas. En el caso del conjunto vacío, cualquier interpretación hace ciertas (y falsas) todas las fórmulas. Por eso, el conjunto vacío es satisfacible.

Se tiene entonces que $\Gamma$ es insatisfacible si no existe ninguna interpretación $I$ que haga ciertas todas las fórmulas. Si $\Gamma \neq \emptyset$ esto es equivalente a que para cualquier interpretación $I$ existe un elemento $\alpha \in \Gamma$ tal que $I(\alpha) = 0$.

**Proposición 5.2.1.** *Sea $\Gamma = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ un conjunto de fórmulas. Entonces son equivalentes:*

1. *$\Gamma$ es insatisfacible*
2. *$\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n$[1] es contradicción.*
3. *Para cualquier interpretación $I$, $I(\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n) = 0$.*
4. *Para cualquier interpretación $I$, $\prod_{i=1}^{n} I(\gamma_i) = 0$.*

Notemos que si $\Gamma = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ es un conjunto de fórmulas, y una (o más) de las fórmulas $\gamma_i$ es de la forma $\gamma_i = \gamma_{i1} \wedge \gamma_{i2}$, entonces $\Gamma$ es insatisfacible si, y sólo si, lo es el conjunto que resulta de sustituir en $\Gamma$ la fórmula $\gamma_i$ por las dos fórmulas $\gamma_{i1}$ y $\gamma_{i2}$.

**Ejemplo 5.2.6.** *Sean $\gamma_1 = p \vee \neg q \rightarrow q$, $\gamma_2 = p \leftrightarrow q$ y $\gamma_3 = q \rightarrow (p \leftrightarrow \neg q)$. Entonces el conjunto $\Gamma = \{\gamma_1, \gamma_2, \gamma_3\}$ es insatisfacible, pues no hay ninguna interpretación para la que las tres fórmulas sean ciertas. Para esto, construimos la tabla de verdad de las tres fórmulas (no vamos a indicar los pasos intermedios)*

[1] En principio, la notación $\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n$ puede ser ambigua, pues no hemos visto que la conjunción sea asociativa. Entenderemos entonces que$\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n$ se corresponde con la fórmula $(\cdots(\gamma_1 \wedge \gamma_2) \wedge \cdots \wedge \gamma_n)$

| $p$ | $q$ | $p \vee \neg q \to p$ | $p \leftrightarrow \neg q$ | $q \to (p \leftrightarrow \neg q)$ |
|---|---|---|---|---|
| *0* | *0* | *0* | *1* | *1* |
| *0* | *1* | *1* | *0* | *0* |
| *1* | *0* | *1* | *0* | *1* |
| *1* | *1* | *1* | *1* | *0* |

*y vemos que no hay ninguna interpretación para la que las tres fórmulas sean ciertas. Obviamente, si calculáramos la tabla de verdad de* $\gamma_1 \wedge \gamma_2 \wedge \gamma_3$ *nos quedaría una columna con todo ceros.*

| $p$ | $q$ | $p \vee \neg q \to p$ | $p \leftrightarrow \neg q$ | $q \to (p \leftrightarrow \neg q)$ | $(\gamma_1 \wedge \gamma_2) \wedge \gamma_3$ |
|---|---|---|---|---|---|
| *0* | *0* | *0* | *1* | *1* | *0* |
| *0* | *1* | *1* | *0* | *0* | *0* |
| *1* | *0* | *1* | *0* | *1* | *0* |
| *1* | *1* | *1* | *1* | *0* | *0* |

### 5.2.4. Inciso

**FORMALIZACIÓN DEL CASTELLANO UTILIZANDO LOS ESCASOS RECURSOS DE PROPOSICIONAL.**

Del libro: Razón, dulce razón; T. Tymoczko y J. Henle (F-4 TYM- raz) (Páginas 139 en adelante)

Algunos libros de texto de lógica dedican un tiempo considerable a formalizar enunciados (o argumentos) del castellano ordinario al lenguaje simple de Proposicional. Creemos que esto es un error [ ]. Queremos investigar cómo de bien la lógica proposicional da cuenta del castellano habitual; es decir, cómo de bien *and*, *or* e *implica* simulan las operaciones habituales del castellano expresadas por *y*, *o* y *si ... entonces*. [ ] La interpretación mediante tablas de verdad de las conectivas *and*, *or* y *implica* es simple y precisa; los usos en castellano de *y*, *o* y *si ... entonces* parecen complicados e irregulares.

*and* e *y*

Algunos lógicos creen que hay un sentido especial, o significado de la palabra castellana *y* que conecta enunciados de una manera dependiente del tiempo. Desde este punto de vista, *Mel se aburrió y Mel se marchó de la fiesta* no es equivalente a ( y por tanto no significa lo mismo que) *Mel se marchó de la fiesta y Mel se aburrió*

El filósofo Paul Grice sugirió [ ] distinguir entre (1) lo que significa una oración y (2) la información que una audiencia típica puede obtener de un uso típico de esa oración.

*or* y *o*

La principal preocupación respecto a la traducción del castellano *o* por la conectiva *or* tiene que ver con la primera línea de la tabla de verdad. Mucha gente cree que *P o Q* debería ser falso cuando ambos, P y Q son verdaderos. De hecho existe toda una respetable función lógica llamada *o exclusivo* [ ]. (ambas están relacionadas ) $A \oplus B \equiv (A \vee B) \wedge \neg(A \wedge B)$; $A \vee B \equiv (A \oplus B) \oplus (A \wedge B)$

El mejor argumento para *or* es la simplicidad del esquema resultante. Consideremos lo siguiente: *Ni P ni Q* es la negación castellana de *o bien P, o bien Q*. Ahora, *Ni P ni Q* es equivalente en castellano a *No P y no Q*. Además, $\neg(P \vee Q)$ es lógicamente equivalente a $\neg P \wedge \neg Q$, pero $\neg(P \oplus Q)$ no lo es.

Ejemplo: *O limpias la habitación o no sales a jugar*, le dice papá Homer a su hijo Bart. Significa eso que Homer habría dicho una falsedad si Bart limpia su habitación pero no sale a jugar? Qué ocurriría se viene un huracán entre tanto, o si Bart rompe la cama mientras limpia?

*implica* y *Si ... entonces*

Un argumento simple (de Samuel Gutteplan) es éste: Los hablantes del castellano se inclinan a aceptar que Si $A \wedge B$, entonces A. Pero entonces se deduce que *Si Jim y Tom son profesores, entonces Jim es un*

*profesor* (esto debe ser verdadero, por tanto *si V entonces V* es V) y *Si Jim es un profesor y Tom es un pingüino, entonces Jim es un profesor* (esto debe ser verdadero, por tanto *si F entonces V* es V) y *Si Jim es un pingüino y Tom es un profesor, entonces Jim es un pingüino* (esto debe ser verdadero, por tanto *si F entonces F* es V). Y, por supuesto, sabemos que tenemos que interpretar *si V entonces F* como F. Esto justifica las cuatro líneas de que consta la tabla de verdad de la implicación.

## 5.3. Equivalencia Lógica

**Definición 52.** *Dadas dos fbfs $\alpha$, $\beta$, se dice que son* **lógicamente equivalentes** *si bajo cualquier interpretación $I$ se tiene que $I(\alpha) = I(\beta)$.*

Para determinar la equivalencia lógica de dos fórmulas podemos usar los dos métodos que hemos descrito en la sección anterior. Podemos también utilizar el siguiente resultado:

Sean $\alpha$ y $\beta$ dos fbfs. Son equivalentes:

1. $\alpha$ y $\beta$ son lógicamente equivalentes:
2. $\alpha \leftrightarrow \beta$ es una tautología.
3. $\alpha \leftrightarrow \neg\beta$ es una contradicción.
4. $\alpha \rightarrow \beta$ y $\beta \rightarrow \alpha$ son tautologías.

**Observación:** Si $\alpha$ es una fórmula, $\beta_1$ es una subfórmula de $\alpha$ y $\beta_2$ es una fórmula lógicamente a $\beta_1$, entonces la fórmula que resulta de sustituir en $\alpha$ una aparición de $\beta_1$ por $\beta_2$ es lógicamente equivalente a $\alpha$.

Enumeramos a continuación una serie de equivalencias lógicas que es conveniente memorizar.

$\alpha \equiv \neg\neg\alpha$
$\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta$
$\alpha \leftrightarrow \beta \equiv (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$
$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$
$\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$
$\alpha \vee (\beta \vee \gamma) \equiv (\alpha \vee \beta) \vee \gamma$
$\alpha \wedge (\beta \wedge \gamma) \equiv (\alpha \wedge \beta) \wedge \gamma$
$\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \wedge \gamma)$
$\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$

Cuadro 5.3: Equivalencias

**Pregunta:** ¿Pueden ser lógicamente equivalentes dos fórmulas en las que aparezcan conjuntos distintos de proposiciones atómicas?

## 5.4. Consecuencia lógica

Dado un conjunto de fórmulas $\Gamma$, y una fórmula $\alpha$, decimos que $\alpha$ es consecuencia lógica de $\Gamma$ si para cualquier interpretación que haga ciertas simultáneamente todas las proposiciones de $\Gamma$ se tiene que la fórmula $\alpha$ es también cierta.

En tal caso, escribiremos:

$$\Gamma \models \alpha$$

y leeremos

$$\alpha \text{ es consecuencia lógica de } \Gamma$$

o también

$$\Gamma \text{ implica semánticamente } \alpha.$$

A las fórmulas del conjunto $\Gamma$ se les llama **premisas** mientras que $\alpha$ se llama **conclusión**. La expresión $\Gamma \models \alpha$ corresponde un razonamiento lógicamente correcto.

**Observación:**
Si $\Gamma = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ y $\Gamma \models \alpha$, escribiremos
$\gamma_1, \gamma_2, \cdots, \gamma_n \models \alpha$.

Para ver si $\gamma_1, \gamma_2, \cdots, \gamma_n \models \alpha$ tenemos que comprobar que ocurre **sólo** en las interpretaciones en que las premisas sean ciertas. Si para esas interpretaciones la conclusión ($\alpha$) es también cierta, entonces la implicación semántica será cierta.

Cuando el conjunto $\Gamma$ sea vacío, la expresión $\Gamma \models \alpha$ significa que $\alpha$ es una tautología. En tal caso, escribiremos $\models \alpha$.

**Teorema 5.4.1.** . *Sea $\Gamma$ un conjunto de fórmulas y $\alpha$ otra fórmula. Son equivalentes:*

1. $\Gamma \models \alpha$
2. $\Gamma \cup \{\neg\alpha\}$ *es insatisfacible.*
3. *Para cualquier interpretación $I$, se tiene que* $[\prod_{\gamma\in\Gamma} I(\gamma)](1 + I(\alpha)) = 0$

*Demostración:* La equivalencia entre 1 y 2 puede verse como sigue:

Supongamos que $\Gamma \models \alpha$. Vamos a comprobar que no hay ninguna interpretación que haga simultáneamente ciertas a las fórmulas $\gamma_1, \gamma_2, \cdots, \gamma_n, \neg\alpha$.

De existir esa interpretación, tendríamos que $I(\gamma_1) = I(\gamma_2) = \cdots I(\gamma_n) = 1$, y por ser $\alpha$ consecuencia lógica de $\Gamma$ tendríamos que $I(\alpha) = 1$, luego $I(\neg\alpha) = 0$. Luego no pueden ser ciertas simultáneamente las fórmulas de $\Gamma \cup \neg\{\alpha\}$.

Si ahora tenemos que $\Gamma \cup \{\neg\alpha\}$ es insatisfacible e $I$ es una interpretación que hace ciertas todas las premisas, entonces no puede hacer cierta a $\neg\alpha$, luego $I(\neg\alpha) = 0$ y por tanto $I(\alpha) = 1$.

La equivalencia entre 2 y 3 es inmediata a partir de la proposicion 5.2.1. ■

**Ejemplo 5.4.1.** *Probaremos que* $\{p \vee q \to r, \neg r\} \models \neg q$

**Método 1: Tablas de verdad**

*Necesitamos construir la tabla de verdad de todas las fórmulas que aparecen*

| | $p$ | $q$ | $r$ | $p \vee q$ | $p \vee q \to r$ | $\neg r$ | $\neg q$ |
|---|---|---|---|---|---|---|---|
| $I_1$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| $I_2$ | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| $I_3$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| $I_4$ | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| $I_5$ | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| $I_6$ | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| $I_7$ | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| $I_8$ | 1 | 1 | 1 | 1 | 1 | 0 | 0 |

*Ahora sobre la tabla de verdad debemos fijarnos en las filas en las que el valor de TODAS las fórmulas del conjunto inicial $\{p \vee q \to r, \neg r\}$ sea 1 SIMULTÁNEAMENTE: en este caso sólo $I_1$, es decir la primera línea de la tabla de verdad.*

*Para esta interpretación, el valor de verdad de la fórmula $\neg q$ es también 1. Por tanto, la implicación es cierta.*

*Notemos que lo que ocurre en el resto de las filas no nos dice nada acerca de si la implicación es o no cierta.*

*Si construimos la tabla de verdad de las fórmulas del conjunto $\{p \vee q \to r,\ \neg r, \neg\neg q \equiv q\}$ nos resulta:*

| | $p$ | $q$ | $r$ | $p \vee q$ | $p \vee q \rightarrow r$ | $\neg r$ | $q$ |
|---|---|---|---|---|---|---|---|
| $I_1$ | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| $I_2$ | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| $I_3$ | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| $I_4$ | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| $I_5$ | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| $I_6$ | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| $I_7$ | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| $I_8$ | 1 | 1 | 1 | 1 | 1 | 0 | 1 |

*y vemos como el conjunto* $\{p \vee q \rightarrow r,\ \neg r, \neg\neg q \equiv q\}$ *es insatisfacible.*

**Método 2: Ecuaciones en** $\mathbb{Z}_2$ *En este caso el proceso consiste en la manipulación de varias ecuaciones en* $\mathbb{Z}_2$

*Si* $I$ *es una interpretación bajo la cual*

$$\left.\begin{array}{l} I(p \vee q \rightarrow r) = 1 \\ I(\neg r) = 1 \end{array}\right\}$$

*desarrollando ambas ecuaciones*

$$\left.\begin{array}{l} 1 + I(p \vee q) + I(p \vee q)I(r) = 1 \\ 1 + I(r) = 1 \end{array}\right\} \qquad \left.\begin{array}{l} I(p \vee q) + I(p \vee q)I(r) = 0 \\ I(r) = 0 \end{array}\right\}$$

*sustituyendo el valor* $I(r)$ *en la primera ecuación*

$$\left.\begin{array}{l} I(p \vee q) = 0 \\ I(r) = 0 \end{array}\right\}$$

*y de aquí se obtiene que* $I$ *es:*

$$\left.\begin{array}{l} I(p) = I(q) = 0 \\ I(r) = 0 \end{array}\right\}$$

*y bajo ella* $I(\neg q) = 1$

En este proceso hemos partido de las ecuaciones que resultan de imponer que las premisas son ciertas, y hemos operado hasta obtener como resultado que $I(\neg q) = 1$, es decir, que entonces también lo es la conclusión).

**Nota:** Si $\Gamma$ es un conjunto insatisfacible, y $\alpha$ es una fórmula cualquiera, entonces el conjunto $\Gamma \cup \{\neg\alpha\}$ es insatisfacible, luego $\Gamma \models \alpha$. Es decir, *a partir de algo falso se puede deducir cualquier cosa.*

**PASATIEMPO:**
Se conocen los siguientes hechos sobre cuatro personas A, H, C, O:

1. Si A quiere ver una película, entonces H también quiere verla.
2. C y O no ven una película juntos.
3. Respecto de H y C, o bien ven la película juntos o bien ninguno de los dos la ve.
4. Si A decide no ir a ver la película, entonces H y C querrán verla.

¿Quiénes estarán viendo la película?

**SOLUCIÓN:**
Llamaremos:
a = A está viendo la película h = H está viendo la película c = C está viendo la película o = O está viendo la película
Traducimos los hechos que se suponen ciertos a la lógica proposicional:

1. $a \to h$
2. $c \to \neg o$
3. $(h \wedge c) \vee (\neg h \wedge \neg c)$
4. $\neg a \to h \wedge c$

El problema se traduce en calcular $I(a), I(h), I(c), I(o)$ a partir de las condiciones

1. $I(a \to h) = 1$
2. $I(c \to \neg o) = 1$
3. $I((h \wedge c) \vee (\neg h \wedge \neg c)) = 1$
4. $I(\neg a \to h \wedge c) = 1$.

## 5.5. Teorema de La Deducción

Una de las herramientas más útiles en los problemas de consecuencia lógica es el siguiente resultado, conocido como Teorema de la Deducción, y que reencontraremos en la segunda parte de la asignatura.

**Teorema 5.5.1.** *de la DeducciónDado un conjunto de fórmulas $\Gamma$, y dos fórmulas más $\alpha$, $\beta$, las siguientes afirmaciones son equivalentes:*

1. $\Gamma \models \alpha \to \beta$
2. $\Gamma \cup \{\alpha\} \models \beta$

*Demostración:* Usando el resultado que ya conocemos la primera afirmación se traduce en que

$$[\prod_{\gamma \in \Gamma} I(\gamma)](1 + I(\alpha \to \beta)) = 0$$

si desarrollamos el segundo paréntesis

$$(1 + I(\alpha \to \beta) = 1 + 1 + I(\alpha) + I(\alpha)I(\beta) = I(\alpha)(1 + I(\beta))$$

con lo que queda

$$[\prod_{\gamma \in \Gamma} I(\gamma)]I(\alpha)(1 + I(\beta)) = 0$$

que también se puede escribir agrupando el producto de los términos en $\Gamma$ con $\alpha$

$$[\prod_{\gamma\in\Gamma\cup\{\alpha\}} I(\gamma)](1+I(\beta))=0$$

que es la traducción a interpretaciones de la segunda afirmación.

■

**Ejercicio:** Usando el Teorema de la Deducción prueba que las siguientes proposiciones son tautologías:

1. $\alpha\to(\beta\to\alpha)$ (Ley de afortiori)
2. $(\alpha\to(\beta\to\gamma))\to((\alpha\to\beta)\to(\alpha\to\gamma))$ (autodistributiva de la implicación)
3. $(\neg\alpha\to\neg\beta)\to((\neg\alpha\to\beta)\to\alpha)$ (ley clásica de reducción al absurdo)

**Ejercicio del examen de Septiembre de 2005:**
Prueba:

$$\models\big(\big(((\varphi\to\psi)\to(\neg\chi\to\neg\theta))\to\chi\big)\to\tau\big)\to\big((\tau\to\varphi)\to(\theta\to\varphi)\big)$$

**Una solución:**

En primer lugar transformamos el problema en uno más sencillo usando 3 veces el Teorema de la Deducción:

$$\{\big(((\varphi\to\psi)\to(\neg\chi\to\neg\theta))\to\chi\big)\to\tau,\tau\to\varphi,\theta\}\models\varphi$$

Usaremos la caracterización de consecuencia lógica y el cálculo de interpretaciones en la siguiente forma: si $I$ es una interpretación para la que $I(\varphi)=0$ pero $I(\theta)=1$ y $I(\tau\to\varphi)$=1 entonces probaremos que

$$I(\big(((\varphi\to\psi)\to(\neg\chi\to\neg\theta))\to\chi\big)\to\tau)=0$$

Para simplificar la notación llamaremos

$$\delta=(\varphi\to\psi)\to(\neg\chi\to\neg\theta)$$

$$\alpha=\delta\to\chi$$

Nuestras ecuaciones de partida son:

$$\begin{cases} I(\varphi)=0\\ I(\tau\to\varphi)=1\\ I(\theta)=1\end{cases}$$

usando la primera y la segunda transformamos el sistema en

$$\begin{cases} I(\varphi)=0\\ I(\tau)=0\\ I(\theta)=1\end{cases}$$

y ahora vamos a calcular

$$I(\neg\chi\to\neg\theta)=1+I(\neg\chi)+I(\neg\chi)I(\neg\theta)$$

como $I(\theta)=1$ entonces $I(\neg\theta)=0$ y se tiene

$$I(\neg\chi\to\neg\theta)=I(\chi)$$

y como $I(\phi)=0$ entonces

$$I(\varphi\to\psi)=1+I(\varphi)+I(\varphi)I(\psi)=1+0+0=1$$

que podemos sustituir en

$$I(\delta) = 1 + 1 + I(\chi) = I(\chi)$$

Por último calculamos

$$I(\alpha) = 1 + I(\delta) + I(\delta)I(\chi) = 1 + I(\chi) + I(\chi)^2 = 1$$

Usando este resultado y que $I(\tau) = 0$ nos queda que la primera premisa bajo esta interpretación es necesariamente falsa, es decir,

$$I(\alpha \to \tau) = 0.$$

Un intento de resolver este ejercicio usando tablas de verdad es tedioso (como son 5 proposiciones básicas la tabla de verdad tiene $2^5 = 32$ filas y hay también demasiadas subfórmulas que evaluar) así que por su extensión tiene una alta probabilidad de error.

**Algunas equivalencias referentes al problema de la implicación semántica:**
Hemos visto el teorema de la deducción, que nos dice que los siguientes enunciados son equivalentes:

- $\Gamma \models \alpha \to \beta$.
- $\Gamma \cup \alpha \models \beta$.

Con una forma similar a este teorema, podemos también recoger los siguientes resultados:

1. Son equivalentes:
   a) $\Gamma \models \alpha \to \beta$.
   b) $\Gamma \cup \{\neg\beta\} \models \neg\alpha$.
   c) $\Gamma \cup \{\alpha, \neg\beta\}$ es insatisfacible.
2. Son equivalentes:
   a) $\Gamma \models \alpha \vee \beta$.
   b) $\Gamma \cup \{\neg\alpha\} \models \beta$.
   c) $\Gamma \cup \{\neg\beta\} \models \alpha$.
   d) $\Gamma \cup \{\neg\alpha, \neg\beta\}$ es insatisfacible.
3. Son equivalentes:
   a) $\Gamma \models \alpha \wedge \beta$.
   b) $\Gamma \models \alpha$ y $\Gamma \models \beta$.
   c) $\Gamma \cup \{\neg\alpha\}$ y $\Gamma \cup \{\neg\beta\}$ son insatisfacibles.
4. Son equivalentes:
   a) $\Gamma \models \alpha \leftrightarrow \beta$.
   b) $\Gamma \models \alpha \to \beta$ y $\Gamma \models \beta \to \alpha$.
   c) $\Gamma \cup \{\alpha\} \models \beta$ y $\Gamma \cup \{\beta\} \models \alpha$.
   d) $\Gamma \cup \{\alpha, \neg\beta\}$ y $\Gamma \cup \{\neg\alpha, \beta\}$ son insatisfacibles.

## 5.6. Forma clausular de una fórmula.

### 5.6.1. Definición de cláusula.

Dado un lenguaje proposicional, un **literal** es una proposición atómica o su negada. Por ejemplo, son literales $a$, $\neg c$, $b$. No es un literal $\neg\neg b$ (aunque sea lógicamente equivalente a $b$, que sí es un literal).

Si $\lambda$ es un literal, denotaremos como $\lambda^c$ al literal que es o bien el negado de $\lambda$ o lógicamente equivalente con él. Así, si $\lambda = a$ entonces $\lambda^c = \neg a$, mientras que si $\lambda = \neg a$, entonces $\lambda^c = a$ (que es equivalente a $\neg\neg a$).

Una **cláusula** es una **disyunción de literales**, de forma que no haya dos literales que provengan de la misma proposición atómica. Es decir, si aparece el literal $\lambda$, éste sólo lo puede hacer una vez, y no puede estar el literal $\lambda^c$.

**Observación:** Dada una proposición atómica $a$, la disyunción $a \vee \neg a$ es una tautología, por tanto lo será cualquier fórmula de la forma $a \vee \neg a \vee \beta$ donde $\beta$ representa a cualquier fórmula bien formada.

◇ Todo literal es una cláusula.

◇ También se considera como cláusula a la "disyunción de cero literales". Dicha cláusula se denomina como cláusula vacía, la denotamos por $\square$.

◇ Son ejemplos de cláusulas: $a$, $\neg b \vee c$, $a \vee \neg b \vee \neg c$, $\neg b \vee a \vee c$.

◇ No son cláusulas: $a \vee a$, $a \vee b \vee \neg a$, $a \wedge b$.

### 5.6.2. Forma clausular de una fórmula.

Una fórmula se dice que está en **forma clausular** si es una cláusula o está expresada como **conjunción de cláusulas**.

Son fórmulas en forma clausular las siguientes:

$$(a \vee \neg b) \wedge (b \vee c)$$

$$b \vee c$$

$$a \wedge b$$

$$b \wedge \neg b$$

$$(b \vee a \vee \neg c) \wedge (b \vee \neg a \vee \neg c)$$

La primera fórmula es la conjunción de dos cláusulas: $a \vee \neg b$ y $b \vee c$.
La segunda es una cláusula.
La tercera es conjunción de las cláusulas $a$ y $b$.
La cuarta, conjunción de las cláusulas $b$ y $\neg b$.
La quinta es conjunción de las cláusulas $b \vee a \vee \neg c$ y $b \vee \neg a \vee \neg c$.

No están en forma clausular las siguientes fórmulas:

$$\neg(a \wedge b)$$

$$(a \wedge \neg b) \vee (\neg a \vee c)$$

**Teorema 5.6.1.** *Toda fórmula (que no sea tautología) puede transformarse en una fórmula lógicamente equivalente con ella que esté en forma clausular.*

Así, la fórmula $\neg(a \wedge b)$ es equivalente a $\neg a \vee \neg b$ que está en forma clausular, mientras que la fórmula $(a \wedge \neg b) \vee (\neg a \vee c)$ podemos transformarla en

$$(a \vee \neg a \vee c) \wedge (\neg b \vee \neg a \vee c)$$

Ahora observamos que el primer paréntesis corresponde a una tautología y por tanto puede eliminarse ese factor de la conjunción y se obtiene una fórmula equivalente, en este caso:

$$\neg b \vee \neg a \vee c$$

que está en forma clausular.

### 5.6.3. Un método para calcular la forma clausular.

A continuación veremos qué pasos podemos dar para transformar una fórmula en otra equivalente a ella que esté en forma clausular:

1. Si tenemos una subfórmula de la forma $\alpha \leftrightarrow \beta$, la sustituimos por $(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$.
2. Si tenemos una subfórmula de la forma $\alpha \rightarrow \beta$ la sustituimos por $\neg\alpha \vee \beta$.
3. Cualquier subfórmula de la forma $\neg\neg\alpha$ la sustituimos por $\alpha$.
4. Introducimos la conectiva $\neg$ dentro de los paréntesis utilizando las equivalencias lógicas:

$$\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$$

$$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$$

.

Si al hacer esto nos apareciera una nueva subfórmula de la forma $\neg\neg\alpha$, la sustituimos por $\alpha$.

Una vez ejecutados estos pasos, nos encontramos con una fórmula en la que sólo intervienen las conectivas $\vee$, $\wedge$ y $\neg$. Además, ésta última únicamente actúa sobre proposiciones atómicas. Ahora puede ser necesario el uso de la distributividad de las conectivas $\vee$ y $\wedge$, es decir el uso de las siguientes equivalencias lógicas:

1. $(a \wedge b) \vee c \equiv (a \vee c) \wedge (b \vee c)$
2. $a \vee (b \wedge c) \equiv (a \vee b) \wedge (a \vee c)$

Pensemos que el objetivo para encontrar la forma clausular es encontrar una fórmula en donde dentro de los paréntesis no puede haber ninguna conectiva $\wedge$. Se trata entonces de que, siempre que encontremos una subfórmula de la forma $(\alpha) \vee (\beta)$, proceder como sigue según los casos:

- Si $\alpha$ es de la forma $\alpha_1 \wedge \alpha_2$ (daría igual si fuera conjunción de tres o más fórmulas), entonces

$$\alpha \vee \beta \ \equiv \ (\alpha_1 \vee \beta) \wedge (\alpha_2 \vee \beta)$$

y ahora estudiaríamos por separado las fórmulas $\alpha_1 \vee \beta$ y $\alpha_2 \vee \beta$.

- Si $\beta$ es de la forma $\beta_1 \wedge \beta_2$, sustituimos $\alpha \vee \beta$ por

$$\alpha \vee \beta \ = \alpha \vee (\beta_1 \wedge \beta_2) \ \equiv \ (\alpha \vee \beta_1) \wedge (\alpha \vee \beta_2)$$

y estudiaríamos ahora las fórmulas $\alpha \vee \beta_1$ y $\alpha \vee \beta_2$.

Por ejemplo, si tenemos una fórmula de la forma $\delta = \alpha \vee \beta$, con $\alpha = \alpha_1 \wedge \alpha_2 \wedge \alpha_3$ y $\beta = \beta_1 \wedge \beta_2$, entonces aplicando varias veces las reglas anteriores tendríamos:

$$\delta \equiv (\alpha_1 \vee \beta_1) \wedge (\alpha_2 \vee \beta_1) \wedge (\alpha_3 \vee \beta_1) \wedge (\alpha_1 \vee \beta_2) \wedge (\alpha_2 \vee \beta_2) \wedge (\alpha_3 \vee \beta_2)$$

Para actuar de manera ordenada es conveniente, bien empezar por las subfórmulas más pequeñas, e ir yendo progresivamente hacia subfórmulas más grandes, bien empezar por las subfórmulas más grandes y seguir el camino inverso al anterior. Veamos aquí un ejemplo, empezando por las subfórmulas pequeñas.

**Ejemplo 5.6.1.** *Queremos hallar la forma clausular de*

$$\big[\big(a \vee ((b \wedge c) \vee (d \wedge \neg e))\big) \wedge (\neg b \vee c)\big] \vee \big[(a \wedge \neg c) \wedge (c \vee \neg b \vee d)\big]$$

*Notemos que no tenemos ninguna conectiva $\rightarrow$, ninguna conectiva $\leftrightarrow$, y las conectivas $\neg$ actúa únicamente sobre fórmulas atómicas. Entonces, hemos de aplicar sólo la propiedad distributiva.*

*Buscamos las subfórmulas más pequeñas donde nos encontremos la conectiva $\wedge$ dentro de un paréntesis, y vemos que esto ocurre en $(b \wedge c)$, $(d \wedge \neg e)$ y $(a \wedge \neg c)$, si bien, este último podría eliminarse por la propiedad asociativa de la conectiva $\wedge$.*

*Sustituimos entonces $(b \wedge c) \vee (d \wedge \neg e)$ por*

$$(b \vee d) \wedge (b \vee \neg e) \wedge (c \vee d) \wedge (c \vee \neg e)$$

*y nos queda*

$$\big[\big(a \vee ((b \vee d) \wedge (b \vee \neg e) \wedge (c \vee d) \wedge (c \vee \neg e))\big) \wedge (\neg b \vee c)\big] \vee \big[a \wedge \neg c \wedge (c \vee \neg b \vee d)\big]$$

*La siguiente sufórmula donde encontramos la conectiva $\wedge$ dentro de paréntesis es*

$$\beta = (b \vee d) \wedge (b \vee \neg e) \wedge (c \vee d) \wedge (c \vee \neg e)$$

*Sustituimos entonces $a \vee \beta$ por $(a \vee \beta_1) \wedge (a \vee \beta_2) \wedge (a \vee \beta_3) \wedge (a \vee \beta_4)$ y nos queda*

$$\big[\big((a \vee b \vee d) \wedge (a \vee b \vee \neg e) \wedge (a \vee c \vee d) \wedge (a \vee c \vee \neg e)\big) \wedge (\neg b \vee c)\big] \vee \big[a \wedge \neg c \wedge (c \vee \neg b \vee d)\big]$$

*que por la asociatividad de $\wedge$ podemos cambiar por*

$$\big((a \vee b \vee d) \wedge (a \vee b \vee \neg e) \wedge (a \vee c \vee d) \wedge (a \vee c \vee \neg e) \wedge (\neg b \vee c)\big) \vee \big(a \wedge \neg c \wedge (c \vee \neg b \vee d)\big)$$

*Y nos encontramos ahora con una fórmula que responde a la forma*

$$\alpha \vee \beta = (\alpha_1 \wedge \alpha_2 \wedge \alpha_3 \wedge \alpha_4 \wedge \alpha_5) \vee (\beta_1 \wedge \beta_2 \wedge \beta_3)$$

*luego la fórmula de partida es equivalente a:*

$$(a \vee b \vee d \vee a) \wedge (a \vee b \vee \neg e \vee a) \wedge (a \vee c \vee d \vee a) \wedge (a \vee c \vee \neg e \vee a) \wedge (\neg b \vee c \vee a) \wedge$$
$$\wedge (a \vee b \vee d \vee \neg c) \wedge (a \vee b \vee \neg e \vee \neg c) \wedge (a \vee c \vee d \vee \neg c) \wedge (a \vee c \vee \neg e \vee \neg c) \wedge (\neg b \vee c \vee \neg c) \wedge$$
$$\wedge (a \vee b \vee d \vee c \vee \neg b \vee d) \wedge (a \vee b \vee \neg e \vee c \vee \neg b \vee d) \wedge (a \vee c \vee d \vee c \vee \neg b \vee d) \wedge$$
$$\wedge (a \vee c \vee \neg e \vee c \vee \neg b \vee d) \wedge (\neg b \vee c \vee c \vee \neg b \vee d)$$

*Y finalmente, para obtener la forma clausular, eliminamos aquellos términos en los que aparezca $\lambda \vee \lambda^c$, puesto que son tautologías, y los literales repetidos haciendo uso de la equivalencia $a \vee a \equiv a$:*

$$(a \vee b \vee d) \wedge (a \vee b \vee \neg e) \wedge (a \vee c \vee d) \wedge (a \vee c \vee \neg e) \wedge (a \vee \neg b \vee c) \wedge (a \vee b \vee \neg c \vee d) \wedge$$
$$\wedge (a \vee b \vee \neg c \vee \neg e) \wedge (a \vee \neg b \vee c \vee d) \wedge (a \vee \neg b \vee c \vee d \vee \neg e) \wedge (\neg b \vee c \vee d)$$

**¡Esta ya es una forma clausular!** *Ahora bien,* **podemos reducirla** *observando la siguiente equivalencia lógica:*

$$(\alpha \vee \beta) \wedge \alpha \equiv \alpha$$

*por lo que*

$$(a \vee \neg b \vee c) \wedge (a \vee \neg b \vee c \vee d) \wedge (a \vee \neg b \vee c \vee d \vee \neg e) \equiv a \vee \neg b \vee c$$

*y también*

$$(a \vee b \vee d) \wedge (a \vee b \vee \neg c \vee d) \equiv a \vee b \vee d$$

*y por tanto, otra forma clausular es:*

$$(a \vee b \vee d) \wedge (a \vee b \vee \neg e) \wedge (a \vee c \vee d) \wedge (a \vee c \vee \neg e) \wedge (a \vee \neg b \vee c) \wedge$$

$$\wedge (a \vee b \vee \neg c \vee \neg e) \wedge (\neg b \vee c \vee d)$$

El seguimiento de las etapas aquí descritas nos asegura la consecución de la forma clausular de una fórmula. **No es sin embargo la única opción para obtener la forma clausular de una fórmula**. **La práctica** nos indicará cual es el mejor camino para obtener la forma clausular.

