Apuntes de Fundamentos de Teoría de la Computación

Lilian Salinas

6 de julio de 2020

b

Índice general

Parte I

Preliminares

Capítulo 1

Introducción

1.1. ¿Qué es lógica?

Definición 1.1. Es el estudio de métodos y principios usados para distinguir entre razonamientos válidos o correctos e incorrectos

Esto puede parecer que no es nada divertido, pero la verdad es que lo es. Ser capaces de usar la lógica es lo que necesitamos para juegos como: buscaminas, sudoku, kakuro, ajedrez, etc.

La lógica nos permite razonar. La capacidad de razonar o inferir, es la capacidad de obtener conclusiones correctas a partir de la evidencia, y esta capacidad es la base del conocimiento. Más aún, es la base de la creación del conocimiento.

Gran parte de nuestro conocimiento es inferencial, es decir no se obtiene de la observación directa, se obtiene de inferir una cosa a partir de otra. Por ejemplo: meteorología, diagnóstico médico, etc.

La inferencia es un proceso que comienza con las premisas (conocimiento base) probablemente observado a partir de un experimento y termina con las conclusiones que es un conocimiento nuevo. Es una manera de expandir el conocimiento.

Premisa: Señal o indicio por donde se infiere algo o se viene en conocimiento de ello. Sentencia que es verdad y se considera cierta en un razonamiento.

1.2. ¿Por qué estudiar lógica?

- Porque nos entrega la capacidad de construir argumentos correctos.

- Nos ayuda a distinguir entre argumentos correctos e incorrectos.

- como estudiantes de informática, es una disciplina fundamental en varios campos de las ciencias de la computación.

1.3. Algunos conceptos importantes

Estamos hablando de dar buenos o malos argumentos, correctos o incorrectos. Pero ¿Qué es un argumento? Es el razonamiento para probar o demostrar una proposición, o para convencer de lo que se afirma o se niega. Es la expresión verbal del razonamiento. Es un conjunto de oraciones que consiste de una o más premisas que contienen evidencias o conclusiones

¡Uf! esto parece derecho y no ingeniería.

La lógica es una empresa fiscalizadora cuyo trabajo es evaluar argumentos.

Es importante notar que la validez o correctitud de los argumentos depende de la conexión que existe premisas y conclusiones y no de la veracidad de las premisas.

Ejemplo: Los caballos son verdes, las cosas verdes son plásticas, por lo tanto los caballos son plásticos.

En un argumento deductivo válido la veracidad de las premisas fuerza la veracidad de la conclusión.

En este curso nos ocuparemos de la lógica deductiva y no inductiva. Cabe notar que hay quienes dicen que la lógica inductiva no existe, pero esa es una discusión para los filósofos…

Capítulo 2

Lógica proposicional

2.1. Proposiciones

En lógica es absolutamente esencial ser capaces de analizar la estructura de las proposiciones lógicas y argumentos.

Definición 2.1. Una proposición lógica es una sentencia declarativa que adquiere un valor de verdad (Verdadero o Falso)

Ejemplos:

- Hoy llueve.
- 1+1 =2.
- La mesa es café.
- Hay vida en Marte.

Note que si bien es cierto todas las proposiciones lógicas deben tener un valor de verdad, no es necesario que nosotros lo conozcamos para que sea un proposición lógica. Cuando decimos “Hay vida en Marte”, no sabemos si hay o no hay vida, pero ciertamente esa sentencia tiene un cierto valor aunque sea desconocido para nosotros.

No todas las sentencias son proposiciones lógicas

Ejemplo:

- ¿Qué hora es?
- Hola.
- ¡Auxilio!

Definición 2.2. Una sentencia declarativa es compuesta si contiene otra sentencia declarativa completa como un componente.

Ejemplo: "Juan ama a María y María ama a David". Claramente es una proposición compuesta porque existen dos proposiciones completas: "Juan ama a María" y "María ama a David". "Juan cree que María ama a David" también es compuesta porque contiene "María ama a David". Notemos que el hecho de ser compuesta no se relaciona con el largo de la sentencia, por ejemplo, "La persona que come la torta tiene sentimiento de culpa" es una proposición simple.

2.1.1. Operadores lógicos

Un operador lógico es un símbolo que modifica una proposición lógica o actúa como un conector entre dos proposiciones lógicas. Algunos conectores logran que dos proposiciones lógicas, se transformen en una proposición compuesta.

Algunos operadores son:

- $\wedge$: "y", conjunción. La conjunción de dos proposiciones lógicas indica que ambas son verdaderas. Cuando decimos "y" estamos diciendo que para que esta proposición sea verdadera ambas componente deben ser verdaderas, en realidad estamos diciendo que dos cosas ocurren. Por ejemplo:

  p: "Juan ama a María".
  q: "María ama a Juan".
  $p \wedge q$: "Juan ama a María y María Ama a Juan".

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

- $\vee$: "o", disyunción. La disyunción de dos proposiciones lógicas indica que al menos una de las dos es verdadera. Cuando decimos "o" estamos diciendo que para que esta proposición sea verdadera decimos que la primera es verdadera o la segunda es verdadera o ambas, notemos que el "o" también incluye la posibilidad de que ambas cosas ocurran. Por ejemplo:

  p: "La mesa es café".
  q: "La silla es negra".
  $p \vee q$: "La mesa es café o la silla es negra".

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

- $\neg$: "no", negación. La negación corresponde a decir que la proposición lógica que sucede al operador no es cierta. La negación no es lo mismo que un antónimo por ejemplo la negación de "La camisa es blanca" no es "La camisa es negra". La negación correcta es "La camisa no es blanca", lo que significa que la camisa puede ser de cualquier color excepto blanco.

  Por ejemplo:

p	$\neg p$
Hoy llueve	Hoy no llueve
La camisa es blanca	La camisa no es blanca
$5 > 3$	$5 \leq 3$

p	$\neg p$
V	F
F	V

- $\Rightarrow$: "implica", "entonces". La implicación de dos proposiciones lógicas indica que si la primera es cierta, la segunda también lo será. Note que si la primera proposición (antecedente) no es cierta no sabemos que ocurre con la segunda, puede ser verdadera o falso, lo único que no puede ocurrir en esta forma es que se cumpla la primera y no la segunda. Por ejemplo:

  p: "Llueve".
  q: "Hay nubes".
  $p \Rightarrow q$: "Si llueve, hay nubes".

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

  Note además que $\Rightarrow$ no es conmutativo, es decir no es lo mismo $p \Rightarrow q$ que $q \Rightarrow p$, es fácil ver esto con el mismo ejemplo anterior, "Si llueve, hay nubes", pero "si hay nubes no necesariamente llueve".

- $\Leftrightarrow$: "si y solo si". La doble implicancia o equivalencia, indica que ambas proposiciones lógicas se dan en exactamente las mismas circunstancias. Es decir si una es cierta, la otra también lo será y, si una es falsa, la otra también. Por ejemplo:

  p: "Apruebo lógica".
  q: "mi promedio de lógica es mayor o igual a 4".
  $p \Leftrightarrow q$: "Apruebo lógica si y solo si mi promedio de lógica es mayor o igual a 4".

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

- $\veebar$: "o exclusivo". Esta disyunción indica que una y solo una de las proposiciones se cumple. Otra manera de verlo es que ambas proposiciones tienen distinto valor de verdad, de ese modo nos aseguramos que siempre hay una que es verdadera y la otra es falsa. Por ejemplo:

  p: "La silla es roja".
  q: "la mesa es roja".
  $p \veebar q$: "La silla es roja o la mesa es roja, pero no ambas".

p	q	$p \veebar q$
V	V	F
V	F	V
F	V	V
F	F	F

Definiciones 2.3. 1. Una proposición es compuesta si contiene otra proposición completa como un componente.

2. Una proposición es simple si y solo si no es compuesta.

3. Una proposición es una componente de otra proposición cuando al ser reemplazada en la otra proposición por otra proposición declarativa el resultado sigue siendo una proposición lógica.

2.2. Formas bien formadas

Cuando vemos una fórmula Booleana debemos saber si está bien escrita o no, de este modo sabremos si tiene o no sentido, por ejemplo en una fórmula aritmética $(2+3)\times 5$ es una fórmula bien formada y somos capaces de obtener un resultado, pero si escribimos $2()+\times 3\ 5$, esta expresión no tiene ningún sentido y no sabríamos que calcular. Del mismo modo definiremos cómo obtener una fórmula bien formada en lógica proposicional. Para comenzar damos la definición de fórmula atómica y literal.

Definición 2.4. Un literal es una fórmula atómica (p, q, etc.) o la negación de una fórmula atómica ($\neg p$, $\neg q$, etc.).

Para definir una fórmula bien formada, se da una descripción de qué objetos son fórmulas bien formadas.

Definición 2.5. Una fórmula bien formada es:

1. Un literal. Ejemplo: $p, \neg q, r$.

2. La negación de una fórmula bien formada.

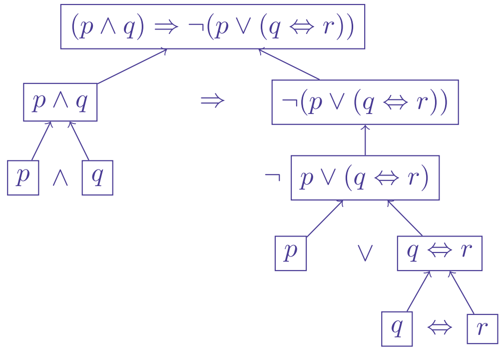
$$A \text{ es FBF} \implies \neg A \text{ es una FBF}$$

3. La conjunción, disyunción, implicancia, equivalencia y disyunción excluyente de fórmulas bien formadas.

$$\begin{aligned}
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \wedge B) \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \vee B) \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \Rightarrow B) \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \Leftrightarrow B) \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \veebar B) \text{ es una fórmula bien formada}
\end{aligned}$$

Ejemplos. Para verificar que una fórmula es bien formada,debemos ir identificando el operador principal e ir descomponiendo la fórmula en fórmulas más pequeñas siguiendo las reglas anteriores, hasta llegar a fórmulas atómicas.

1. $(p \wedge q) \Rightarrow \neg(p \vee (q \Leftrightarrow r))$



Es fórmula bien formada

2. Note que según la definición que dimos $(p \wedge q \wedge r) \vee s$ no sería una fórmula bien formada, sin embargo muchos de ustedes habrán visto esta expresión como una expresión correcta. En realidad esa expresión está correcta porque la operación $\wedge$ (al igual que $\vee$ y $\veebar$) son operaciones asociativas, esto lo probaremos en la sección siguiente. Sin embargo no funcionaría si en vez de $\wedge$ tuviésemos $\Rightarrow$.

2.3. Tautologías

Cuando tenemos fórmulas Booleanas lo que tenemos en realidad es una composición de proposiciones lógicas que forman una nueva proposición lógica, esta nueva proposición lógica tendrá un valor de verdad que depende de los valores de verdad de la proposiciones componentes, pero existen casos donde este valor de verdad es independiente de los valores de la proposiciones componentes, por dar un ejemplo simple $p \Rightarrow p \vee q$ siempre será verdadero, no importa cuales sean los valores de verdad de p y q, esto es lo que llamaremos una tautología.

Definiciones 2.6. Dada una proposición lógica compuesta.

1. Si independiente del valor de verdad de sus proposiciones componentes, resulta ser siempre verdadera diremos que es una tautología.

2. Si siempre es falsa es una contradicción,

3. en caso contrario será una contingencia.

A continuación listamos algunas tautologías importantes, para probar que son tautologías analizamos todos las combinaciones de valores de verdad de sus proposiciones componentes y vemos que en todo los casos obtenemos verdadero, este método se conoce como tablas de verdad.

1. $p \vee \neg p$

p	$\neg p$	(1)
V	F	V
F	V	V

Esta tautología es bastante evidente, una afirmación es cierta o no, eso siempre es cierto y es todo lo que tenemos que entender para entender la validez de esta tautología.

2. $p \Leftrightarrow \neg\neg p$

p	$\neg p$	$\neg\neg p$	(2)
V	F	V	V
F	V	F	V

La doble negación se trata de negar lo ya negado, por ejemplo una manera de negar "Esto es legal" es decir: "esto es ilegal", así si decimos: "esto no es ilegal" tenemos una doble negación que significa "esto es legal"

3. a) $(p \wedge V) \Leftrightarrow p$

p	$p \wedge V$	(3a)
V	V	V
F	F	V

Esta tautología dice que si hacemos la conjunción de una proposición lógica p con una tautología, la proposición compuesta tendrá el mismo valor de verdad que p.

b) $(p \vee F) \Leftrightarrow p$

p	$p \vee F$	(3b)
V	V	V
F	F	V

Como en el caso anterior, si tenemos una disyunción de una proposición lógica p con una contradicción, la proposición compuesta tendrá el mismo valor de verdad que p.

4. a) $(p \vee V) \Leftrightarrow V$

p	$p \vee V$	(4a)
V	V	V
F	V	V

b) $(p \wedge F) \Leftrightarrow F$

p	$p \wedge F$	(4b)
V	F	V
F	F	V

5. a) $(p \wedge q) \Leftrightarrow (q \wedge p)$

p	q	$p \wedge q$	$q \wedge p$	(5a)
V	V	V	V	V
V	F	F	F	V
F	V	F	F	V
F	F	F	F	V

b) $(p \vee q) \Leftrightarrow (q \vee p)$

p	q	$p \vee q$	$q \vee p$	(5b)
V	V	V	V	V
V	F	V	V	V
F	V	V	V	V
F	F	F	F	V

c) $(p \veebar q) \Leftrightarrow (q \veebar p)$

p	q	$p \veebar q$	$q \veebar p$	(5c)
V	V	F	F	V
V	F	V	V	V
F	V	V	V	V
F	F	F	F	V

d) $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$

p	q	$p \Leftrightarrow q$	$q \Leftrightarrow p$	(5d)
V	V	V	V	V
V	F	F	F	V
F	V	F	F	V
F	F	V	V	V

Estas propiedades corresponden a la conmutatividad de las operaciones $\wedge, \vee, \veebar$ y $\Leftrightarrow$, las que resultan muy intuitivas.

6. a) $((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$

   b) $((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$

Note que las propiedades 6a y 6b prueban la asociatividad de las operaciones $\wedge$ y $\vee$, de este modo vemos que $p \wedge (q \wedge r)$ y $(p \wedge q) \wedge r$ son equivalentes, por lo tanto, podemos obviar los paréntesis y escribir simplemente $p \wedge q \wedge r$. El caso $\vee$ es análogo. Este procedimiento se puede extender a cualquier número de conjunciones (o disyunciones), así, si tenemos $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ se entiende que se hace la conjunción de todas las proposiciones lógicas componentes asociándolas de cualquier manera, esto también se puede denotar por $\bigwedge_{i=1}^{n} p_i$. El caso $\vee$ es análogo.

Note que la asociatividad no es válida en el caso $\Rightarrow$, $p \Rightarrow (q \Rightarrow r)$ no es equivalente a $(p \Rightarrow q) \Rightarrow r$.

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$	(6a)
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	F	F	F	V
V	F	F	F	F	F	F	V
F	V	V	F	F	V	F	V
F	V	F	F	F	F	F	V
F	F	V	F	F	F	F	V
F	F	F	F	F	F	F	V

7. a) $(p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$

   b) $(p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r))$

Esta es la propiedad distributiva que se da tanto para la disyunción con respecto a la conjunción, como para la conjunción respecto a la disyunción.

Algo importante es que, si no ponemos paréntesis, debemos estar seguros que el operador es el mismo en todas las operaciones, no se puede mezclar $\wedge$ y $\vee$. Si bien es cierto en aritmética se hace $1 + 2 \times 3$ esto resulta porque existe una regla de precedencia para las operaciones aritméticas que dice que $\times$ se opera primero y luego se opera $+$; en lógica existen algunas reglas de precedencia ($\wedge, \vee$ se operan antes que $\Rightarrow$ y $\Leftrightarrow$), pero cuando se trata de precedencia entre $\wedge$ y $\vee$ se utilizan paréntesis para no incurrir en errores. Por ejemplo:

$$p \wedge q \Rightarrow p \vee q \text{ es lo mismo que } (p \wedge q) \Rightarrow (p \vee q)$$

pero $p \wedge q \vee r$ se considera ambiguo.

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$	(7a)
V	V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V	V
V	F	V	V	V	F	V	V	V
V	F	F	F	F	F	F	F	V
F	V	V	V	F	F	F	F	V
F	V	F	V	F	F	F	F	V
F	F	V	V	F	F	F	F	V
F	F	F	F	F	F	F	F	V

8. $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$

p	q	$p \Rightarrow q$	$\neg p$	$\neg p \vee q$	(8)
V	V	V	F	V	V
V	F	F	F	V	V
F	V	V	V	F	V
F	F	V	V	V	V

Esta tautología es muy útil, ya que permite representar una proposición compuesta usando solo los operadores $\neg, \wedge, \vee$. Esta tautología ayuda a eliminar los $\Rightarrow$ y, como veremos más adelante, los $\Leftrightarrow$.

9. $[(p \Rightarrow q) \wedge (q \Rightarrow p)] \Leftrightarrow (p \Leftrightarrow q)$

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$	$p \Leftrightarrow q$	(9)
V	V	V	V	V	V	V
V	F	F	V	F	F	V
F	V	V	F	F	F	V
F	F	V	V	V	V	V

Esta tautología deja en evidencia como la equivalencia es una implicancia en ambas direcciones, esto es simple de ver cuando leemos $p \Leftrightarrow q$ como p si y solo si q, ya que p si q es $q \rightarrow p$ y p solo si q es $p \Rightarrow q$, luego p si y solo si q es la conjunción de $p \Rightarrow q$ y $q \Rightarrow p$. Además, nos permite eliminar los $\Leftrightarrow$ de una proposición compuesta.

10. $[(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)] \Rightarrow (p \Leftrightarrow r)$

p	q	r	$p \Leftrightarrow q$	$q \Leftrightarrow r$	$(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)$	$p \Leftrightarrow r$	(10)
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	F	F	V	V
V	F	F	F	V	F	F	V
F	V	V	F	V	F	F	V
F	V	F	F	F	F	V	V
F	F	V	V	F	F	F	V
F	F	F	V	V	V	V	V

Esta tautología muestra la transitividad de la equivalencia, que es bastante intuitiva, ya que uno tiende a asociarla a la igualdad en general.

11. $(p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ Al igual que el caso anterior, esta tautología es bastante intuitiva y más adelante veremos que esta tautología la usaremos como regla de inferencia.

12. a) $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$

    b) $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	(12a)
V	V	V	F	F	F	F	V
V	F	F	V	F	V	V	V
F	V	F	V	V	F	V	V
F	F	F	V	V	V	V	V

Estas últimas tautologías son conocidas como Leyes de De Morgan. Podemos extender su acción cuando tenemos una conjunción o disyunción de múltiples proposiciones, es decir:

$$\neg(p \wedge q \wedge r \wedge s) \Leftrightarrow (\neg p \vee \neg q \vee \neg r \vee \neg s)$$
$$\neg(p \vee q \vee r \vee s) \Leftrightarrow (\neg p \wedge \neg q \wedge \neg r \wedge \neg s)$$

2.4. Formas normales

Como ya comenzamos a ver con las tautologías existen muchas fórmulas Booleana equivalentes, es decir, que tiene el mismo valor de verdad. A veces es útil tener una forma simple de expresar estas fórmulas con operaciones simples y con una estructura dada. Una forma simple de presentar una proposición compuesta es a través de su forma normal conjuntiva o disyuntiva.

Definición 2.7. Una fórmula Booleana ϕ está en Forma Normal Conjuntiva (FNC) si es una conjunción de disyunciones de literales. Es decir:

$$\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

donde $C_i = p_{i,1} \vee \cdots \vee p_{i,m_i}$ y $p_{i,j}$ son proposiciones simples (p, q, r, etc.) o negaciones de estas.

Ejemplos de forma normal conjuntiva:

- $(p \vee \neg q) \wedge (q \vee r)$
- $(p \vee r) \wedge \neg q$
- $\neg p \vee r \vee q$
- $p \wedge \neg q$

Las siguientes fórmulas no están en FNC:

- $\neg(q \vee r)$
- $(p \wedge q) \vee r$

- $p \wedge (q \vee (r \wedge s))$

Cada fórmula puede ser equivalentemente escrita como una fórmula en forma normal conjuntiva. En particular, este es el caso para los tres contraejemplos recién mencionados; que son, respectivamente, equivalentes a las siguientes tres fórmulas, que están en forma normal conjuntiva:

- $\neg q \wedge \neg r$
- $(p \vee r) \wedge (q \vee r)$
- $p \wedge (q \vee r) \wedge (q \vee s)$

Definición 2.8. Una fórmula Booleana ϕ está en Forma Normal Disyuntiva (FND) si es una disyunción de conjunciones de literales. Es decir:

$$\phi = C_1 \vee C_2 \vee \cdots \vee C_n$$

donde $C_i = p_{i,1} \wedge \cdots \wedge p_{i,m_i}$ y $p_{i,j}$ son proposiciones simples $(p, q, r$, etc.$)$ o negaciones de estas.