Veamos a continuación otros ejemplos completos de cómo obtener la forma clausular de una fórmula.

**Ejemplo 5.6.2.** *Partimos de la fórmula*

$$((a \vee \neg b) \rightarrow (\neg c \rightarrow b)) \wedge ((a \rightarrow b) \leftrightarrow c)$$

*El primer paso consiste en sustituir la conectiva $\leftrightarrow$. Nos queda entonces:*

$$\big((a \vee \neg b) \rightarrow (\neg c \rightarrow b)\big) \wedge \big[\big((a \rightarrow b) \rightarrow c\big) \wedge \big(c \rightarrow (a \rightarrow b)\big)\big]$$

*El siguiente paso consiste en sustituir las conectivas $\rightarrow$. El orden en que se haga esto no es importante. Una forma de hacerlo podría ser:*

$$\big(\neg(a \vee \neg b) \vee (\neg c \rightarrow b)\big) \wedge \big[\big((\neg a \vee b) \rightarrow c\big) \wedge \big(c \rightarrow (\neg a \vee b)\big)\big]$$

$$\big(\neg(a \vee \neg b) \vee (\neg\neg c \vee b)\big) \wedge \big[\big(\neg(\neg a \vee b) \vee c\big) \wedge \big(\neg c \vee (\neg a \vee b)\big)\big]$$

*Eliminamos la doble negación*

$$\big(\neg(a \vee \neg b) \vee (c \vee b)\big) \wedge \big[\big(\neg(\neg a \vee b) \vee c\big) \wedge \big(\neg c \vee (\neg a \vee b)\big)\big]$$

*Introducimos las conectivas $\neg$ en los paréntesis.*

$$\big((\neg a \wedge \neg\neg b) \vee (c \vee b)\big) \wedge \big[\big((\neg\neg a \wedge \neg b) \vee c\big) \wedge \big(\neg c \vee (\neg a \vee b)\big)\big]$$

*Y volvemos a eliminar la doble negación que ha aparecido:*

$$\big((\neg a \wedge b) \vee (c \vee b)\big) \wedge \big[\big((a \wedge \neg b) \vee c\big) \wedge \big(\neg c \vee (\neg a \vee b)\big)\big]$$

*Como podemos ver, únicamente tenemos las conectivas $\vee$, $\wedge$ y $\neg$, y la conectiva $\neg$ afecta únicamente a proposiciones atómicas.*

*Nuestra fórmula es ahora conjunción de tres subfórmulas:*
$(\neg a \wedge b) \vee (c \vee b)$, $(a \wedge \neg b) \vee c$ *y* $\neg c \vee (\neg a \vee b)$
*Hallamos la forma clausular de cada una de estas subfórmulas:*

$$(\neg a \wedge b) \vee c \vee b \equiv (\neg a \vee b \vee c) \wedge (b \vee c \vee b) \equiv (\neg a \vee b \vee c) \wedge (b \vee c)$$

$$(a \wedge \neg b) \vee c \equiv (a \vee c) \wedge (\neg b \vee c)$$

$$\neg c \vee (\neg a \vee b) \equiv \neg a \vee b \vee \neg c$$

*Por tanto, una forma clausular de la fórmula de partida es:*

$$(\neg a \vee b \vee c) \wedge (b \vee c) \wedge (a \vee c) \wedge (\neg b \vee c) \wedge (\neg a \vee b \vee \neg c)$$

*Aunque también podemos simplificarla utilizando la siguiente equivalencia lógica:*

$$(\alpha \vee \beta) \wedge (\alpha \vee \neg\beta) \equiv \alpha$$

*aplicada a*

$$(\neg a \vee b \vee c) \wedge (\neg a \vee b \vee \neg c) \equiv \neg a \vee b$$

*y nos quedará:*

$$(\neg a \vee b) \wedge (b \vee c) \wedge (a \vee c) \wedge (\neg b \vee c)$$

**Ejemplo 5.6.3.** *Vamos a calcular la forma clausular de:*

$$\alpha = \big[\big((a \to b) \wedge \neg c\big) \to \big(\neg b \leftrightarrow (c \vee a)\big)\big] \vee \big[d \vee \big(\neg c \to (a \wedge b)\big)\big]$$

*En este caso vamos a seguir un orden diferente al del ejemplo anterior.*
*La fórmula dada es equivalente a*

$$\big[\neg\big((a \to b) \wedge \neg c\big) \vee \big(\neg b \leftrightarrow (c \vee a)\big)\big] \vee \big[d \vee \big(\neg c \to (a \wedge b)\big)\big]$$

*que está expresada como disyunción de tres fórmulas:*

$$\neg\big((a \to b) \wedge \neg c\big) \qquad \neg b \leftrightarrow (c \vee a) \qquad d \vee \big(\neg c \to (a \wedge b)\big)$$

*Calculamos la forma clausular de cada una de estas fórmulas por separado.*

| | | |
|---|---|---|
| $\neg\big((a \to b) \wedge \neg c\big)$ | $\neg b \leftrightarrow (c \vee a)$ | $d \vee \big(\neg c \to (a \wedge b)\big)$ |
| $\neg\big((\neg a \vee b) \wedge \neg c\big)$ | $\big(\neg b \to (c \vee a)\big) \wedge \big((c \vee a) \to \neg b\big)$ | $d \vee \big(\neg\neg c \vee (a \wedge b)\big)$ |
| $\neg(\neg a \vee b) \vee \neg\neg c$ | $\big(\neg\neg b \vee (c \vee a)\big) \wedge \big(\neg(c \vee a) \vee \neg b\big)$ | $d \vee \big(c \vee (a \wedge b)\big)$ |
| $(\neg\neg a \wedge \neg b) \vee \neg\neg c$ | $\big(b \vee (c \vee a)\big) \wedge \big((\neg c \wedge \neg a) \vee \neg b\big)$ | $d \vee \big((c \vee a) \wedge (c \vee b)\big)$ |
| $(a \wedge \neg b) \vee c$ | $(a \vee b \vee c) \wedge \big((\neg c \vee \neg b) \wedge (\neg a \vee \neg b)\big)$ | $(d \vee c \vee a) \wedge (d \vee c \vee b)$ |
| $(a \vee c) \wedge (\neg b \vee c)$ | $(a \vee b \vee c) \wedge (\neg a \vee \neg b) \wedge (\neg b \vee \neg c)$ | $(a \vee c \vee d) \wedge (b \vee c \vee d)$ |

*Es decir, hemos llegado a que la fórmula inicial es equivalente a una de la forma*

$$(C_1 \wedge C_2) \vee (C_1' \wedge C_2' \wedge C_3') \vee (C_1'' \wedge C_2'')$$

*que es equivalente a*

$$(C_1 \vee C_1' \vee C_1'') \wedge (C_1 \vee C_1' \vee C_2'') \wedge (C_1 \vee C_2' \vee C_1'') \wedge (C_1 \vee C_2' \vee C_2'') \wedge$$

$$\wedge (C_1 \vee C_3' \vee C_1'') \wedge (C_1 \vee C_3' \vee C_2'') \wedge$$

$$\wedge (C_2 \vee C_1' \vee C_1'') \wedge (C_2 \vee C_1' \vee C_2'') \wedge (C_2 \vee C_2' \vee C_1'') \wedge (C_2 \vee C_2' \vee C_2'') \wedge$$

$$\wedge (C_2 \vee C_3' \vee C_1'') \wedge (C_2 \vee C_3' \vee C_2'')$$

*Y ahora $C_1 \vee C_1' \vee C_1' = (a \vee c) \vee (a \vee b \vee c) \vee (a \vee c \vee d) \equiv a \vee b \vee c \vee d$, también $C_1 \vee C_1' \vee C_2'' = a \vee b \vee c \vee d$ mientras que el resto se pueden eliminar puesto que contienen al mismo tiempo un literal y su negación.*
*Y así, podemos concluir que la fórmula $\alpha$ es equivalente a*

$$a \vee b \vee c \vee d$$

## 5.7. El problema de la implicación semántica

Hemos definido en secciones precedentes lo que significa

$$\Gamma \models \alpha$$

que viene a decirnos cuando un razonamiento es correcto desde el punto de vista lógico. Vamos a desarrollar técnicas que nos permitan dar respuesta a este problema dentro de la lógica proposicional.

Ya conocemos una forma de resolver el problema. Hallamos las tablas de verdad de las fórmulas de $\Gamma$ y de $\alpha$, y si en todas las interpretaciones en las que las fórmulas de $\Gamma$ sean ciertas también lo es $\alpha$, la implicación es cierta.

Sin embargo, en lo que sigue vamos a basarnos en el teorema 5.4.1, que entre otras cosas decía que la respuesta a los problemas

$$\Gamma \models \alpha \qquad \text{y} \qquad \Gamma \cup \{\neg\alpha\}$$

es siempre la misma.

Es decir, el problema de implicación semántica podemos transformarlo en un problema de decidir si un conjunto de fórmulas es insatisfacible o no.

De momento, vamos a aparcar el tema de la implicación semática, y vamos a fijarnos únicamente en la insatisfacibilidad de un conjunto de fórmulas.

En la sección anterior aprendimos a calcular, dada una fórmula, otra fórmula lógicamente equivalente a ella y que está en forma clausular.

Entonces, a la hora de determinar si un conjunto de cláusulas es insatisfacible o no, podemos sustituir cada fórmula por otra que esté en forma clausular.

**Teorema 5.7.1.** *Sea $\Omega$ un conjunto de fórmulas; $\Omega'$ un conjunto de fórmulas que se obtiene sustituyendo cada fórmula por una forma clausular de esa fórmula, y $\Omega''$ el conjunto que resulta de sustituir cada fórmula de $\Omega'$ por las cláusulas que la forman. Entonces son equivalentes:*

1. *$\Omega$ es insatisfacible,*
2. *$\Omega'$ es insatisfacible.*
3. *$\Omega''$ es insatisfacible.*

Reuniendo ahora los resultados anteriores podemos observar cómo el problema tipo del que partíamos se transforma en el problema de estudiar si un conjunto de cláusulas es insatisfacible o no.

**En resumen: el conjunto del que tenemos que estudiar la satisfacibilidad será el formado por las cláusulas que aparecen para el conjunto de fórmulas $\Gamma \cup \{\neg\alpha\}$.**

## 5.8. Algoritmo de Davis-Putnam:

Vamos entonces a estudiar cuando un conjunto de cláusulas es o no satisfacible. Para esto emplearemos un algoritmo debido a Davis y Putnam.

Antes de describir el algoritmo, denotaremos, dada una claúsula $C$ y un literal $\lambda$ que forme parte de $C$, como $C - \lambda$ a la cláusula que resulta de eliminar el literal $\lambda$ de $C$. Así, si $C = a \vee \neg b \vee d$ entonces $C - a = \neg b \vee d$, mientras que $C - \neg b = a \vee d$. Admitiremos ahora que hay una cláusula que no contiene ningún literal, la **cláusula vacía**, que denotaremos por $\square$ y que para cualquier interpretación verifica que $I(\square) = 0$; de esta forma si $C = b$ entonces $C - b = \square$, la cláusula vacía. Un conjunto en el que aparece la cláusula vacía es siempre insatisfacible.

El algoritmo de Davis-Putnam se basa en tres resultados, los cuales permiten ir reduciendo el conjunto de cláusulas. Estos resultados son:

1. Sea $\Sigma$ un conjunto de cláusulas. Supongamos que tenemos una cláusula con un único literal $\lambda$ (diremos que ésta cláusula es una **cláusula unit**). Sea $\Sigma'$ el conjunto que resulta de suprimir todas las cláusulas que contengan el literal $\lambda$, y sustituir las cláusulas $C$ que contengan a $\lambda^c$ por $C - \lambda^c$.

   Es decir: si

   $$\Sigma = \{\lambda,\ \lambda \vee C_1,\ \lambda \vee C_2,\ \cdots,\lambda \vee C_n,\ \lambda^c \vee C'_1,\ \lambda^c \vee C'_2,\ \cdots,\lambda^c \vee C'_m,$$
   $$C''_1,\ C''_2,\ \cdots,C''_p\}$$

   entonces

   $$\Sigma' = \{C'_1,\ C'_2,\ \cdots,C'_m, C''_1,\ C''_2,\ \cdots,C''_p\}$$

   En tal caso, se verifica que $\Sigma$ es satisfacible si, y sólo si, $\Sigma'$ lo es.

   La justificación de este resultado podría ser como sigue:

   Supongamos en primer lugar que $\lambda = a$ o $\lambda = \neg a$.

   Si $I$ es una interpretación para la que se satisfacen todas las cláusulas de $\Sigma$, entonces $I(\lambda) = 1$, lo que implica que $I(\lambda^c) = 0$. Puesto que $I(\lambda^c \vee C'_i) = 1$ deducimos que $I(C'_i) = 1$. Por tanto, $I$ es una interpretación para la que todas las cláusulas de $\Sigma'$ son ciertas.

   Recíprocamente, si $I$ es una interpretación para la que todas las cláusulas de $\Sigma'$ son ciertas, definimos $I'$ como la interpretación que actúa igual que $I$ sobre todas las proposiciones atómicas salvo sobre $a$, mientras que $I'(a)$ lo definimos de forma que $I'(\lambda) = 1$. Es claro entonces que bajo la interpretación $I'$ todas las cláusulas de $\Sigma$ son ciertas.

2. Supongamos que en el conjunto $\Sigma$ hay una cláusula en la que aparece un literal $\lambda$ de forma que $\lambda^c$ no aparece en ninguna cláusula (en este caso, diremos que el literal $\lambda$ es un **literal puro**). Sea entonces $\Sigma'$ el conjunto de cláusulas que resulta de suprimir todas las cláusulas en las que interviene el literal $\lambda$.

   Es decir, si

   $$\Sigma = \{\lambda \vee C_1,\ \lambda \vee C_2,\ \cdots,\lambda \vee C_n,\ C'_1,\ C'_2,\ \cdots,C'_m\}$$

   tendríamos

   $$\Sigma' = \{C'_1,\ C'_2,\ \cdots,C'_m\}$$

   Entonces $\Sigma$ es satisfacible si, y sólo si, $\Sigma'$ es satisfacible.

   Al igual que antes, suponemos que $\lambda = a$ o $\lambda = \neg a$.

   Claramente, si $I$ es una interpretación que hace ciertas las cláusulas de $\Sigma$ entonces $I$ hace ciertas las cláusulas de $\Sigma'$.

   Recíprocamente, si $I$ hace ciertas las cláusulas de $\Sigma'$, definimos $I'$ como la interpretación que actúa igual que $I$ sobre todas las proposiciones atómicas salvo sobre $a$, mientras que $I'(a)$ lo definimos de forma que $I'(\lambda) = 1$. Es claro entonces que bajo la interpretación $I'$ todas las cláusulas de $\Sigma$ son ciertas.

3. Sea $\Sigma$ un conjunto de cláusulas y $a$ una proposición atómica. Supongamos que $\Sigma$ es de la forma:

   $$\Sigma = \{a \vee C_1,\ a \vee C_2,\ \cdots,a \vee C_n,\ \neg a \vee C'_1,\ \neg a \vee C'_2,\ \cdots,\neg a \vee C'_m,$$
   $$C''_1,\ C''_2,\ \cdots,C''_p\}$$

   Sean

   $$\Sigma_1 = \{C'_1,\ C'_2,\ \cdots,C'_m,\ C''_1,\ C''_2,\ \cdots,C''_p\}$$
   $$\Sigma_2 = \{C_1,\ C_2,\ \cdots,C_n,\ C''_1,\ C''_2,\ \cdots,C''_p\}$$

   Entonces $\Sigma$ es insatisfacible si, y sólo si, $\Sigma_1$ y $\Sigma_2$ son insatisfacibles, o dicho de otra forma, $\Sigma$ es satisfacible si, y sólo si, $\Sigma_1$ o $\Sigma_2$ es satisfacible.

Supongamos que $I$ es una interpretación que hace ciertas todas las cláusulas de $\Sigma$. Entonces:

- Si $I(a) = 1$ entonces $I(\neg a) = 0$, y como $I(\neg a \vee C_i') = 1$ deducimos que $I(C_i') = 1$. Por tanto, todas las cláusulas de $\Sigma_1$ son interpretadas como ciertas por $I$, luego $\Sigma_1$ es satisfacible.
- Si $I(a) = 0$ en este caso, lo que se tiene es que todas las cláusulas de $\Sigma_2$ son ciertas bajo $I$, luego es $\Sigma_2$ quien es satisfacible.

Recíprocamente, si es $\Sigma_1$ quien es satisfacible bajo una interpretación $I$, consideramos la interpretación $I'$ que coincide con $I$ en todas las proposiciones atómicas salvo eventualmente en $a$, sobre la que vale 1. Bajo esta interpretación se tiene que:
- $I'(a \vee C_i) = 1$, pues $I'(a) = 1$.
- $I'(\neg a \vee C_i') = 1$, pues $I'(C_i') = I(C_i') = 1$.
- $I'(C_i'') = 1$, pues $I'(C_i'') = I(C_i'') = 1$.

**Resumen:**

El algoritmo de Davis-Putnam nos dice cuando un conjunto de cláusulas es satisfacible o no. Caso de ser satisfacible, nos da una interpretación que hace ciertas todas las cláusulas.

Consiste en partir de un conjunto de cláusulas, e ir reduciéndolo, hasta llegar a uno del que sepamos con claridad si es o no satisfacible.

Comprobamos si hay alguna cláusula unit. Si la respuesta es afirmativa, y $\lambda$ es dicha cláusula, reducimos el conjunto de cláusulas tal y como hemos visto en 1., anotamos el literal $\lambda$ y volvemos al principio con el nuevo conjunto de cláusulas.

Si la respuesta es negativa, comprobamos si existe un literal puro. De existir, procedemos como hemos dicho en 2., anotamos dicho literal y volvemos al inicio con el nuevo conjunto de cláusulas.

De no existir, elegimos una proposición atómica $a$. Abrimos dos ramas, tal y como hemos visto en 3. y analizamos cada una de las ramas. Al analizar la rama con $\Sigma_1$, anotamos el literal $a$, mientras que al hacerlo con $\Sigma_2$ anotamos el literal $\neg a$.

Después de que el conjunto de cláusulas haya sido modificado, se vuelve a comenzar el algoritmo, y si han aparecido varios conjuntos se aplica sobre cada uno de ellos.

El algoritmo acaba cuando podamos decidir fácilmente que el conjunto es satisfacible (por ejemplo cuando contenga una sola cláusula que no sea la vacía) o insatisfacible (por ejemplo cuando aparezca en él la cláusula vacía).

Si al final llegamos a que alguna rama es satisfacible, entonces una interpretación para la que todas las cláusulas son ciertas es aquella que vale 1 sobre todos los literales que hemos ido anotando.

Notemos que las reglas 1 y 2 son casos particulares de la regla 3.

En el caso de que tengamos una cláusula unit $\lambda$ y aplicamos la regla 3 tomando como proposición atómica la que aparece en $\lambda$ (es decir, $\lambda$ ó $\lambda^c$) entonces uno de los dos conjuntos que nos resultan contiene la cláusula vacía, mientras que el otro es el que obtendríamos aplicando la regla 1.

En el caso de que tengamos un literal puro $\lambda$, es decir, tenemos un conjunto de cláusulas

$$\Sigma = \{\lambda \vee C_1,\ \lambda \vee C_2,\ \cdots,\lambda \vee C_n,\ C_1',\ C_2',\ \cdots,C_m'\}$$

La regla 3 (tomando como proposición atómica la que aparece en el literal $\lambda$) nos diría que $\Sigma$ es satisfacible si, y sólo si, lo es uno de los dos conjuntos siguientes:

$$\Sigma_1 = \{C_1',\ C_2',\ \cdots,C_m'\}$$
$$\Sigma_2 = \{C_1,\ C_2,\ \cdots,\ C_n,\ C_1',\ C_2',\ \cdots,C_m'\}$$

pero como $\Sigma_1 \subseteq \Sigma_2$ entonces si $\Sigma_2$ es satisfacible, también lo es $\Sigma_1$. Por tanto, si uno de los dos conjuntos ($\Sigma_1$ ó $\Sigma_2$) es satisfacible, entonces $\Sigma_1$ lo es.

**Ejemplo 5.8.1.** *Vamos a demostrar que la fórmula*

$$(a \to (b \to c)) \to (\neg(a \to \neg b) \to c)$$

*es una tautología. Esto sabemos que es equivalente a probar:*

$$\models (a \to (b \to c)) \to (\neg(a \to \neg b) \to c)$$

*por el teorema de la deducción esto se traduce en demostrar que*

$$\{a \to (b \to c)\} \models \neg(a \to \neg b) \to c$$

*y aplicando otra vez el teorema de la deducción nos queda el problema*

$$\{a \to (b \to c), \neg(a \to \neg b)\} \models c$$

*Lo que es equivalente a demostrar que el conjunto*

$$\{a \to (b \to c), \neg(a \to \neg b), \neg c\}$$

*es insatisfacible.*

*Hallamos la forma clausular de cada una de las fórmulas anteriores:*

| | | |
|---|---|---|
| $a \to (b \to c)$ | $\neg(a \to \neg b)$ | $\neg c$ |
| $\neg a \vee (b \to c)$ | $\neg(\neg a \vee \neg b)$ | |
| $\neg a \vee (\neg b \vee c)$ | $\neg\neg a \wedge \neg\neg b$ | |
| $\neg a \vee \neg b \vee c$ | $a \wedge b$ | |

*Y entonces lo que nos queda probar es que el siguiente conjunto de cláusulas es insatisfacible:*

$$\{\neg a \vee \neg b \vee c,\ a,\ b,\ \neg c\}$$

*Tenemos una cláusula unit a, por tanto, el conjunto nos queda*

$$\{\neg b \vee c,\ b,\ \neg c\}$$

*En este conjunto tenemos también una cláusula unit (b), por tanto, el conjunto de cláusulas se reduce a:*

$$\{c, \neg c\}$$

*que claramente es insatisfacible.*

*También, y puesto que en este conjunto tenemos una cláusula unit, podríamos reducir el conjunto y nos quedaría*

$$\{\square\}$$

*El proceso seguido al utilizar el algoritmo de Davis-Putnam lo podemos representar como sigue:*

$$\begin{array}{c} \{\neg a \vee \neg b \vee c,\ a,\ b,\ \neg c\} \\ \Big| \ \lambda = a \\ \{\neg b \vee c,\ b,\ \neg c\} \\ \Big| \ \lambda = b \\ \{c, \neg c\} \\ \Big| \ \lambda = c \\ \{\square\} \end{array}$$

**Ejemplo 5.8.2.** *Vamos a demostrar que*

$$\models ((((\alpha \to \beta) \to (\neg\gamma \to \neg\delta)) \to \gamma) \to \varphi) \to ((\varphi \to \alpha) \to (\delta \to \alpha))$$

*Por el teorema de la deducción, lo que hemos de demostrar es que:*

$$((((\alpha \to \beta) \to (\neg\gamma \to \neg\delta)) \to \gamma) \to \varphi) \models ((\varphi \to \alpha) \to (\delta \to \alpha))$$

*que es equivalente, usando nuevamente el teorema de la deducción a:*

$$\{[[(\alpha \to \beta) \to (\neg\gamma \to \neg\delta)] \to \gamma] \to \varphi, \quad (\varphi \to \alpha)\} \models \delta \to \alpha$$

*Por tanto, lo que vamos a probar es que el conjunto de fórmulas*

$$\{[[(\alpha \to \beta) \to (\neg\gamma \to \neg\delta)] \to \gamma] \to \varphi, \quad \varphi \to \alpha, \quad \neg(\delta \to \alpha)\}$$

*es insatisfacible.*

*Hallamos la forma clausular de cada una de las fórmulas que intervienen. De las dos últimas se hace fácilmente:*

$$\varphi \to \alpha \;\equiv\; \neg\varphi \vee \alpha; \qquad \neg(\delta \to \alpha) \;\equiv\; \neg(\neg\delta \vee \alpha) \;\equiv\; \neg\neg\delta \wedge \neg\alpha \;\equiv\; \delta \wedge \neg\alpha$$

*Hallemos entonces la forma clausular de*

$$[[(\alpha \to \beta) \to (\neg\gamma \to \neg\delta)] \to \gamma] \to \varphi$$

$$\begin{gathered}
\neg[[(\alpha \to \beta) \to (\neg\gamma \to \neg\delta)] \to \gamma] \vee \varphi \\
\neg[\neg[(\alpha \to \beta) \to (\neg\gamma \to \neg\delta)] \vee \gamma] \vee \varphi \\
\neg[\neg[\neg(\alpha \to \beta) \vee (\neg\gamma \to \neg\delta)] \vee \gamma] \vee \varphi \\
\neg[\neg[\neg(\neg\alpha \vee \beta) \vee (\neg\neg\gamma \vee \neg\delta)] \vee \gamma] \vee \varphi \\
[\neg\neg[\neg(\neg\alpha \vee \beta) \vee (\neg\neg\gamma \vee \neg\delta)] \wedge \neg\gamma] \vee \varphi \\
[[\neg(\neg\alpha \vee \beta) \vee (\gamma \vee \neg\delta)] \wedge \neg\gamma] \vee \varphi \\
[[(\neg\neg\alpha \wedge \neg\beta) \vee (\gamma \vee \neg\delta)] \wedge \neg\gamma] \vee \varphi \\
[[(\alpha \wedge \neg\beta) \vee (\gamma \vee \neg\delta)] \wedge \neg\gamma] \vee \varphi \\
[[(\alpha \vee \gamma \vee \neg\delta) \wedge (\neg\beta \vee \gamma \vee \neg\delta)] \wedge \neg\gamma] \vee \varphi \\
[(\alpha \vee \gamma \vee \neg\delta \vee \varphi) \wedge (\neg\beta \vee \gamma \vee \neg\delta \vee \varphi)] \wedge (\neg\gamma \vee \varphi)
\end{gathered}$$

*Por tanto, hemos de probar que el conjunto de cláusulas*

$$\{\alpha \vee \gamma \vee \neg\delta \vee \varphi, \quad \neg\beta \vee \gamma \vee \neg\delta \vee \varphi, \quad \neg\gamma \vee \varphi, \quad \alpha \vee \neg\varphi, \quad \neg\alpha, \quad \delta\}$$

*es insatisfacible.*

$$\begin{gathered}
\{\alpha \vee \gamma \vee \neg\delta \vee \varphi, \quad \neg\beta \vee \gamma \vee \neg\delta \vee \varphi, \quad \neg\gamma \vee \varphi, \quad \alpha \vee \neg\varphi, \quad \neg\alpha, \quad \delta\} \\
\Big| \; \lambda = \neg\alpha \\
\{\gamma \vee \neg\delta \vee \varphi, \quad \neg\beta \vee \gamma \vee \neg\delta \vee \varphi, \quad \neg\gamma \vee \varphi, \quad \neg\varphi, \; \delta\} \\
\Big| \; \lambda = \neg\varphi \\
\{\gamma \vee \neg\delta, \quad \neg\beta \vee \gamma \vee \neg\delta, \quad \neg\gamma, \; \delta\} \\
\Big| \; \lambda = \neg\gamma \\
\{\neg\delta, \quad \neg\beta \vee \neg\delta, \; \delta\} \\
\Big| \; \lambda = \neg\delta \\
\{\square\}
\end{gathered}$$

**Ejemplo 5.8.3.** *Estudia si es cierto que*

$$(a \to \neg c) \to a, \quad a \to \neg b, \quad \neg(\neg c \wedge \neg b) \models (\neg c \to a) \to b$$

*Lo primero que hacemos es transformar este problema en un problema de satisfacibilidad o insatisfacibilidad de un conjunto de fórmulas.*

*Por el teorema de la deducción, este problema es equivalente a*

$$(a \to \neg c) \to a, \quad a \to \neg b, \quad \neg(\neg c \wedge \neg b), \quad \neg c \to a \models b$$

*y a su vez, este es equivalente a comprobar si el siguiente conjunto de fórmulas*

$$\{(a \to \neg c) \to a, \quad a \to \neg b, \quad \neg(\neg c \wedge \neg b), \quad \neg c \to a, \quad \neg b\}$$

*es insatisfacible.*

*Calculamos entonces la forma clausular de cada una de las fórmulas:*

| | | | | |
|---|---|---|---|---|
| $(a \to \neg c) \to a$ | $a \to \neg b$ | $\neg(\neg c \wedge \neg b)$ | $\neg c \to a$ | $b$ |
| $(\neg a \vee \neg c) \to a$ | $\neg a \vee \neg b$ | $c \vee b$ | $c \vee a$ | |
| $\neg(\neg a \vee \neg c) \vee a$ | | | | |
| $(a \wedge c) \vee a$ | | | | |
| $(a \vee a) \wedge (c \vee a)$ | | | | |
| $a$ | $\neg a \vee \neg b$ | $b \vee c$ | $a \vee c$ | $\neg b$ |

*Por tanto, nos proponemos estudiar si el conjunto de cláusulas*

$$\{a, \quad \neg a \vee \neg b, \quad b \vee c, \quad a \vee c, \quad \neg b\}$$

*es o no insatisfacible. Aplicamos para ello el algoritmo de Davis-Putnmam.*

$$\begin{array}{c} \{a, \quad \neg a \vee \neg b, \quad b \vee c, \quad a \vee c, \quad \neg b\} \\ \Big| \ \lambda = a \\ \{\neg b, \quad b \vee c, \quad \neg b\} \\ \Big| \ \lambda = \neg b \\ \{c\} \\ \Big| \ \lambda = c \\ \emptyset \end{array}$$

*Al haber llegado al conjunto vacío, el conjunto de cláusulas del que partíamos es satisfacible, y por tanto, la respuesta a si*

$$(a \to \neg c) \to a, \quad a \to \neg b, \quad \neg(\neg c \wedge \neg b) \models (\neg c \to a) \to b$$

*es que no.*

*Pero con lo que hemos hecho, podemos decir algo más.*

*El algoritmo de Davis-Putnam nos ha dicho que el conjunto de cláusulas es satisfacible. Además, nos da una interpretación para la que todas las cláusulas son ciertas. Esta es*

$$I(a) = 1; \quad I(b) = 0; \quad I(c) = 1$$

*Y esta es justamente una interpretación que nos dice que la implicación semántica anterior no es cierta, pues con esa interpretación se tiene:*

$I((a \to \neg c) \to a) = 1$*;* $I(a \to \neg b) = 1$*;* $I(\neg(\neg c \wedge \neg b)) = 1$*, mientras que* $I((\neg c \to a) \to b) = 0$*.*

*Es decir, $I$ es una interpretación que hace ciertas todas las premisas, pero que hace falsa la conclusión. Luego esta conclusión no puede deducirse de las premisas.*

## 5.9. Método de Resolución

Para determinar si un conjunto de cláusulas es insatisfacible puede utilizarse otro método basado en el siguiente resultado:

**Teorema 5.9.1.** *Sean $\alpha$, $\beta$, $\gamma$ tres fórmulas en un lenguaje proposicional. Entonces*

$$\{\alpha \vee \beta, \neg\alpha \vee \gamma\} \models \beta \vee \gamma$$

*Demostración:*
Sea $I$ una interpretación para la que $I(\alpha \vee \beta) = 1$ y $I(\neg\alpha \vee \gamma) = 1$. Pueden darse dos casos:

- $I(\beta) = 1$, en cuyo caso $I(\beta \vee \gamma) = 1$.
- $I(\beta) = 0$. Ahora, puesto que $I(\alpha \vee \beta) = 1$ deducimos que $I(\alpha) = 1$, es decir, $I(\neg\alpha) = 0$, y como $I(\neg\alpha \vee \gamma) = 1$ podemos concluir que $I(\gamma) = 1$, lo que implica que $I(\beta \vee \gamma) = 1$.

■

Observemos que un caso particular podría ocurrir cuando tenemos dos cláusulas unitarias de la forma

$$a \text{ y } \neg a$$

entonces, aplicando el teorema obtendríamos como consecuencia lógica una cláusula que no tiene ningún literal, es decir, la cláusula vacía $\square$. Observemos que el conjunto $\{a, \neg a\}$ es insatisfacible y hemos obtenido que

$$\{a, \neg a\} \models \square$$

### 5.9.1. El concepto de Resolvente

Supongamos que $C$ es una cláusula, y que $\lambda$ es un literal que aparece en la cláusula $C$. Como en la sección anterior denotaremos por $C - \lambda$ a la cláusula que resulta de eliminar el literal $\lambda$ de la cláusula $C$. Por ejemplo, si $C = a \vee \neg b \vee d$ entonces $C - a = \neg b \vee d$, mientras que $C - \neg b = a \vee d$. Si $C = b$ entonces $C - b = \square$.