Al igual que en forma normal conjuntiva, los únicos operadores proposicionales en FND son la conjunción, disyunción y negación. Una negación solo se puede aplicar a un literal, lo que significa que solo puede preceder a una variable proposicional. Al igual que en el caso de FNC, cada fórmula puede ser equivalentemente escrita como una fórmula en forma normal disyuntiva. Algunos ejemplos de FND son:

- $(\neg p \wedge q) \vee (q \wedge r)$
- $(p \wedge \neg r) \vee q$
- $p \vee \neg r \vee q$
- $\neg p \wedge q$

Teorema 2.1. *Toda fórmula booleana tiene una FNC y una FND equivalentes.*

2.4.1. Algoritmo para llevar a formas normales

1. Eliminar $\veebar$, $\Rightarrow$ y $\Leftrightarrow$
2. Aplicar leyes de De Morgan para eliminar $\neg(\dots)$
3. Eliminar doble negación
4. Aplicar conmutatividad, asociatividad y distributividad.
5. Opcionalmente, para hacer la fórmula más pequeña se pueden usar las siguientes identidades:

a) $p \wedge p \Leftrightarrow p$

b) $p \vee p \Leftrightarrow p$

c) $p \wedge \neg p \Leftrightarrow F$

d) $p \vee \neg p \Leftrightarrow V$

e) $p \wedge V \Leftrightarrow p$

f) $p \wedge F \Leftrightarrow F$

g) $p \vee V \Leftrightarrow V$

h) $p \vee F \Leftrightarrow p$

i) $p \wedge (p \vee q) \Leftrightarrow p$

j) $p \vee (p \wedge q) \Leftrightarrow p$

k) $p \wedge (\neg p \vee q) \Leftrightarrow p \wedge q$

l) $p \vee (\neg p \wedge q) \Leftrightarrow p \vee q$

m) $(p \vee \neg q) \wedge (p \vee q) \Leftrightarrow p$

n) $(p \wedge \neg q) \vee (p \wedge q) \Leftrightarrow p$

Encuentre la forma normal conjuntiva y la forma normal disyuntiva para:

1. $[(p \Rightarrow q) \Rightarrow (r \vee \neg s)] \wedge [(\neg p \vee r) \Rightarrow (q \vee s)]$

$$[(p \Rightarrow q) \Rightarrow (r \vee \neg s)] \wedge [(\neg p \vee r) \Rightarrow (q \vee s)] \tag{2.1}$$
$$[\neg(\neg p \vee q) \vee r \vee \neg s] \wedge [\neg(\neg p \vee r) \vee q \vee s] \tag{2.2}$$
$$[(p \wedge \neg q) \vee r \vee \neg s] \wedge [(p \wedge \neg r) \vee q \vee s] \tag{2.3}$$
$$(p \vee r \vee \neg s) \wedge (\neg q \vee r \vee \neg s) \wedge [(p \vee q \vee s) \wedge (\neg r \vee q \vee s) \qquad \text{FNC} \tag{2.4}$$

para la FND retomamos desde (2.3):

$$[(p \wedge \neg q) \vee r \vee \neg s] \wedge [(p \wedge \neg r) \vee q \vee s] \tag{2.5}$$
$$\begin{aligned}&(p \wedge \neg q \wedge p \wedge \neg r) \vee \cancel{(p \wedge \neg q \wedge q)} \vee (p \wedge \neg q \wedge s) \vee \\ &\quad \cancel{(r \wedge p \wedge \neg r)} \vee (r \wedge q) \vee (r \wedge s) \vee (\neg s \wedge p \wedge \neg r) \vee (\neg s \wedge q) \vee \cancel{(\neg s \wedge s)}\end{aligned} \tag{2.6}$$
$$(p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge s) \vee (r \wedge q) \vee (r \wedge s) \vee (\neg s \wedge p \wedge \neg r) \vee (\neg s \wedge q) \tag{2.7}$$

2. $[(p \wedge q) \Rightarrow r] \Leftrightarrow \neg[(s \vee t) \Rightarrow (p \wedge q)]$

$$[(p \wedge q) \Rightarrow r] \Leftrightarrow \neg[(s \vee t) \Rightarrow (p \wedge q)] \tag{2.8}$$
$$[\neg(p \wedge q) \vee r] \Leftrightarrow \neg[\neg(s \vee t) \vee (p \wedge q)] \tag{2.9}$$
$$(\neg p \vee \neg q \vee r) \Leftrightarrow [(s \vee t) \wedge \neg(p \wedge q)] \tag{2.10}$$
$$(\neg p \vee \neg q \vee r) \Leftrightarrow [(s \vee t) \wedge (\neg p \vee \neg q)] \tag{2.11}$$
$$[(\neg p \vee \neg q \vee r) \Rightarrow [(s \vee t) \wedge (\neg p \vee \neg q)]] \wedge [[(s \vee t) \wedge (\neg p \vee \neg q)] \Rightarrow (\neg p \vee \neg q \vee r)] \tag{2.12}$$
$$[(p \wedge q \wedge \neg r) \vee [(s \vee t) \wedge (\neg p \vee \neg q)]] \wedge [[\neg(s \vee t) \vee \neg(\neg p \vee \neg q)] \vee \neg p \vee \neg q \vee r] \tag{2.13}$$
$$[(p \wedge q \wedge \neg r) \vee [(s \vee t) \wedge (\neg p \vee \neg q)]] \wedge [(\neg s \wedge \neg t) \vee (p \wedge q) \vee \neg p \vee \neg q \vee r] \tag{2.14}$$
$$[(p \wedge q \wedge \neg r) \vee [(s \vee t) \wedge (\neg p \vee \neg q)]] \wedge [(\neg s \wedge \neg t) \vee \underbrace{(p \wedge q) \vee \neg(p \wedge q)}_{V} \vee r] \tag{2.15}$$
$$(p \wedge q \wedge \neg r) \vee [(s \vee t) \wedge (\neg p \vee \neg q)] \tag{2.16}$$
$$(p \wedge q \wedge \neg r) \vee (s \wedge \neg p) \vee (s \wedge \neg q) \vee (t \wedge \neg p) \vee (t \wedge \neg q) \qquad \text{FND} \tag{2.17}$$

Para la FNC retomamos desde (2.16)

$$(p \wedge q \wedge \neg r) \vee [(s \vee t) \wedge (\neg p \vee \neg q)] \tag{2.18}$$
$$(p \vee s \vee t) \wedge \cancel{(p \vee \neg p \vee \neg q)} \wedge (q \vee s \vee t) \wedge \cancel{(q \vee \neg p \vee \neg q)} \wedge (\neg r \vee s \vee t) \wedge (\neg r \vee \neg p \vee \neg q) \tag{2.19}$$
$$(p \vee s \vee t) \wedge (q \vee s \vee t) \wedge (\neg r \vee s \vee t) \wedge (\neg r \vee \neg p \vee \neg q) \qquad \text{FNC} \tag{2.20}$$

2.4.2. Algoritmos para encontrar una fórmula a partir de una tabla de verdad

Dada una tabla de verdad es posible encontrar una fórmula para esa tabla. La manera más fácil es encontrar una forma normal conjuntiva o disyuntiva. Para encontrar una forma normal disyuntiva.

Dada $\Phi : \{V,F\}^n \to \{V,F\}$, sea $X_V = \{y \in \{V,F\}^n : \Phi(y) = V\}$. Luego:

$$\Phi(x) = \bigvee_{y \in X_V} \bigwedge_{i=1}^{n} l(y_i) \text{ donde } l(y_i) = \begin{cases} x_i & \text{Si } y_i = V \\ \neg x_i & \text{Si } y_i = F \end{cases}$$

Para encontrar una forma normal conjuntiva.

Dada $\Phi : \{V,F\}^n \to \{V,F\}$, sea $X_F = \{y \in \{V,F\}^n : \Phi(y) = F\}$. Luego:

$$\Phi(x) = \bigwedge_{y \in X_F} \bigvee_{i=1}^{n} l(y_i) \text{ donde } l(y_i) = \begin{cases} x_i & \text{Si } y_i = F \\ \neg x_i & \text{Si } y_i = V \end{cases}$$

Ejemplo:

x_1	x_2	x_3	$\Phi(x)$
V	V	V	F
V	V	F	V
V	F	V	V
V	F	F	F
F	V	V	V
F	V	F	F
F	F	V	V
F	F	F	F

En forma normal disyuntiva:

$$\Phi(x) = (x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3)$$
$$\Phi(x) = (x_1 \wedge x_2 \wedge \neg x_3) \vee (\neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \tag{2.21}$$

En forma normal conjuntiva:

$$\Phi(x) = (\neg x_1 \vee \neg x_2 \vee \neg x_3) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_3) \tag{2.22}$$

2.5. Del castellano a la lógica simbólica

Hasta ahora hemos visto muchos símbolos, pero cuando comenzamos el curso dijimos que queríamos saber si una razonamiento era correcto o no, y no es claro como hacer esto operando fórmulas matemáticas. Por eso vamos a ver como modelar con proposiciones lógicas algunos razonamientos.

Aprender las técnicas de demostración con lógica simbólica no servirá de nada a menos que podamos aplicar estas técnicas en distintos contextos.

Veamos un ejemplo de un razonamiento y como podríamos simbolizarlo.

Ejemplo 2.1. Aquí presentamos un argumento y nos gustaría saber si es válido o no.
Cuando llueve hay nubes. Hoy brilla el sol no hay nubes en el cielo. Por lo tanto, no llueve.

La proposiciones componentes son:

l : llueve
n: hay nubes
b : brilla el sol

Luego la simbolización de este argumento es:

$$[(l \Rightarrow n) \wedge (b \wedge \neg n)] \implies \neg l$$

Ahora nos gustaría saber si este argumento es válido o no. Por el momento podríamos hacer una tabla de verdad, más adelante en el curso estudiaremos otras técnicas para verificarlo.

l	n	b	$l \Rightarrow n$	$b \wedge \neg n$	$(l \Rightarrow n) \wedge (b \wedge \neg n)$	$\neg l$	$[(l \Rightarrow n) \wedge (b \wedge \neg n)] \implies \neg l$
V	V	V	V	F	F	F	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	F	V
V	F	F	F	F	F	F	V
F	V	V	V	F	F	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	F	F	V	V

Así podemos ver que el argumento es correcto.

Para lograr hacer estas simbolizaciones veremos algunas reglas que no ayudan a escribirlas,

$p \wedge q$ Algunas maneras de representar esta expresión son:

- p y q.
- p, pero q.
- p, sin embargo q.
- p a pesar de q.
- p, aún así q.
- p, aunque q.
- p, más aún q.
- p, además q.

Debemos tomar en cuenta cualquier expresión que agregue información. También podemos tomar en cuenta que podemos enumerar varias sentencias y al terminar la enumeración poner un “y” o un “etc.”, esto quiere decir que debemos considerar la conjunción de todas. Por ejemplo: “El campus de la universidad tiene césped, árboles, asientos, etc.”

Ejemplos:

Juan ama a María, si embargo, ella apenas lo tolera.

Está lloviendo, a pesar de esto, iremos de pícnic.

no se puede confiar en Juan, aún así, me cae bien.

Sé que es un lindo día, pero igual quiero quedarme en casa y leer un libro.

Juan consiguió el trabajo, a pesar de que no usó corbata en la entrevista.

No me rendiré aunque no es seguro que tenga éxito.

Juan es dulce, además es inteligente.

A María le gusta la música clásica y también el rock.

María no solo es artista, también es científica.

Ana se casará con Juan, a pesar de que él no sabe cocinar.

Juan no tiene trabajo, más aún, no sabe cocinar.

$p \vee q$ Algunas maneras de representar esta expresión son:

- p o q.
- p y/o q.
- p o si no q.

Note que el "o" es inclusivo, es decir, también se puede dar que ambas proposiciones sean verdaderas. Además, debemos tener en cuenta expresiones como: "Ocurre alguna de las siguientes opciones: está nublado, llueve, brilla el sol, hay cielo parcial", en este caso tendríamos un $\vee$ de las cuatro alternativas, cabe destacar que hay algunas que pueden ocurrir simultáneamente, como que llueve y está nublado al mismo tiempo.

Ejemplos:

Sales de aquí o llamo a la policía.

Tendremos un presidente de izquierda o de derecha.

Hace calor aquí, o si no me estoy enfermando.

$\veebar$ p o q, pero no ambos. Solo p o solo q.

Este es el caso del "o" exclusivo aquí solo una de las dos opciones puede ocurrir.