Sean $C_1$ y $C_2$ dos cláusulas. Supongamos que $\lambda$ es un literal tal que aparece en la cláusula $C_1$ y $\lambda^c$ aparece en $C_2$. Una cláusula que sea equivalente a $(C_1 - \lambda) \vee (C_2 - \lambda^c)$ es lo que se denomina una **resolvente** de $C_1$ y $C_2$.

El teorema nos dice que si $C_1$ y $C_2$ son cláusulas y $R$ una resolvente suya, entonces $\{C_1, C_2\} \models R$.

**Ejemplo 5.9.1.** *Si tenemos las cláusulas $C_1 = \neg a \vee b$ y $C_2 = a$ entonces una resolvente de $C_1$ y $C_2$ es $b$. Nótese que $C_1 \equiv a \to b$, luego al obtener esta resolvente lo que estamos afirmando es que*

$$\{a, a \to b\} \models b$$

*un hecho conocido como "modus ponens".*

**Ejemplo 5.9.2.** *Supongamos que $C_1 = a \vee \neg c \vee d$ y $C_2 = b \vee c \vee d$. Entonces $C_1 - \neg c = a \vee d$ y $C_2 - c = b \vee d$, luego $(C_1 - \neg c) \vee (C_2 - c) = (a \vee d) \vee (b \vee d) \equiv a \vee b \vee d$.*

**Observación:** Puede ocurrir que $(C_1 - \lambda) \vee (C_2 - \lambda^c)$ sea una tautología, en cuyo caso no podemos obtener una resolvente de esta forma.

El **método de resolución** (sin variables) pretende, dado un conjunto de cláusulas, obtener resolventes de dichas cláusulas que son añadidas al conjunto (estas nuevas cláusulas se dice que se han deducido por resolución). Si entre estas cláusulas se encuentra la cláusula vacía, entonces el conjunto de partida es insatisfacible.

**El Principio de Resolución afirma que un conjunto de cláusulas es insatisfacible si, y sólo si, a partir de ellas es posible encontrar la cláusula vacía mediante resolución.**

### 5.9.2. Ejemplos de aplicación del Principio de Resolución:

**Ejemplo 5.9.3.** *Vamos a demostrar que la fórmula*

$$(a \to (b \to c)) \to (\neg(a \to \neg b) \to c)$$

*es una tautología. Esto sabemos que es equivalente a probar:*

$$\models (a \to (b \to c)) \to (\neg(a \to \neg b) \to c)$$

*aplicando el teorema de la deducción dos veces el problema se transforma en*

$$\{a \to (b \to c), \neg(a \to \neg b)\} \models c$$

*o equivalentemente, en demostrar que el conjunto*

$$\{a \to (b \to c), \neg(a \to \neg b), \neg c\}$$

*es insatisfacible.*

*Hallamos la forma clausular de cada una de las fórmulas anteriores:*

$$\begin{array}{l|l|l} a \to (b \to c) & \neg(a \to \neg b) & \neg c \\ \neg a \vee (b \to c) & \neg(\neg a \vee \neg b) & \\ \neg a \vee (\neg b \vee c) & \neg\neg a \wedge \neg\neg b & \\ \neg a \vee \neg b \vee c & a \wedge b & \end{array}$$

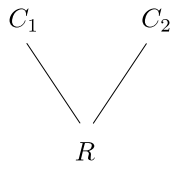
*Y entonces lo que nos queda probar es que el siguiente conjunto de cláusulas es insatisfacible;*

$$\{\neg a \vee \neg b \vee c,\ a,\ b,\ \neg c\}$$

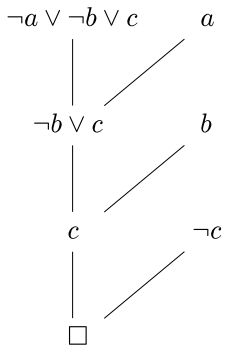
*Y ahora:*
*Una resolvente de* $\neg a \vee \neg b \vee c$ *y* $a$ *es* $\neg b \vee c$.
*Una resolvente de esta última y* $b$ *es* $c$.
*Una resolvente de* $c$ *y* $\neg c$ *es* $\square$.
*Como hemos deducido por resolución la cláusula vacía concluimos que el conjunto de cláususlas es insatisfacible, y por tanto, la primera fórmula es una tautología.*

#### Una representación gráfica del método de resolución

Supongamos que $C_1$ y $C_2$ son dos cláusulas, y $R$ es una resolvente de ambas. Esto entonces podemos representarlo como sigue:




En tal caso, el proceso seguido en el ejemplo precedente podríamos haberlo representado:



**Ejemplo 5.9.4.** *Vamos a demostrar que*

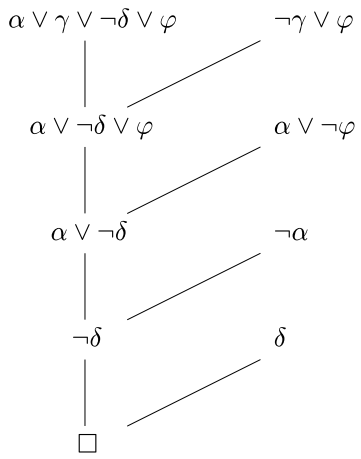
$$\models \big(\big(((\alpha \to \beta) \to (\neg\gamma \to \neg\delta)) \to \gamma\big) \to \varphi\big) \to \big((\varphi \to \alpha) \to (\delta \to \alpha)\big)$$

*utilizando el Principio de Resolución. En primer lugar necesitamos transformar el problema en otro equivalente que consiste en decidir si un conjunto de cláusulas es satisfacible o insatisfacible. Como esto ya se ha hecho en la sección del algoritmo de Davis-Putnam, copiamos el resultado: hemos de probar que el conjunto de cláusulas*

$$\{\alpha \vee \gamma \vee \neg\delta \vee \varphi, \quad \neg\beta \vee \gamma \vee \neg\delta \vee \varphi, \quad \neg\gamma \vee \varphi, \quad \alpha \vee \neg\varphi, \quad \neg\alpha, \quad \delta\}$$

*es insatisfacible.*

*Tratamos entonces de deducir la cláusula vacía.*




*Al haber obtenido la cláusula vacía, concluimos que la fórmula inicial es una tautología.*

### 5.9.3. Cómo se prueba que algo *no* es consecuencia lógica de un conjunto de proposiciones

Consideremos el problema de estudiar si es cierto que

$$\{q \to p \vee r\} \models (p \to q) \to \big(p \to ((r \to q) \to r)\big)$$

y apliquemos todas las técnicas que hemos estudiado.

En primer lugar usamos el Teorema de la Deducción tantas veces como sea posible, en este caso hasta 3 veces, y el problema queda

$$\{q \to p \vee r, p \to q, p, r \to q\} \models r$$

**Método 1: Cálculo de interpretaciones en $\mathbb{Z}_2$**

Si tenemos el sistema de ecuaciones

$$\left.\begin{array}{l} I(q \to p \vee r) = 1 \\ I(p \to q) = 1 \\ I(r \to q) = 1 \\ I(p) = 1 \end{array}\right\}$$

usando

$$\left.\begin{array}{l} I(p \to q) = 1 \\ I(p) = 1 \end{array}\right\} \quad \left.\begin{array}{l} 1 + I(p) + I(p)I(q) = 1 \\ I(p) = 1 \end{array}\right\} \quad \left.\begin{array}{l} I(q) = 1 \\ I(p) = 1 \end{array}\right\}$$

(a este sistema de dos ecuaciones lo llamaremos **modus ponens**) y nos queda

$$\left.\begin{array}{l} I(q \to p \vee r) = 1 \\ I(q) = 1 \\ I(r \to q) = 1 \\ I(p) = 1 \end{array}\right\}$$

ahora, de nuevo modus ponens con las dos primeras ecuaciones nos da

$$\left.\begin{array}{l} I(p \vee r) = 1 \\ I(q) = 1 \\ I(r \to q) = 1 \\ I(p) = 1 \end{array}\right\}$$

y como $I(q) = 1$, la ecuación 3 se puede eliminar porque no añade ninguna condición, además la ecuación 1 es consecuencia de la cuarta y no nos queda imposición sobre $I(r)$. Es decir, el sistema se cumple siempre que $I(p) = 1$ y $I(q) = 1$ sin importar el valor de $I(r)$. Eso nos hace ver que la interpretación $I(p) = 1, I(q) = 1, I(r) = 0$ prueba que la consecuencia lógica no se verifica.

**Método 2: Algoritmo de Davis-Putnam**

En primer lugar calculamos la forma clausular de todas las premisas y la negación de la conclusión:

$$\{\neg p \vee q, \neg q \vee p \vee r, p, \neg r \vee q, \neg r\}$$

Aplicando el primer paso del algoritmo a la cláusula unit $p$, nos queda

$$\{q, \neg r \vee q, \neg r\}$$

y de nuevo el paso uno para la cláusula unit $q$ nos reduce el conjunto de cláusulas a $\{\neg r\}$ que es claramente satisfacible. Por tanto el conjunto de partida es satisfacible y para la interpretación 1 de todas las cláusulas unit $I(p) = 1, I(q) = 1, I(\neg r) = 1$ tenemos un modelo en el que se satisface. Por tanto la consecuencia lógica no ocurre.

**Método 3: Resolución**

Partimos del conjunto de cláusulas que teníamos en el método anterior:

$$\{\neg p \vee q, \neg q \vee p \vee r, p, \neg r \vee q, \neg r\}$$

y tratamos de encontrar una resolución que nos lleve a la cláusula vacía. Para ello intentamos clacular todas las resolventes posibles. Empecemos añadiendo al conjunto las resolventes de la cláusula $p$ con todas las posibles:

$$\{\neg p \vee q, \neg q \vee p \vee r, p, \neg r \vee q, \neg r\} \cup \{q\}$$

ahora las obtenidas al resolver con $\neg r$

$$\{\neg p \vee q, \neg q \vee p \vee r, p, \neg r \vee q, \neg r\} \cup \{q\} \cup \{\neg q \vee p\}$$

ahora resolvemos con $q$

$$\{\neg p \vee q, \neg q \vee p \vee r, p, \neg r \vee q, \neg r\} \cup \{q\} \cup \{\neg q \vee p\} \cup \{p \vee r\}$$

ahora calculamos una resolvente de $q$ y $\neg q \vee p$

$$\{\neg p \vee q, \neg q \vee p \vee r, p, \neg r \vee q, \neg r\} \cup \{q\} \cup \{\neg q \vee p\} \cup \{p \vee r\} \cup \{p\}$$

aún se pueden obtener nuevas cláusulas, por ejemplo la resolvente de $\neg p \vee q$ y $p \vee r$ nos da $q \vee r$ y el problema de encontrar la resolución se hace más complicado....

¿No somos capaces de encontrar la resolución o es que no existe?

No obstante, en este caso, podríamos ver que el conjunto es satisfacible.

Entre las cláusulas que hemos obtenido nos encontramos con las cláusulas $p$, $q$, $\neg r$. Si el conjunto fuera satisfacible, habría una interpretación que sobre todas las cláusulas que nos han ido apareciendo valdría 1. En particular, $I(p) = 1$, $I(q) = 1$ e $I(r) = 0$.

Probamos si esa interpretación hace ciertas todas las cláusulas y podemos comprobar que así es. Por tanto, el conjunto de cláusulas del que partíamos es satisfacible.

# Capítulo 6

# Lenguajes de Primer Orden

## 6.1. Elementos del lenguaje

A partir de ahora nuestra manera de formalizar el lenguaje natural se complica un poco más. Empecemos con un ejemplo:

La frase

Juan es alto

es considerada en lógica proposicional como una fórmula atómica, lo mismo que otras frases que tienen elementos comunes con ésta: Juan es albañil o Pedro es alto.

Recordando nuestros primeros conocimientos de sintaxis de español diremos que una frase tiene dos elementos distinguidos: el sujeto y el predicado. Los correspondientes conceptos en la lógica de primer orden son los de "término" y "predicado" o relación.

### 6.1.1. Términos

Si tenemos un conjunto de sujetos posibles, digamos los miembros de una familia, entonces podemos construir frases con predicado"ser alto":

Juan es alto
Todos son altos
Algunos son altos
El padre de Juan es alto
El segundo hijo del tio mayor de Juan es alto

Observemos que hay distintas formas de referirse al sujeto:

- con un nombre propio (Juan)
- sin hacer referencia explícita al sujeto, digamos de forma general (alguien, todos)
- por medio de una referencia que lo determina (el padre de Juan)

Estas formas distintas de nombrar a un elemento de un conjunto se van a traducir mediante símbolos distintos que son:

- Símbolos de constante: $a, b, c, \ldots$ y a veces $a_1, a_2, \ldots$ (en general las primeras letras del alfabeto en minúscula).
- Simbolos de variable: $x, y, z, \ldots$ y a veces $x_1, x_2, \ldots$ (en general las últimas letras del alfabeto en minúscula).
- Símbolos de función: $f, g, h, \ldots$ y si es necesario usando subíndices.

Un **término** es la forma de hacer referencia a un elemento. Tanto los símbolos de constantes como los de variables son **términos**; **también son términos** las expresiones de la forma

$$f(t), g(t_1, t_2), h(t_1, t_2, t_3), \ldots$$

donde $t, t_1, t_2, t_3$ representan términos. Observamos que estos símbolos de función tienen la misma forma que las funciones que nos hemos encontrado en otras partes de las matemáticas, y también pueden ser suceptibles de aplicarse a un número de términos que varía de unas a otras, que es lo que llamaremos la **ariedad** de una función. Además como el resto de funciones pueden componerse, de forma que también son términos las expresiones:

$$f(g(x, a)),\ g(h(y, z, x)),\ f(f(a)),\ f(f(x)), \ldots$$

### 6.1.2. Predicados o relaciones

El predicado de la oración contiene la parte fundamental del significado de ésta y se combina con los distintos sujetos dando lugar a oraciones diferentes. Los **predicados o relaciones** en lógica de primer orden se nombran por las letras intermedias del alfabeto en minúscula o mayúscula según los autores: p, q, r, P, Q, R,... o también se usan combinaciones de éstas.

**Ejemplo 6.1.1.** *El predicado "ser alto" podemos nombrarlo como SA, al individuo "Juan" por la letra minúscula j y a la función "el padre de ..." por f; entonces podemos construir las expresiones:*

- $SA(j)$ *que correspondería con la frase "Juan es alto"*
- $SA(f(j))$ *que sería la traducción de "El padre de Juan es alto"*

En el ejemplo hemos visto que un predicado se acompaña del término que actúa como sujeto, pero no nos dejemos engañar por los ejemplos más sencillos. Como en el lenguaje natural, los predicados pueden no tener sujeto como en la frase "LLueve", así el correspondiente predicado en lógica de primer orden no necesita ningún término, diremos que es 0-ario. La **ariedad** de un predicado, como la de una función, es el número de términos que requiere para completar un significado. Es fácil imaginar un predicado 2-ario: "ser la madre de", "contratar a ", "suspender a", etc. En lógica **hay predicados con cualquier número natural como ariedad**.

### 6.1.3. Conectivas

Las conectivas que se usan en lógica de primer orden son las mismas que en lógica proposicional ($\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$) más dos nuevas llamadas **cuantificadores**:

$\forall$ es el cuantificador universal y se lee **para todo**

$\exists$ es el cuantificador existencial y se lee **existe**

como una primera aproximación podríamos decir que se usan para escribir frases del tipo:

**Todos son altos** que se traduce por $\forall x SA(x)$.

o

**Alguien es alto** que se traduce por $\exists x SA(x)$.

Como en lógica proposicional, haremos uso también de los paréntesis, aunque no se consideran símbolos del lenguaje sino auxiliares.

## 6.2. Lenguajes de primer orden

Un lenguaje de primer orden concreto **L** consta entonces de

1. Un conjunto de **símbolos de constantes**,
2. Un conjunto de **símbolos de función** y declaración de la ariedad de cada una de ellas,

3. Un conjunto de **símbolos de predicado** y la declaración de ariedad de cada uno de ellos.

además de los **símbolos de variable** que sean necesarios y los **símbolos de conectivas** que son comunes a todos los lenguajes de primer orden.

**Ejemplo 6.2.1.** *Consideramos el lenguaje* $\boldsymbol{L}$ *dado por*

- $Cons = \{j, a\}$ *como símbolos de constante;*
- $Fun = \{f\}$ *el conjunto de las funciones, con* $f$ *de ariedad 1 y*
- $Pred = \{SA\}$ *donde* $SA$ *tiene ariedad 1.*

Al conjunto de términos que se pueden escribir con los símbolos del lenguaje se le suele denotar por $Term(\mathbf{L})$. Tenemos que definir ahora qué será considerado como una **fórmula bien formada** del lenguaje de primer orden dado. Comencemos con las **fórmulas atómicas** (las más pequeñas que pueden dotarse de significado) que son las que se construyen con un predicado conteniendo a los términos que indique su ariedad.

**Ejemplo 6.2.2.** *Son fórmulas atómicas del lenguaje del ejemplo anterior:*
$SA(j), SA(a), SA(f(x)), SA(y), SA(f(j)), SA(f(f(j))), \ldots$

### 6.2.1. Gramática

Las reglas para construir f.b.f.s. a partir de otras son:

- Las fórmulas atómicas son f.b.f.s..
- Si $\alpha$ es una f.b.f., entonces $\neg\alpha$ también lo es.
- Si $\alpha$ y $\beta$ son f.b.f.s. entonces lo son:

  $\alpha \wedge \beta$
  $\alpha \vee \beta$
  $\alpha \rightarrow \beta$
  $\alpha \leftrightarrow \beta$

- Si $\alpha$ es una f.b.f. y $x$ es una variable, entonces $\forall x\alpha$ es una f.b.f..
- Si $\alpha$ es una f.b.f. y $x$ es una variable, entonces $\exists x\alpha$ es una f.b.f..
- Toda f.b.f. se genera aplicando las reglas anteriores un número finito de veces.

**Ejemplo 6.2.3.** *Son fórmulas bien formadas del lenguaje del ejemplo anterior:*

1. $SA(j)$
2. $\neg(SA(j) \wedge SA(a))$
3. $\forall x(SA(x) \vee \neg SA(x))$
4. $\forall x \neg SA(x) \rightarrow \exists y SA(f(y))$
5. $\forall x(SA(j) \rightarrow SA(f(x))) \rightarrow SA(j)$
6. $\forall x(SA(j) \rightarrow SA(f(x))) \rightarrow \neg SA(j)$
7. $\exists y \forall x(SA(y) \rightarrow SA(f(x))) \rightarrow \forall z SA(z)$

*No son fórmulas bien formadas:*

1. $SA(\forall x)$
2. $\forall x SA(a, f(x))$

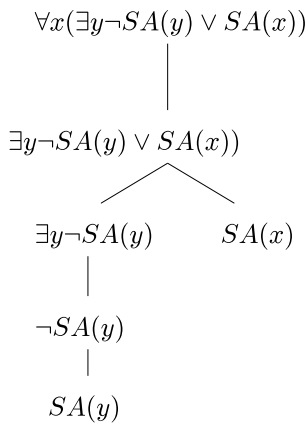
3. $SA(a \to j)$
4. $f(x) \to SA(j)$
5. $\forall x f(x)$
6. $SA(f(x) \wedge j)$
7. $\exists x(f(x) \wedge j)$
8. $\exists SA(x)$
9. $j \vee \exists x SA(x)$
10. $\exists x SA(x) \neg SA(a)$
11. $SA(a) \wedge SA(j) \vee SA(x)$

Como en lógica proposicional, los paréntesis se usan para indicar qué conectivas tienen preferencia sobre las demás. Se mantienen los criterios que ya conocemos y sólo queda añadir que los cuantificadores, así como la negación, tienen preferencia sobre el resto, y cuando varios de éstos aparecen juntos entonces se ejecutan de izquierda a derecha desde la fórmula sobre la que actúan.

**Ejemplo 6.2.4.** *Para la fórmula*

$$\forall x(\exists y \neg SA(y) \vee SA(x))$$

*podemos dibujar el árbol que la desglosa hasta llegar a las fórmulas atómicas que intervienen:*




### 6.2.2. Ocurrencias libres y ligadas de una variable

En una fórmula bien formada la aparición de una variable puede ocurrir en dos formas distintas que será importante distinguir antes de entrar en la semántica o interpretación de fórmulas. Observemos la variable $x$ en las dos fórmulas siguientes:

$$\forall x Q(x, a)$$
$$\forall y Q(x, y)$$

en la primera la $x$ aparece dentro de un predicado que va precedido por un cuantificador que lleva la variable $x$, de una manera informal podemos decir que eso obliga a que el valor de la variable recorra todas las posibilidades, en ese caso decimos que la ocurrencia de la variable $x$ es **ligada** ; sin embargo, en la segunda el predicado que contiene a $x$ no va precedido por ningún cuantificador que contenga a la variable denominada $x$, decimos entonces que la ocurrencia de la variable $x$ es **libre**.

Para formalizar un poco estos conceptos empecemos definiendo quÚ entendemos por el **radio de acción de un cantificador**: es la subfórmula a la que afecta ese cuantificador. Como los cuantificadores tienen preferencia sobre las demás conectivas, entonces el radio de acción es siempre la subfórmula que está inmediatamente a su derecha. Usando el desglose en árbol de la sección anterior, el radio de acción es exactamente el nodo que cuelga de la rama en la que se deshace el cuantificador.

**Ejemplo 6.2.5.** *En la f.b.f.*

$$\forall x R(x,z) \to Q(x,y,z)$$

*el radio de acción de* $\forall x$ *es la subfórmula (atómica en este caso)* $R(x,z)$*. En la f.b.f.*

$$\forall z[\forall x P(x,z) \to \exists y(Q(x,y,z) \wedge R(y,z)]$$

*el radio de acción de* $\forall x$ *es* $P(x,z)$*; el de* $\exists y$ *es la subfórmula* $Q(x,y,z) \wedge R(y,z)$ *y por último, el de* $\forall z$ *es* $\forall x P(x,z) \to \exists y(Q(x,y,z) \wedge R(y,z)$*.*

Ahora la aparición de una variable se dirá que es una **ocurrencia ligada** (o simplemente que la variable es ligada), cuando

⋆ es la que acompaña un cuantificador, o bien

⋆ está en el radio de acción de un cuantificador que va seguido de **esa misma** variable.

En otro caso diremos que la variable es **libre**.

**Ejemplo 6.2.6.** *En la f.b.f.*

$$\forall x R(x,z) \to Q(x,y,z)$$

*la primera y la segunda aparición (de izquierda a derecha) de la vatriable* $x$ *son* **ligadas**, *mientras que la tercera ocurrencia es* **libre**. *Todas las apariciones de las variables* $y$ *y* $z$ *son libres puesto que no hay ningún cuantificador en la fórmula conteniendo a estas variables.*

*En la f.b.f.*

$$\forall z[\forall x P(x,z) \to \exists y(Q(x,y,z) \wedge R(y,z)]$$

*la primera aparición de* $x$ *es ligada porque es la que acompaña a un cuantificador, la segunda tambiÚn es ligada puesto que está en el radio de acción de* $\forall x$*; la tercera aparición es libre. Las tres apariciones de la variable* $y$ *son ligadas y todas las apariciones de* $z$ *también son ligadas, la primera por acompañar al cuantificador y las demás porque están en el radio de acción de dicho cuantificador.*

## 6.3. Interpretaciones: Estructura

Ahora, como en la lógica proposicional, esperamos obtener las reglas para asignar un valor de verdad a cada fórmula. En aquel caso el procedimiento consistía sencillamente en considerar una asignación a las proposiciones atómicas y tener en cuenta las reglas para las conectivas que aparecían. Como entonces el valor de verdad de una fórmula podrá ser **1** (verdadero) o **0** (falso), pero el procedimiento para establecer el significado de cada fórmula atómica es un poco más complicado.

**Definición 53.** *Una* **estructura** *para un lenguaje de primer orden es una descripción en la que se declaran:*

*Un conjunto no vacío* $D$*, denominado* **universo o dominio** *de la estrutura.*

*Para cada símbolo de constante que se use en el lenguaje, un elemento concreto del conjunto* $D$*.*

*Para cada símbolo de función, digamos* $f$*, una aplicación de* $D^n$ *en* $D$*, donde* $n$ *es la ariedad de la función. Es decir, una manera de asignar un elemento a cada* $n$*-upla de elementos del conjunto* $D$*.*

*Para cada predicado con ariedad* $m$*, una lista de* $m$*-uplas de elementos de* $D$ *(o lo que es lo mismo, un subconjunto de* $D^m$*). También podría definirse con una aplicación* $D^m \to \mathbb{Z}_2$*.*

**Ejemplo 6.3.1.** *Consideremos las fórmulas*

1. $SA(j)$,
2. $SA(a)$,
3. $SA(f(a))$.

*Un lenguaje de primer orden en el que las tres son fórmulas bien formadas está constituido por:*

*Las constantes $a$ y $j$;*

*la función 1-aria $f$;*

*el predicado 1-ario $SA$.*

*Una estructura para este lenguaje puede ser:*

**Dominio** $D = \{$ *Juan, Antonio, Eva, David* $\}$

**Constantes** $a =$*Antonio,* $j =$*Juan;*

**Función** $f(Juan) = Antonio;\ f(Antonio) = David;\ f(Eva) = Antonio;\ f(David) = Eva;$

**Predicados** $SA = \{Juan, Antonio\}$, *lo que podría entenderse como que Juan y Antonio son altos mientras que el resto de los individuos del conjunto no lo son.*

*Con estas descripciones las fórmulas adquieren un significado de tal forma que puede determinarse el valor de verdad de cada una de ellas. Veamos cuál es el resultado en nuestro ejemplo:*

1. $SA(j)$ *es cierto, Juan es alto;*
2. $SA(a)$ *es cierto, Antonio es alto;*
3. $SA(f(a))$ *es falso, $f(a)$ representa al individuo David, que no es alto ($David \notin SA$).*

**Ejemplo 6.3.2.** *Tengamos ahora las fórmulas:*

1. $R(f(a))$
2. $Q(g(a,a), f(c))$
3. $Q(c, f(x))$

*Un lenguaje de primer orden, $\mathcal{L}$, en el que todas son f.b.f.s. está dado por:*

**Constantes** $a, c$

**Variables** $x$

**Funciones** $f, g$, *la primera 1-aria y la segunda 2-aria.*

**Predicados** $R, Q$ *el primero 1-ario y el segundo 2-ario.*

*Una* **estructura** $\mathcal{E}$ *para este lenguaje $\mathcal{L}$, puede ser:*

**Dominio** $D = \mathbb{Z}_3$

**Constantes** $a = 0,\ c = 2;$

**Funciones** $f(x) = x + 1;\ g(x, y) = x + y;$

**Predicados** $R = \{0\},\ Q = \{(0,1), (1,2), (2,0)\}$

*Una forma alternativa de describir a los predicados es utilizar lenguaje natural o lenguaje matemático, por ejemplo:*

*$R(x)$ es cierto cuando $x = 0$; $Q(x, y)$ es cierto cuando $x + 1 = y$.*

*El valor de verdad de las fórmulas con esta estructura será:*

1. *$R(f(a))$ es $R(f(0)) = R(0 + 1) = R(1)$ que es falso.*
2. *$Q(g(a, a), f(c))$ es $Q(0 + 0, 1 + 1) = Q(0, 2)$ que es falso puesto que el par $(0, 2)$ no aparece en la descripción de $Q$, o bien puesto que $0 + 1 \neq 2$.*
3. *¡Pero no podemos decidir sobre $Q(c, f(x))$! El valor de verdad dependerá del elemento del dominio que se representa por $x$.*

   *Así que aún nos faltan elementos para interpretar esta fórmula, en concreto elegir el valor que toma la variable $x$.*

### 6.3.1. Interpretaciones: Valoración

**Definición 54.** *Una* **valoración** *$v$ para un lenguaje $\mathcal{L}$ y una estructura $\mathcal{E}$ es una aplicación*

$$v : Var(\mathcal{L}) \to D$$

*que declara un valor para cada variable del lenguaje.*

Notemos que cualquier valoración puede extenderse a una aplicación $Ter(\mathcal{L}) \to D$, que denotaremos de la misma forma que la valoración.

Esto se hace como sigue:

Para una constante $a$, $v(a)$ es el elemento de $D$ que se le ha asignado al símbolo de constante $a$ al definir la estructura.

Para las variables ya está definido.

Si $t_1, t_2, \cdots, t_n$ son términos y $f$ es un símbolo de función $n$-ario, entonces $v(f(t_1, t_2, \cdots, t_n)) = f(v(t_1), v(t_2), \cdots, v(t_n))$. Recordemos que todo término se puede obtener a partir de los términos básicos (símbolos de constante y de función) mediante aplicaciones sucesivas de la regla:

> Si $t_1, t_2, \cdots, t_n$ son términos y $f$ es un símbolo de función, entonces $f(t_1, t_2, \cdots, t_n)$ es un témino.
>
> En la definición anterior, la $f$ que aparece en el miembro de la izquierda representa el símbolo de función $f$, mientras que la que aparece en el miembro de la derecha representa la función $D^n \to D$ que se le ha asignado al símbolo de función $f$.

**Ejemplo 6.3.3.** *En la estructura del ejemplo anterior, consideramos la valoración $v : Var(\mathcal{L}) \to D$ dada por $x \mapsto 0$. En tal caso, tenemos:*

$v(x) = 0 \qquad v(a) = 0 \qquad v(c) = 2$
$v(f(x)) = f(v(x)) = f(0) = 1 \qquad v(f(c)) = f(v(c)) = f(2) = 0$
$v(g(a, f(x))) = g(v(a), v(f(x))) = g(0, 1) = 1$
$v(f(g(a, f(x)))) = f(v(g(a, f(x)))) = f(1) = 2$
$v(g(a, c)) = g(v(a), v(c)) = g(0, 2) = 2$
$v(g(g(a, c), f(g(a, f(x))))) = g(v(g(a, c)), v(f(g(a, f(x))))) = g(2, 2) = 1$
$v(g(f(c), f(x)) = g(v(f(c)), v(f(x)) = g(0, 1) = 1$

*Para calcular el valor de un término podemos proceder como sigue:*

$$\begin{aligned} v(g(f(f(x)), g(f(a), g(a, f(c))))) &= f(f(x)) + g(f(a), g(a, f(c))) \\ &= f(f(0)) + g(f(0), g(0, f(2))) \\ &= f(0 + 1) + (f(0) + g(0, f(2))) \\ &= (1 + 1) + (1 + (0 + f(2))) \\ &= 2 + (1 + (0 + 0)) = 0. \end{aligned}$$

Ahora, con ambas cosas, una estructura y una valoración podemos decidir el valor de verdad de cada fórmula, es decir, podemos **interpretar** cada f.b.f. escrita en el lenguaje $L$.

**Definición 55.** *Una* **interpretación** $I^v = (\mathcal{E}, v)$ *para un lenguaje* $\mathcal{L}$ *es el par formado por una estructura* $\mathcal{E}$*, y una valoración* $v$*.*

*Toda interpretación determina un valor de verdad para cualquier fórmula.*

*Dada una fórmula* $\varphi$ *denotaremos por* $I^v(\varphi)$ *al valor de verdad de la fórmula con esta interpretación.*

**Ejemplo 6.3.4.** *Con la valoración del ejemplo anterior*

$$v : Var(\mathcal{L}) \to D \qquad x \mapsto 0$$

*Podemos calcular la interpretación de la fórmula* $Q(c, f(x))$ *haciendo referencia a la valoración que utilizamos:*

$$I^v(Q(c, f(x))) = I^v(Q(2, 0 + 1)) = 0$$

*puesto que el par* $(2, 1)$ *no cumple la condición* $x + 1 = y$*.*

*Para la valoración*

$$v' : Var(\mathcal{L}) \to D \text{ dada por } x \mapsto 2$$

*la interpretación de la fórmula será:*

$$I^{v'}(Q(c, f(x))) = I^{v'}(Q(2, 2 + 1)) = I^{v'}(Q(2, 0)) = 1$$

*puesto que el par* $(2, 0)$ *cumple la condición* $x + 1 = y$*.*

### 6.3.2. Conectivas

Hasta ahora sólo hemos visto ejemplos de interpretación de fórmulas atómicas, nos queda todavía introducir la forma de interpretar una fórmula cuando aparecen las conectivas. En cuanto a las que estudiamos en lógica proposicional se siguen las mismas reglas:

$I^v(\neg\varphi) = 1 + I^v(\varphi)$ en $\mathbb{Z}_2$;

$I^v(\varphi \wedge \psi) = I^v(\varphi)I^v(\psi)$ en $\mathbb{Z}_2$;

$I^v(\varphi \vee \psi) = I^v(\varphi) + I^v(\psi) + I^v(\varphi)I^v(\psi)$ en $\mathbb{Z}_2$;

$I^v(\varphi \to \psi) = 1 + I^v(\varphi) + I^v(\varphi)I^v(\psi)$ en $\mathbb{Z}_2$;

$I^v(\varphi \leftrightarrow \psi) = 1 + I^v(\varphi) + I^v(\psi)$ en $\mathbb{Z}_2$;

**Ejemplo 6.3.5.** *Con la estructura dada en el último ejemplo y la valoración* $v : x \mapsto 1$ *calcularemos la interpretación de las fórmulas:*

1. $\alpha = R(f(a)) \to Q(g(a, a), f(c))$
2. $\beta = Q(g(a, a), f(c)) \vee Q(c, f(x))$

*Para la primera* $I^v(R(f(a)) = 0$ *pero también* $I^v(Q(g(a, a), f(c))) = 0$ *así que la implicación es verdadera, es decir,* $I^v(\alpha) = 1$*.*

*En cuanto a la segunda debemos calcular* $I^v(Q(c, f(x))) = I^v(Q(0, 1 + 1)) = I^v(Q(0, 2)) = 0$ *puesto que el par* $(0, 2)$ *no verifica la condición* $x+1 = y$*; por otro lado* $I^v(Q(g(a, a), f(c))) = I^v(Q(0+0, 2+1)) = I^v(Q(0, 0)) = 0$ *porque el par* $(0, 0)$ *no aparece en la descripción de* $Q$*. Así, la interpretación de la fórmula es* $I^v(\beta) = 0$ *por ser disyunción de dos fórmulas falsas.*

Presentamos ahora las reglas para los cuantificadores. Antes de esto, definamos para cada valoración $v : Var(\mathcal{L}) \to D$, cada variable $x$ y cada elemento $e \in D$ una nueva valoración $v_{x|e} : Var(\mathcal{L}) \to D$ como:

$$v_{x|e}(y) = \begin{cases} v(y) & \text{si } y \neq x \\ e & \text{si } y = x \end{cases}$$

Es decir, $v_{x|e}$ actúa igual que $v$ sobre todas las variables salvo eventualmente $x$.