Note que a diferencia de $\wedge$ y $\vee$ aquí es difícil trabajar como una enumeración de eventos posibles. Lo primero que se nos ocurre es pensar que si decimos "Una y solo una de las siguientes opciones ocurre: a, b o c" esto podríamos modelarlo como $a \veebar b \veebar c$, sin embargo, no es así; para que $p_1 \veebar \cdots \veebar p_n$ sea verdadera se debe cumplir que un número impar de proposiciones p_i, sean verdaderas, no solo una necesariamente.

Ejemplo:

Juan quiere ser médico o abogado, pero no ambos.

$\neg p$ Algunas maneras de representar esta expresión son: no p, no q y tampoco p $(\neg q \wedge \neg p)$, ni p ni q $(\neg q \wedge \neg p)$, prefijos como, des... (desafortunado).

En estos casos hay que tener mucho cuidado con los antónimos, no ser algo, no quiere decir serlo contrario, por lo tanto hay que tener cuidado.

Ejemplos:

Juan no es un buen estudiante.

Juan es infeliz (ojo con esto, puede ser más fuerte que o ser feliz)

La pintura es incolora.

La situación no es ni buena ni mala.

$p \Rightarrow q$ Algunas maneras de representar esta expresión son:

- si p entonces q.
- q si p.
- p solo si q.
- q siempre que p.
- siempre que p, q.
- q en el caso que p.
- en el caso que p, q.
- q es condición necesaria para p.
- p es condición suficiente para q.
- $\neg p$ a menos que q.
- p a menos que q ($\neg q \Rightarrow p$).

Ejemplos:

1. Si llueve hay nubes.
2. Iré de pícnic si hay un lindo día.
3. Llueve solo si hay nubes.
4. Gano la lotería solo si compro un billete.
5. Iré de pícnic si no llueve.
6. No llueve siempre que hay un lindo día.
7. Siempre que hay un lindo día hago deporte.
8. Haremos clases online en el caso que no podamos asistir a la universidad.
9. En el caso que Juan obtiene un 5, aprueba la asignatura.
10. No estar enfermo es condición necesaria para estudiar apropiadamente.
11. Tener buena salud es suficiente para ir al viaje.
12. Iremos de pícnic a menos que llueva.
13. Dado que estudiaste obtuviste una buena calificación.

$p \Leftrightarrow q$ Algunas maneras de representar esta expresión son:

- p si y solo si q.
- p en el caso y solo en el caso que q.
- p ocurre en exactamente las mismas circunstancias que q.
- p es equivalente a q.
- p es condición necesaria y suficiente para q.
- p se define como q.

Ejemplos:

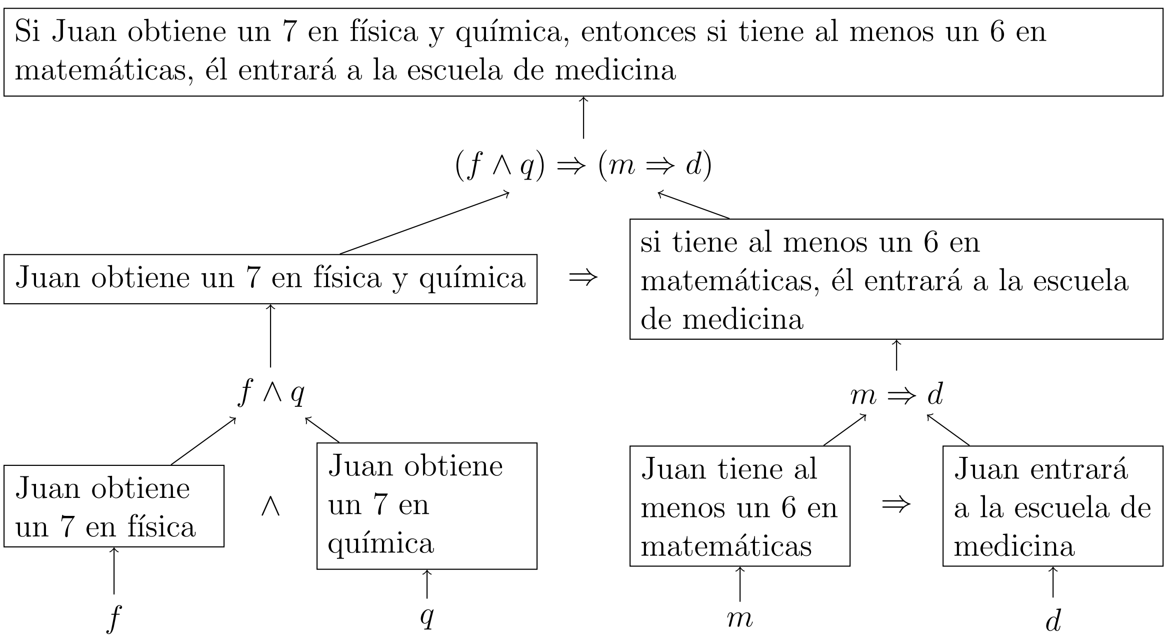
Apruebo la asignatura si y solo si obtengo calificación mayor o igual a 5.

2.5.1. Simbolizar oraciones complejas

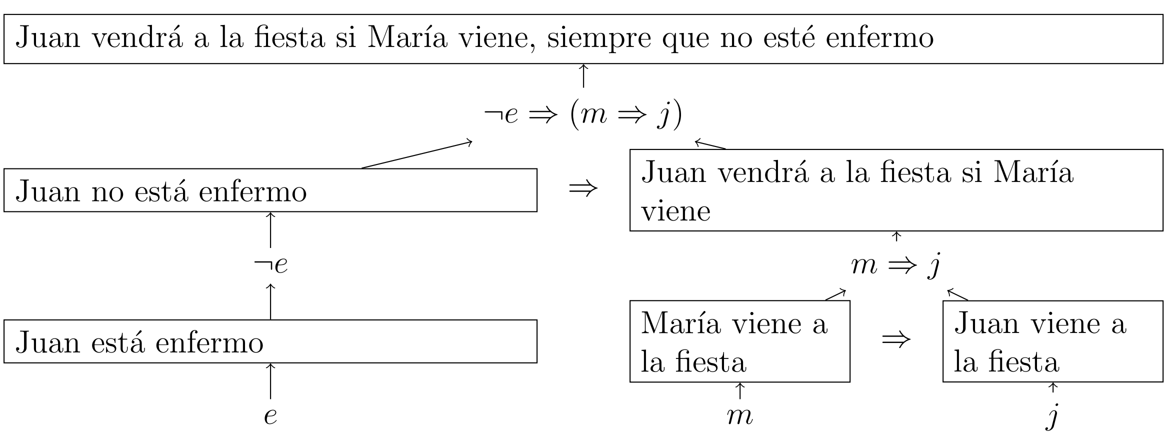
Para simbolizar sentencias complejas se debe hacer por partes. Lo primero es identificar cual es el principal operador en la sentencia y, descomponer la sentencia en las componentes con ese operador y luego seguir descomponiendo cada parte hasta que o sea posible descomponer más.

Veremos esto con ejemplos:

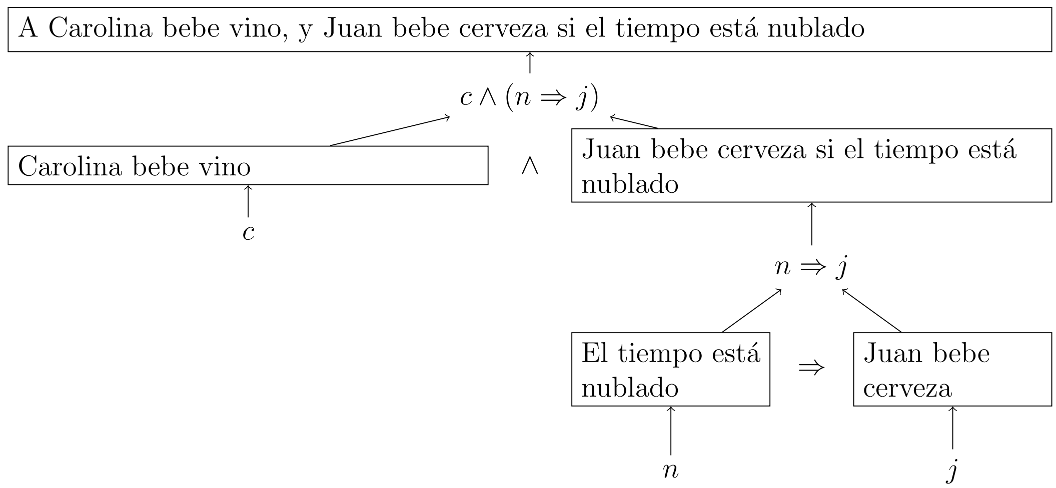
1. Si Juan obtiene un 7 en física y química, entonces si tiene al menos un 6 en matemáticas, él entrará a la escuela de medicina.



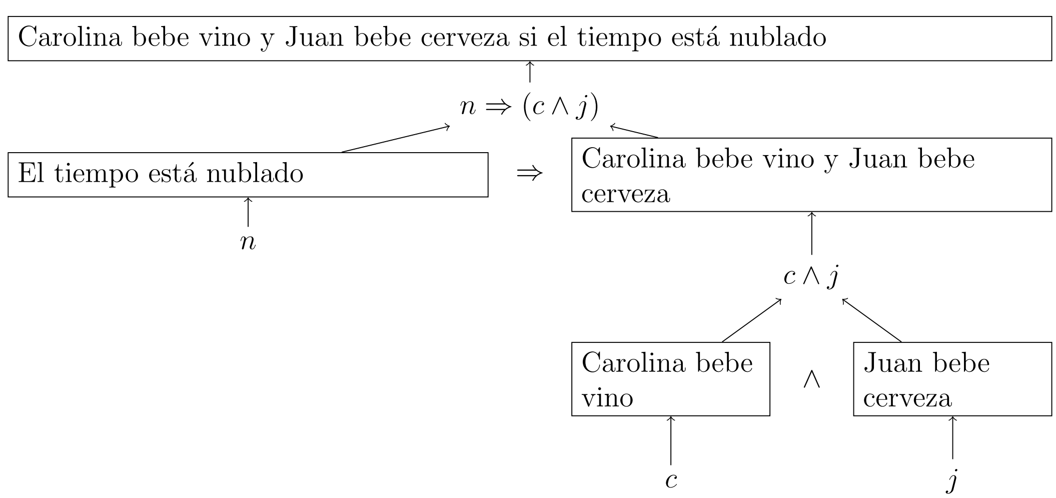
2. Juan vendrá a la fiesta si María viene, siempre que no esté enfermo.



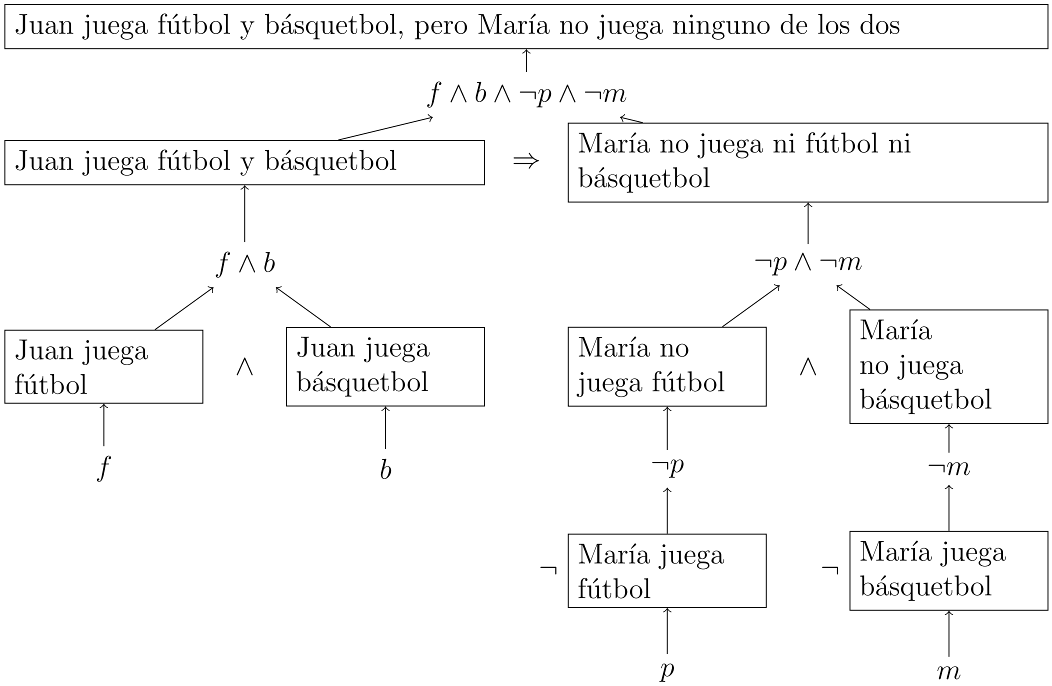
3. Carolina bebe vino, y Juan bebe cerveza si el tiempo está nublado.



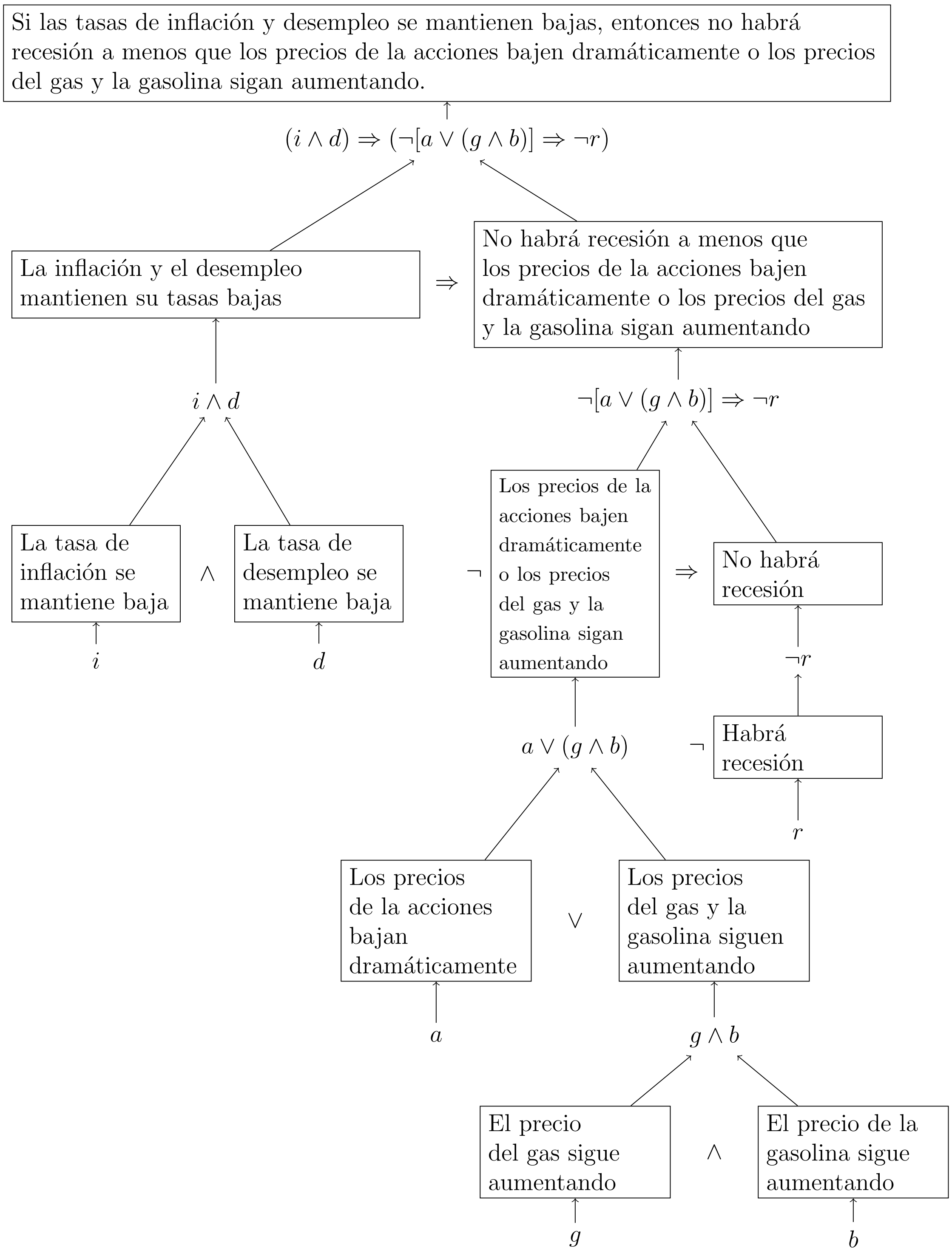
4. Carolina bebe vino y Juan bebe cerveza, si el tiempo está nublado.



5. Juan juega fútbol y básquetbol, pero María no juega ninguno de los dos.


Juan juega fútbol y básquetbol, pero María no juega ninguno de los dos
$f \wedge b \wedge \neg p \wedge \neg m$
Juan juega fútbol y básquetbol
$\Rightarrow$
María no juega ni fútbol ni básquetbol
$f \wedge b$
$\neg p \wedge \neg m$
Juan juega fútbol
$\wedge$
Juan juega básquetbol
María no juega fútbol
$\wedge$
María no juega básquetbol
f
b
$\neg p$
$\neg m$
$\neg$
María juega fútbol
$\neg$
María juega básquetbol
p
m

6. Si la inflación y el desempleo mantienen su tasas bajas, entonces no habrá recesión a menos que los precios de la acciones bajen dramáticamente o los precios del gas y la gasolina sigan aumentando.



2.6. Reglas de inferencia

Ahora si vamos a comenzar con las demostraciones, si bien es cierto las tablas de verdad son útiles, esto solo sirve cuando tenemos un pequeño número de proposiciones componentes, a a partir de ahora veremos algunas técnicas de demostración que nos ayudarán a verificar la veracidad de los argumentos.

Una regla de inferencia es un patrón de razonamiento básico, de acuerdo al cual se infiere una conclusión a partir de premisas de una cierta forma. Una premisa es una afirmación o idea que se da como cierta y que sirve de base a un razonamiento o una discusión. De este modo cuando establecemos un argumento del tipo:

$$\begin{array}{l} \mathrm{Pr}_1 \\ \vdots \\ \mathrm{Pr}_n \\ \hline \therefore\ C \end{array}$$

Se plantea que bajo el supuesto de que las premisas Pr_1 a Pr_n son ciertas, entonces la conclusión C es también cierta. O lo que es equivalente:

$$\bigwedge_{i=1}^{n} \mathrm{Pr}_n \implies C$$

Una regla de inferencia no es una regla que te obligue a hacer algo, es más bien una regla que te permite inferir algo, pero no te obliga a ello. En esta parte daremos 8 reglas básicas, a partir de estas pueden derivarse otras que, más adelante iremos ocupando, pero es importante ceñirse a estas 8 en un principio para no caer en la tentación de utilizar reglas erróneas que no hemos estudiado con suficiente cuidado. Para probar estas reglas se pueden usar tablas de verdad o simplemente sacar conclusiones como si fuera una ecuación, donde queremos saber cual es el valor de verdad de la conclusión propuesta.

Modus Ponens (M.P.)
$$\begin{array}{l} p \Rightarrow q \\ p \\ \hline \therefore\ q \end{array}$$

El *Modus Ponendo Ponens* es, probablemente la regla de inferencia más fundamental de la lógica, se conoce de manera más familiar como Modus Ponens. Esta regla dice que dado un condicional y el antecedente de este condicional es posible concluir el consecuente del condicional.

Por ejemplo, podemos establecer como primera premisa que "cuando llueve hay nubes", esto lo podemos modelar como:

p:	Llueve
q:	hay nubes
$p \Rightarrow q$:	Cuando llueve hay nubes

Como segunda premisa podemos establecer que "hoy llueve", es decir p, luego podemos concluir sin necesidad de hacer otra verificación que "hay nubes" q.

Todo este argumento parece muy simple, pero suelen cometerse errores cuando se usa esta regla de inferencia, la más usual es establecer como premisas $p \Rightarrow q$ y q y concluir p, esto es muy simple de entender cuando usamos nuestro ejemplo, ya que el hecho que hayan nubes no implica que llueva. La sentencia "hay nubes" puede ocurrir en un día con sol donde solo se ven algunas nubes en el cielo, pero no es necesario que llueva.

Es importante recordar que $p \Rightarrow q$ quiere decir que p es una condición suficiente para tener q, pero q no necesariamente es suficiente para tener p.

Modus Tollens (M.T.)

$$\begin{array}{l} p \Rightarrow q \\ \neg q \\ \hline \therefore\ \neg p \end{array}$$

El *Modus Tollendo Tollens* es otra regla que utiliza un condicional, se conoce de manera más familiar como Modus Tollens. Esta regla dice que dado un condicional y la negación de este condicional es posible concluir el consecuente del condicional, esta regla también es bastante intuitiva, otra manera de decirlo es que si no tenemos la condición necesaria para algo, ese algo no se cumplirá.

Por ejemplo, si retomamos las proposiciones lógicas del ejemplo anterior tendríamos "Cuando llueve hay nubes" ($p \Rightarrow q$) y "hoy no hay nubes" ($\neg q$), entonces podemos concluir que "no llueve" ($\neg p$).

Este es uno de los motivos por los que se suele cometer el error mencionado en el Modus Ponens ya que se confunde la regla al no tomar en cuenta la negación.

Recordemos que otro significado de $p \Rightarrow q$ es q es condición necesaria para p, por lo tanto, si no tengo q es imposible que tenga p.

Silogismo Hipotético (S.H.)

$$\begin{array}{l} p \Rightarrow q \\ q \Rightarrow r \\ \hline \therefore\ p \Rightarrow r \end{array}$$

Esta regla corresponde a la transitividad de la implicancia lógica, que ya hemos visto como una tautología. Por lo demás, es una regla bastante intuitiva, esta regla nos dice que dados dos condicionales, donde el consecuente de uno, es el antecedente del otro, podemos concluir otro condicional donde cuyo antecedente es el antecedente del primero y el consecuente es el consecuente del segundo.