**Ejemplo 6.3.6.** *Consideramos un lenguaje de primer orden con 3 símbolos de variable $x, y, z$, y consideramos una estructura en la que $D = \mathbb{Z}$. Sea $v$ la valoración $x \mapsto -2$, $y \mapsto 1$, $z \mapsto 5$.*

*Consideramos entonces distintas valoraciones:*

$$\begin{array}{ccccc} v_{x|2} & v_{x|5} & v_{y|-1} & v_{z|3} & v_{z|5} \\ x \mapsto 2 & x \mapsto 5 & x \mapsto -2 & x \mapsto -2 & x \mapsto -2 \\ y \mapsto 1 & y \mapsto 1 & y \mapsto -1 & y \mapsto 1 & y \mapsto 1 \\ z \mapsto 5 & z \mapsto 5 & z \mapsto 5 & z \mapsto 3 & z \mapsto 5 \end{array}$$

*Nótese que $v_{z|5} = v$. En general, se tiene que $v_{x|e} = v$ cuando $v(x) = e$.*

$$I^v(\forall x\varphi) = \begin{cases} 1 & \text{si } I^{v_{x|a}}(\varphi) = 1 \text{ para todos los elementos } a \in D. \\ 0 & \text{en otro caso} \end{cases}$$

$$I^v(\exists x\varphi) = \begin{cases} 1 & \text{si } I^{v_{x|a}}(\varphi) = 1 \text{ para algún elemento } a \in D \\ 0 & \text{en otro caso} \end{cases}$$

**Ejemplo 6.3.7.** *Con el lenguaje y la estructura de ejemplos anteriores calculemos la interpretación de las fórmulas:*

1. $\forall x Q(x, f(x))$,
2. $\forall x Q(x, c)$
3. $\exists x Q(x, f(c))$,
4. $\exists x Q(x, f(f(x)))$
5. $\exists x(R(x) \to \neg R(x))$

1. *Puesto que aparece un cuantificador afectado por la variable $x$, debemos considerar las valoraciones que llevan $x$ en cada uno de los elementos del dominio. Para ellos dibujamos una tabla en la que aparecen todas (es una ventaja de que el dominio sea finito!):*

| $v : x \mapsto$ | $Q(x, f(x))$ |
|---|---|
| 0 | 1 |
| 1 | 1 |
| 2 | 1 |

*Así que $I(\forall x Q(x, f(x))) = 1$*

**Observación:** *Aunque aparecía la variable $x$ no ha sido necesario fijar una valoración puesto que estamos obligados a usar todos los posibles valores de $x$ para interpretar el cuantificador. Esto es, cuando la variable es* **ligada** *no es necesario fijar valoración para ella.*

2. *Igual que en el caso anterior escribimos la tabla:*

| $v : x \mapsto$ | $Q(x, c)$ |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 0 |

*Así que $I(\forall x Q(x, c)) = 0$*

3. *También ahora necesitamos todas las valoraciones sobre la variable $x$, escribimos la tabla:*

| $v : x \mapsto$ | $Q(x, f(c))$ |
|---|---|
| 0 | 0 |
| 1 | 0 |
| 2 | 1 |

*Así que* $I(\exists x Q(x, f(c))) = 1$

4. *La tabla es:*

| $v : x \mapsto$ | $Q(x, f(f(x)))$ |
|---|---|
| 0 | 0 |
| 1 | 0 |
| 2 | 0 |

*Así que* $I(\exists x Q(x, f(f(x))) = 0$

5. *En este caso la tabla es:*

| $v : x \mapsto$ | $R(x)$ | $\neg R(x)$ | $R(x) \to \neg R(x)$ |
|---|---|---|---|
| 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 2 | 0 | 1 | 1 |

*Así que* $I(\exists x(R(x) \to \neg R(x))) = 1$

## 6.4. Satisfacibilidad

**Definición 56.** *Dada una fórmula $\varphi$ en un lenguaje de primer orden, una interpretación $I^v = (\mathcal{E}, v)$ se dice que es un* **modelo** *para $\varphi$ si $I^v(\varphi) = 1$; es decir, si la fórmula es verdadera bajo esa interpretación.*

Con esta definición haremos una clasificación de las fórmulas bien formadas.

**Definición 57.** *Una fórmula es* **satisfacible** *si existe un modelo para ella. Cuando una fórmula* **no** *es satisfacible, esto es, es falsa bajo cualquier interpretación, la llamamos* **contradicción**.

**Definición 58.** *Una fórmula es* **refutable** *si existe una interpretación que* **no** *es un modelo para ella. Cuando una fórmula* **no** *es refutable es cierta bajo cualquier interpretación, decimos que es* **universalmente válida**.

Observemos entonces que cualquier fórmula bien formada puede encuadrarse en uno de los siguientes tipos:

- UNIVERSALMENTE VÁLIDA
- SATISFACIBLE Y REFUTABLE
- CONTRADICCIÓN

Por el momento será más fácil probar cuando una fórmula es satisfacible y refutable puesto que para ello es suficiente dar dos ejemplos de interpretaciones: una para la que sea falsa y una para la que sea verdadera (un modelo).

Veamos algunas fórmulas y su clasificación:

**Ejemplo 6.4.1.** $\exists x(P(x) \to P(a))$ *es* UNIVERSALMENTE VÁLIDA

*Para convencernos trazamos la tabla que deberíamos elaborar para calcular una interpretación:*

| $x$ | $P(x)$ | $P(a)$ | $P(x) \to P(a)$ | $\exists x(P(x) \to P(a))$ |
|---|---|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | |
| $a$ | $I(P(a))$ | $I(P(a))$ | 1 | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | |

*y observamos que en la línea correspondiente al valor del dominio que toma la constante $a$ obtenemos que ambos miembros de la implicación tienen el mismo valor de verdad (puede que sea $0$ o $1$, pero ambas el mismo), por lo que la implicación es verdadera. Una línea con un $1$ nos hace obtener una interpretación verdadera para el cuantificador existencial. Y desde luego no depende de la interpretación elegida.*

$\forall x(P(x) \to P(a))$ *es* SATISFACIBLE Y REFUTABLE. *Para probarlo tenemos que dar dos ejemplos de interpretaciones:*

1. *Tomemos $D = \mathbb{N}$, $P(x) \equiv$ "$x$ es par", $a = 3$ y obtenemos*

| $x$ | $P(x)$ | $P(a)$ | $P(x) \to P(a)$ | $\forall x(P(x) \to P(a))$ |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | |
| 1 | 0 | 0 | 1 | 0 |
| 2 | 1 | 0 | 0 | |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | |

*y la primera línea ya nos informa de que la interpretación del cuantificador universal es $0$ y por tanto la fórmula es* REFUTABLE

2. *Sin embargo para la interpretación $D = \mathbb{N}$, $P(x) \equiv$ "$x$ es par", $a = 2$ obtenemos*

| $x$ | $P(x)$ | $P(a)$ | $P(x) \to P(a)$ | $\forall x(P(x) \to P(a))$ |
|---|---|---|---|---|
| 0 | 1 | 1 | 1 | |
| 1 | 0 | 1 | 1 | 1 |
| 2 | 1 | 1 | 1 | |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | |

*una tabla en la que la columna del segundo miembro de la implicación es siempre verdadera, así que la implicación lo es en cada línea y con ello la fórmula es verdadera. Así también es* SATISFACIBLE.

$\forall x(P(x) \to \neg P(a))$ *es* SATISFACIBLE Y REFUTABLE. *Y puede probarse usando las mismas interpretaciones que en el anterior (aunque los resultados están intercambiados).*

$\exists x(P(x) \to \neg P(a))$ *es* SATISFACIBLE Y REFUTABLE. *En este caso los dos ejemplos de interpretaciones anteriores nos dan que la fórmula es* SATISFACIBLE. *¿Será universalmente válida? No, podemos forzar la estructura que tomemos de forma que haya una única línea en la tabla, así esta línea sería la de la constante $a$; por ejemplo tomando $D = \{0\}$, $P(x) \equiv$ "$x$ es par", $a = 0$ (claro, es la única elección posible), entonces nos queda:*

| $x$ | $P(x)$ | $\neg P(0)$ | $P(x) \to \neg P(a)$ | $\exists x(P(x) \to \neg P(a))$ |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |

*(la idea ha surgido cuando se observa que la línea correspondiente a la constante en los dos ejemplos anteriores da el valor $0$). Por tanto la fórmula también es* REFUTABLE.

$\forall x \neg(P(x) \to P(a))$ *es* CONTRADICCIÓN. *Como en el primer caso tenemos que intuir qué ocurre en la tabla:*

| $x$ | $P(x)$ | $P(a)$ | $P(x) \to P(a)$ | $\neg(P(x) \to P(a))$ | $\forall x \neg(P(x) \to P(a))$ |
|---|---|---|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | |
| $a$ | $I(P(a))$ | $I(P(a)$ | 1 | 0 | 0 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | | |

*y nos damos cuenta de que siempre aparecerá una línea (la que corresponde al valor de la constante) que nos da un cero que se transmite al cuantificador universal.*

$\exists x \neg(P(x) \to P(a))$ *es* SATISFACIBLE Y REFUTABLE. *De nuevo pueden usarse los ejemplos de interpretaciones del segundo caso.*

**Ejercicio 6.4.1.** *Prueba las siguientes afirmaciones:*

1. $\exists x P(x) \to P(a)$ *es satisfacible y refutable.*
2. $\forall x P(x) \to P(a)$ *es universalmente válida.*
3. $\forall x P(x) \to \neg P(a)$ *es satisfacible y refutable.*
4. $\exists x P(x) \to \neg P(a)$ *es satisfacible y refutable.*
5. $\exists x P(x) \to \forall x P(x)$ *es satisfacible y refutable.*
6. $\forall x P(x) \to \exists x P(x)$ *es universalmente válida.*

## 6.5. Consecuencia lógica

**Definición 59.** *Dado un conjunto de fórmulas $\Gamma \cup \{\varphi\}$ diremos que $\Gamma$ implica semánticamente a $\varphi$ o que $\varphi$ es consecuencia lógica de $\Gamma$ y se escribe*

$$\Gamma \models \varphi$$

*si para toda interpretación $I^v = (\mathcal{E}, v)$ que es un modelo para todas las fórmulas de $\Gamma$* **simultáneamente** *entonces $I^v$ también es un modelo para $\varphi$.*

**Ejemplo 6.5.1.** *Es cierta la afirmación*

$$\{\forall x P(x)\} \models P(a)$$

*puesto que cualquier interpretación que haga cierta la fórmula $\forall x P(x)$ necesariamente hace cierta la fórmula $P(a)$. Para convencernos observemos la siguiente tabla:*

| $x$ | $P(x)$ | $\forall x P(x)$ |
|---|---|---|
| $\vdots$ | 1 | |
| $a$ | 1 | 1 |
| $\vdots$ | 1 | |

*Para obtener 1 como resultado de la interpretación de la conectiva $\forall$ cada una de las líneas de $P(x)$ cuando $x$ recorre el dominio tiene que ser un 1, en particular la del valor que se le asigne a la constante $a$.*

**Ejemplo 6.5.2.** *Es cierta la afirmación*

$$\{P(a)\} \models \exists x P(x)$$

*puesto que cualquier interpretación que haga cierta la fórmula $P(a)$ necesariamente hace cierta la fórmula $\exists x P(x)$. En efecto, si esbozamos la tabla que nos permite calcular la interpretación de $\exists x P(x)$:*

| $x$ | $P(x)$ | $\exists x P(x)$ |
|---|---|---|
| $\vdots$ | $\vdots$ | |
| $a$ | 1 | 1 |
| $\vdots$ | $\vdots$ | |

*Para obtener* 1 *como resultado de la interpretación de la conectiva* $\exists$ *es suficiente que una de las líneas de* $P(x)$ *contenga un* 1*, lo que en este caso ocurre para el valor* $x = a$*.*

**Ejemplo 6.5.3.** *Para probar que*

$$\{\exists x P(x)\} \not\models P(a)$$

*es suficiente dar un* **ejemplo de interpretación** *para la que la premisa es cierta mientras que la conclusión es falsa. Así que la interpretación:* $D = \mathbb{Z}$*,* $a = 3$*,* $P(x) \equiv$*"x es par" hace que* $\exists x P(x)$ *sea verdadera, puesto que existen números pares en el dominio mientras que* $P(a) = P(3)$ *es falso porque* 3 *no es par.*

**Observación** Para el conjunto vacío, $\emptyset$, cualquier interpretación es un modelo.

Usando ahora el símbolo de consecuencia lógica, como en el tema anterior, podemos escribir el hecho de que una fórmula $\varphi$ sea universalmente válida de la siguiente forma:

$$\emptyset \models \varphi$$

Así mismo tendremos una útil herramienta para cambiar, cuando sea necesario, un problema de consecuencia lógica por otro más sencillo: el Teorema de la Deducción, que volvemos a enunciar para este contexto.

**Teorema 6.5.1. de la deducción** *Dado un conjunto de fórmulas* $\Gamma \cup \{\varphi, \psi\}$ *en un lenguaje de primer orden, son equivalentes las siguientes afirmaciones:*

1. $\Gamma \models \varphi \to \psi$,
2. $\Gamma \cup \{\varphi\} \models \psi$

Por ejemplo, usando este Teorema podemos afirmar que

$$\emptyset \models \forall x P(x) \to P(a)$$

es decir, que la fórmula es UNIVERSALMENTE VÁLIDA puesto que hemos probado que es cierta la afirmación

$$\{\forall x P(x)\} \models P(a)$$

### 6.5.1. Lema de coincidencia

Esta sección contiene un resultado formal que ya habíamos intuído cuando aprendimos a interpretar fórmulas. En el caso particular de que en una fórmula no haya **variables libres** para calcular una interpretación sólo necesitamos de la estructura y no de la valoración de valores a las variables.

**Lema 6.5.1.** *Sea* $\varphi$ *una fórmula y designemos por* $W = \{x_1, x_2, \ldots, x_n\}$ *al conjunto de las variables libre que aparecen en ella. Sea* $\mathcal{E}$ *una estructura; si* $v_1$ *y* $v_2$ *son dos valoraciones tales que*

$$v_1(x_1) = v_2(x_1); \quad v_1(x_2) = v_2(x_2); \quad \cdots \quad v_1(x_n) = v_2(x_n)$$

*entonces:*

$$I^{v_1}(\varphi) = I^{v_2}(\varphi)$$

Es decir, a la hora de interpretar una fórmula, no importa como actúe la valoración sobre las variables ligadas. Sólo tiene relevancia sobre las variables libres.

Como consecuencia, si la fórmula es una **sentencia**, es decir, una fórmula sin variables libres, entonces la valoración no es relevante para calcular la interpretación.

## 6.6. Consecuencia lógica y conjuntos insatisfacibles

Como en el tema anterior un conjunto de fórmulas se dice que es **insatisfacible** si no existe ninguna interpretación que haga ciertas simultáneamente todas las fórmulas del conjunto.

Un problema de consecuencia lógica se puede transformar en el de comprobar la insatisfacibilidad de un conjunto de fórmulas usando el siguiente resultado:

**Teorema 6.6.1.** *Sea $\Gamma \cup \{\varphi\}$ un conjunto de fórmulas en un lenguaje de primer orden. Entonces las siguientes afirmaciones son equivalentes:*

1. $\Gamma \models \varphi$,
2. $\Gamma \cup \{\neg\varphi\}$ *es insatisfacible.*

## 6.7. Algunas equivalencias lógicas

Pretendemos en estas notas dar una lista de equivalencias lógicas, que serán usadas posteriormente para hallar las formas normales de una fórmula. Vamos a tratar de estudiar como se comportan los cuantificadores $\forall$ y $\exists$ con respecto a los conectores lógicos $\neg$, $\vee$, $\wedge$, $\rightarrow$.

Dada una fórmula $\alpha$, denotaremos como $\alpha_{x|t}$ a la fórmula que resulta de sustituir cualquier ocurrencia libre de $x$ en $\alpha$ por el término $t$.

### 6.7.1. Negación y cuantificadores

Vamos, en primer lugar, a justificar que para cualquier fórmula $\alpha$, las fórmulas $\neg\forall x\alpha$ y $\exists x\neg\alpha$ son equivalentes.

Consideramos, por ejemplo, el enunciado *Todos los cuervos son negros*. Este enunciado podemos decirlo en un lenguaje de primer orden con la sentencia $\forall x N(x)$, donde el universo sería el conjunto de todos los cuervos, y el predicado $N(x)$ significa *$x$ es negro*.

¿Cuándo diríamos que este enunciado es falso?, o dicho de otra forma; ¿cómo podríamos decir *No todos los cuervos son negros*?

Obviamente, una forma de decirlo es mediante la fórmula $\neg\forall x N(x)$. Pero decir que no todos los cuervos son negros es lo mismo que decir que hay un cuervo que no es negro, es decir, se puede decir mediante la fórmula $\exists x\neg N(x)$.

Por tanto, las fórmulas $\neg\forall x N(x)$ y $\exists x\neg N(x)$ nos dicen en este caso lo mismo.

Nótese que el anterior enunciado podíamos haberlo traducido a un lenguaje de primer orden como $\forall x(C(x) \rightarrow N(x))$, donde ahora el predicado $C(x)$ significa *$x$ es cuervo*, y el universo podría ser el de todos los animales, o el de todos los seres vivos.

La negación diría ahora que existe un animal (o un ser vivo) que es cuervo y no es negro, es decir, $\exists x(C(x) \wedge \neg N(x))$. Sabemos que

$$\exists x(C(x) \wedge \neg N(x)) \equiv \exists x\neg(\neg C(x) \vee N(x)) \equiv \exists x\neg(C(x) \rightarrow N(x))$$

Es decir, las fórmulas $\neg\forall x\alpha$ y $\exists x\neg\alpha$, donde $\alpha = C(x) \rightarrow N(x)$ son equivalentes.

¿Es cierto que todos los primos son impares?. La respuesta es que no, pues existe un primo que no es impar (el 2).

Podemos también aproximarnos a esta equivalencia como sigue.

Supongamos que tenemos una fórmula de la forma $\forall x\alpha$, y tomamos una estructura donde el universo es finito. Supongamos que el universo es $\{a_1, a_2, \ldots, \alpha_n\}$. En tal caso, el cuantificador $\forall$ podría ser sustituido por un número finito de conectores $\wedge$, es decir:

$$\forall x\alpha \equiv \alpha_{x|a_1} \wedge \alpha_{x|a_2} \wedge \cdots \wedge \alpha_{x|a_n}$$

mientras que el cuantificador $\exists$ podría ser sustituido por un número finito de conectores $\vee$:

$$\exists x\alpha \equiv \alpha_{x|a_1} \vee \alpha_{x|a_2} \vee \cdots \vee \alpha_{x|a_n}$$

Tendríamos entonces que

$$\neg\forall x\alpha \equiv \neg(\alpha_{x|a_1} \wedge \alpha_{x|a_2} \wedge \cdots \wedge \alpha_{x|a_n}) \equiv \neg\alpha_{x|a_1} \vee \neg\alpha_{x|a_2} \vee \cdots \vee \neg\alpha_{x|a_n} \equiv \exists x\neg\alpha$$

Es decir, podríamos ver la equivalencia $\neg\forall x\alpha \equiv \exists x\neg\alpha$ como una generalización de la ley de De Morgan $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$.

**Ejemplo 6.7.1.** *Considermos el lenguaje de primer orden con tres símbolos de constante $a$, $b$, $c$ y un símbolo de predicado $P^1$. Sea $\alpha$ la fórmula $\forall xP(x)$ Tomamos una estructura en la que:*

$$\mathcal{U} = \mathbb{Z}_3; \qquad a \mapsto 0, \quad b \mapsto 1, \quad c \mapsto 2$$

*En este caso, la fórmula $\alpha$ es cierta si, y sólo si, lo es la fórmula $P(a) \wedge P(b) \wedge P(c)$. Por tanto, la fórmula $\neg\alpha$ será cierta si, y sólo si, lo es la fórmula $\neg(P(a) \wedge P(b) \wedge P(c)) \equiv \neg P(a) \vee \neg P(b) \vee \neg P(c)$, y esta fórmula será cierta si, y sólo si, lo es $\exists x\neg P(x)$.*

*Por ejemplo, asignemos el predicado $P$ de la siguiente forma:*

$$P(x) = \begin{cases} 1 & si\ x^2 = x \\ 0 & si\ x^2 \neq x \end{cases}$$

| $x$ | $P(x)$ | $\forall xP(x)$ | $\neg\forall xP(x)$ |
|---|---|---|---|
| 0 | 1 | 0 | 1 |
| 1 | 1 | | |
| 2 | 0 | | |

| $x$ | $P(x)$ | $\neg P(x)$ | $\exists x\neg P(x)$ |
|---|---|---|---|
| 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | |
| 2 | 0 | 1 | |

*La aparición de un 0 en la columna $P(x)$ de la primera tabla, hace que el valor de verdad de la fórmula $\forall xP(x)$ sea 0, y por tanto el valor de verdad de $\neg\forall xP(x)$ es 1.*

*La aparición de este 0 se traduce en un 1 en la columna $\neg P(x)$ de la segunda tabla, lo que da lugar a que el valor de verdad de $\exists x\neg P(x)$ sea 1.*

De la misma forma, si toda la columna $P(x)$ fuera 1, entonces $I(\forall xP(x)) = 1$, luego $I(\neg\forall xP(x)) = 0$. En este caso, toda la columna $\neg P(x)$ es cero, luego $I(\exists x\neg P(x)) = 0$.

| $P(a)$ | $P(b)$ | $P(c)$ | $P(a) \wedge P(b) \wedge P(c)$ | $\neg(P(a) \wedge P(b) \wedge P(c))$ |
|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 |

| $P(a)$ | $P(b)$ | $P(c)$ | $\neg P(a)$ | $\neg P(b)$ | $\neg P(c)$ | $\neg P(a) \vee \neg P(b) \vee \neg P(c)$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 | 1 | 1 |

Tenemos por tanto la equivalencia

$$\neg\forall x\alpha \equiv \exists x\neg\alpha.$$

De forma análoga se razona que

$$\neg\exists x\alpha \equiv \forall x\neg\alpha.$$

A partir de estas dos, obtenemos:

$$\forall x\alpha \equiv \neg\neg\forall x\alpha \equiv \neg\exists x\neg\alpha; \qquad \exists x\alpha \equiv \neg\neg\exists x\alpha \equiv \neg\forall x\neg\alpha$$

En resumen, tenemos las siguientes equivalencias:

1. $\neg\forall x\alpha \equiv \exists x\neg\alpha$.
2. $\neg\exists x\alpha \equiv \forall x\neg\alpha$.
3. $\neg\forall x\neg\alpha \equiv \exists x\alpha$.
4. $\neg\exists x\neg\alpha \equiv \forall x\alpha$.

### 6.7.2. Inclusión de $\vee$ o $\wedge$ en el radio de acción de un cuantificador (I)

Sean $\alpha$ y $\beta$ dos fórmulas, y consideramos la fórmula $\forall x\alpha \wedge \beta$. En este caso, la fórmula $\beta$ queda fuera del radio de acción del cuantificador $\forall x$. ¿Es posible introducir la fórmula $\beta$ dentro del radio de acción de $\forall x$?.

Vamos a suponer que el valor de verdad de $\beta$ no depende de la valoración que hagamos de la variable $x$. Sabemos que esta dependencia se da cuando había alguna ocurrencia libre de $x$ en $\beta$. Supondremos por tanto que esto no se da, es decir, la variable $x$ no aparece en la fórmula $\beta$, o las ocurrencias de $x$ en $\beta$ son ligadas.

En función de los valores de verdad de $\forall x\alpha$ y $\beta$ pueden darse los cuatro casos siguientes:

| $x$ | $\alpha$ | $\forall x\alpha$ | $\beta$ | $\forall x\alpha \wedge \beta$ | $\alpha \wedge \beta$ | $\forall x(\alpha \wedge \beta)$ |
|---|---|---|---|---|---|---|
| $\vdots$ | $*$ | 0 | 0 | 0 | 0 | 0 |
| $a_i$ | 0 | | | | 0 | |
| $\vdots$ | $*$ | | | | 0 | |
| $\vdots$ | $*$ | 0 | 1 | 0 | $*$ | 0 |
| $a_i$ | 0 | | | | 0 | |
| $\vdots$ | $*$ | | | | $*$ | |
| $a_1$ | 1 | 1 | 0 | 0 | 0 | 0 |
| $a_2$ | 1 | | | | 0 | |
| $\vdots$ | 1 | | | | 0 | |
| $a_i$ | 1 | | | | 0 | |
| $\vdots$ | 1 | | | | 0 | |
| $a_1$ | 1 | 1 | 1 | 1 | 1 | 1 |
| $a_2$ | 1 | | | | 1 | |
| $\vdots$ | 1 | | | | 1 | |
| $a_i$ | 1 | | | | 1 | |
| $\vdots$ | 1 | | | | 1 | |

donde $*$ significa que es indiferente el valor de verdad que tome.

Vemos que en los cuatro casos, $\forall x\alpha \wedge \beta$ y $\forall x(\alpha \wedge \beta)$ tienen el mismo valor de verdad.

De la misma forma se comprueba que si la variable $x$ no tiene ninguna ocurrencia libre en la fórmula $\beta$ se dan las siguientes equivalencias:

1. $\forall x\alpha \vee \beta \equiv \forall x(\alpha \vee \beta)$.
2. $\exists x\alpha \wedge \beta \equiv \exists x(\alpha \wedge \beta)$.
3. $\exists x\alpha \vee \beta \equiv \exists x(\alpha \vee \beta)$.

Nótese que, dado que $\alpha \vee \beta \equiv \beta \vee \alpha$ y $\alpha \wedge \beta \equiv \beta \wedge \alpha$ se tienen las siguientes equivalencias

1. $\alpha \wedge \forall x\beta \equiv \forall x(\alpha \wedge \beta)$.
2. $\alpha \vee \forall x\beta \equiv \forall x(\alpha \vee \beta)$.
3. $\alpha \wedge \exists x\beta \equiv \exists x(\alpha \wedge \beta)$.
4. $\alpha \vee \exists x\beta \equiv \exists x(\alpha \vee \beta)$.

El caso de que la variable $x$ tenga alguna ocurrencia libre en $\beta$ se estudiará más adelante. El siguiente ejemplo nos muestra, no obstante que el resultado no es cierto.

**Ejemplo 6.7.2.** *Sean las fórmulas*
$\varphi = \forall x(C(x,a) \to U(x)) \wedge P(x)$
$\phi = \forall x((C(x,a) \to U(x)) \wedge P(x))$.
*Consideramos la estructura siguiente:*

$$\mathcal{U} = \mathbb{Z}_5; \qquad a \mapsto 1; \qquad C(x,y) = \begin{cases} 1 & si\ x^2 = y \\ 0 & si\ x^2 \neq y \end{cases}$$

$$U(x) = \begin{cases} 1 & si\ x\ es\ unidad \\ 0 & si\ x\ no\ es\ unidad \end{cases} \qquad P(x) = \begin{cases} 1 & si\ x^2 = x \\ 0 & si\ x^2 \neq x \end{cases}$$

*Para la valoración $v(x) = 0$ los valores de verdad de ambas fórmulas son:*

| $x$ | $C(x,a)$ | $U(x)$ | $C(x,a) \to U(x)$ | $\forall x(C(x,a) \to U(x))$ | $P(x)_{\ x=0}$ | $\varphi$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | | | |
| 1 | 1 | 1 | 1 | | | |
| 2 | 0 | 1 | 1 | 1 | 1 | 1 |
| 3 | 0 | 1 | 1 | | | |
| 4 | 1 | 1 | 1 | | | |

| $x$ | $C(x,a)$ | $U(x)$ | $C(x,a) \to U(x)$ | $P(x)$ | $(C(x,a) \to U(x)) \wedge P(x)$ | $\phi$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 1 | |
| 1 | 1 | 1 | 1 | 1 | 1 | |
| 2 | 0 | 1 | 1 | 0 | 0 | 0 |
| 3 | 0 | 1 | 1 | 0 | 0 | |
| 4 | 1 | 1 | 1 | 0 | 0 | |

*Vemos entonces que no son equivalentes.*

**Ejercicio:**
Da ejemplos que muestren que en general no son ciertas las equivalencias

1. $\forall x\alpha \vee \beta \equiv \forall x(\alpha \vee \beta)$.
2. $\exists x\alpha \wedge \beta \equiv \exists x(\alpha \wedge \beta)$.
3. $\exists x\alpha \vee \beta \equiv \exists x(\alpha \vee \beta)$.

**Ejercicio:**
Comprueba que si la variable $x$ no tiene ninguna ocurrencia libre en $\beta$ entonces $\beta \to \forall x\alpha \equiv \forall x(\beta \to \alpha)$, pero que en general $\forall x\alpha \to \beta$ no es equivalente a $\forall x(\alpha \to \beta)$.

**Ejercicio:**
Busca una fórmula equivalente a $\forall x\alpha \to \beta$ de forma que el radio de acción del cuantificador incluya a $\beta$.

**Ejercicio:**
Repite el ejercicio anterior con las fórmulas $\exists x\alpha \to \beta$ y $\beta \to \exists x\alpha$.

### 6.7.3. Sacar factor común

Ahora nos encontramos con fórmulas de la forma $\forall x\alpha \wedge \forall x\beta$ y $\forall x\alpha \vee \forall x\beta$. Nos preguntamos si son equivalentes a las fórmulas $\forall x(\alpha \wedge \beta)$ y $\forall x(\alpha \vee \beta)$ respectivamente. Es decir, tratamos de "sacar factor común" $\forall x$.

Enseguida podemos darnos cuenta que en el segundo caso no es posible. Consideramos los enunciados:
*Todo número entero es par o impar.*
*Todo número entero es par o todo número entero es impar.*
El primer enunciado es claramente cierto, mientras que el segundo no (pues no todo número entero es par ni todo número entero es impar). Basta encontrar una traducción a un lenguaje de primer orden de ambos enunciados, que adopten la forma $\forall x(\alpha \vee \beta)$ y $\forall x\alpha \vee \forall x\beta$ para convencernos de que no son equivalentes.

Para comprobar que en el primer caso sí se da la equivalencia, vamos a construir una tabla como en la sección anterior.

| $x$ | $\alpha$ | $\beta$ | $\alpha \wedge \beta$ | $\forall x\alpha$ | $\forall x\beta$ | $\forall x\alpha \wedge \forall x\beta$ | $\forall x(\alpha \wedge \beta)$ |
|---|---|---|---|---|---|---|---|
| $\vdots$ | $*$ | $*$ | $*$ | | | | |
| $a_i$ | 0 | $*$ | 0 | | | | |
| $\vdots$ | $*$ | $*$ | $*$ | 0 | 0 | 0 | 0 |
| $a_j$ | $*$ | 0 | 0 | | | | |
| $\vdots$ | $*$ | $*$ | $*$ | | | | |
| $\vdots$ | $*$ | 1 | $*$ | | | | |
| $a_i$ | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| $\vdots$ | $*$ | 1 | $*$ | | | | |
| $\vdots$ | 1 | $*$ | $*$ | | | | |
| $a_i$ | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| $\vdots$ | 1 | $*$ | $*$ | | | | |
| $\vdots$ | 1 | 1 | 1 | | | | |
| $a_i$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\vdots$ | 1 | 1 | 1 | | | | |

Basándonos en esta equivalencia ($\forall x(\alpha \wedge \beta) \equiv \forall x\alpha \wedge \forall x\beta$), en las vistas en la primera sección y en las leyes de De Morgan obtenemos:

$$\exists x\alpha \vee \exists x\beta \equiv \neg\neg(\exists x\alpha \vee \exists x\beta) \equiv \neg(\neg\exists x\alpha \wedge \neg\exists x\beta) \equiv \neg(\forall x\neg\alpha \wedge \forall x\neg\beta) \equiv$$
$$\equiv \neg(\forall x(\neg\alpha \wedge \neg\beta)) \equiv \neg\forall x\neg(\alpha \vee \beta) \equiv \exists x\neg\neg(\alpha \vee \beta) \equiv \exists x(\alpha \vee \beta)$$

**Ejercicio:**
Busca un ejemplo que muestre que $\exists x\alpha \wedge \exists x\beta$ y $\exists x(\alpha \wedge \beta)$ no son equivalentes.
**Ejercicio:**
Estudia si alguna de las siguientes fórmulas puede transformarse en alguna equivalente con un único cuantificador.