Por ejemplo, modelemos "Si obtengo nota 5, apruebo la asignatura. Si apruebo la asignatura, estoy feliz. Por lo tanto, si obtengo nota 5 estoy feliz". Para modelar este argumento tenemos:

p:	obtengo nota 5
q:	apruebo la asignatura
r:	estoy feliz
$p \Rightarrow q$:	Si obtengo nota 5, apruebo la asignatura
$q \Rightarrow r$:	Si apruebo la asignatura, estoy feliz
$p \Rightarrow r$:	Si obtengo nota 5, estoy feliz

Notemos que la conclusión de este argumento es un condicional, un error frecuente es concluir r (estoy feliz), pero en realidad la conclusión es que "si obtengo un 5 en la asignatura estoy feliz", en la circunstancia que no obtengo un 5 no sabemos si estoy feliz o no. Este argumento no concluye el valor de verdad de r solo dice que obtener nota 5 es una condición suficiente para estar feliz.

Simplificación (Simp.) $\dfrac{p \wedge q}{\therefore\ p}$ $\qquad$ $\dfrac{p \wedge q}{\therefore\ q}$

Esta regla es tal vez la más simple de todas, y usualmente es una de las que primero se usa. Básicamente nos dice que si sabemos que dos proposiciones en su conjunto son ciertas, podemos tener certeza de cada una por separado, esto resulta muy útil en las demostraciones, como veremos más adelante y la verdad es muy simple de comprender.

Note que si tenemos una conjunción de varias proposiciones lógicas, por ejemplo $p \wedge q \wedge r \wedge s$, podemos simplificar cualquiera de ellas, es decir

$$\frac{p \wedge q \wedge r \wedge s}{\therefore\ p} \qquad \frac{p \wedge q \wedge r \wedge s}{\therefore\ q} \qquad \frac{p \wedge q \wedge r \wedge s}{\therefore\ r} \qquad \frac{p \wedge q \wedge r \wedge s}{\therefore\ s}$$

Un error frecuente es aplicar la simplificación cuando tenemos $\vee$ en vez de $\wedge$. Claramente esto no es correcto, ya que cuando tenemos una disyunción sabemos que una de sus proposiciones componentes es cierta, pero no podemos estar seguros que todas lo sean.

Conjunción (Conj.)

$$\begin{array}{l} p \\ q \\ \hline \therefore\ p \wedge q \end{array}$$

En este caso, nos encontramos con la operación inversa de la simplificación, aquí decimos que si dos proposiciones se cumplen por separado, también lo harán en conjunto. Esta regla es bastante simple, pero es importante recordar que debemos tener ambas proposiciones por separado antes de hacer la conjunción y no como parte de otra proposición.

Al igual que en el caso anterior, gracias a las propiedades de conmutatividad y asociatividad de la conjunción, podemos aplicar la conjunción de múltiples premisas.

$$\begin{array}{l} p \\ q \\ r \\ s \\ \hline \therefore\ p \wedge q \wedge r \wedge s \end{array}$$

Silogismo Disyuntivo (S.D.)

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore\ q \end{array} \qquad \begin{array}{l} p \vee q \\ \neg q \\ \hline \therefore\ p \end{array}$$

Esta regla de inferencia resulta muy útil ya que usualmente no sabemos como concluir la veracidad de una de las componentes de una disyunción, debido a que si la disyunción es verdadera, una o ambas proposiciones componentes son verdaderas, pero en principio no sabemos cual. De este modo si sabemos que una de estas componentes es falsa, la única forma que la disyunción sea verdadera es que la otra proposición sea verdadera, recordemos que $p \vee F \Leftrightarrow p$.

Dilema (Dil.)

$$\begin{array}{l} p \Rightarrow q \\ r \Rightarrow s \\ p \vee r \\ \hline \therefore\ q \vee s \end{array}$$

Esta regla resulta la menos intuitiva de todas, combina varias premisas: dos condicionales y una disyunción. En términos simples dice que si estamos seguros de la certeza de al menos uno de los antecedentes de los condicionales, entonces sabemos que alguno de los consecuentes se cumple.

Adición (Ad).

$$\begin{array}{l} p \\ \hline \therefore\ p \vee q \end{array} \qquad \begin{array}{l} q \\ \hline \therefore\ p \vee q \end{array}$$

Esta regla suele parecer bastante absurda, y a primera vista, parece incorrecta. Porque si decimos que la premisa p es “este es el planeta Tierra” (algo en lo que todos estamos de acuerdo que es cierto) ahora puedo concluir que este es el planeta Tierra o los cerdos son verdes. Cuando escuchamos como parte de la proposición que los cerdos son verdes, uno tiende a decir que esto es una estupidez, pero como el operador es un “o”, esto no es un problema ya que basta con que “este sea el planeta Tierra” para que esta sentencia sea verdadera, por muy absurda que pueda parecer la segunda proposición componente.

Ejemplos:

1)	$p \Rightarrow (q \vee r)$	
2)	$p \wedge \neg q$	
	$\therefore\ r$	
3)	p	Simp. 2
4)	$q \vee r$	M.P. 3 y 1
5)	$\neg q$	Simp. 2
6)	r	S.D. 4 y 5

1)	$a \vee \neg b$	
2)	$\neg c \vee b$	
3)	$\neg a$	
	$\therefore\ \neg c$	
4)	$\neg b$	S.D. 1 y 3
5)	$\neg c$	S.D. 2 y 4

1)	$f \Rightarrow (g \wedge \neg h)$	
2)	$z \Rightarrow h$	
3)	f	
	$\therefore\ \neg z$	
4)	$g \wedge \neg h$	M.P. 1 y 3
5)	$\neg h$	Simp. 4
6)	$\neg z$	M.T. 2 y 5

1)	$w \wedge s$	
2)	$(w \wedge s \wedge (r \vee f)) \Rightarrow (p \vee m)$	
3)	$p \Rightarrow b$	
4)	$\neg b \wedge l$	
5)	$\neg r \wedge f$	
	$\therefore\ m$	
6)	f	Simp. 5
7)	$r \vee f$	Ad. 6
8)	$w \wedge s \wedge (r \vee f)$	Conj. 1 y 7
9)	$p \vee m$	M.P. 2 y 8
10)	$\neg b$	Simp. 4
11)	$\neg p$	M.T. 3 y 10
12)	m	S.D. 9 y 11

1)	$(a \vee b) \Rightarrow (c \vee d)$	
2)	$(c \vee f) \Rightarrow h$	
3)	$e \wedge \neg d$	
4)	$e \Rightarrow a$	
	$\therefore\ h \vee i$	
5)	e	Simp. 3
6)	a	M.P. 4 y 5
7)	$a \vee b$	Ad. 6
8)	$c \vee d$	M.P. 1 y 7
9)	$\neg d$	Simp. 3
10)	c	S.D. 8 y 9
11)	$c \vee f$	Ad. 10
12)	h	M.P. 2 y 11
13)	$h \vee i$	Ad. 12

Supongamos que se plantea el siguiente argumento:

1)	$a \vee b$	
2)	$b \Rightarrow c$	
3)	$\neg a \wedge \neg c$	
	$\therefore\ f \Rightarrow g$	
4)	$\neg a$	Simp. 3
5)	$\neg c$	Simp. 3
6)	$\neg b$	M.T. 2 y 5
7)	b	S.D. 1 y 4
8)	$b \vee (f \Rightarrow g)$	Ad. 7
9)	$f \Rightarrow g$	S.D. 6 y 8

Cuando se ve este argumento a primera vista uno cree que puede estar mal, pero si lo ven con detención verán que todas las reglas fueron aplicadas correctamente. Entonces la pregunta es ¿Porqué podemos concluir acerca de una proposición de la que no tenemos ninguna información? si miran los pasos 6 y 7 verán que tenemos b y $\neg b$, es decir, si hacemos una conjunción tendríamos $b \wedge \neg b$ lo que es falso, por lo tanto a partir de algo falso se puede concluir cualquier cosa, esto es lo que ya vimos cuando explicamos el operador $\Rightarrow$ y vimos que $F \Rightarrow V$ y $F \Rightarrow F$ es verdadero.

1) $(a \vee b) \Rightarrow (\neg c \Rightarrow (f \Rightarrow h))$
2) $a \wedge \neg c$
3) $h \Rightarrow c$
$\therefore\ \neg f$

1) $a \Rightarrow (b \vee c)$
2) $b \Rightarrow f$
3) $a \wedge \neg f$
4) $(a \vee h) \Rightarrow d$
$\therefore\ c \wedge d$

2.7. Reglas de reemplazo

Las reglas de reemplazo son un complemento a las reglas de inferencia, en este caso decimos que ambas proposiciones lógicas son equivalentes, es decir tienen exactamente el mismo valor de verdad, de este modo podemos reemplazar una proposición por la otra como lo hacemos con igualdades en ecuaciones algebraicas.

Estas reglas ya fueron estudiadas como tautologías cuando estudiamos las tablas de verdad, la única que no habíamos visto previamente es la exportación. De modo que no necesitamos probarlas nuevamente, solo daremos la demostración de la exportación por tabla de verdad.

Doble negación (D.N.) $\quad p \Leftrightarrow \neg\neg p$

1)	$\neg p \Rightarrow q$	
2)	$\neg q$	
	$\therefore\ p$	
3)	$\neg\neg p$	M.T. 1 y 2
4)	p	D.N. 3

Duplicación (Dup.) $\quad p \Leftrightarrow (p \vee p)$

$p \Leftrightarrow (p \wedge p)$

Conmutatividad (Conm.) $(p \vee q) \Leftrightarrow (q \vee p)$
$(p \wedge q) \Leftrightarrow (q \wedge p)$

Asociatividad (Asoc.) $((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$
$((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$

Contrarrecíproca (Cont.) $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$

1)	$p \Rightarrow q$	
2)	$\neg r \Rightarrow \neg q$	
	$\therefore\ p \Rightarrow r$	
3)	$q \Rightarrow r$	Cont. 2
4)	$p \Rightarrow r$	S.H. 1 y 3

Leyes de De Morgan (L.M.) $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$
$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$

1)	$p \Rightarrow q$	
2)	$\neg(r \vee q)$	
	$\therefore\ \neg p$	
3)	$\neg r \wedge \neg q$	L.M. 2
4)	$\neg q$	Simp. 3
5)	$\neg p$	M.T. 1 y 4

Bicondicional (Bicon.) $(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$

1)	$p \Rightarrow q$	
2)	$q \Leftrightarrow r$	
	$\therefore\ p \Rightarrow r$	
3)	$(q \Rightarrow r) \wedge (r \Rightarrow q)$	Bicon. 2
4)	$q \Rightarrow r$	Simp. 3
5)	$p \Rightarrow r$	S.H. 1 y 4

Condicional (Cond.) $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$

1)	$\neg p$	
	$\therefore\ p \Rightarrow q$	
2)	$\neg p \vee q$	Ad. 1
3)	$p \Rightarrow q$	Cond. 2

1)	q	
	$\therefore\ p \Rightarrow q$	
2)	$\neg p \vee q$	Ad. 1
3)	$p \Rightarrow q$	Cond. 2

Distributividad (Dist.) $(p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$
$(p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r))$

1) $p \Rightarrow (q \wedge r)$

$\therefore\ p \Rightarrow q$

2) $\neg p \vee (q \wedge r)$ Cond. 1

3) $(\neg p \vee q) \wedge (\neg p \vee r)$ Dist. 2

4) $\neg p \vee q$ Simp. 3

5) $p \Rightarrow q$ Cond. 4

Exportación (Exp.) $((p \wedge q) \Rightarrow r) \Leftrightarrow (p \Rightarrow (q \Rightarrow r))$