1. $\forall x\alpha \to \forall x\beta$.
2. $\forall x\alpha \to \exists x\beta$.
3. $\exists x\alpha \to \forall x\beta$.
4. $\exists x\alpha \to \exists x\beta$.

### 6.7.4. Cambio de variable

Sabemos que al interpretar una fórmula con una variable ligada, el valor que se le dé a dicha variable no interviene en la interpretación. Es decir, la variable en cuestión no es significativa. Nos preguntamos si una variable ligada podría ser cambiada por otra.

El siguiente ejemplo sencillo nos muestra que no siempre puede hacerse así:

**Ejemplo 6.7.3.** *Sea la fórmula $\exists z\forall xP(x,y,z)$, consideramos la estructura siguiente:*

$$\mathcal{U} = \mathbb{Z}_3; \qquad P(x,y,z) := \begin{cases} 1 & si\ xy = z \\ 0 & si\ xy \neq z \end{cases}$$

*Con la valoración $v(x) = 1$, $v(y) = 0$, $v(z) = 1$ se tiene:*

| $z$ | $x$ | $P(x,y,z)_{y=0}$ | $\forall x P(x,y,z)$ | $\exists z \forall x P(x,y,z)$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 |
| | 1 | 1 | | |
| | 2 | 1 | | |
| 1 | 0 | 0 | 0 | |
| | 1 | 0 | | |
| | 2 | 0 | | |
| 2 | 0 | 0 | 0 | |
| | 1 | 0 | | |
| | 2 | 0 | | |

*Si cambiamos $x$ por $y$, tenemos la fórmula $\exists z \forall y P(y,y,z)$, en cuyo caso tenemos*

| $z$ | $y$ | $P(y,y,z)$ | $\forall y P(y,y,z)$ | $\exists z \forall y P(y,y,z)$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 |
| | 1 | 0 | | |
| | 2 | 0 | | |
| 1 | 0 | 0 | 0 | |
| | 1 | 1 | | |
| | 2 | 0 | | |
| 2 | 0 | 0 | 0 | |
| | 1 | 0 | | |
| | 2 | 0 | | |

*El problema aquí es que la variable $y$ por la que cambiamos la $x$ ya aparece en la fórmula.*

*Supongamos que $\alpha$ es una fórmula en la que no hay ninguna ocurrencia de la variable $y$ (ni libre ni ligada).*

*Entonces $\forall x\alpha \equiv \forall y \alpha_{x|y}$, y $\exists x\alpha \equiv \exists y \alpha_{x|y}$.*

### 6.7.5. Inclusión de $\vee$ o $\wedge$ en el radio de acción de un cuantificador (II)

En la sección segunda estudiamos cómo incluir los conectores $\vee$ o $\wedge$ dentro del radio de acción de un cuantificador. Necesitábamos entonces que en una fórmula, una determinada variable no tuviera ocurrencias libres.

Supongamos ahora que tenemos una fórmula de la forma $\forall x\alpha \wedge \beta$, y que ahora la variable $x$ aparece libremente en $\beta$. Entonces elegimos una variable que no tenga ninguna ocurrencia (ni libre ni ligada) en $\alpha$ ni ninguna ocurrencia libre en $\beta$. Sea ésta variable $y$. Entonces, sabemos que $\forall x\alpha \equiv \forall y \alpha_{x|y}$.

Entonces, la fórmula de partida es equivalente a $\forall y \alpha_{x|y} \wedge \beta$, y ésta, a su vez es equivalente a $\forall y(\alpha_{x|y} \wedge \beta)$.

De esta forma, ya hemos incluido el conector $\wedge$ en el radio de acción del cuantificador.

**Ejemplo 6.7.4.** *Sea $\varphi = \forall x P(x) \vee \exists y Q(x,y)$*

*Puesto que la variable $z$ no aparece en $P(x)$ ni en $\exists y Q(x,y)$, se tiene que*

$$\varphi \equiv \forall z P(z) \vee \exists y Q(x,y) \equiv \forall z (P(z) \vee \exists y Q(x,y)).$$

*Nos fijamos ahora en $P(z) \vee \exists y Q(x,y)$. Puesto que la variable $y$ no aparece en $P(z)$, ésta fórmula es equivalente a $\exists y(P(z) \vee Q(x,y))$.*

*Con esto, concluimos que*

$$\varphi \equiv \forall z \exists y (P(z) \vee Q(x,y)).$$

*Nótese que en un principio podríamos haber sustituido la variable $x$ por la variable $y$ (ya que $y$ no aparece en $P(x)$, y su única ocurrencia en $\exists y Q(x,y)$ es ligada). En tal caso, tendríamos*

$$\varphi \equiv \forall y P(y) \vee \exists y Q(x,y) \equiv \forall y (P(y) \vee \exists y Q(x,y))$$

*Ahora, al centrarnos en $P(y) \vee \exists y Q(x,y)$ necesitamos hacer un cambio de variable, pues la variable $y$ tiene una ocurrencia libre en $P(y)$. Nos queda entonces:*

$$\varphi \equiv \forall y(P(y) \vee \exists y Q(x,y)) \equiv \forall y(P(y) \vee \exists z Q(x,z)) \equiv \forall y \exists z(P(y) \vee Q(x,z))$$

*También podríamos haber procedido como sigue:*

$$\varphi \equiv \exists y(\forall x P(x) \vee Q(x,y)) \equiv \exists y(\forall z P(z) \vee Q(x,y)) \equiv \exists y \forall z(P(z) \vee Q(x,y))$$

*Notemos que nos ha salido que*

$$\varphi \equiv \forall z \exists y(P(z) \vee Q(x,y)) \equiv \exists y \forall z(P(z) \vee Q(x,y))$$

*lo cual podría inducirnos a error, pues podría parecer que es posible intercambiar los cuantificadores.*

**Ejercicio:**
Calcula el valor de verdad de las fórmulas $\forall x \exists y P(x,y)$ y $\exists y \forall x P(x,y)$ en la estructura con universo $\mathcal{U} = \mathbb{Z}$, y $P(x,y) \equiv x = -y$.

### 6.7.6. Eliminación de cuantificadores

Consideramos la fórmula $\forall x \exists x P(x)$
Sea $\mathcal{U} = \mathbb{Z}_2$, y $P = \{1\}$. Entonces:

| $x$ | $x$ | $P(x)$ | $\exists x P(x)$ | $\forall x \exists x P(x)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 |
| | 1 | 1 | | |
| 1 | 0 | 0 | 1 | |
| | 1 | 1 | | |

Vemos que lo realmente importante es la interpretación de la fórmula $\exists x P(x)$. Es decir, el cuantificador $\forall x$ podríamos eliminarlo.

En general, si $C_1$ y $C_2$ son dos cuantificadores (podrían coincidir), y $\alpha$ es una fórmula, entonces las fórmulas $C_1 x C_2 x \alpha$ y $C_2 x \alpha$ son equivalentes (si en una fórmula, una ocurrencia de una variable está cuantificada dos veces, el cuantificador que aparece más a la izquierda no influye sobre ella).

### 6.7.7. Resumen

Como resumen de todo esto, nos quedamos con la siguiente lista de equivalencias:

1. $\neg\forall x\alpha \equiv \exists x\neg\alpha$.
2. $\neg\exists x\alpha \equiv \forall x\neg\alpha$.
3. $\forall x\alpha \wedge \beta \equiv \forall x(\alpha \wedge \beta)$ si $x$ no es libre en $\beta$.
4. $\forall x\alpha \vee \beta \equiv \forall x(\alpha \vee \beta)$ si $x$ no es libre en $\beta$.
5. $\exists x\alpha \wedge \beta \equiv \exists x(\alpha \wedge \beta)$ si $x$ no es libre en $\beta$.
6. $\exists x\alpha \vee \beta \equiv \exists x(\alpha \vee \beta)$ si $x$ no es libre en $\beta$.
7. $\forall x\alpha \wedge \forall x\beta \equiv \forall x(\alpha \wedge \beta)$.
8. $\exists x\alpha \vee \exists x\beta \equiv \exists x(\alpha \vee \beta)$.
9. $\forall x\alpha \equiv \forall y\alpha_{x|y}$ si $y$ no aparece en la fórmula $\alpha$.
10. $\exists x\alpha \equiv \exists y\alpha_{x|y}$ si $y$ no aparece en la fórmula $\alpha$.
11. $\forall x\forall x\alpha \equiv \forall x\alpha$.
12. $\forall x\exists x\alpha \equiv \exists x\alpha$.
13. $\exists x\forall x\alpha \equiv \forall x\alpha$.
14. $\exists x\exists x\alpha \equiv \exists x\alpha$.

# Capítulo 7

# Formas Normales

## 7.1. Formas normales

En esta sección vamos a tratar de obtener, a partir de una sentencia (una fórmula en la que no aparecen variables libres), una fórmula más sencilla para el tratamiento posterior. La forma que necesitamos es la **forma clausular** y son pasos previos las formas prenexa y de Skolem.

### 7.1.1. Forma normal prenexa.

Para este apartado, no necesitamos que la fórmula sea una sentencia.
Una fórmula se dice que está en forma prenexa si se escribe:

$$C_1 x_1 C_2 x_2 \dots C_n x_n \Phi$$

donde $C_i$ es un cuantificador (universal o existencial) y $\Phi$ es una fórmula sin cuantificadores.

**Ejemplo 7.1.1.**

1. $\forall x(H(x) \wedge Q(x,a))$
2. $\exists x \forall y(P(x,y) \vee Q(b))$
3. $\forall x \exists y(P(x,y) \rightarrow Q(b))$
4. $H(a)$
5. $\exists x H(x)$
6. $\forall x \exists y \exists z R(x,y,z)$

### 7.1.2. Método para calcular la forma prenexa de una fórmula

Para esto, utilizaremos las equivalencias explicadas en *Algunas equivalencias lógicas*, y que recordaremos a continuación, así como las equivalencias dadas en el tema primero cuando estudiamos la lógica proposicional.

1. $\neg \forall x \alpha \equiv \exists x \neg \alpha$.
2. $\neg \exists x \alpha \equiv \forall x \neg \alpha$.
3. $\forall x \alpha \wedge \beta \equiv \forall x(\alpha \wedge \beta)$ si $x$ no es libre en $\beta$.
4. $\forall x \alpha \vee \beta \equiv \forall x(\alpha \vee \beta)$ si $x$ no es libre en $\beta$.
5. $\exists x \alpha \wedge \beta \equiv \exists x(\alpha \wedge \beta)$ si $x$ no es libre en $\beta$.

6. $\exists x\alpha \vee \beta \equiv \exists x(\alpha \vee \beta)$ si $x$ no es libre en $\beta$.
7. $\forall x\alpha \wedge \forall x\beta \equiv \forall x(\alpha \wedge \beta)$.
8. $\exists x\alpha \vee \exists x\beta \equiv \exists x(\alpha \vee \beta)$.
9. $\forall x\alpha \equiv \forall y\alpha_{x|y}$ si $y$ no aparece en la fórmula $\alpha$.
10. $\exists x\alpha \equiv \exists y\alpha_{x|y}$ si $y$ no aparece en la fórmula $\alpha$.
11. $\forall x\alpha \equiv \alpha$ si $x$ no es libre en $\alpha$.
12. $\exists x\alpha \equiv \alpha$ si $x$ no es libre en $\alpha$.
13. $\forall x\forall y\alpha \equiv \forall y\forall x\alpha$.
14. $\exists x\exists y\alpha \equiv \exists y\exists x\alpha$.

**Ejemplo 7.1.2.**

**1** $\forall x S(x) \to \exists z\forall y R(z,y)$

*Sustituimos la implicación*

*a)* $\neg\forall x S(x) \vee \exists z\forall y R(z,y)$

*Intercambiamos cuantificador y negación (equivalencia primera)*

*b)* $\exists x\neg S(x) \vee \exists z\forall y R(z,y)$

*Llegados aquí tenemos tres opciones para continuar. Analicemos las tres:*

**Opción 1**

*Puesto que la variable $x$ no es libre en la fórmula $\exists z\forall y R(z,y)$, podemos incluirla dentro del radio de acción de $\exists x$ (equivalencia sexta).*

*c-1)* $\exists x(\neg S(x) \vee \exists z\forall y R(z,y))$.

*Como no hay ninguna ocurrencia libre de $z$ en $\neg S(x)$, introducimos $\neg S(x)$ en el radio de acción de $\exists z$ (equivalencia sexta).*

*d-1)* $\exists x\exists z(\neg S(x) \vee \forall y R(z,y))$.

*Y como la variable $y$ no aparece en $\neg S(x)$, podemos introducirla, en virtud de la equivalencia cuarta, en el radio de acción de $\forall y$.*

*e-1)* $\exists x\exists z\forall y(\neg S(x) \vee R(z,y))$.

*Y llegamos así a una fórmula, equivalente a la de partida, que se encuentra en forma prenexa.*

**Opción 2**

*Introducimos $\exists x\neg S(x)$ en el radio de acción de $\exists z$, lo que podemos hacer pues la variable $z$ no aparece de forma libre en $\exists x\neg S(x)$*

*c-2)* $\exists z(\exists x\neg S(x) \wedge \forall y R(z,y))$.

*Repetimos lo mismo con $\forall y$.*

*d-2)* $\exists z\forall y(\exists x\neg S(x) \wedge R(z,y))$.

*Y por último introducimos $R(z,y)$ en el radio de acción de $\exists x$.*

*e-2)* $\exists z\forall y\exists x(\neg S(x) \wedge R(z,y))$.

**Opción 3**

*Puesto que tenemos la disyunción de dos fórmulas, ambas iniciadas con el cuantificador $\exists$, renombramos las variables para poder hacer uso de la equivalencia octava. En este caso, cambiamos la variable $z$ por $x$ (equivalencia décima), ya que $x$ no aparece en la fórmula $R(z,y)$.*

*c-3)* $\exists x\neg S(x) \vee \exists x\forall y R(x,y)$.

*"Sacamos factor común" $\exists x$ (equivalencia octava)*

*d-3)* $\exists x(\neg S(x) \vee \forall y R(x,y))$

*Por último, como $y$ no es libre en la fórmula $\neg S(x)$, podemos desplazar el cuantificador correspondiente (equivalencia cuarta).*

*e-3)* $\exists x \forall y(\neg S(x) \vee R(x,y))$.

*Las tres fórmulas son equivalentes, y están en forma prenexa. Sin embargo, la última es más sencilla al aparecer en ella menos cuantificadores y menos variables. Y de las dos primeras, aunque aparentemente tienen la misma forma, es mejor la primera, pues los cuantificadores existenciales se encuentran más a la izquierda que en la segunda. En el siguiente apartado, veremos el porqué de esta última afirmación.*

**2** $\forall x(R(x,y) \wedge \neg \forall y R(x,y))$

*Nótese que esta fórmula no es una sentencia pues la primera aparición de la variable y es libre. Veremos, no obstante, como obtener una forma normal prenexa.*

*Al obtener la forma prenexa, las variables que tenga una ocurrencia libre, seguirán siendo libres en la forma prenexa.*

*Intercambiamos la negación y el cuantificador (equivalencia primera)*

*a)* $\forall x(R(x,y) \wedge \exists y \neg R(x,y))$

*La variable y es libre en la fórmula $R(x,y)$ así que no puede incluirse en el radio de acción de un cuantificador con la misma variable. Renombramos entonces la variable y como z (equivalencia décima)*

*b)* $\forall x(R(x,y) \wedge \exists z \neg R(x,z))$

*Desplazamos el cuantificador $\exists z$ (equivalencia quinta)*

*c)* $\forall x \exists z(R(x,y) \wedge \neg R(x,z))$

*Y obtenemos y una forma normal prenexa. La ocurrencia libre de y se ha mantenido, mientras que la ocurrencia ligada se ha sustituido por otra variable (z) que sigue estando cuantificada.*

**3** $\exists x R(x,y) \vee [\forall x S(x) \wedge \neg \exists z R(a,z)]$

*Intercambiamos negación y cuantificador (equivalencia segunda).*

*a)* $\exists x R(x,y) \vee [\forall x S(x) \wedge \forall z \neg R(a,z)]$

*Tenemos ahora la conjunción de dos fórmulas que se inician con $\forall$. Si renombramos las variables de forma que tengamos la misma en ambas, podremos reducir un cuantificador. Por tanto, y puesto que en $R(a,z)$ no aparece la variable x, cambiamos la z por x (equivalencia novena)*

*b)* $\exists x R(x,y) \vee [\forall x S(x) \wedge \forall x \neg R(a,x)]$

*Y ahora, por la equivalencia séptima obtenemos*

*c)* $\exists x R(x,y) \vee \forall x(S(x) \wedge \neg R(a,x))$

*También aquí podemos tomar dos caminos:*

**Opción 1**

*Como x no es libre en $\forall x(S(x) \wedge \neg R(a,x))$, podemos incluirlo en el radio de acción de $\exists x$*

*d-1)* $\exists x(R(x,y) \vee \forall x(S(x) \wedge \neg R(a,x)))$

*Pero ahora no podemos incluir $R(x,y)$ en el radio de acción de $\forall x$, pues la ocurrencia de x en $R(x,y)$ es libre (aunque no lo sea en la fórmula total). Renombramos entonces la variable x de $\exists x$ por z (también podríamos cambiar $\forall x$ por $\forall z$, y el resultado sería el mismo). En tal caso, en el radio de acción de $\exists x$, es decir, en $R(x,y) \vee \forall x(S(x) \wedge \neg R(a,x))$ debemos sustituir todas las ocurrencias libres de x por z. Nos queda entonces (equivalencia décima)*

*e-1)* $\exists z(R(z,y) \vee \forall x(S(x) \wedge \neg R(a,x)))$

*Nótese que las apariciones de x en $S(x)$ y $R(a,x)$ son ligadas, por tanto no se realiza ninguna sustitución.*

*Ahora ya sí podemos incluir $R(z,y)$ dentro del radio de acción de $\forall x$ (equivalencia cuarta)*

*f-1)* $\exists z \forall x(R(z,y) \vee (S(x) \wedge \neg R(a,x)))$.

*Que está en forma prenexa.*

**Opción 2**

*Como x no es libre en $\exists x R(x,y)$, por la equivalencia cuarta tenemos*

*d-2)* $\forall x(\exists x R(x,y) \vee (S(x) \wedge \neg R(a,x)))$.

*Al ser la variable $x$ libre en $S(x) \wedge \neg R(a,x)$, cambiamos $x$ por $z$ (equivalencia décima)*

*e-2)* $\forall x(\exists z R(z,y) \vee (S(x) \wedge \neg R(a,x)))$.

*Y ahora sí podemos introducir $S(x) \wedge \neg R(a,x)$ en el radio de acción de $\exists z$ (equivalencia sexta).*

*f-2)* $\forall x \exists z(R(z,y) \vee (S(x) \wedge \neg R(a,x)))$.

*Si comparamos las dos fórmulas que nos han salido, vemos que la única diferencia está en el orden de los cuantificadores. En general, no es posible intercambiar los cuantificadores $\forall$ y $\exists$, aunque como vemos en este caso, en ocasiones sí pueden ser intercambiados. En general, esto podrá hacerse cuando las variables cuantificadas con $\forall$ y $\exists$ no aparezcan en un mismo predicado.*

*De las dos formas prenexas que nos han salido, aunque son equivalentes, es preferible quedarnos con la primera, pues al hacer la forma de Skolem nos va a resultar una fórmula más sencilla.*

**4** $\forall x \forall z(\forall z P(x,z) \wedge \forall x P(x,z)) \rightarrow \forall x(\exists y P(x,y) \wedge \forall x Q(x))$

*Comenzamos sustituyendo la implicación.*

*a)* $\neg \forall x \forall z(\forall z P(x,z) \wedge \forall x P(x,z)) \vee \forall x(\exists y P(x,y) \wedge \forall x Q(x))$

*Intercambiamos cuantificador y negación (equivalencia primera). Hacemos esto dos veces.*

*b)* $\exists x \exists z \neg(\forall z P(x,z) \wedge \forall x P(x,z)) \vee \forall x(\exists y P(x,y) \wedge \forall x Q(x))$

*Con las leyes de De Morgan*

*c)* $\exists x \exists z(\neg \forall z P(x,z) \vee \neg \forall x P(x,z)) \vee \forall x(\exists y P(x,y) \wedge \forall x Q(x))$

*Otra vez intercambiamos cuantificador y negación*

*d)* $\exists x \exists z(\exists z \neg P(x,z) \vee \exists x \neg P(x,z)) \vee \forall x(\exists y P(x,y) \wedge \forall x Q(x))$

*Vamos a seguir dos caminos a partir de aquí (que realmente podrían ser 4, pues inicialmente vamos a trabajar independientemente las dos partes de la fórmula).*

**Opción 1**

*Puesto que la variable $z$ aparece libre en $\exists x \neg P(x,z)$, sustituimos $z$ por otra variable que no puede ser $x$. Tomamos, por ejemplo, $y$.*

*En la segunda parte de la fórmula, introducimos $\forall x Q(x)$ en el radio de acción de $\exists y$.*

*e-1)* $\exists x \exists z(\exists y \neg P(x,y) \vee \exists x \neg P(x,z)) \vee \forall x(\exists y(P(x,y) \wedge \forall x Q(x)))$

*Introducimos $\exists x \neg P(x,z)$ en el radio de acción de $\exists y$ (equivalencia sexta) y renombramos la variable $x$ en $\forall x Q(x)$ (equivalencia novena).*

*f-1)* $\exists x \exists z(\exists y(\neg P(x,y) \vee \exists x \neg P(x,z))) \vee \forall x \exists y(P(x,y) \wedge \forall z Q(z))$

*Renombramos la variable $x$ de $\exists x \neg P(x,z)$ (no podemos usar ni $y$ ni $z$) e introducimos $P(x,y)$ en el radio de acción de $\forall z$.*

*g-1)* $\exists x \exists z \exists y(\neg P(x,y) \vee \exists t \neg P(t,z)) \vee \forall x \exists y \forall z(P(x,y) \wedge Q(z))$

*Extendemos $\exists t$ hasta $\neg P(x,y)$ (equivalencia sexta)*

*h-1)* $\exists x \exists z \exists y \exists t(\neg P(x,y) \vee \neg P(t,z)) \vee \forall x \exists y \forall z(P(x,y) \wedge Q(z))$

*Renombramos las variables de la segunda parte de la fórmula (equivalencias novena y décima)*

*i-1)* $\exists x \exists z \exists y \exists t(\neg P(x,y) \vee \neg P(t,z)) \vee \forall u \exists v \forall w(P(u,v) \wedge Q(w))$

*Y ahora, en siete pasos, introducimos todo en el radio de acción de los cuantificadores.*

*j-1)* $\exists x \exists z \exists y \exists t \forall u \exists v \forall w(\neg P(x,y) \vee \neg P(t,z)) \vee (P(u,v) \wedge Q(w))$

*Aunque al estar unidas ambas fórmulas por un conector $\vee$ podríamos haber procedido, desde h-1), como sigue:*

*i-1)* $\exists x \exists z \exists y \exists t(\neg P(x,y) \vee \neg P(t,z)) \vee \forall u \exists t \forall w(P(u,t) \wedge Q(w))$

*j-1)* $\exists x \exists z \exists y(\exists t(\neg P(x,y) \vee \neg P(t,z)) \vee \forall u \exists t \forall w(P(u,t) \wedge Q(w)))$

*k-1)* $\exists x \exists z \exists y \forall u(\exists t(\neg P(x,y) \vee \neg P(t,z)) \vee \exists t \forall w(P(u,x) \wedge Q(w)))$

*l-1)* $\exists x \exists z \exists y \forall u \exists t((\neg P(x,y) \vee \neg P(t,z)) \vee \forall w(P(u,x) \wedge Q(w)))$

*m-1)* $\exists x\exists z\exists y\forall u\exists t\forall w((\neg P(x,y)\vee\neg P(t,z))\vee(P(u,x)\wedge Q(w)))$

**Opción 2**

*En la primera parte de la fórmula hacemos uso de la equivalencia sexta, pero en sentido inverso al que lo hemos hecho habitualmente (la variable $z$ no es libre en $\exists z\neg P(x,z)$), mientras que en la segunda parte usamos la séptima (también en sentido inverso al usado en otras ocasiones).*

*e-2)* $\exists x(\exists z\neg P(x,z)\vee\exists z\exists x\neg P(x,z))\vee(\forall x\exists y P(x,y)\wedge\forall x\forall x Q(x))$

*Ahora, en la primera parte repetimos lo que acabamos de hacer, mientras que en la segunda parte hacemos uso de la undécima equivalencia*

*f-2)* $(\exists x\exists z\neg P(x,z)\vee\exists z\exists x\neg P(x,z))\vee(\forall x\exists y P(x,y)\wedge\forall x Q(x))$

*Las equivalencias décimo cuarta y séptima nos transforman esta fórmula en:*

*g-2)* $(\exists x\exists z\neg P(x,z)\vee\exists x\exists z\neg P(x,z))\vee\forall x(\exists y P(x,y)\wedge Q(x))$

*Y ahora, como $\alpha\vee\alpha\equiv\alpha$, y por la equivalencia quinta tenemos:*

*h-2)* $\exists x\exists z\neg P(x,z)\vee\forall x\exists y(P(x,y)\wedge Q(x))$

*Renombramos las variables en la segunda parte:*

*i-2)* $\exists x\exists z\neg P(x,z)\vee\forall y\exists z(P(y,z)\wedge Q(y))$

*j-2)* $\exists x\forall y(\exists z\neg P(x,z)\vee\exists z(P(y,z)\wedge Q(y)))$

*k-2)* $\exists x\forall y\exists z(\neg P(x,z)\vee(P(y,z)\wedge Q(y)))$.

Tras estos ejemplos, no es difícil ver que se tiene el siguiente teorema.

**Teorema 7.1.1.** *Para toda fórmula existe otra que es lógicamente equivalente con ella y está en forma normal prenexa.*

### 7.1.3. Forma normal de Skolem

Una fórmula está en forma normal de Skolem si está en forma prenexa y en ella no aparecen cuantificadores existenciales. Por tanto una fórmula en forma de Skolem tiene la apariencia

$$\forall x_1\forall x_2\ldots\forall x_n\Phi$$

donde $\Phi$ es una fórmula sin cuantificadores.

**Ejemplo 7.1.3.** *Las siguientes fórmulas están en forma de Skolem.*

1. $\forall x(H(x)\wedge Q(x,a))$
2. $\forall y(P(a,y)\vee Q(b))$
3. $\forall x(P(x,f(x))\rightarrow Q(b))$
4. $\forall x\forall y(Q(x,y)\rightarrow H(x))$
5. $H(b)$
6. $\forall x R(x,f(x),g(x))$

### 7.1.4. Método para calcular una forma de Skolem de una fórmula en forma prenexa

En general, no para toda fórmula existe otra que sea equivalente a ella y que esté en forma de Skolem. Entonces, si queremos calcular una forma de Skolem vamos a tener que perder la equivalencia.

Recordemos que nuestro problema a resolver era estudiar si un conjunto de fórmulas es o no satisfacible.

Vamos entonces a transformar cada fórmula de un conjunto dado en otra que esté en forma de Skolem, de forma que, aunque no sea equivalente podamos asegurar que el conjunto inicial es satisfacible si, y sólo si, lo es el conjunto con las fórmulas transformadas.

Para esto, sólo hay que aprender cómo eliminar los cuantificadores existenciales. Para ello cada variable cuantificada existencialmente se va a sustituir por un **término** al mismo tiempo que se elimina el cuantificador correspondiente. El término por el que se sustituye será:

**Caso 1** Un símbolo de constante si el cuantificador existencial que la acompaña no va precedido por ningún cuantificador universal. El nombre del símbolo debe ser elegido entre los que no aparezcan en la fórmula (o en el conjunto de fórmulas que se maneje).

**Caso 2** Un símbolo de función cuya ariedad sea igual al número de variables cuantificadas universalmente y que precedan a la variable a sustituir. La función debe aplicarse a todas estas variables, y el símbolo elegido no puede aparecer en la fórmula ni en el conjunto de fórmulas que se maneje.

**Ejemplo 7.1.4.**

1. $\exists x \forall y(\neg S(x) \vee R(x,y))$.

   *Como el cuantificador existencial no va precedido por ninguno universal estamos en el Caso 1 y la variable correspondiente, $x$, se sustituye por una constante que no aparezca en la fórmula, por ejemplo $a$; entonces la forma de Skolem queda*

   $$\forall y(\neg S(a) \vee R(a,y))$$

2. $\forall x \exists z(R(x,y) \wedge \neg R(x,z))$.

   *Como el cuantificador existencial va precedido por uno universal estamos en el Caso 2, elegimos un símbolo de función que no aparezca, por ejemplo $f$ y sustituimos la variable $z$ por el término $f(x)$, por ser $x$ la variable que acompaña al cuantificador universal que precede al existencial que vamos a eliminar. La forma de Skolem queda:*

   $$\forall x(R(x,y) \wedge \neg R(x,f(x)))$$

3. $\forall x \exists y \exists z R(x,y,z)$.

   *Primero eliminamos el cuantificador que lleva la variable $y$, como lo precede uno universal con la variable $x$, sustituimos $y$ por una función de $x$, por ejemplo $f(x)$ puesto que el símbolo $f$ no aparece. Queda entonces $\forall x \exists z R(x,f(x),z)$ y ahora procedemos a eliminar el cuantificador que acompaña a $z$, como el símbolo de función $f$ ya aparece tomamos por ejemplo $g$, sustituimos entonces $z$ por $g(x)$ y obtenemos*

   $$\forall x R(x,f(x),g(x))$$

4. $\forall x \exists y \forall z \exists u(R(x,y,u) \vee S(y,f(z)))$ *Para eliminar el cuantificador que acompaña a $y$ elegimos un símbolo de función que no aparezca, por ejemplo $g$ y sustituimos $y$ por $g(x)$, queda*

   $$\forall x \forall z \exists u(R(x,g(x),u) \vee S(g(x),f(z)))$$

   *ahora $u$ tiene que ser sustituída por otro término con un símbolo de función diferente, digamos $h$, en el que intervienen las dos variables cuantificadas universalmente que preceden a $u$, $x$ y $z$, así nos queda:*

   $$\forall x \forall z(R(x,g(x),h(x,z)) \vee S(g(x),f(z)))$$

5. $\forall x \forall y \exists u(R(x,y,u) \vee S(y,f(u)))$

   *En este caso $u$ se sustituye por una función que depende de $x$ y $y$, digamos $g(x,y)$ y por supuesto en todas las apariciones:*

   $$\forall x \forall y(R(x,y,g(x,y)) \vee S(y,f(g(x,y))))$$

**Observaciones:**

1. La forma de Skolem de una fórmula no es única, aunque por abuso del lenguaje utilizamos el artículo determinado para nombrarla.

2. La forma de Skolem puede calcularse para cualquier fórmula, no es necesario que se trate de una sentencia. Si la fórmula no está en forma prenexa es conveniente transformarla previamente en una fórmula en forma prenexa.

3. Una fórmula y su forma de Skolem no son necesariamente lógicamente equivalentes (de hecho, lo normal es que no lo sean). Sin embargo tenemos el siguiente resultado:

**Teorema 7.1.2.** *Sea $\Gamma$ un conjunto de fórmulas, y sea $\Gamma^*$ el conjunto que resulta de sustituir cada fórmula de $\Gamma$ por su forma de Skolem. Entonces*

$$\Gamma \text{ es insatisfacible si, y sólo sí, } \Gamma^* \text{ es insatisfacible}$$

Lo que sigue, hasta que se inicia el aparatado de *Forma Clausular* es una justificación (no una demostración) del teorema que acabamos de dar. Es conveniente leerlo, aunque no necesario.

Para esto, vamos a analizar algunos ejemplos.

**Ejemplo 7.1.5.** *Comenzamos con una fórmula sencilla. Por ejemplo, $\exists x \forall y P(x,y)$*

*Dicha fórmula es satisfacible. Para comprobarlo, vamos a dar una estructura en la que se interprete como cierta.*

- *El universo es* $\mathbb{Z}$
- $P(x,y) = \begin{cases} 1 & si\ x \cdot y = 0 \\ 0 & si\ x \cdot y \neq 0 \end{cases}$

*Claramente, la fórmula es válida en la estructura dada, pues existe un número entero (el cero) que al multiplicarlo por cualquier entero sale* 0.

*Consideramos ahora la forma de Skolen de la fórmula dada, que sería $\forall y P(a,y)$*

*Para comprobar que es satisfacible esta fórmula, basta considerar la estructura que hemos tomado en la fórmula anterior, pero ahora debemos también asignar un valor a la constante $a$. Le asignamos el valor* 0 *(que es el valor que le dábamos a $x$ en la primera fórmula, y que hacía cierta la fórmula $\forall y P(x,y)$). Es decir, consideramos la estructura*

- *El universo es* $\mathbb{Z}$
- $a = 0$
- $P(x,y) = \begin{cases} 1 & si\ x \cdot y = 0 \\ 0 & si\ x \cdot y \neq 0 \end{cases}$

*Y la fórmula $\forall x P(a,x)$ es válida en esa estructura. El hecho de encontrar una estructura que hace satisfacible a la fórmula $\exists x \forall y P(x,y)$ nos da una estructura en la que es satisfacible su forma de Skolem.*

*Es claro que las fórmulas $\exists x \forall y P(x,y)$ y $\forall y P(a,y)$ no son equivalentes. Basta, por ejemplo, considerar la estructura*

- *El universo es* $\mathbb{Z}$
- $a = 1$
- $P(x,y) = \begin{cases} 1 & si\ x \cdot y = 0 \\ 0 & si\ x \cdot y \neq 0 \end{cases}$

*Hemos tomado $\alpha = \exists y \forall x P(x,y)$, y a partir de que $\alpha$ es satisfacible (pues hemos encontrado una estructura que la hace cierta) hemos visto que su forma de Skolem es también satisfacible (encontrando una estructura, relacionada con la primera, que la hace cierta).*

*Vamos a ver que si partimos de una estructura que hace cierta a $\forall x P(a,x)$ (la forma de Skolem de $\alpha$ podemos obtener una estructura que hace cierta a $\alpha$.*

*Consideramos por ejemplo la estructura dada por*

- *El universo es* $\mathbb{N}$
- $a = 0$
- $P(x,y) = \begin{cases} 1 & si\ x \leq y \\ 0 & si\ x > y \end{cases}$

*Obviamente, para esta estructura se tiene que $I(\forall x P(a,x)) = 1$. Consideramos ahora la estructura con el mismo universo y la misma asignación del predicado $P$ (no necesitamos asignar constantes), es decir,*

- *El universo es* $\mathbb{N}$

- $P(x,y) = \begin{cases} 1 & si\ x \leq y \\ 0 & si\ x > y \end{cases}$

*Entonces se tiene que* $I(\alpha) = 1$*, pues existe un valor de la variable* $y$ *(concretamente* $y = 0$*) para el que es cierta* $\forall x P(x,y)$.