Demostración.

p	q	r	$p \wedge q$	$(p \wedge q) \Rightarrow r$	$q \Rightarrow r$	$p \Rightarrow (q \Rightarrow r)$	**(Exp)**
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	V	V	V
V	F	F	F	V	V	V	V
F	V	V	F	V	V	V	V
F	V	F	F	V	F	V	V
F	F	V	F	V	V	V	V
F	F	F	F	V	V	V	V

■

1) $(p \wedge q) \Rightarrow r$

2) $p \wedge \neg r$

$\therefore\ \neg q$

3) p Simp. 2

4) $\neg r$ Simp. 2

5) $p \Rightarrow (q \Rightarrow r)$ Exp. 1

6) $q \Rightarrow r$ M.P. 3 y 5

7) $\neg q$ M.T. 4 y 6

Ejemplos:

1) $f \Leftrightarrow \neg d$

2) $d \Rightarrow c$

3) $\neg(b \vee c) \vee \neg(a \vee d)$

4) a

$\therefore\ f \vee g$

5) $(\neg b \wedge \neg c) \vee (\neg a \wedge \neg d)$ L.M. 3

6) $((\neg b \wedge \neg c) \vee \neg a) \wedge ((\neg b \wedge \neg c) \vee \neg d)$ Dist. 5

7) $(\neg b \wedge \neg c) \vee \neg a$ Simp. 6

8) $(\neg b \vee \neg a) \wedge (\neg c \vee \neg a)$ Dist. 7

9) $\neg c \vee \neg a$ Simp. 8

10) $\neg c$ S.D. 4 y 9

11) $\neg d$ M.T. 2 y 10

12) $(f \Rightarrow \neg d) \wedge (\neg d \Rightarrow f)$ Bicon. 1

13) $\neg d \Rightarrow f$ Simp. 12

14) f M.P. 11 y 13

15)	$f \vee g$	Ad. 14

1)	$(a \vee b) \Rightarrow (c \wedge d)$	
2)	$\neg d$	
	$\therefore\ \neg a$	
3)	$\neg c \vee \neg d$	Ad. 2
4)	$\neg(c \wedge d)$	L.M. 3
5)	$\neg(a \vee b)$	M.T. 1 y 3
6)	$\neg a \wedge \neg b$	L.M. 5
7)	$\neg a$	Simp. 6

2.8. Sistemas deductivos

2.8.1. Demostración condicional

Un condicional es una fórmula que asevera que *si* un evento (digamos p) ocurre, *entonces* ocurre otro evento (digamos q). Una manera de probar un condicional es derivar la disyunción correspondiente y luego usar la regla de reemplazo del condicional, pero esta no es una manera directa ni intuitiva de validar la proposición *Si-entonces*. Una manera mucho más simple es suponer que el primer evento, p, ocurre y a partir de esto y las premisas deducir que q ocurre. Si esto es así, podemos justificar que *Si* p*, entonces* q. Esto es la regla de la demostración condicional.

p_1	
$\vdots$	
p_n	
$\therefore\ p \Rightarrow q$	
p	Suposición D.C.
$\vdots$	
q	
$p \Rightarrow q$	D.C.

Veamos un ejemplo simple:

1)	$(a \vee b) \Rightarrow (c \wedge d)$	
	$\therefore\ a \Rightarrow c$	
2)	a	Suposición D.C.
3)	$a \vee b$	Ad. 2
4)	$c \wedge d$	M.P. 1 y 3
5)	c	Simp. 4
6)	$a \Rightarrow c$	D.C. 2–5

1)	$(a \vee b) \Rightarrow \neg(c \vee d)$

2)	$(\neg c \wedge e) \Rightarrow (f \wedge \neg o)$	
3)	$(f \vee h) \Rightarrow (j \wedge \neg k)$	
	$\therefore\ (a \wedge e) \Rightarrow \neg k$	
4)	Supongamos $a \wedge e$	Suposición D.C.
5)	a	Simp. 4
6)	$a \vee b$	Ad. 5
7)	$\neg(c \vee d)$	M.P. 1 y 6
8)	$\neg c \wedge \neg d$	L.M. 7
9)	$\neg c$	Simp. 8
10)	e	Simp. 4
11)	$\neg c \wedge e$	Conj. 9 y 10
12)	$f \wedge \neg o$	M.P. 2 y 11
13)	f	Simp. 12
14)	$f \vee h$	Ad. 13
15)	$j \wedge \neg k$	M.P. 3 y 14
16)	$\neg k$	Simp. 15
17)	$(a \wedge e) \Rightarrow \neg k$	D.C. 4–16

Veamos el caso en que se nos pide demostrar:

$$(a \Rightarrow (b \Rightarrow c)) \Rightarrow [(\neg b \Rightarrow \neg a) \Rightarrow (a \Rightarrow c)]$$

Esto es equivalente a demostrar: $\dfrac{a \Rightarrow (b \Rightarrow c)}{\therefore\ (\neg b \Rightarrow \neg a) \Rightarrow (a \Rightarrow c)}$

Hagamos esta demostración como ejemplo:

1)	$a \Rightarrow (b \Rightarrow c)$	
	$\therefore\ (\neg b \Rightarrow \neg a) \Rightarrow (a \Rightarrow c)$	
2)	Supongamos $\neg b \Rightarrow \neg a$	Suposición D.C.
3)	Supongamos a	Suposición D.C.
4)	b	M.T. 2 y 3
5)	$b \Rightarrow c$	M.P. 1 y 3
6)	c	M.P. 4 y 5
7)	$a \Rightarrow c$	D.C. 3–6
8)	$(\neg b \Rightarrow \neg a) \Rightarrow (a \Rightarrow c)$	D.C. 2–7

2.8.2. Reducción al absurdo

La reducción al absurdo es un método en el que se pretende demostrar que la negación de lo queremos demostrar es insatisfacible. Recuerde que:

$$\neg((\mathrm{Pr}_1 \wedge \cdots \wedge \mathrm{Pr}_n) \Rightarrow C) \iff (\mathrm{Pr}_1 \wedge \cdots \wedge \mathrm{Pr}_n \wedge \neg C)$$

Por lo tanto si queremos demostrar que $(\mathrm{Pr}_1 \wedge \cdots \wedge \mathrm{Pr}_n) \Rightarrow C$ es una tautología es equivalente a demostrar que a partir de $(\mathrm{Pr}_1 \wedge \cdots \wedge \mathrm{Pr}_n \wedge \neg C)$ encontramos una contradicción.

$$
\begin{array}{ll}
p_1 & \\
\vdots & \\
\underline{p_n} & \\
\therefore\ C & \\
\ulcorner \neg C & \text{Suposición R.A.} \\
\mid\ \vdots & \\
\llcorner \text{ Falso} & \rightarrow\leftarrow \\
\text{C} & \text{R.A.}
\end{array}
$$

Veamos un ejemplo:

$$
\begin{array}{rll}
1) & a \Rightarrow \neg(b \vee c) & \\
2) & (\neg b \vee \neg d) \Rightarrow f & \\
3) & \underline{f \Rightarrow \neg a} & \\
 & \therefore\ \neg a & \\
4) & \ulcorner\ a & \text{Suposición R.A.} \\
5) & \mid\ \neg(b \vee c) & \text{M.P. 1 y 4} \\
6) & \mid\ \neg b \wedge \neg c & \text{L.M. 5} \\
7) & \mid\ \neg b & \text{Simp. 6} \\
8) & \mid\ \neg b \vee \neg d & \text{Ad. 7} \\
9) & \mid\ f & \text{M.P. 2 y 8} \\
10) & \mid\ \neg a & \text{M.P. 3 y 9} \\
11) & \llcorner\ a \wedge \neg a & \text{Conj. 4 y 10} \\
12) & \neg a & \text{R.A. 4–11}
\end{array}
$$

$$
\begin{array}{rll}
1) & a \Rightarrow (\neg f \Rightarrow d) & \\
2) & d \Rightarrow ((b \vee \neg c) \Rightarrow f) & \\
3) & \underline{\neg(e \Rightarrow f)} & \\
 & \therefore\ \neg(a \wedge b) & \\
4) & \ulcorner\ \text{Supongamos } a \wedge b & \text{Suposición R.A.} \\
5) & \mid\ a & \text{Simp. 4} \\
6) & \mid\ b & \text{Simp. 4} \\
7) & \mid\ \neg f \Rightarrow d & \text{M.P. 1 y 6} \\
8) & \mid\ \neg(\neg e \vee f) & \text{Cond. 3} \\
9) & \mid\ e \wedge \neg f) & \text{L.M. 8 + D.N.} \\
10) & \mid\ \neg f) & \text{Simp. 9} \\
11) & \mid\ d & \text{M.P. 7 y 10} \\
12) & \mid\ (b \vee \neg c) \Rightarrow f & \text{M.P. 2 y 11} \\
13) & \mid\ \neg(b \vee \neg c) & \text{M.T. 10 y 12} \\
14) & \mid\ b \vee \neg c & \text{Ad. 6} \\
15) & \llcorner\ \neg(b \vee \neg c) \wedge (b \vee \neg c) & \text{Conj. 13 y 14 } \rightarrow\leftarrow \\
16) & \neg(a \wedge b) & \text{R.A. 4–15}
\end{array}
$$

2.9. Método de resolución

El método de resolución no es otra cosa que el método de reducción al absurdo. Sin embargo, para plantear las premisas y la negación de la conclusión se hará en formato de clausulas y se utilizará una única regla de inferencia llamada resolvente. Esta es:

$$\begin{array}{l} p_1 \vee p_2 \vee \cdots \vee p_k \vee r \\ q_1 \vee q_2 \vee \cdots \vee q_l \vee \neg r \\ \hline \therefore\ p_1 \vee p_2 \vee \cdots \vee p_k \vee q_1 \vee q_2 \vee \cdots \vee q_l \end{array}$$

Note que cuando aplicamos la resolvente sobre p y $\neg p$, obtenemos la resolvente vacía esto es equivalente a haber encontrado una contradicción.

Ejemplo:

$$\begin{array}{l} (a \vee b) \Rightarrow (c \vee d) \\ (c \vee f) \Rightarrow h \\ e \wedge \neg d \\ e \Rightarrow a \\ \hline \therefore\ h \vee i \end{array}$$

Primero se deben transformar la premisas y la negación de la conclusión en FNC.

$$\begin{aligned} [(a \vee b) \Rightarrow (c \vee d)] &\iff \neg(a \vee b) \vee (c \vee d) \\ &\iff (\neg a \wedge \neg b) \vee (c \vee d) \\ &\iff (\neg a \wedge \neg b) \vee c \vee d \\ &\iff (\neg a \vee c \vee d) \wedge (\neg b \vee c \vee d) \\ [(c \vee f) \Rightarrow h] &\iff \neg(c \vee f) \vee h \\ &\iff (\neg c \wedge \neg f) \vee h \\ &\iff (\neg c \vee h) \wedge (\neg f \vee h) \\ \neg(h \vee i) &\iff \neg h \wedge \neg i \end{aligned}$$

$$\begin{array}{rll} 1) & (a \vee b) \Rightarrow (c \vee d) & \\ 2) & (c \vee f) \Rightarrow h & \\ 3) & e \wedge \neg d & \\ 4) & e \Rightarrow a & \\ \cline{2-2} & \therefore\ h \vee i & \\ 5) & \neg a \vee c \vee d & \\ 6) & \neg b \vee c \vee d & \\ 7) & \neg c \vee h & \\ 8) & \neg f \vee h & \\ 9) & e & \\ 10) & \neg d & \\ 11) & \neg e \vee a & \\ 12) & \neg h & \text{Neg. Conclusión} \\ 13) & \neg i & \text{Neg. Conclusión} \end{array}$$

14)	$\neg a \vee c$	Res. 5 y 10
15)	$\neg a \vee h$	Res. 7 y 14
16)	a	Res. 9 y 11
17)	h	Res. 15 y 16
18)	$\varnothing$	Res. 12 y 17
19)	$h \vee i$	

2.10. Ejercicios

P1. Determine si las siguientes son fórmulas bien formadas.