*Por tanto, de la satisfacibilidad de* $\forall x P(a,x)$ *hemos deducido la satisfacibilidad de* $\exists y \forall x P(x,y)$.

*Vamos a ver ahora un caso en el que el cuantificador existencial no se encuentra en primer lugar. Por ejemplo, consideramos la fórmula* $\forall x \exists y P(x,y)$

*La fórmula es satisfacible, pues es válida en la siguiente estructura*

- *El universo es* $\mathbb{Z}$

- $P(x,y) = \begin{cases} 1 & si\ x+y=3 \\ 0 & si\ x+y \neq 3 \end{cases}$

*En este caso, la existencia de un valor de la variable* $y$ *que haga cierta la fórmula está ligado al valor de* $x$*. Por tanto, este valor de* $y$ *será función (dependerá) del valor que tome la variable* $x$*. Habrá que sustituirlo entonces por una función que dependa de* $x$.

*En nuestro ejemplo, se tiene que* $y = 3 - x$*. Por tanto, la siguiente estructura*

- *El universo es* $\mathbb{Z}$

- $f(x) = 3 - x$

- $P(x,y) = \begin{cases} 1 & si\ x+y=3 \\ 0 & si\ x+y \neq 3 \end{cases}$

*es un modelo para la fórmula* $\forall x P(x, f(x))$*, que es la forma de Skolen de* $\forall x \exists y P(x,y)$.

*Al igual que antes, es fácil ver que de un modelo de* $\forall x P(x, f(x))$ *podemos obtener un modelo para* $\forall x \exists y P(x,y)$.

*Vamos por último a ver un ejemplo en el que intervienen varias fórmulas:*

*Sea* $\Gamma = \{\forall x(Q(x) \to \exists y R(y,x));\ \forall x \exists y R(x,y);\ \exists x \exists y \neg R(x,y)\}$

*Puesto que la primera fórmula no está en forma prenexa, la pasamos a dicha forma canónica, y nos queda entonces:*

$$\Gamma = \{\forall x \exists y(Q(x) \to R(y,x));\ \forall x \exists y R(x,y);\ \exists x \exists y \neg R(x,y)\}$$

*Este conjunto es satisfacible. Basta considerar la estructura:*

- *Como universo, los números enteros.*

- $Q(x) = \begin{cases} 1 & si\ x\ es\ par \\ 0 & si\ x\ es\ impar \end{cases}$

- $R(x,y) = \begin{cases} 1 & si\ 2x = y \\ 0 & si\ 2x \neq y \end{cases}$

*La primera fórmula es válida en esta estructura, pues dado un número par podemos encontrar otro número entero que al hacerle el doble nos de el de partida; la segunda también es válida, pues para cualquier* $x$ *basta tomar* $y = 2x$ *para hacerla cierta; la tercera es obviamente válida.*

*Calculamos la forma de Skolen de cada una de las fórmulas. Para la primera, como la variable* $y$*, que es la cuantificada existencialmente está precedida por una variable cuantificada universalmente, la sustituimos por una función monaria. Nos queda entonces* $\forall x(Q(x) \to R(f(x),x))$

*Para la segunda procedemos de igual forma, pero no podemos utilizar ahora el mismo símbolo de función que en la primera fórmula. Sustituimos entonces* $y$ *por* $g(x)$*. Queda entonces* $\forall x R(x, g(x))$

*En la tercera fórmula, sustituimos cada una de las variables por constantes (distintas).*

*Nos queda entonces el conjunto*

$$\Gamma^* = \{\forall x(Q(x) \to R(f(x),x));\ \forall x R(x,g(x));\ \neg R(a,b)\}$$

*El hecho de que el conjunto $\Gamma$ fuera satifacible en la estructura dada, se traduce ahora en que $\Gamma^*$ es satisfacible en la siguiente estructura.*

- *Como universo, los números enteros.*
- $Q(x) = \begin{cases} 1 & si\ x\ es\ par \\ 0 & si\ x\ es\ impar \end{cases}$
- $R(x,y) = \begin{cases} 1 & si\ 2x = y \\ 0 & si\ 2x \neq y \end{cases}$
- $f(x) = E\left(\frac{x}{2}\right)$ *(donde $E(x)$ denota la parte entera de $x$)*
- $g(x) = 2x$
- $a = 2$; $b = 5$.

*Nótese que si hubiésemos empleado el mismo símbolo de función en la primera y en la segunda fórmula, no habríamos podido encontrar así una función $f$ que hiciera válida a las dos fórmulas.*

### 7.1.5. Forma clausular

En primer lugar debemos establecer la definición de **cláusula** para lo que describimos algunos conceptos previos:

**Literal** es una fórmula atómica o la negación de una fórmula atómica.

**Ejemplo 7.1.6.**

1. $P(a)$
2. $Q(x,y,b)$
3. $\neg H(x, f(x,a), y)$

**Cierre universal** de una fórmula sin cuantificadores es la fórmula que resulta al cuantificar universalmente **todas** las variables que aparezcan.

**Ejemplo 7.1.7.**

1. $P(a)$ *es su propio cierre universal,*
2. $Q(x,y,b)$ *tiene cierre universal* $\forall x \forall y Q(x,y,b)$,
3. *el cierre universal de* $\neg H(x, f(x,a), y)$ *es* $\forall x \forall y \neg H(x, f(x,a), y)$
4. $P(a) \vee Q(x,y,b) \vee \neg H(x, f(x,a), y)$ *tiene cierre universal*

$$\forall x \forall y \forall z (P(a) \vee Q(x,y,b) \vee \neg H(x, f(x,a), z))$$

**Cláusula** es el cierre universal de una disyunción de literales.

**Ejemplo 7.1.8.**

1. $P(a)$,
2. $\forall x \forall y Q(x,y,b)$,
3. $\forall x \forall y \neg H(x, f(x,a), y)$
4. $\forall x \forall y \forall z (P(a) \vee Q(x,y,b) \vee \neg H(x, f(x,a), z))$

Por último, una fórmula está en **forma normal clausular** si es conjunción de cláusulas.

**Observaciones:**

1. No toda fórmula tiene forma clausular, sólo si es **sentencia**.
2. Toda sentencia que esté en forma de Skolem es semánticamente equivalente a una forma clausular.
3. Se incluye como fórmula en forma clausular aquella que es disyunción de cero literales. Dicha fórmula se denomina *cláusula vacía*, la representaremos como $\square$, y por definición es insatisfacible.

### 7.1.6. Método para calcular la forma de clausular de una fórmula en forma de Skolem

Puesto que la forma de Skolem es prenexa, obviamos los cuantificadores y trabajamos con la fórmula sin ellos. Sobre ésta usaremos las propiedades

1. $\alpha \to \beta \equiv \neg\alpha \vee \beta$,
2. $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$
3. $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$
4. $\neg\neg\alpha \equiv \alpha$
5. $\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$

de una forma similar a como se hace en lógica proposicional hasta llegar a una **conjunción** de fórmulas del tipo

$$C_1 \vee C_2 \vee \cdots \vee C_n$$

donde $C_i$ es un literal. Una vez obtenida esta forma, utilizamos la propiedad

$$\forall x(\Phi \wedge \Psi) \equiv \forall x\Phi \wedge \forall x\Psi$$

para llegar a la forma clausular. Esto supone que **en la práctica sólo hay que trabajar con la fórmula sin cuantificadores de la forma normal de Skolem.**

**Ejemplo 7.1.9.**

1. $\forall x(P(x, f(x)) \to Q(b))$.

   *Puesto que trabajamos sólo con los literales podemos olvidarnos por el momento de los términos que involucran y usar una notación abreviada con los símbolos de predicados, es decir, en este caso:*

   $$P \to Q$$

   *entonces* $P \to Q \equiv \neg P \vee Q$ *que ya es una disyunción de literales. Por tanto, la forma clausular de la fórmula de partida tiene una sola cláusula que es*

   $$\forall x(\neg P(x, f(x)) \vee Q(b))$$

2. $\forall x \forall y(R(x) \vee (Q(x, y) \wedge P(y) \wedge R(x)))$.

   *Trabajamos con* $R \vee (Q \wedge P \wedge R))$ *y obtenemos* $R \vee (Q \wedge P \wedge R)) \equiv (R \vee Q) \wedge (R \vee P) \wedge (R \vee R)$ *lo que nos daría tres cláusulas (dos conjunciones separan tres cláusulas), y en la última nos queda* $R(x) \vee R(x) \equiv R(x)$ *así, tendríamos la fórmula*

   $$\forall x \forall y(R(x) \vee Q(x, y)) \wedge (R(x) \vee P(y)) \wedge R(x) \equiv$$

   $$\equiv \forall x \forall y(R(x) \vee Q(x, y)) \wedge \forall x \forall y(R(x) \vee P(y)) \wedge \forall x R(x)$$

   *donde en la última cláusula se ha eliminado el cuantificador* $\forall y$ *puesto que en la fórmula que le sigue la variable* $y$ *no es libre (en este caso porque no aparece).*

   **Observación:** *Si la fórmula anterior hubiese sido*

   $$\forall x \forall y(R(x) \vee (Q(x, y) \wedge P(y) \wedge R(f(x))))$$

   *el procedimiento sería similar, pero habría que tener en cuenta que en la última cláusula las dos apariciones de* $R$ *no son el mismo literal puesto que en uno aparece una variable y en el otro una función :* $R(x) \vee R(f(x))$ *y por tanto no puede simplificarse a* $R(x)$.

**Teorema 7.1.3.** *Sea $\Gamma = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ un conjunto de sentencias. Para cada fórmula $\gamma_i \in \Gamma$ calculamos su forma clausular. Supongamos que esta forma clausular es $C_{i1} \wedge C_{i2} \wedge \cdots \wedge C_{im_i}$. Formamos el conjunto $\Gamma^{**}$ con todas las cláusulas que aparecen en las distintas formas clausulares (es decir, $\Gamma^{**} = \{C_{11}, C_{12}, \cdots, C_{nm_n}\}$).*

*Entonces se tiene que $\Gamma$ es insatisfacible si, y sólo si, $\Gamma^{**}$ es insatisfacible.*

En el caso de que no todas las fórmulas de que partimos sean sentencias, tenemos un resultado similar que vamos a ver a continuación. Antes necesitamos los siguientes lemas.

**Lema 7.1.1.** *Sea $\Gamma = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ un conjunto de fórmulas, y $\gamma = \gamma_1 \wedge \gamma_2 \cdots \gamma_n$.*

*Entonces $\Gamma$ es insatisfacible si, y sólo si, $\gamma$ es una contradicción.*

Intuitivamente, el lema es claro.

Decir que $\Gamma$ es insatisfacible significa que no puede haber ninguna interpretación para la que todas las fórmulas sean ciertas a la vez. Es decir, para cualquier estructura y cualquier valoración $v$, hay alguna fórmula del conjunto $\Gamma$, digamos $\gamma_i$ tal que $I^v(\gamma_i) = 0$. Pero esto es lo mismo que decir que $I^v(\gamma_1) \cdot I^v(\gamma_2) \cdots I^v(\gamma_n) = 0$.

Tenemos por tanto que $I^v(\gamma) = I^v(\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n) = 0$ para cualquier interpretación $I^v$.

**Lema 7.1.2.** *Sea $\alpha$ una fórmula en un lenguaje de primer orden, y sea $x$ una variable que aparece libre en la fórmula $\alpha$. Entonces $\alpha$ es contradicción si, y sólo si, $\exists x\alpha$ es una contradicción.*

También este lema es claro. El que $\alpha$ sea una contradicción se traduce en que, dada una estructura, para cualquier valor que le demos a la variable $x$, $v(x)$, se tiene que $I^v(\alpha) = 0$. Pero esto significa que $I^v(\exists x\alpha) = 0$.

Por tanto, tenemos que, dada una estructura, la fórmula $\exists x\alpha$ se interpreta como falsa.

**Teorema 7.1.4.** *Sea $\Gamma = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$. Supongamos que el conjunto de variables que tienen alguna ocurrencia libre en las fórmulas de $\Gamma$ es $\{x_1, x_2, \cdots, x_m\}$.*

*Entonces $\Gamma$ es insatisfacible si, y sólo si, la fórmula $\exists x_1 \exists x_2 \cdots \exists x_n(\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n)$ es una contradicción.*

Notemos que la fórmula $\exists x_1 \exists x_2 \cdots \exists x_n(\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n)$ es una sentencia, y por tanto a esta fórmula le podemos hacer su forma clausular y reducir el problema a estudiar si un conjunto de cláusulas es satisfacible o insatisfacible.

**Ejemplo 7.1.10.** *Sean las fórmulas*

$$\alpha_1 = \forall x(P(x) \wedge \neg Q(x) \rightarrow \exists y(R(x,y) \wedge S(y))).$$
$$\alpha_2 = \exists y \forall x((R(y,x) \rightarrow T(x)) \wedge T(y) \wedge P(y).$$
$$\alpha_3 = \exists x(T(x) \wedge (Q(x) \vee S(x))).$$

*Supongamos que queremos ver si $\{\alpha_1, \alpha_2\} \vDash \alpha_3$.*

*Vamos a transformar este problema en estudiar si un conjunto de cláusulas es o no insatisfacible. Para ello, vemos en primer lugar que lo anterior es equivalente a probar que el conjunto $\{\alpha_1, \alpha_2, \neg\alpha_3\}$ es insatisfacible. Calculamos una forma clausular de cada una de las fórmulas.*

- *Para $\alpha_1$ tenemos:*

| | |
|---|---|
| $\forall x(P(x) \wedge \neg Q(x) \rightarrow \exists y(R(x,y) \wedge S(y)))$ | |
| $\forall x(\neg(P(x) \wedge \neg Q(x)) \vee \exists y(R(x,y) \wedge S(y)))$ | |
| $\forall x((\neg P(x) \vee Q(x)) \vee \exists y(R(x,y) \wedge S(y)))$ | |
| $\forall x \exists y((\neg P(x) \vee Q(x)) \vee (R(x,y) \wedge S(y)))$ | *Forma normal prenexa* |
| $\forall x((\neg P(x) \vee Q(x)) \vee (R(x,f(x)) \wedge S(f(x))))$ | *Forma normal de Skolem* |
| $\forall x((\neg P(x) \vee Q(x) \vee R(x,f(x))) \wedge (\neg P(x) \vee Q(x) \vee S(f(x))))$ | |
| $\forall x(\neg P(x) \vee Q(x) \vee R(x,f(x))) \wedge \forall x(\neg P(x) \vee Q(x) \vee S(f(x)))$ | *Forma clausular* |

- *Para $\alpha_2$:*

| | |
|---|---|
| $\exists y \forall x((R(y,x) \rightarrow T(x)) \wedge T(y) \wedge P(y))$ | *Forma normal prenexa* |
| $\forall x((R(a,x) \rightarrow T(x)) \wedge T(a) \wedge P(a))$ | *Forma normal de Skolem* |
| $\forall x((\neg R(a,x) \vee T(x)) \wedge T(a) \wedge P(a))$ | |
| $\forall x(\neg R(a,x) \vee T(x)) \wedge T(a) \wedge P(a)$ | *Forma clausular* |

- *Y para* $\neg\alpha_3$*:*

$$\begin{array}{ll}
\neg\exists x(T(x)\wedge(Q(x)\vee S(x))) & \\
\forall x\neg(T(x)\wedge(Q(x)\vee S(x))) & \textit{Forma normal prenexa y de Skolem}\\
\forall x(\neg T(x)\vee\neg(Q(x)\vee S(x))) & \\
\forall x(\neg T(x)\vee(\neg Q(x)\wedge\neg S(x))) & \\
\forall x((\neg T(x)\vee\neg Q(x))\wedge(\neg T(x)\vee\neg S(x))) & \\
\forall x(\neg T(x)\vee\neg Q(x))\wedge\forall x(\neg T(x)\vee\neg S(x)) & \textit{Forma clausular}
\end{array}$$

*Y el problema es ahora probar que el siguiente conjunto de cláusulas*

$$\Gamma=\left\{\begin{array}{lll}\neg P(x)\vee Q(x)\vee R(x,f(x)); & \neg R(a,x)\vee T(x); & T(a);\quad P(a)\\ \neg P(x)\vee Q(x)\vee S(f(x)); & \neg T(x)\vee\neg Q(x); & \neg T(x)\vee\neg S(x)\end{array}\right\}$$

*es o no insatisfacible. Esto lo veremos más adelante, cuando estudiemos resolución.*

*Al escribir las cláusulas no escribimos los cuantificadores. Esto no significa que no estén. Pero como en una cláusula todas las variables están cuantificadas universalmente, no es necesario especificarlo cuando las escribimos (se sobreentiende que es así).*

# Capítulo 8

# Unificación

## 8.1. Unificación

### 8.1.1. Sustituciones

El objetivo de esta sección es, dados dos o más literales (fórmulas atómicas), estudiar si es posible transformarlas de forma que sean iguales. Las transformaciones que van a estar permitidas son aquellas en las que una variable se sustituye por un término. Llamaremos a este tipo de transformaciones "sustituciones".

Recordemos que un literal es una fórmula atómica o la negación de una fórmula atómica.

**Definición 60.** *Sea $\alpha$ un literal, $x$ una variable con alguna ocurrencia en la fórmula $\alpha$ y $t$ un término cualquiera. La* sustitución elemental *de $x$ por $t$ es la transformación de la fórmula $\alpha$ en otra fórmula en la que cada ocurrencia de la variable $x$ es sustituida por el término $t$.*

*Dicha sustitución la representaremos como $\sigma = (x|t)$, y la fórmula resultante de aplicar la sustitución $\sigma$, como $\sigma(\alpha)$*

**Ejemplo 8.1.1.**

*En la fórmula $R(f(x), a, g(h(x), y))$ realizamos la sustitución $(x|g(a, y))$. Nos queda entonces la fórmula $R(f(g(a, y)), a, g(h(g(a, y)), y))$.*

Al sustituir una variable $x$ por un término, dicha variable puede aparecer en el término por el que sustituimos, así, podemos hacer la sustitución $\sigma = (x|f(x))$, y así, si $\alpha$ es la fórmula del ejemplo anterior, entonces

$$\sigma(\alpha) = R(f(f(x)), a, g(h(f(x)x), y)).$$

Obviamente, a la fórmula que resulta de aplicarle una sustitución elemental podemos aplicarle otra sustitución elemental. Si $\sigma_0$ es la primera sustitución que hacemos, y $\sigma_1$ la segunda, escribiremos la sustitución total como $\sigma_1\sigma_0$. Dicha sustitución la denominaremos *composición de $\sigma_0$ y $\sigma_1$*

**Ejemplo 8.1.2.**

*Según el ejemplo anterior, el resultado de aplicar la sustitución $\sigma_0 = (x|g(a, y))$ a la fórmula $R(f(x), a, g(h(x), y))$ es $R(f(g(a, y)), a, g(h(g(a, y)), y))$.*

*Si ahora sustituimos la variable $y$ por $g(a, h(a))$ (es decir, aplicamos la sustitución $(y|g(a, h(a)))$), obtenemos la fórmula*

$$R(f(g(a, g(a, h(a)))), a, g(h(g(a, g(a, h(a)))), g(a, h(a))))$$

*La sustitución realizada es entonces $\sigma = (y|g(a, h(a)))\ (x|g(a, y))$*

*Notemos que el orden en que tomamos las sustituciones elementales es importante. Puede comprobarse que no es lo mismo $\sigma = (y|g(a, h(a)))\ (x|g(a, y))$ que $\tau = (x, g(a, y))\ (y|g(a, h(a)))$.*

*En este segundo caso, el resultado de aplicarle a $R(f(x), a, g(h(x), y))$ la sustitución $\tau$ es*

$$R(f(g(a, y)), a, g(h(g(a, y)), g(a, h(a))))$$

*Comprueba que efectivamente éste es el resultado, y constata que es diferente al de aplicar la sustitución $\sigma$.*

Si observamos el ejemplo anterior, vemos que el efecto de la sustitución $\sigma$ es el de cambiar cada aparición de $x$ por el término $g(a, g(a, h(a)))$, y cada aparición de $y$ por $g(a, h(a))$. Dicha sustitución podemos representarla como

$$\sigma = (x|g(a, g(a, h(a)));\ y|g(a, h(a)))$$

Nótese que en este caso el orden en que lo escribamos no influye, es decir,

$$(x|g(a, g(a, h(a)));\ y|g(a, h(a))) = (y|g(a, h(a));\ x|g(a, g(a, h(a))))$$

La composición en orden inverso, es decir, la sustitución $\tau$ podríamos representarla ahora como

$$(x|g(a, y);\ y|g(a, h(a)))$$

que claramente no coincide con la sustitución $\sigma$.

En general, podemos dar la siguiente definición.

**Definición 61.** *Sea $\alpha$ un literal en un lenguaje de primer orden.*

*Una sustitución en $\alpha$ es la transformación que consiste en sustituir algunas (o todas) de las variables que aparecen en $\alpha$ por términos del lenguaje.*

*Si $x_1, x_2, \cdots, x_n$ son las variables que vamos a sustituir, y $t_1, t_2, \cdots, t_n$ los términos por los que las sustituimos, entonces representaremos la sustitución como*

$$(x_1|t_1;\ x_2|t_2;\ \cdots\ x_n|t_n)$$

**Ejercicio 8.1.1.** *Comprueba que las sustituciones $(x|y)$ $(y|x)$, $(y|x)$ $(x|y)$ y $(x|y;\ y|x)$ son todas distintas, y expresa la última como composición de sustituciones elementales.*

### 8.1.2. Unificadores

A continuación pasamos a dar el concepto de *unificador*. Más adelante veremos como calcular un unificador para dos o más literales.

**Definición 62.** *Dado un conjunto de literales $\alpha_1, \alpha_2, \cdots, \alpha_n$, un unificador para tales fórmulas es una sustitución $\sigma$ de forma que $\sigma(\alpha_1) = \sigma(\alpha_2) = \cdots = \sigma(\alpha_n)$.*

**Ejemplo 8.1.3.**

1. *Dadas las fórmulas $P(x)$ y $P(a)$, un unificador de ambas es, por ejemplo, $(x|a)$.*
2. *Las fórmulas $P(x)$ y $P(f(x))$ no tienen unificador, pues para cualquier sustitución $\sigma = (x|t)$ nos va a quedar que $\sigma(P(x)) = P(t)$ mientras que $\sigma(P(f(x))) = P(f(t))$, y estas fórmulas van a ser siempre distintas.*
3. *Las fórmulas $Q(x, a)$ y $Q(y, b)$ no tienen unificador, pues no podemos sustituir las constantes por ningún término, por tanto, para cualquier sustitución $\sigma$ que hagamos nos quedará $\sigma(Q(x, a)) = Q(t_1, a)$ y $\sigma(Q(y, b)) = Q(t_2, b)$.*
4. *Para las fórmulas $P(a, x, f(g(y)))$, $P(z, f(z), f(u))$ sí existen unificadores. Por ejemplo, es un unificador $(x|f(a);\ y|f(x);\ z|a;\ u|g(f(x)))$.*

   *También $(x|f(a);\ y|a;\ z|a;\ u|g(a))$ es un unificador para estas dos fórmulas.*

Un conjunto de literales se dice unificable si existe un unificador para ellas. Caso contrario, dicho conjunto se dice que no es unificable.

Nótese que si $\sigma$ es un unificador para un conjunto de fórmulas $\alpha_1, \alpha_2, \cdots, \alpha_n$ y $\tau$ es una sustitución cualquiera, entonces $\tau\sigma$ es también un unificador para $\alpha_1, \alpha_2, \cdots, \alpha_n$.

**Ejemplo 8.1.4.**

*Dadas las fórmulas $P(a, x, f(g(y)))$, $P(z, f(z), f(u))$, sabemos que*

$$\sigma = (x|f(a);\ y|f(x);\ z|a;\ u|g(f(x)))$$

*es un unificador para ambas. Sea ahora* $\tau = (x|g(a))$. *En tal caso, se tiene que*

$$\tau\sigma = (x|f(a);\ y|f(g(a));\ z|a;\ u|g(f(g(a))))$$

*que es también un unificador para* $P(a, x, f(g(y)))$ *y* $P(z, f(z), f(u))$.

*Nótese que* $\sigma\tau$ *no es unificador para las dos fórmulas, pues*

$$\sigma\tau = (x|g(a);\ y|f(x);\ z|a;\ u|g(f(x)))$$

*y se tiene que*

$$\sigma\tau(P(a, x, f(g(y)))) = P(a, g(a), f(g(f(x))))$$
$$\sigma\tau(P(z, f(z), f(u)) = P(a, f(a), f(g(f(x))))$$

Si analizamos el ejemplo precedente, vemos que para lograr que las fórmulas $P(a, x, f(g(y)))$ y $P(z, f(z), f(u))$ sean iguales después de realizar sustituciones, entonces $z$ debe sustituirse por $a$ (para igualar la primera componente), $x$ debe sustituirse por $f(z) = f(a)$, mientras que $u$ debe sustituirse por lo que le demos a $g(y)$, independientemente del valor de $y$. Los unificadores que hemos dado para ambas fórmulas satisfacían estas condiciones, y sobre lo que teníamos libertad, que era el término que sustituye a $y$, ha tomado un valor en cada uno de los casos.

En el primer caso, sustituíamos $y$ por $f(x)$ (y por tanto, $u$ por $g(y) = f(g(x))$)

En el segundo caso, sustituíamos $y$ por $a$

Y en el tercero, sustituíamos $y$ por $f(g(a))$.

Vemos entonces que hay una condición, que podemos representar en la sustitución $(z|a;\ x|f(a);\ u|g(y))$ que debe satisfacer cualquier unificador.

Esta idea, vamos a formalizarla en la siguiente definición.

**Definición 63.** *Sean* $\alpha_1, \alpha_2, \cdots, \alpha_n$ *literales en un lenguaje de primer orden, y sea* $\sigma$ *una sustitución.*

*Se dice que* $\sigma$ *es un* **unificador principal** *para* $\alpha_1, \alpha_2, \cdots, \alpha_n$ *(también se llama* **unificador más general***) si:*

*-* $\sigma$ *es un unificador para* $\alpha_1, \alpha_2, \cdots, \alpha_n$.

*- Si* $\tau$ *es otro unificador para* $\alpha_1, \alpha_2, \cdots, \alpha_n$, *entonces existe una sustitución* $\tau_1$ *de forma que* $\tau = \tau_1\sigma$

Es decir, $\sigma$ es un unificador principal si todos los unificadores pueden obtenerse a partir de $\sigma$.

**Ejemplo 8.1.5.**

1. *Consideramos nuevamente las fórmulas* $P(a, x, f(g(y)))$ *y* $P(z, f(z), f(u))$. *Entonces un unificador principal es*

$$(z|a;\ x|f(a);\ u|g(y)) \ = \ (x|f(a);\ z|a;\ u|g(y))$$

   *La sustitución* $(x|f(a);\ y|f(x);\ z|a;\ u|g(f(x)))$, *que es un unificador para ambas fórmulas, se puede expresar como* $(y|f(x))\ (x|f(a);\ z|a;\ u|g(y))$

   *La sustitución* $(x|f(a);\ y|a;\ z|a;\ u|g(a))$, *que también es un unificador para ambas fórmulas, se puede expresar como* $(y|a)\ (x|f(a);\ z|a;\ u|g(y))$

   *Por último, la sustitución* $(x|f(a);\ y|f(g(a));\ z|a;\ u|g(f(g(a))))$ *puede expresarse como la composición* $(y|f(g(a)))\ (x|f(a);\ z|a;\ u|g(y))$

2. *Un conjunto de literables unificable puede tener más de un unificador principal. Así, las sustituciones* $\sigma_1 = (x|y)$, *y* $\sigma_2 = (y|x)$ *son unificadores principales de las fórmulas* $P(x, y)$ *y* $P(y, x)$

Vamos a dar a continuación dos métodos para decidir si dado un conjunto de literales, éstos son unificables, y caso de serlo, encontrar un unificador principal.

**Algoritmo de Unificación**

Este algoritmo nos permite un cálculo automático de un unificador más general para un conjunto de literales.

**Datos de entrada:** literales a unificar (conjunto $W$)

**Salida:** un unificador principal o la respuesta "no son unificables"

**Conjunto de discordancia para un par de literales:** son los (**primeros**) términos en los que difieren. Para obtenerlo se recorren los literales de izquierda a derecha y se marcan los términos que siendo diferentes ocupan idénticas posiciones en los literales.

**Ejemplo 8.1.6.**

1. $\{P(x), P(y)\}$ *los literales difieren en los términos que ocupan la posición en negrita* $P(\mathbf{x})$, $P(\mathbf{y})$ *Luego el conjunto de discordancia es* $\{x, y\}$
2. $\{Q(x, f(x, y)); Q(x, f(y, y))\}$ *los literales difieren en los términos que ocupan la posición en negrita* $Q(x, f(\mathbf{x}, y)); Q(x, f(\mathbf{y}, y))$ *Luego el conjunto de discordancia es* $\{x, y\}$
3. $\{R(g(x)), R(f(y))\}$ *los literales difieren en los términos que ocupan la posición en negrita* $R(\mathbf{g}(\mathbf{x})), R(\mathbf{f}(\mathbf{y}))$ *Luego el conjunto de discordancia es* $\{g(x), f(y)\}$

**Descripción del algoritmo:**

**Inicialización** $W_0 = W$, $\sigma_0$ =Identidad

**Bucle: Si** el número de elementos del conjunto $W_k$ es 1, entonces el proceso acaba. **Salida:** $\sigma_k$ es un unificador principal.

**En otro caso** calcular el conjunto de discordancia de $W_k$ , $D$.

**Si** en $D$ no aparece ninguna variable o aparece alguna variable, pero los demás términos en D dependen de ella, entonces el proceso termina porque los literales no son unificables. **Salida:** No son unificables.

**Si** existe una variable $v_k$ y un término $t_k$ en el que no aparece la variable $v_k$, **entonces** hacemos $\sigma_{k+1} = (v_k|t_k) \circ \sigma_k$; aplicamos la sustitución $(v_k|t_k)$ en $W_k$ para obtener $W_{k+1}$ y volver a ejecutar el bucle.

**Ejemplo 8.1.7.**

$$W = \{P(a, x, f(g(y))), P(z, f(z), f(u))\}$$

**Inicialización:**

$$W_0 = \{P(a, x, f(g(y))), P(z, f(z), f(u))\}$$

$$\sigma_0 = identidad$$

**Primera pasada por el bucle:** *El conjunto tiene más de un elemento. Calculamos el conjunto de discordancia* $D = \{a, z\}$. *Tiene una variable y un término que no depende de ella, se añade a la sustitución inicial* $(z|a)$ *(entonces* $\sigma_1 = (z|a)$ *) y se calcula* $W_1$ *aplicando esta sustitución a* $W_0$*:*

$$W_1 = \{P(a, x, f(g(y))), P(a, f(a), f(u))\}$$

**Segunda pasada por el bucle:** *El conjunto tiene más de un elemento. Calculamos el conjunto de discordancia* $D = \{x, f(a)\}$ *Tiene una variable y un término que no depende de ella, se añade a la sustitución inicial* $(x|f(a))$ *(entonces* $\sigma_2 = (z|a; x|f(a))$ *y se calcula* $W_2$*:*

$$W_2 = \{P(a, f(a), f(g(y))), P(a, f(a), f(u))\}$$

**Tercera pasada por el bucle:** *El conjunto tiene más de un elemento. Calculamos el conjunto de discordancia* $D = \{g(y), u\}$. *Tiene una variable y un término que no depende de ella, se añade a la sustitución inicial* $(u|g(y))$ *(entonces* $\sigma_3 = (z|a; x|f(a); u|g(y)))$, *y se calcula* $W_3$

$$W_3 = \{P(a, f(a), f(g(y)))\}$$

**Cuarta pasada por el bucle:** $W_3$ *tiene un solo elemento* **FIN**

**Salida:**

$$\sigma = \sigma_3 = (z|a; x|f(a); u|g(y))$$

*es un unificador principal para el conjunto de literales dado.*

### Sistemas de ecuaciones en términos

A continuación vamos a dar otro método para decidir cuando un conjunto de fórmulas atómicas es o no unificable.

Supongamos que tenemos dos fórmulas atómicas $\alpha$ y $\beta$, que queremos ver si son o no unificables. Supongamos que $\alpha = R(t_1, t_2, \cdots, t_n)$ y $\beta = R(t'_1, t'_2, \cdots, t'_n)$. Obviamente, si las fórmulas empiezan por diferentes símbolos de predicado, entonces no son unificables.

Lo que tratamos es de encontrar una sustitución $\sigma$ de forma que $\sigma(\alpha) = \sigma(\beta)$. En definitiva, lo que buscamos es una sustitución que transforme el término $t_1$ en lo mismo que el término $t'_1$; el término $t_2$ en lo mismo que el término $t'_2$, y así hasta el término $t_n$ que debe ser transformado en lo mismo que el término $t'_n$.

Lo que tenemos podemos representarlo como $n$ ecuaciones en términos como sigue:

$$\begin{array}{ccc} t_1 & = & t'_1 \\ t_2 & = & t'_2 \\ \cdots & \cdots & \cdots \\ t_n & = & t'_n \end{array}$$

Cada una de las expresiones $t_i = t'_i$ es una ecuación del sistema $e_i$. Un sistema de ecuaciones es por tanto un conjunto de ecuaciones $E = \{e_1, e_2, \cdots, e_n\}$

Una solución del sistema es una sustitución $\sigma$ que transforme cada término $t_i$ en lo mismo que el término $t'_i$.

Si un sistema tiene solución, entonces existe una sustitución $\sigma$ de forma que cualquier solución del sistema $\tau$ se puede expresar como $\tau = \tau_1\sigma$ para alguna sustitución $\tau_1$. Dicha solución se llamará *solución principal*

Dos sistemas de ecuaciones en términos son equivalentes si tienen las mismas soluciones.

Vamos a dar un método que permita, dado un sistema de ecuaciones en términos, decidir si tiene o no solución, y caso de tenerla, encontrarlas todas. Este método se basa en varios resultados que enunciamos a continuación. Por ser todos ellos muy intuitivos, los dejamos sin demostración.

Comenzamos con una definición.

**Definición 64.** *Dado un sistema de ecuaciones en términos* $E = \{e_1, e_2, \cdots, e_n\}$, *se dice que está en forma resuelta si:*

- *Cada ecuación del sistema es de la forma* $x_i = t_i$, *con* $x_i$ *una variable.*
- *Las variables* $x_1, x_2, \cdots, x_n$ *son todas distintas.*
- *En los términos* $t_1, t_2, \cdots, t_n$ *no hay ninguna ocurrencia de las variables del conjunto* $\{x_1, x_2, \cdots, x_n\}$

*En tal caso,* $\sigma_E = (x_1|t_1;\ x_2|t_2;\ \cdots\ ; x_n|t_n)$ *es una solución principal del sistema.*

Vamos entonces a ver como transformar (si es posible) un sistema en otro sistema equivalente y que esté en forma resuelta. Para esto, vamos a ver algunos resultados que, bien permiten transformar un sistema en otro equivalente, bien concluir que el sistema no tiene solución.

1. Los sistemas $E \cup \{t = t\}$ y $E$ son equivalentes. Es decir, podemos eliminar las ecuaciones en las que el término de la derecha y el de la izquierda coinciden.

2. Los sistemas $E \cup \{t_1 = t_2\}$ y $E \cup \{t_2 = t_1\}$ son equivalentes.

3. Los sistemas

$$E \cup \{f(t_1, \cdots, t_m) = f(t'_1, \cdots, t'_m)\} \text{ y } E \cup \{t_1 = t'_1, \cdots, t_m = t'_m\}$$

son equivalentes.

4. Los sistemas $E \cup \{x = t\}$, donde $x$ es una variable que no aparecen en el término $t$, y $\sigma(E) \cup \{x = t\}$ son equivalentes, donde $\sigma$ es la sustitución $\sigma = (x|t)$.

En este caso, $\sigma(E)$ es el sistema formado por las ecuaciones que resultan de realizar la sustitución $\sigma$ en cada uno de los términos que intervienen en el sistema $E$.

5. Un sistema de la forma $E \cup \{x = t\}$ donde $t$ es un término en el que interviene la variable $x$, y $t \neq x$ no tiene solución.

6. Un sistema de la forma $E \cup \{f(t_1, \cdots, t_n) = g(t'_1, \cdots, t'_m)\}$, con $f$ y $g$ símbolos de función distintos, no tiene solución.

7. Un sistema de la forma $E \cup \{f(t_1, \cdots, t_n) = a\}$, o de la forma $E \cup \{a = b\}$, donde $a$ y $b$ son constantes distintas, no tiene solución.

Utilizando los resultados que acabamos de enunciar, podemos, dado un sistema de ecuaciones en términos, bien transformarlo en un sistema en forma resuelta, bien concluir que no tiene solución. Veamos algunos ejemplos:

**Ejemplo 8.1.8.**

1. *Vamos a resolver el sistema:*

$$\left.\begin{array}{lcl} a & = & z \\ x & = & f(z) \\ f(g(y)) & = & f(u) \end{array}\right\}$$

*El resultado* 2 *permite transformarlo en*

$$\left.\begin{array}{lcl} z & = & a \\ x & = & f(z) \\ f(g(y)) & = & f(u) \end{array}\right\}$$

*Ahora, por el resultado cuatro, y con la sustitución* $(z|a)$ *transformamos el sistema en*

$$\left.\begin{array}{lcl} z & = & a \\ x & = & f(a) \\ f(g(y)) & = & f(u) \end{array}\right\}$$

*Por el apartado* 3 *llegamos a*

$$\left.\begin{array}{lcl} z & = & a \\ x & = & f(a) \\ g(y) & = & u \end{array}\right\}$$

*Y por último, con el apartado segundo transformamos el sistema en*

$$\left.\begin{array}{lcl} z & = & a \\ x & = & f(a) \\ u & = & g(y) \end{array}\right\}$$

*que es un sistema en forma resuelta.*

2. *Vamos a estudiar si el conjunto de fórmulas*

$$\{P(x,y),\ P(f(z),x),\ P(u,f(x))\}$$

*es unificable o no.*

*Para esto, planteamos el sistema de ecuaciones en términos y tratamos de resolverlo. En negrita representamos la ecuación que vamos a utilizar en el paso siguiente.*

$$\left.\begin{array}{lcl} \mathbf{x} & = & \mathbf{f(z)} \\ y & = & x \\ x & = & u \\ y & = & f(x) \end{array}\right\} \overset{(4)}{\Longrightarrow} \left.\begin{array}{lcl} x & = & f(z) \\ y & = & f(z) \\ \mathbf{f(z)} & = & \mathbf{u} \\ y & = & f(f(z)) \end{array}\right\} \overset{(2)}{\Longrightarrow} \left.\begin{array}{lcl} x & = & f(z) \\ \mathbf{y} & = & \mathbf{f(z)} \\ u & = & f(z) \\ y & = & f(f(z)) \end{array}\right\} \overset{(4)}{\Longrightarrow}$$

$$\left.\begin{array}{lcl} x & = & f(z) \\ y & = & f(z) \\ u & = & f(z) \\ \mathbf{f(z)} & = & \mathbf{f(f(z))} \end{array}\right\} \overset{(3)}{\Longrightarrow} \left.\begin{array}{lcl} x & = & f(z) \\ y & = & f(z) \\ u & = & f(z) \\ z & = & f(z) \end{array}\right\}$$

*y al quedarmos al final la ecuación $z = f(z)$ concluimos que el conjunto no es unificable (resultado 5).*

3. *Vamos por último a comprobar si el conjunto de dos fórmulas*

$$\{P(x,g(x),y,h(x,y),z,k(x,y,z));\ P(u,v,e(v),w,f(v,w),t)\}$$

*es unificable o no. Para ello, vamos a plantear el sistema de ecuaciones en términos y vamos a tratar de llevarlo a forma resuelta.*

$$\left\{\begin{array}{lcl} x & = & u \\ g(x) & = & v \\ y & = & e(v) \\ h(x,y) & = & w \\ z & = & f(v,w) \\ k(x,y,z) & = & t \end{array}\right. \overset{(4)}{\longleftarrow} \left\{\begin{array}{lcl} x & = & u \\ g(u) & = & v \\ y & = & e(v) \\ h(u,y) & = & w \\ z & = & f(v,w) \\ k(u,y,z) & = & t \end{array}\right. \overset{(2)}{\longleftarrow} \overset{(2)}{\longleftarrow} \overset{(2)}{\longleftarrow}$$

$$\left\{\begin{array}{lcl} x & = & u \\ v & = & g(u) \\ y & = & e(v) \\ w & = & h(u,y) \\ z & = & f(v,w) \\ t & = & k(u,y,z) \end{array}\right. \overset{(4)}{\longleftarrow} \left\{\begin{array}{lcl} x & = & u \\ v & = & g(u) \\ y & = & e(g(u)) \\ w & = & h(u,y) \\ z & = & f(g(u),w) \\ t & = & k(u,y,z) \end{array}\right. \overset{(4)}{\longleftarrow}$$

$$\left\{\begin{array}{lcl} x & = & u \\ v & = & g(u) \\ y & = & e(g(u)) \\ w & = & h(u,e(g(u))) \\ z & = & f(g(u),w) \\ t & = & k(u,e(g(u)),z) \end{array}\right. \overset{(4)}{\longleftarrow} \left\{\begin{array}{lcl} x & = & u \\ v & = & g(u) \\ y & = & e(g(u)) \\ w & = & h(u,e(g(u))) \\ z & = & f(g(u),h(u,e(g(u)))) \\ t & = & k(u,e(g(u)),z) \end{array}\right. \overset{(4)}{\longleftarrow}$$

$$\left\{\begin{array}{lcl} x & = & u \\ v & = & g(u) \\ y & = & e(g(u)) \\ w & = & h(u,e(g(u))) \\ z & = & f(g(u),h(u,e(g(u)))) \\ t & = & k(u,e(g(u)),f(g(u),h(u,e(g(u))))) \end{array}\right.$$

*Y hemos llegado a un sistema de ecuaciones, equivalente al de partida, y que está en forma resuelta.*

# Capítulo 9

# Resolución

Al igual que en el tema 6, dedicado a la lógica proposicional, vamos a intentar aquí, dado un conjunto de cláusulas, obtener la cláusula vacía usando resolución. Para eso necesitamos antes el concepto de *resolvente*.

Dadas dos cláusulas $C_1$ y $C_2$, una resolvente suya será una nueva cláusula $C_3$ que se deduzca de las dos dadas, es decir, que se verifique que $\{C_1, C_2\} \vDash C_3$.

## 9.1. Resolventes

### 9.1.1. Resolventes binarias

Comenzamos por un ejemplo sencillo.

Supongamos que tenemos las cláusulas $C_1 = \neg P(x) \vee Q(b)$ y $C_2 = P(a)$ y que ambas son ciertas.

La primera cláusula la podemos escribir como $\forall x(P(x) \rightarrow Q(b))$, es decir, que sea quien sea $x$ la fórmula $P(x) \rightarrow Q(b)$ es cierta. En particular, será cierto $P(a) \rightarrow Q(b)$. Como además $P(a)$ es cierto podemos deducir que $Q(b)$ es cierto. Es decir, tenemos que

$$\{\neg P(x) \vee Q(b), P(a)\} \vDash Q(b)$$

Otra forma de llegar a la misma conclusión podría ser:

1. Tomamos las cláusulas $C_1$ y $C_2$.
2. Elegimos los literales $L_1 = \neg P(x)$ y $L_2 = P(a)$ de la primera y segunda cláusulas respectivamente.
3. Comprobamos si $L_1^C$ y $L_2$ son unificables. En este caso lo son, y un unificador principal es $\sigma = (x|a)$.
4. Hallamos $\sigma(C_1) = \neg P(a) \vee Q(b)$ y $\sigma(C_2) = P(a)$
5. Eliminamos de $\sigma(C_1)$ y $\sigma(C_2)$ los literales $\sigma(L_1)$ y $\sigma(L_2)$, y formamos una cláusula con los literales restantes (aquí procedemos de igual forma a como hacíamos en el tema sexto cuando calculábamos resolventes). La cláusula resultante es consecuencia lógica de las dos primeras.

Vamos a repetir este proceso con las cláusulas

$$C_1 = P(x, b) \vee Q(x, a); \qquad C_2 = \neg P(a, z) \vee R(z)$$

1. Tomamos el literal $L_1 = P(x, b)$ de la primera cláusula, y el literal $L_2 = \neg P(a, z)$ de la segunda.
2. Buscamos un unificador principal para $L_1^C$ y $L_2$. Este unificador existe, y es $\sigma = (x|a; z|b)$.
3. Calculamos $\sigma(C_1) = P(a, b) \vee Q(a, a)$ y $\sigma(C_2) = \neg P(a, b) \vee R(b)$.
4. Eliminamos los literales $\sigma(L_1)$ y $\sigma(L_2)$ de las cláusulas $\sigma(C_1)$ y $\sigma(C_2)$. Nos queda la cláusula $C_3 = Q(a, a) \vee R(b)$

Vamos a ver que $\{C_1, C_2\} \models C_3$.

Suponemos que $I(C_1) = I(C_2) = 1$.

Entonces $I(\forall x(P(x,b) \vee Q(x,a))) = 1$. Significa esto que $P(x,b) \vee Q(x,a)$ será cierto sea cual sea el valor de $x$. En particular, $I(P(a,b) \vee Q(a,a)) = 1$.

De la misma forma, como $I(C_2) = 1$, entonces $I(\neg P(a,b) \vee R(b)) = 1$.

Pueden ocurrir ahora dos cosas:

$I(P(a,b)) = 1$

En este caso $I(\neg P(a,b)) = 0$, luego $I(R(b)) = 1$ (ya que $I(\neg P(a,b) \vee R(b)) = 1$). Por tanto, $I(Q(a,a) \vee R(b)) = I(C_3) = 1$.

$I(P(a,b)) = 0$

En este caso $I(Q(a,a))$ debe valer uno, luego $I(C_3) = 1$.

Luego en cualquiera de los casos deducimos que $I(C_3) = 1$, es decir,

$$\{C_1, C_2\} \models C_3.$$

Notemos que la cláusula $C_2$ es equivalente a $\forall x(\neg P(a,x) \vee R(x))$. Pero ahora, cuando intentamos buscar un unificador para $P(x,b)$ y $P(a,x)$ vemos que no existe, luego no podríamos seguir el proceso anterior. Hay que tener en cuenta que **las variables de dos cláusulas distintas son distintas, aunque tengan el mismo nombre. Caso de que coincidan los nombres es conveniente cambiar el nombre de las variables de alguna de ellas.**

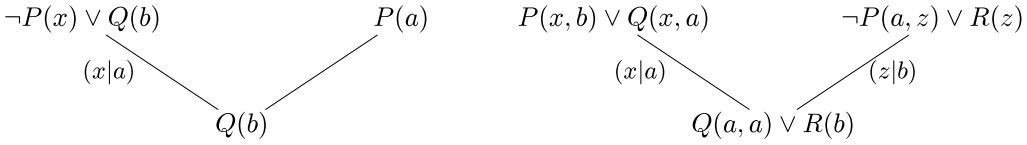
Definimos ya lo que es una resolvente binaria de dos cláusulas:

**Definición 65.** *Sean $C_1$ y $C_2$ dos cláusulas que no tienen variables comunes. Supongamos que $C_i = L_i \vee C_i'$, donde $L_i$, $i = 1,2$ es un literal y $C_i, i = 1,2$ es una cláusula (que podría ser la vacía), y que los literales $L_1$ y $L_2^C$ tienen un unificador principal $\sigma$.*

*Entonces la cláusula $\sigma(C_1') \vee \sigma(C_2')$ es una resolvente binaria de $C_1$ y $C_2$.*

Por ejemplo, $Q(b)$ es una resolvente binaria de las cláusulas $\neg P(x) \vee Q(b)$ y $P(a)$, mientras que $Q(a,a) \vee R(b)$ es una resolvente binaria de $P(x,b) \vee Q(x,a)$ y $\neg P(a,z) \vee R(z)$.

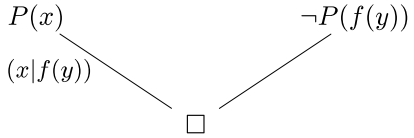
Normalmente, para indicar que una cláusula se obtiene como resolvente binaria de otras dos usaremos la notación siguiente:




Una vez visto cómo obtener una resolvente, podemos afirmar que si de un conjunto de cláusulas podemos obtener la cláusula vacía haciendo resolventes, entonces el conjunto es insatisfacible.

Por ejemplo, podemos ver que el conjunto $\{P(x), \neg P(f(x))\}$ es insatisfacible.

En principio podría parecer que no es posible obtener ninguna resolvente, pues $P(x)$ y $P(f(x))$ no son unificables. Sin embargo, hemos dicho que cuando tengamos variables que aparecen en dos cláusulas, podemos cambiar las de una de ellas. En este caso nos quedaría el conjunto de cláusulas como $\{P(x), \neg P(f(y))\}$, y ahora si podemos hacer resolventes:




Tomamos el conjunto $\{P(x) \vee P(y), \neg P(z) \vee \neg P(u)\}$. Este es también insatisfacible y sin embargo no podemos obtener de ninguna forma la cláusula vacía haciendo resolventes binarias.

Necesitamos por tanto extender el concepto de resolvente para que podamos contemplar casos como este (y otros algo más complicados).

### 9.1.2. Resolventes

Para definir una resolvente, necesitamos previamente el concepto de factor.

Sea $C$ una cláusula. Supongamos que en $C$ hay dos o más literales que son unificables, y sea $\sigma$ un unificador principal. En ese caso, diremos que $\sigma(C)$ es un **factor** de $C$. En el caso de que $\sigma(C)$ sea un factor de $C$ se verifica que $C \vDash \sigma(C)$.

Por ejemplo, si $C = P(x) \vee P(f(a)) \vee Q(x, b)$ entonces $P(f(a)) \vee Q(f(a), b)$ es un factor de $C$ (hemos unificado los dos primeros literales con la sustitución $(x|f(a))$).

Notemos que si queremos hallar un factor de una cláusula, y en dos o más literales tenemos variables repetidas, para obtener un unificador **no podemos** renombrar las variables (salvo que a todas las apariciones de la variable en la cláusula le demos el mismo nombre).

**Definición 66.** *Sean $C_1$ y $C_2$ dos cláusulas. Se dice que $C$ es una* **resolvente** *de $C_1$ y $C_2$ si $C$ responde a alguna de las cuatro posibilidades siguientes:*

1. *$C$ es una resolvente binaria de $C_1$ y $C_2$.*
2. *$C$ es una resolvente binaria de $C_1$ y un factor de $C_2$.*
3. *$C$ es una resolvente binaria de un factor de $C_1$ y de $C_2$.*
4. *$C$ es una resolvente binaria de un factor de $C_1$ y un factor de $C_2$.*

Notemos que si $C$ es una resolvente de $C_1$ y $C_2$ entonces $\{C_1, C_2\} \vDash C$.

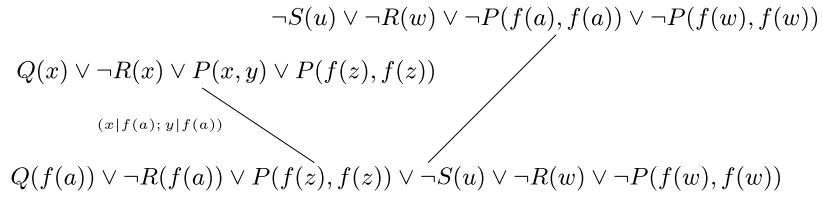
**Ejemplo 9.1.1.**

1. *Consideramos las cláusulas $C_1 = P(x) \vee P(y)$ y $C_2 = \neg P(z) \vee \neg P(u)$. Entonces $P(x)$ es un factor de $C_1$, $\neg P(z)$ es un factor de $C_2$, y $\square$ es una resolvente binaria de $P(x)$ y $\neg P(z)$. Por tanto, $\square$ es una resolvente de $C_1$ y $C_2$.*

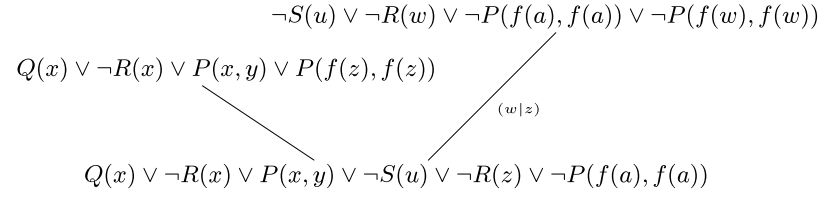
   *Vemos así que el conjunto $\{P(x) \vee P(y), \neg P(z) \vee \neg P(u)\}$ es insatisfacible.*

2. *Vamos ahora a obtener varias resolventes de las cláusulas*

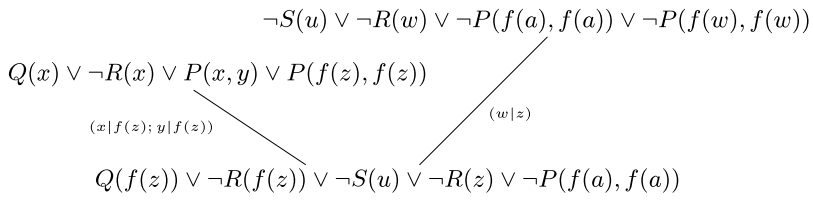
$$C_1 = Q(x) \vee \neg R(x) \vee P(x, y) \vee P(f(z), f(z))$$
$$C_2 = \neg S(u) \vee \neg R(w) \vee \neg P(f(a), f(a)) \vee \neg P(f(w), f(w))$$



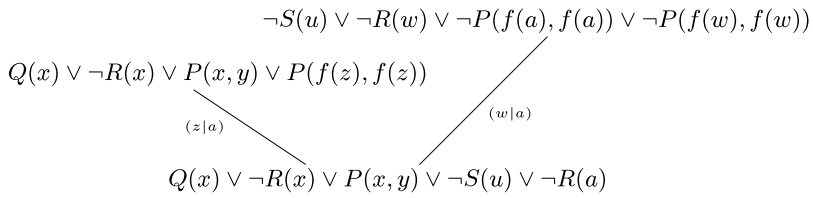

*En este caso se ha obtenido una resovente binaria de $C_1$ y $C_2$.*



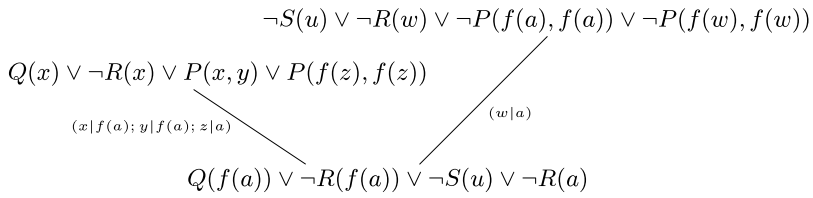
*En este caso, también hemos obtenido una resolvente binaria de $C_1$ y $C_2$. Podemos conseguir dos más.*




*Aquí hemos hecho una resolvente binaria de un factor de $C_1$ y $C_2$. Podríamos hacer otra más.*




*Aquí, una resolvente binaria de $C_1$ y un factor de $C_2$. Se puede hacer otra más.*




*Por último, lo que hemos hecho es una resolvente binaria de un factor de $C_1$ y un factor de $C_2$.*

### 9.1.3. Deducciones y principio de resolución.

Sea $\Gamma$ un conjunto de cláusulas, y $C$ una cláusula. Una *deducción* de $C$ a partir de $\Gamma$ es una sucesión finita de cláusulas $C_1, C_2, \cdots C_n$ donde $C_n = C$, y para $i < n$, $C_i$ es una cláusula, que bien es un elemento de $\Gamma$, bien es una resolvente de dos cláusulas que la preceden.

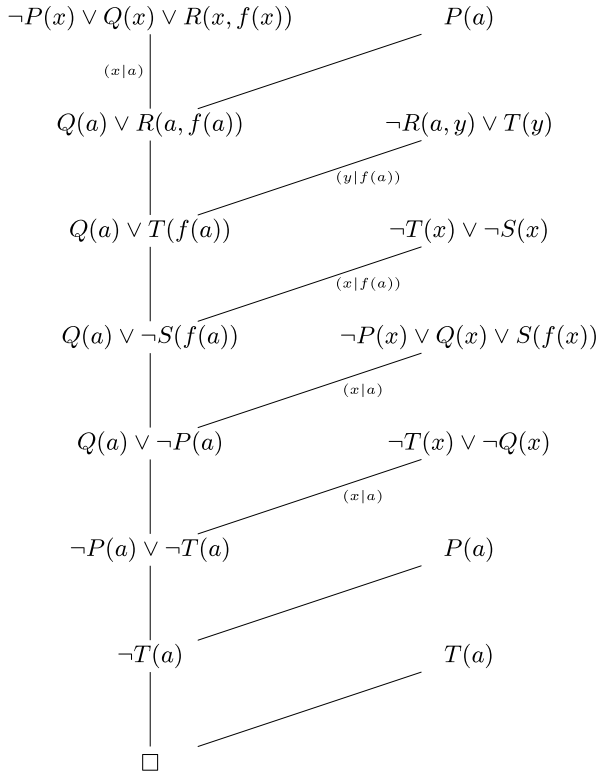
**Ejemplo 9.1.2.** *En el ejemplo 7.1.10 estuvimos viendo que para comprobar si*

$$\left\{ \begin{array}{l} \forall x(P(x) \wedge \neg Q(x) \to \exists y(R(x,y) \wedge S(y))) \\ \exists y \forall x((R(y,x) \to T(x)) \wedge T(y) \wedge P(y) \end{array} \right\} \models \exists x(T(x) \wedge (Q(x) \vee S(x)))$$

*bastaba con comprobar si el conjunto de cláusulas*

$$\Gamma = \left\{ \begin{array}{lll} \neg P(x) \vee Q(x) \vee R(x, f(x)); & \neg R(a,y) \vee T(y); & T(a); \quad P(a) \\ \neg P(x) \vee Q(x) \vee S(f(x)); & \neg T(x) \vee \neg Q(x); & \neg T(x) \vee \neg S(x) \end{array} \right\}$$

*es insatisfacible. Ahora vamos a ver que este conjunto es insatisfacible, para lo cual vamos a dar una deducción de la cláusula vacía.*




*Si consideramos las cláusulas:*

$$C_1 = \neg P(x) \vee Q(x) \vee R(x, f(x)); C_2 = P(a); C_3 = Q(a) \vee R(a, f(a)); C_4 = \neg R(a, y) \vee T(y);$$
$$C_5 = Q(a) \vee T(f(a)); C_6 = \neg T(x) \vee \neg S(x); C_7 = Q(a) \vee \neg S(f(a)); C_8 = \neg P(x) \vee Q(x) \vee S(f(x));$$
$$C_9 = Q(a) \vee \neg P(a); C_{10} = \neg T(x) \vee \neg Q(x); C_{11} = \neg P(a) \vee \neg T(a); C_{12} = \neg T(a); C_{13} = T(a); C_{14} = \square$$

*entonces:*

1. $C_1$ *y* $C_2$ *son elementos de* $\Gamma$.
2. $C_3$ *es resolvente de* $C_1$ *y* $C_2$.
3. $C_4$ *es un elemento de* $\Gamma$.
4. $C_5$ *es una resolvente de* $C_3$ *y* $C_4$.
5. $C_6$ *es un elemento de* $\Gamma$.
6. $C_7$ *es una resolvente de* $C_5$ *y* $C_6$.
7. $C_8$ *es un elemento de* $\Gamma$.
8. $C_9$ *es una resolvente de* $C_7$ *y* $C_8$.
9. $C_{10}$ *es un elemento de* $\Gamma$.
10. $C_{11}$ *es una resolvente de* $C_9$ *y* $C_{10}$.
11. $C_{12}$ *es una resolvente de* $C_2$ *y* $C_{11}$.
12. $C_{13}$ *es un elemento de* $\Gamma$.
13. $C_{14}$ *es una resolvente de* $C_{12}$ *y* $C_{13}$.

*Por tanto* $C_{14} = \square$ *se ha deducido a partir de* $\Gamma$.

Una vez visto esto podemos dar el teorema principal de este capítulo:

**Teorema 9.1.1.** *(Completitud del principio de resolución)*

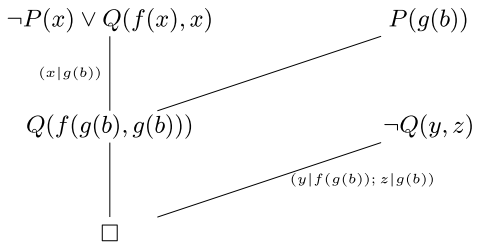
*Sea* $\Gamma$ *un conjunto de cláusulas. Entonces* $\Gamma$ *es insatisfacible si, y sólo si, existe una deducción de* $\square$ *a partir de* $\Gamma$.

**Ejemplo 9.1.3.**

1. *Vamos a comprobar que el conjunto de cláusulas*

$$\Gamma = \{\neg P(x) \vee Q(f(x), x), \quad P(g(b)), \quad \neg Q(y, z)\}$$

*es insatisfacible. Para esto, vamos a obtener una deducción de la cláusula vacía.*




2. *Vamos a comprobar que*

$$\{\forall x Q(x) \vee \exists y P(y),\ \neg\forall y Q(y)\} \vDash \exists x P(x)$$

*Demostrar eso es lo mismo que probar que el conjunto de fórmulas*

$$\{\forall x Q(x) \vee \exists y P(y),\ \neg\forall y Q(y),\ \neg\exists x P(x)\}$$

*es insatisfacible.*

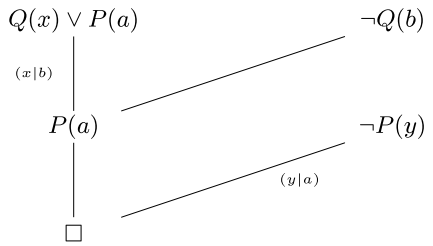
*Para esto, hallamos la forma clausular de cada una de las fórmulas:*

$$\left|\begin{array}{c} \forall x Q(x) \vee \exists y P(y) \\ \exists y \forall x (Q(x) \vee P(y)) \\ \forall x (Q(x) \vee P(a)) \end{array}\right| \left|\begin{array}{c} \neg\forall y Q(y) \\ \exists y \neg Q(y) \\ \neg Q(b) \end{array}\right| \left|\begin{array}{c} \neg\exists x P(x) \\ \forall x \neg P(x) \\ \forall y \neg P(y) \end{array}\right|$$

*Luego debemos ver que el conjunto de cláusulas*

$$\{Q(x) \vee P(a),\ \neg Q(b),\ \neg P(y)\}$$

*es insatisfacible.*



## 9.2. Estrategias de gestión

Podría parecer que con el Teorema de Completitud del Principio de Resolución está resuelto el problema de la insatisfacibilidad de un conjunto de cláusulas, y por tanto el problema de la implicación semántica. Sin embargo, esto está muy lejos de ser cierto.

Sabemos que si un conjunto de cláusulas es insatisfacible, entonces existe una deducción (que contiene un número finito de pasos) de la cláusula vacía. Pero no existe ningún algoritmo que nos dé la respuesta a la pregunta de si un conjunto es o no insatisfacible, aunque, si es insatisfacible, hay algoritmos que nos conducen a la cláusula vacía en un número finito de pasos (otro tema es que eso puede ser computacionalmente muy costoso). La dificultad está en que si el conjunto de cláusulas es satisfacible no hay ningún algoritmo que nos dé la respuesta en un finito de pasos.

Lo que vamos a ver a continuación son distintas estrategias para, dado un conjunto de cláusulas, obtener, si es insatisfacible, una deducción de la cláusula vacía.

### 9.2.1. Estrategia de Saturación

Recordemos que el problema que tenemos en este momento es el de determinar si un conjunto de cláusulas es satisfacible o insatisfatisfacible. La búsqueda de una deducción de la cláusula vacía (también llamada una refutación) o llegar a la conclusión de que ésta no existe puede abordarse calculando todas las posibles resolventes a partir del conjunto de partida. Es la **estrategia de saturación**. El procedimiento puede ejecutarse de una forma algorítmica que describimos a continuación:

Llamamos $S_0 = S$.

Para cada $i$

> Calculamos $S_{i+1}$ como el conjunto que se obtiene de $S_i$ al añadir todas las resolventes que puedan calcularse usando cláusulas de $S_i$.
>
> Si $S_{i+1}$ contiene a la cláusula vacía, entonces el conjunto de partida es **insatisfacible**;
>
> si $S_{i+1} = S_i$, entonces el conjunto de partida es **satisfacible**;
>
> en otro caso incrementar $i$ y volver a ejecutar el bucle.

Este algoritmo nos proporciona una cadena de conjuntos de cláusulas, es decir, una secuencia de conjuntos en el que cada uno está contenido en el siguiente:

$$S_0 \subseteq S_1 \subseteq \cdots \subseteq S_i \subseteq S_{i+1} \subseteq \ldots$$

y de forma que todos tienen el mismo carácter de satisfacibilidad (es decir, uno es insatisfacible si, y sólo si, lo es otro cualquiera).

Cuando en uno de los eslabones aparece la cláusula vacía tenemos asegurada la insatisfacibilidad; cuando la cadena se estabiliza (es decir $S_i = S_{i+1}$, y por tanto todos los siguientes vuelven a ser iguales a $S_i$ puesto que no aparecen nuevas resolventes) entonces ya se tiene que no es posible obtener una deducción de la cláusula vacía, puesto que se han explorado **todas** las posibilidades. Hay dos problemas que presenta este método: la imposibilidad de detener el proceso en un número finito de pasos y que el esfuerzo de cálculo sea inabordable.

**Ejemplo 9.2.1.** *Consideremos el conjunto*

$$S = \{\neg P(x) \vee Q(f(x)),\ P(a),\ \neg P(y) \vee \neg Q(y)\}$$

*Inicializamos $S_0 = S$ y calculamos las posibles resolventes entre sus cláusulas. Las numeramos para obtener una más fácil referencia:*

$C_1 = \neg P(x) \vee Q(f(x))$

$C_2 = P(a)$

$C_3 = \neg P(x) \vee \neg Q(x)$

*entonces podemos obtener las siguientes nuevas cláusulas:*

$C_4 = R(C_1, C_2) = Q(f(a))$ *con el unificador* $(x|a)$*;*

$C_5 = R(C_1, C_3) = \neg P(x) \vee \neg P(f(x))$ *con el unificador* $(y|f(x))$*;*

$C_6 = R(C_2, C_3) = \neg Q(a)$ *con el unificador* $(x|a)$*.*

*El conjunto* $S_1$ *consta de las seis cláusulas que tenemos hasta el momento:*

$$S_1 = \{\neg P(x) \vee Q(f(x)),\ P(a),\ \neg P(y) \vee \neg Q(y),\ Q(f(a)),\ \neg P(x) \vee \neg P(f(x)),\ \neg Q(a)\}$$

*Como no contiene a la cláusula vacía ni coincide con el anterior, entonces proseguimos calculando* $S_2$*:*

*A partir de la* $C_1$ *no es posible calcular nuevas resolventes;*

$C_7 = R(C_2, C_5) = R(C_3, C_4) = \neg P(f(a))$*;*

*tampoco hay más resolventes entre el resto de cláusulas.*

$$S_2 = \left\{ \begin{array}{llll} \neg P(x) \vee Q(f(x)); & P(a); & \neg P(y) \vee \neg Q(y); & Q(f(a)); \\ \neg P(x) \vee \neg P(f(x)); & \neg Q(a); & \neg P(f(a)) & \end{array} \right\}$$

*De nuevo examinamos si aparece la cláusula vacía, lo que no ocurre, y* $S_2 \neq S_1$*, así que debemos continuar calculando* $S_3$*: como sólo hay una cláusula nueva entonces las nuevas resolventes tendrían que serlo de* $C_7$*, pero ésta no admite ninguna resolvente con el resto. Así que*

$$S_3 = S_2$$

*y el algoritmo acaba emitiendo la respuesta:* **el conjunto es satisfacible**.

**Ejemplo 9.2.2.** *Sea ahora* $S_0 = \{A(b),\ \neg M(y) \vee P(b, y),\ \neg P(x, z),\ M(a),\ C(a)\}$ *y comencemos a ejecutar el algoritmo:*

$C_6 = R(C_2, C_3) = \neg M(y)$

$C_7 = R(C_2, C_4) = P(b, a)$

*Así que* $S_1$ *consta de las siete cláusulas descritas, no contiene a la cláusula vacía y tampoco coincide con el anterior. Calculamos* $S_2$ *y encontramos* $C_8 = R(C_4, C_6) = \square$ *con lo que el algoritmo acaba con la respuesta* **el conjunto es insatisfacible**. *Para reconstruir la deducción que nos lleva a la cláusula vacía recorremos el proceso en sentido inverso:*

$\square = R(C_4, C_6)$

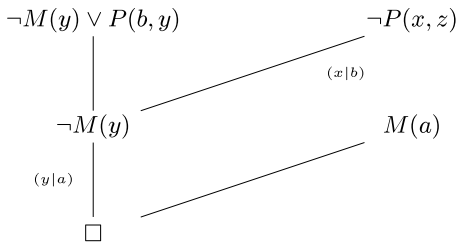
$C_6 = R(C_2, C_3)$

$C_2$ *y* $C_3$ *son cláusulas del conjunto de partida.*

*y la deducción sería:*

1. $C_2$ *está en* $S$*;*
2. $C_3$ *está en* $S$*;*
3. $C_6$ *es resolvente de las dos anteriores;*
4. $\square$ *es resolvente de dos anteriores.*

*o dibujada en forma de árbol:*




Los dos ejemplos anteriores son representativos de la situación habitual, cuando la cantidad de cláusulas que aparecen en los sucesivos conjuntos $S_i$ pueden ser enormes. Se propone como ejercicio realizar los primeros pasos de la estrategia de saturación para el siguiente conjunto de cláusulas:

$$\Gamma = \{\neg E(x,y) \vee \neg E(x,z) \vee E(z,y),\ \neg E(u,v) \vee E(v,u),\ E(a,b),\ E(b,c),\ \neg E(a,c)\ \}$$

Por último, tomamos el conjunto de cláusulas

$$\Gamma = \{\neg P(x) \vee P(f(x));\ P(a)\}$$

Partimos de $S_0 = \Gamma$, y vamos construyendo los distintos conjuntos $S_i$:

$$S_1 = \{\neg P(x) \vee P(f(x));\ P(a);\ P(f(a))\}$$
$$S_2 = \{\neg P(x) \vee P(f(x));\ P(a);\ P(f(a));\ P(f(f(a)))\}$$
$$S_3 = \{\neg P(x) \vee P(f(x));\ P(a);\ P(f(a));\ P(f(f(a)));\ P(f(f(f(a))))\}$$

Y podemos ver como obtenemos una sucesión

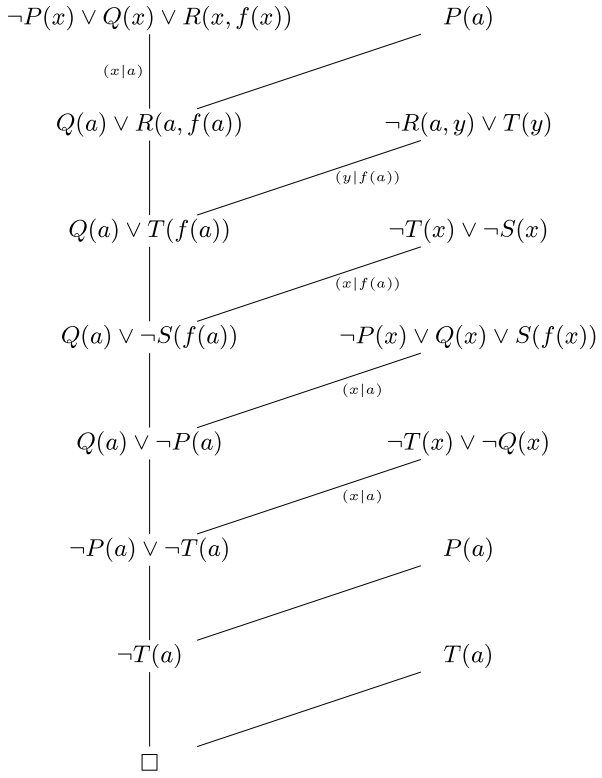
$$S_0 \subsetneq S_1 \subsetneq S_2 \subsetneq S_3 \subsetneq \cdots \subsetneq S_i \subsetneq S_{i+1} \subsetneq \cdots$$

y en la que nunca nos aparecerá la cláusula vacía.

Por tanto, el algoritmo en este caso no terminaría. Si en algún caso no llegamos a ninguna de las dos condiciones de parada, ¿cuándo terminamos?. Si no nos ha salido la cláusula vacía, ¿es porque no se puede obtener, o porque no hemos hecho las iteraciones necesarias para conseguirla?.

### 9.2.2. Deducciones lineales

Hasta ahora hemos escrito y dibujado varios ejemplos de deducciones. Si observamos el esquema de la deducción:

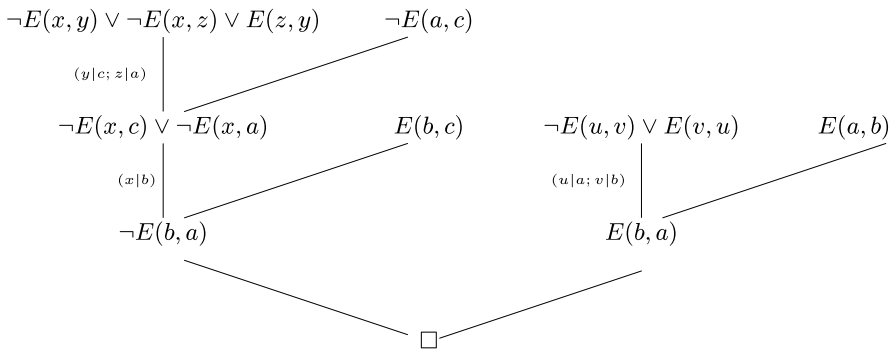



notamos que cada nueva resolvente se ha calculado utilizando justo la que se ha obtenido en el paso anterior. En el dibujo aparece una línea vertical que nos lleva desde la cláusula de partida a la cláusula vacía. Es lo que se llama una **deducción lineal**. No todas las deducciones tienen que verificar esta propiedad:

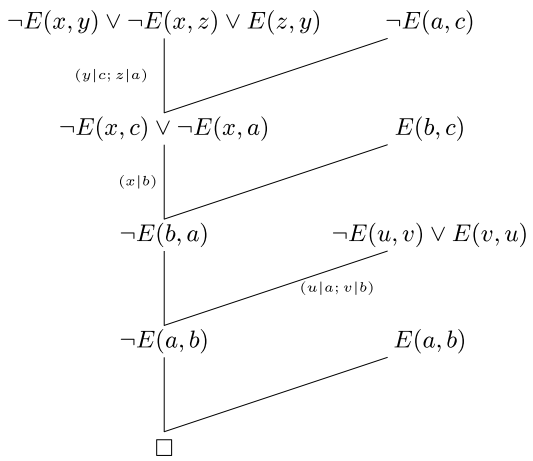
**Ejemplo 9.2.3.** *Veamos el dibujo de una refutación para el conjunto*

$$\Gamma = \{\neg E(x,y) \vee \neg E(x,z) \vee E(z,y),\ \neg E(u,v) \vee E(v,u),\ E(a,b),\ E(b,c),\ \neg E(a,c)\}$$

*que no es lineal:*




*Sin embargo, a partir de cada deducción se puede obtener una que sea* **lineal**. *En este caso podemos modificar la anterior así:*




Esto es un resultado general, se tiene:

**Teorema 9.2.1.** *Si para un conjunto de cláusulas existe una deducción de la cláusula vacía, entonces existe una deducción lineal de la cláusula vacía.*

Y como consecuencia en adelante **nos limitaremos a usar deducciones lineales** (o refutaciones lineales).

### 9.2.3. Deducciones lineales-input

Pero el problema principal que teníamos era el de la gran cantidad de posibilidades para calcular resolventes, que pueden convertir un problema en inabordable en la práctica. Existen distintas opciones de restricción a la hora de elegir resolventes a calcular. En primer lugar observemos que podríamos limitarnos a las deducciones lineales que parten de **una cláusula fija** a la que llamaremos **raíz**. En el deducción lineal del ejemplo anterior se ha usado $\neg E(x,y) \vee \neg E(x,z) \vee E(z,y)$ como raíz de la deducción. Si además limitásemos las posibles cláusulas que pueden entrar para calcular resolventes en la línea, tendríamos un número de posibilidades pequeño. Al conjunto de cláusulas que se elige para entrar a formar resolventes se le suele llamar **conjunto usable**.

Cuando elegimos una raíz y un conjunto usable, podemos dibujar el conjunto de todas las deducciones lineales que parten de la raíz como un árbol en el que en cada nodo aparecen tantas ramas como resolventes podamos hacer con esa cláusula y las del conjunto usable. Cada rama es una deducción lineal, luego debemos buscar una rama que acabe en la cláusula vacía.

El problema es que estas restricciones pueden hacer que la deducción lineal que nos lleva hasta la cláusula vacía no nos parezca entre las calculadas.

**Ejemplo 9.2.4.** *Para el conjunto*

$$\Gamma = \{\neg E(x,y) \vee \neg E(x,z) \vee E(z,y),\ \neg E(u,v) \vee E(v,u),\ E(a,b),\ E(b,c),\ \neg E(a,c)\}$$

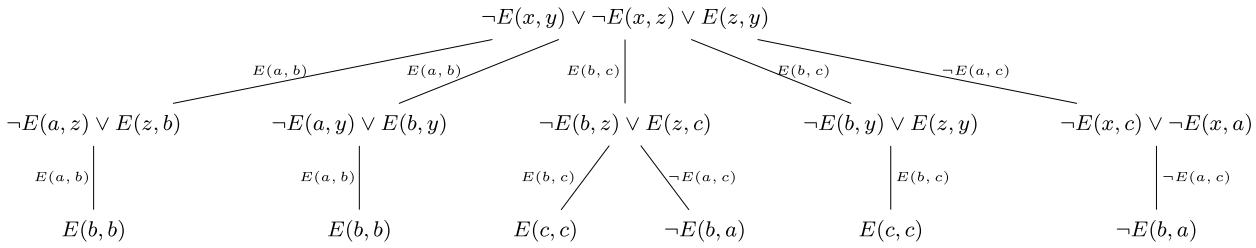
*elegimos como raíz la cláusula*

$$\neg E(x,y) \vee \neg E(x,z) \vee E(z,y)$$

*y tomamos como conjunto usable el de las cláusulas del conjunto de partida que constan de un solo literal (es una estrategia de selección llamada* **UNIT***), es decir*

$$\begin{cases} C_3 = E(a,b) \\ C_4 = E(b,c) \\ C_5 = \neg E(a,c) \end{cases}$$

*Dibujamos el árbol de* **todas** *las deducciones lineales:*




*En las hojas que nos quedan no pueden calcularse nuevas resolventes con el conjunto usable que hemos elegido* $\{C_3, C_4, C_5\}$*, y en ninguna de las ramas del árbol aparece la cláusula vacía, por lo que hemos perdido la solución adecuada del problema.*

En el ejemplo anterior una posible solución es permitir que el conjunto usable se alimente también de las cláusulas unit que se vayan obteniendo como resolvente a lo largo del proceso. Cuando no se permite la introducción de nuevas cláusulas a lo largo del proceso en el conjunto usable decimos que la estrategia es **input**.

**Ejemplo 9.2.5.** *Para otros conjuntos de cláusulas la estrategia puede tener un resultado satisfactorio. Por ejemplo, si tomamos el conjunto*

$$\Gamma = \{\neg P(x) \vee Q(x),\ \neg P(x) \vee \neg Q(x),\ P(a),\ Q(b)\}$$

*la estrategia de obtener las deducciones lineales que parten de la raíz* $\neg P(x) \vee \neg Q(x)$ *y utilizar como conjunto usable el de las cláusulas unit da una respuesta rápidamente. En cambio, con la raíz* $\neg P(x) \vee Q(x)$ *no aparece una solución. Eso significa que la elección de la raíz es esencial en la obtención de una solución.*

La estrategia de selección de deducciones que vamos a utilizar es la de búsqueda de deducciones lineales que son input (esto es, las resolventes que se obtienen **no** se introducen en el conjunto usable) y con conjunto usable todas las cláusulas de partida salvo la que se elige como raíz: son las deducciones **lineales-input**.

Resumimos las características de esta estrategia de elección de deducciones:

- Se elige una cláusula raíz.
- El resto de las cláusulas del conjunto de partida forman el conjunto usable.
- Se consideran deducciones lineales.

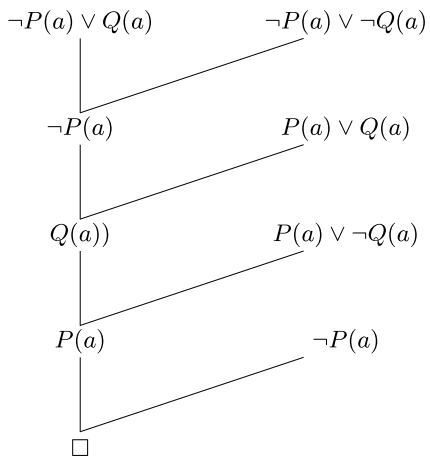
Así podremos construir el **árbol de las deducciones lineales-input** que tendrá por nodo raíz a la cláusula que hayamos elegido. Una deducción lineal-input de la cláusula vacía es un recorrido desde la raíz del árbol a una rama que termine en la cláusula vacía.

Esta estrategia de elección de deducciones lineales-input **no es completa**, es decir, puede que el conjunto sea insatisfacible y no exista ninguna deducción lineal-input.

**Ejemplo 9.2.6.** *Consideremos el conjunto*

$$\{\neg P(a) \vee Q(a),\ \neg P(a) \vee \neg Q(a),\ P(a) \vee Q(a),\ P(a) \vee \neg Q(a)\}$$

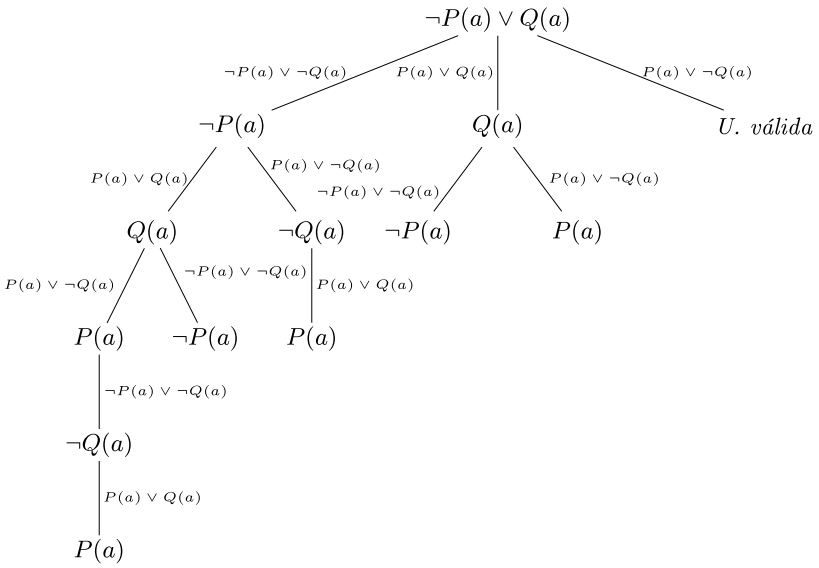
*que es insatisfacible y que tiene como refutación lineal:*




*que* **no es input** *puesto que en la última resolvente participa una cláusula que se ha obtenido en el proceso* ($\neg P(a)$).

*Sin embargo el árbol de las deducciones lineales-input (con cualquier elección de la raíz) no tiene como nodo a la clásula vacía. Podemos intentar construir el que tiene parte de* $\neg P(a) \vee Q(a)$*; para ello ordenamos el resto de cláusulas y construimos el árbol calculando resolventes en el orden en el que se presentan el conjunto usable:*

$$\begin{cases} C_1 = \neg P(a) \vee \neg Q(a), \\ C_2 = P(a) \vee Q(a), \\ C_3 = P(a) \vee \neg Q(a) \end{cases}$$




*Y vemos como cualquier rama que pase por* $P(a)$*, como cualquier rama que pase por* $\neg P(a)$ *puede prolongarse hasta el infinito, y nunca llega a la cláusula vacía.*

*Así que el árbol de todas las deducciones lineales-input no contiene a la cláusula vacía, aunque sabemos que el conjunto es insatisfacible.*

*Si hubiéramos tomado como raíz otra de las cláusulas, nos saldría un árbol de deducciones semejante al que hemos obtenido aquí.*

### 9.2.4. Recorridos en el árbol de las deducciones

Incluso en el caso en que la cláusula vacía aparezca en el árbol de las deducciones lineales-input, a la hora de acometer de forma algorítmica su búsqueda podemos tener problemas prácticos. Suponemos que son conocidas técnicas de recorridos de árboles, en concreto los recorridos primero en anchura y primero en profundidad. Un recorrido explorando primero en profundidad puede encontrar una rama infinita que nos haga imposible el acceso a otras ramas; el recorrido primero en anchura encuentra con seguridad la cláusula vacía si ésta se encuentra entre los nodos, el inconveniente es que los requisitos de memoria de este tipo de exploración puede ser tremendamente costosos. En las implementaciones suelen adoptarse métodos de exploración primero en profundidad pero que contemplen una interrupción forzada después de un determinado número de pasos.

## 9.3. Conjuntos de Horn

En la sección anterior aparecía un ejemplo de conjunto insatisfacible en el que el árbol de las deducciones lineales-input con una raiz determinada no contiene a la cláusula vacía; es decir, la estrategia de reducirse a las deducciones lineales-input no es una estrategia completa en el caso general. Sin embargo la focalización hacia ella que hemos realizado en la sección anterior está totalmente justificada por su importancia en los casos que se ajustan al modelo que presentamos a continuación.

### 9.3.1. Descripción de un conjunto de Horn

**Definición 67.** *Una cláusula se dice que es una* **cláusula de Horn** *si tiene exactamente un literal positivo.*

Entre las cláusulas de Horn podemos distinguir dos tipos según si tienen algún literal negativo, las llamadas **reglas**, o si sólo contienen al literal positivo, los **hechos**.

**Ejemplo 9.3.1.** *La siguiente es una lista de cláusulas de Horn:*

$C(b)$ *es un hecho;*

$D(x) \vee \neg M(x)$ *es una regla;*

$\neg D(x) \vee M(x)$ *es una regla;*

$\neg C(y) \vee CC(f(y), y)$ *es una regla;*

$\neg C(y) \vee \neg CC(x, y) \vee M(x)$ *es una regla.*

En términos del lenguaje de programación **PROLOG** un conjunto de reglas y hechos, es decir, un conjunto de cláusulas de Horn, forman un **programa**.

Cuando una cláusula tiene todos sus literales negativos la llamaremos **cláusula negativa u objetivo**. Un ejemplo de cláusula negativa es

$$\neg M(x) \vee \neg D(x) \vee \neg CC(x, y) \vee \neg C(y)$$

**Definición 68.** *Un conjunto de cláusulas se dice que es un* **conjunto de Horn** *si contiene exactamente una cláusula negativa y el resto son cláusulas de Horn.*

**Ejemplo 9.3.2.** *El conjunto de cláusulas*

$$\{C(b);\ D(x) \vee \neg M(x);\ \neg D(x) \vee M(x);\ \neg C(y) \vee CC(f(y), y);$$
$$\neg C(y) \vee \neg CC(x, y) \vee M(x);\ \neg M(x) \neg D(x) \vee \neg CC(x, y) \neg C(y)\}$$

*es un conjunto de Horn.*

El resultado que nos permite reducirnos a las deducciones lineales-input en el caso de los conjuntos de Horn es el siguiente:

**Teorema 9.3.1.** *Si $\Gamma$ es un conjunto de Horn insatisfacible entonces existe una deducción de la cláusula vacía que es lineal-input y que parte de la cláusula objetivo.*

Es decir, la estrategia de reducirnos a las deducciones lineales-input con raíz la cláusula objetivo (negativa) y conjunto usable el formado por las cláusula de Horn, es completa. Así, en estas circunstancias, será suficiente explorar el árbol de las deducciones lineales-input con raíz el objetivo para determinar si el conjunto es o no insatisfacible. Como ya advertimos en la sección anterior, otro problema es si esta exploración se puede ejecutar de una forma satisfactoria.

### 9.3.2. Resolventes en conjuntos de Horn

Estamos ahora en la situación de calcular deducciones input- lineales partiendo de la cláusula objetivo. Queremos poner de manifiesto qué forma tienen las resolventes que se calculan en cada paso y para ello vamos a trabajar sobre el ejemplo de conjunto de Horn del apartado anterior:

$$\{C(b);\ D(x) \vee \neg M(x);\ \neg D(x) \vee M(x);\ \neg C(y) \vee CC(f(y), y);$$
$$\neg C(y) \vee \neg CC(x, y) \vee M(x);\ \neg M(x)\neg D(x) \vee \neg CC(x, y)\neg C(y)\}$$

La cláusula negativa u **objetivo** es

$$\neg M(x) \vee \neg D(x) \vee \neg CC(x, y) \vee \neg C(y)$$

y el conjunto usable son las cláusulas de Horn en las que hemos situado en primera posición siempre el literal positivo:

1. $C(b)$
2. $D(x) \vee \neg M(x)$
3. $M(x) \vee \neg D(x)$
4. $CC(f(y), y) \vee \neg C(y)$
5. $M(x) \vee \neg C(y) \vee \neg CC(x, y)$

Comencemos calculando la resolvente de la raíz con la primera cláusula que es un **hecho**: unificamos los literales $C(b)$ y $C(y)$ con $(y|b)$ y la resolvente queda:

$$\neg M(x) \vee \neg D(x) \vee \neg CC(x, b)$$

que es **de nuevo una cláusula objetivo**, es decir tiene todos sus literales negativos. Lo mismo ocurre si calculamos resolvente con una regla, veamos una pequeña justificación general:

Tengamos $\neg P_1 \vee \neg P_2 \cdots \vee \neg P_s$ una cláusula objetivo, y $P_1 \vee \neg Q_1 \cdots \vee \neg Q_r$ una regla. Entonces la resolvente (observemos que sólo se puede resolver con el literal positivo de la cláusula de Horn) sería

$$\neg P_2 \cdots \vee \neg P_s \vee \neg Q_1 \cdots \vee \neg Q_r$$

que vuelve a ser una cláusula objetivo.

Así, cuando se calcula el árbol de las deducciones lineales-input en cada nodo se tiene siempre una cláusula negativa u objetivo desde la que se calcularán resolventes con aquellas cláusulas de Horn que tengan el literal positivo unificable con alguno de los del objetivo.

**Ejemplo 9.3.3.** *Partiendo de la raiz $\neg M(x)\neg D(x) \vee \neg CC(x, y) \vee \neg C(y)$ podemos calcular 5 resolventes distintas, esto es, se abren 5 ramas distintas del árbol que organizaríamos de izquierda a derecha según el orden de la cláusula de Horn que usamos:*

1. $\neg M(x) \vee \neg D(x) \vee \neg CC(x, b)$
2. $\neg M(x) \vee \neg CC(x, y) \vee \neg C(y)$
3. $\neg D(x) \vee \neg CC(x, y) \vee \neg C(y)$

4. $\neg M(x)\neg D(x) \vee \neg C(y)$

5. $\neg D(x) \vee \neg CC(x,y) \vee \neg C(y)$

*A partir de cada uno de estos nodos, que de nuevo son objetivos, se vuelven a abrir ramas al resolver con las cláusulas de Horn.*

Tenemos que señalar en este momento que este proceso se puede convertir en automático. Sólo es necesario determinar el orden en que se examinan los objetivos parciales (cada uno de los literales que aparecen en el objetivo) y las cláusulas con un literal positivo.

### 9.3.3. Cómo surge un conjunto de Horn

Cabe preguntarse qué problemas de consecuencia lógica van a producir conjuntos de Horn cuando sean transformados a insatisfacibilidad de un conjunto de cláusulas. Podemos dar una sencilla respuesta sin más examinar los distintos tipos de cláusulas.

Un hecho representa a una afirmación sobre la veracidad de un predicado en un contexto: $C(b)$, es decir, $C$ es cierto para la constante $b$, o $C(x)$ que recordemos que es la manera en la que escribimos $\forall x C(x)$, es decir, $C$ es cierto para todo elemento del dominio.

Para aproximarnos al significado de una regla, digamos $\neg C(y) \vee \neg CC(x,y) \vee M(x)$ observamos que podemos, usando las leyes de Morgan, transformarla en la fórmula lógicamente equivalente $\neg(C(y) \wedge CC(x,y)) \vee M(x)$ que a su vez puede cambiarse por $(C(y) \wedge CC(x,y)) \rightarrow M(x)$. Ahora, recordemos que hay que incluir el cierre universal y leemos $\forall x \forall y[(C(y) \wedge CC(x,y)) \rightarrow M(x)]$: **Si** ocurre $C(y)$ y ocurre $CC(x,y)$, **entonces** ocurre $M(x)$ que tiene la forma del enunciado de una regla.

Por último fijemos nuestra atención en la cláusula negativa y pensemos que proviene de incluir la negación de la consecuencia en el conjunto de premisas; entonces el objetivo $\neg M(x)\neg D(x) \vee \neg CC(x,y) \vee \neg C(y)$ que, como antes, representa a su cierre universal, proviene de la negación de la fórmula

$$\exists x \exists y[M(x) \wedge D(x) \wedge CC(x,y) \wedge C(y)]$$

que es una pregunta de la forma ¿existen elementos para los que son ciertos simultáneamente todos los predicados?

**Ejemplo 9.3.4.** *Vamos a mostrar un ejemplo en el que trataremos de determinar si alguna frase es consecuencia lógica del siguiente conjunto de premisas:*

1. *Adán es una persona*

2. *Eva es una persona*

3. *Eva es la madre de Caín*

4. *Eva es la madre de Abel*

5. *Todo hijo de una persona es una persona*

*Observamos que cada una de estas premisa está enunciada como un hecho o como una regla, en efecto, su traducción al lenguaje de primer orden con elementos*

**constantes:** *e (Eva), c (Caín), a (Abel);*

**Predicados:** $P(x)$ : *x es una persona;* $M(x,y)$ : *x es la madre de y*

*podría ser:*

1. $P(a)$ *(hecho)*

2. $P(e)$ *(hecho)*

3. $M(e,c)$ *(hecho)*

4. $M(e,a)$ *(hecho)*

5. $\forall x \forall y(M(x,y) \wedge P(x) \rightarrow P(y)$ *(regla)*

*y las correspondientes cláusulas (de Horn) que proporcionan (lo que se llamaría un programa en lenguaje PROLOG) son:*

1. $P(a)$ *(hecho)*
2. $P(e)$ *(hecho)*
3. $M(e,c)$ *(hecho)*
4. $M(e,a)$ *(hecho)*
5. $P(y) \vee \neg M(x,y) \vee \neg P(x)$ *(regla)*

*Este conjunto de premisas puede utilizarse para determinar si una serie de preguntas tienen respuesta afirmativa. Estas preguntas darán lugar al objetivo. Para este programa podemos formular preguntas como:*

? *Es Eva una persona*

? *Es Caín una persona*

? *Hay alguna persona*

? *Es Caín hijo*

? *Tiene madre Abel*

? *Hay alguien que sea hijo de Eva.*

? *Tiene madre Eva*

*que se traducen en el lenguaje de primer orden que estamos usando por las fórmulas:*

1. $P(e)$,
2. $P(c)$,
3. $\exists x P(x)$,
4. $\exists x M(x,c)$,
5. $\exists x M(x,a)$
6. $\exists y M(e,y)$

*Cada una de estas preguntas da lugar a un problema de consecuencia lógica y este se convierte en un problema de probar la insatisfacibilidad de un conjunto de Horn; además el conjunto usable es el mismo y sólo varía la cláusula objetivo de la que partimos.*

### 9.3.4. Un programa y varios objetivos

Para el programa (es decir, el conjunto de cláusulas de Horn) del ejemplo anterior
y las correspondientes cláusulas (de Horn) que proporciona (lo que se llamaría un programa en lenguaje PROLOG) son:

1. $P(a)$ (hecho)
2. $P(e)$ (hecho)
3. $M(e,c)$ (hecho)
4. $M(e,a)$ (hecho)
5. $P(y) \vee \neg M(x,y) \vee \neg P(x)$ (regla)

desarrollaremos parte del árbol de las deducciones lineales-input correspondiente a algunos de los objetivos.

**Ejemplo 9.3.5.** *Queremos saber si puede deducirse de nuestro conjunto de premisas que Caín es una persona, es decir, si $P(c)$ es consecuencia lógica del conjunto de fórmulas inicial:*

$$\{P(a);\ P(e);\ M(e,c);\ M(e,a);\ \forall x\forall y(M(x,y)\wedge P(x)\to P(y)\}$$

*En primer lugar tendremos que negar la conclusión :$\neg P(c)$ y a continuación calculamos las deduciones lineales-input partiendo del objetivo:*

$$\neg P(c)$$

$$\overset{5,\,(y|c)}{\Big|}$$

$$\neg M(x,c)\vee\neg P(x)$$

$$\overset{3,\,(x|e)}{\Big|}$$

$$\neg P(e)$$

$$\overset{2}{\Big|}$$

$$\square$$

*Y puesto que hemos obtenido la cláusula vacía, la consecuecnia lógica ocurre.*

**Ejemplo 9.3.6.** *Ahora nos preguntamos si hay alguien que sea hijo de Eva, es decir, queremos comprobar si $\exists yM(e,y)$ es consecuencia lógica de nuestro programa. Negando esta conclusión obtenemos la cláusula objetivo $\neg M(e,y)$ que es la raíz del árbol de las deducciones lineales-input:*

$$\neg M(e,y)$$

$$\overset{3,\,(y|c)}{\Big|}$$

$$\square$$

*y obtenemos que también es consecuencia lógica. Además, si seguimos el valor que toma la variable y para llegar a la cláusula vacía, obtenemos que $y=c$, lo cual se puede interpretar como una respuesta más concreta: Sí, hay alguien que es hijo de Eva y es Caín. Aunque hemos obtenido una respuesta satisfactoria, es obvio que hay otra respuesta posible que se deduce del conjunto de premisas ¿cómo puede obtenerse? Nos estamos adentrando en los procedimientos que se utilizan en el recorrido del árbol de las deducciones.*

*En la deducción anterior se calculó la resolvente del objetivo con la primera (en el orden dado) de las cláusulas de Horn y llegamos al nodo que contenía $\square$; podemos retroceder un paso y volvemos a estar een el objetivo $\neg M(e,y)$ que ahora tratamos de resolver con alguna cláusula que aparezca después de la ya utilizada: en efecto, también se puede resolver con la cláusula 4 $M(e,a)$ efectuando la sustitución $(y|a)$ y de nuevo llegamos a la cláusula vacía obteniendo la respuesta afirmativa: sí, hay alguien que es hijo de Eva y es Abel.*

**Ejemplo 9.3.7.** *Por último veamos cuál es la respuesta a la pregunta ¿Tiene madre Eva? que se traduce por la fórmula $\exists xM(x,e)$ y que al ser negada da el objetivo $\neg M(x,e)$; pero en el conjunto usable no hay ninguna cláusula que conteniendo al predicado $M$ como literal positivo sea unificable con $M(x,e)$. Así que como no es posible obtener la cláusula vacía mediante una deducción lineal-input, la respuesta es negativa: No, no podemos deducir que Eva tenga madre de las hipótesis consideradas.*