1. $(\neg p \wedge p) \Longrightarrow p$
2. $[(\neg p \Rightarrow p) \vee \veebar q] \Longrightarrow p$
3. $\neg p\, q \vee (p \wedge q)$
4. $(p \wedge \neg q) \wedge (\neg r \wedge p)$
5. $(p \wedge \neg q) \neg (\neg r \wedge p)$
6. $[(p \Rightarrow q) \Rightarrow r] \Longrightarrow [p \Rightarrow (q \Rightarrow r)]$

P2. Haga las tablas de verdad y determine si la proposición es una tautología una contradicción o una contingencia.

1. $\neg p \vee \neg q$
2. $\neg p \Rightarrow \neg q$
3. $(p \wedge q) \vee (r \wedge s)$
4. $(p \vee p) \Leftrightarrow p$
5. $(p \wedge p) \Leftrightarrow p$
6. $(p \wedge V) \Leftrightarrow p$
7. $(p \vee V) \Leftrightarrow V$
8. $p \Rightarrow (p \vee q)$
9. $(p \wedge q) \Rightarrow p$, $(p \wedge q) \Rightarrow q$
10. $(p \wedge q) \Rightarrow (p \vee q)$
11. $[(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)] \Rightarrow (p \Leftrightarrow r)$
12. $(p \wedge (p \Rightarrow q)) \Rightarrow q$
13. $(\neg p \Rightarrow p) \Rightarrow p$
14. $((p \wedge \neg q) \Rightarrow q) \Rightarrow (p \Rightarrow q)$

P3. Demuestre las siguientes tautologías sin utilizar tablas de verdad.

1. $\neg(p \Leftrightarrow q) \Longleftrightarrow (p \Leftrightarrow \neg q)$
2. $\neg[(p \wedge \neg q) \vee (\neg p \wedge q)] \Longleftrightarrow (p \Leftrightarrow q)$
3. $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Longrightarrow (p \Rightarrow r)$
4. $[(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)] \Longrightarrow (p \Leftrightarrow r)$
5. $[(p \Leftrightarrow q) \Leftrightarrow r] \Longleftrightarrow [p \Leftrightarrow (q \Leftrightarrow r)]$
6. $[(p \veebar q) \veebar r] \Longleftrightarrow [p \veebar (q \veebar r)]$

P4. Niegue y simplifique.

1. $p \wedge (q \vee r) \wedge (\neg p \vee \neg q \vee r)$
2. $(p \wedge q) \Rightarrow r$
3. $p \Rightarrow (\neg q \wedge r)$

P5. Descubra, si es posible, el valor de la proposición x con la información que se entrega.

1. $x \Rightarrow p$ es Falso.
2. $[p \Rightarrow (\neg x \wedge q)] \Rightarrow [q \wedge (\neg p \vee x)]$ es verdadero y q es Falso.
3. $(p \Leftrightarrow x) \wedge [(p \veebar q) \wedge \neg(p \Rightarrow q)]$ es Verdadero.
4. $(p \Leftrightarrow x) \wedge [(p \veebar q) \wedge (p \Rightarrow q)]$ es Verdadero.

P6. Lleve a Forma normal conjuntiva y Forma normal disyuntiva.

1. $(\neg p \Leftrightarrow q) \Rightarrow (p \wedge q)$
2. $(p \Leftrightarrow q) \Leftrightarrow r$
3. $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$

P7. Determine todas las tablas de verdad y expresiones lógicas que pueden formarse con p y q.

P8. Encuentre la fórmula para las siguientes tablas de verdad y luego reduzca la expresión.

1.

p	q	r	
V	V	V	F
V	V	F	F
V	F	V	F
V	F	F	V
F	V	V	V
F	V	F	V
F	F	V	F
F	F	F	V

2.

p	q	r	
V	V	V	F
V	V	F	V
V	F	V	F
V	F	F	V
F	V	V	F
F	V	F	F
F	F	V	F
F	F	F	F

3.

p	q	r	
V	V	V	V
V	V	F	V
V	F	V	F
V	F	F	V
F	V	V	V
F	V	F	F
F	F	V	V
F	F	F	V

P9. Escriba con símbolos las siguientes proposiciones, usando las abreviaciones dadas.

1. p: Juan va al supermercado — q: María trabaja hasta tarde
   r: María va al supermercado — s: Juan trabaja hasta tarde
   t: Juan tiene hambre — u: El jefe de Juan necesita que Juan trabaje hasta tarde
   v: Es feriado — w: Juan lava la loza.

   1.1) Juan irá al supermercado solo si María trabaja hasta tarde.
   1.2) María irá al supermercado si Juan trabaja hasta tarde.
   1.3) Juan no ira al supermercado a menos que el tenga hambre.
   1.4) Juan y María no irán juntos al supermercado.
   1.5) Juan no trabajará hasta tarde a menos que su jefe lo necesite.
   1.6) Juan y María trabajan hasta tarde solo si no es feriado.
   1.7) Ni Juan ni María van al supermercado si es feriado.
   1.8) Solo si Juan trabaja hasta tarde y no es feriado María ira al supermercado.
   1.9) María ira al supermercado si Juan no va y solo si Juan no va.
   1.10) Juan ira al supermercado y lavara la loza a menos que sea feriado o él este trabajando hasta tarde

2. p: estoy a dieta — q: hago ejercicio — r: engordo
   s: estoy motivado — t: estoy muy cansado — u: estoy deprimido
   v: soy flojo — w: nado — x: corro
   y: voy al trabajo en auto

   2.1) Si no hago dieta o ejercicio, voy a engordar.
   2.2) Haré dieta solo si estoy motivado, y ejercicio, solo si no estoy muy cansado.
   2.3) No haré dieta y ejercicio a menos que esté motivado
   2.4) Haré ejercicio si estoy motivado, siempre que no esté muy cansado o deprimido.
   2.5) No voy a engordar si corro o nado, a menos que vaya al trabajo en auto y no haga dieta.
   2.6) Estaré deprimido si y solo si soy flojo y no hago ni dieta ni ejercicio.
   2.7) Si engordo si y solo si no hago dieta ni ejercicio, entonces nadaré o correré, y además, no iré al trabajo en auto.

2.8) Yo engordo si y solo si no hago dieta, siempre que no estoy motivado y ni nado ni corro.

2.9) Solo si estoy motivado y no estoy muy cansado hago dieta y ejercicio.

2.10) A menos que esté deprimido o flojo, si engordo hago dieta o ejercicio, siempre que estoy motivado y no estoy muy cansado.

P10. Construya una demostración para cada uno de los siguientes argumentos:

1. $$\begin{array}{l} b \Rightarrow a \\ c \Rightarrow b \\ \neg a \\ \hline \therefore\ \neg c \end{array}$$

2. $$\begin{array}{l} (a \vee b) \Rightarrow \neg c \\ c \vee d \\ a \\ \hline \therefore\ d \end{array}$$

3. $$\begin{array}{l} (\neg a \wedge \neg b) \Rightarrow c \\ a \Rightarrow d \\ b \Rightarrow d \\ \neg d \\ \hline \therefore\ c \end{array}$$

4. $$\begin{array}{l} (a \vee b) \Rightarrow c \\ (c \vee d) \Rightarrow (e \vee f) \\ a \wedge \neg e \\ \hline \therefore\ f \end{array}$$

5. $$\begin{array}{l} (a \vee b) \Rightarrow t \\ z \Rightarrow (a \vee b) \\ t \Rightarrow w \\ \neg w \\ \hline \therefore\ \neg z \end{array}$$

6. $$\begin{array}{l} (a \vee b) \Rightarrow (c \vee d) \\ c \Rightarrow e \\ a \wedge \neg e \\ \hline \therefore\ d \vee w \end{array}$$

7. $$\begin{array}{l} (\neg a \vee \neg b) \Rightarrow \neg g \\ \neg a \Rightarrow (f \Rightarrow g) \\ (a \Rightarrow d) \wedge \neg d \\ \hline \therefore\ \neg f \end{array}$$

8. $$\begin{array}{l} (a \vee b) \Rightarrow (c \vee d) \\ c \Rightarrow e \\ c \vee \neg f \\ a \wedge \neg e \\ f \vee (d \Rightarrow z) \\ \hline \therefore\ z \end{array}$$

9. $$\begin{array}{l} (b \vee c) \Rightarrow a \\ a \Rightarrow (s \vee t) \\ b \wedge \neg s \\ (t \wedge a) \Rightarrow (w \Rightarrow s) \\ \hline \therefore\ \neg w \end{array}$$

10. $$\begin{array}{l} a \Rightarrow ((c \vee d) \Rightarrow b) \\ (\neg w \vee \neg t) \Rightarrow (a \wedge c) \\ w \Rightarrow (s \vee p) \\ \neg h \vee \neg(s \vee p) \\ \neg h \Rightarrow z \\ \neg z \wedge \neg y \\ \hline \therefore\ b \wedge \neg y \end{array}$$

11. $$\begin{array}{l} (\neg b \vee \neg c) \Rightarrow (a \Rightarrow w) \\ \neg a \Rightarrow (t \Rightarrow \neg z) \\ t \wedge \neg x \\ x \vee (\neg w \wedge \neg b) \\ \neg z \Rightarrow (\neg s \vee x) \\ \hline \therefore\ \neg s \end{array}$$

12. $$\begin{array}{l} (s \wedge p) \Rightarrow (q \vee \neg r) \\ w \Rightarrow (q \Rightarrow t) \\ w \wedge (a \Rightarrow r) \\ w \Rightarrow (s \vee t) \\ p \wedge \neg t \\ \hline \therefore\ \neg a \end{array}$$

13. $$\begin{array}{l} (p \vee q) \wedge (r \vee s) \\ (q \Rightarrow s) \wedge (s \Rightarrow t) \\ \neg z \wedge \neg t \\ t \vee (d \Rightarrow z) \\ (p \wedge r) \Rightarrow (c \Rightarrow d) \\ \hline \therefore\ \neg c \end{array}$$

14. $$\begin{array}{l} p \Leftrightarrow q \\ \neg(p \vee s) \\ \hline \therefore\ \neg q \end{array}$$

15. $$\begin{array}{l} \neg c \Leftrightarrow a \\ (f \wedge h) \vee \neg c \\ \neg(a \vee b) \\ \hline \therefore\ f \wedge \neg b \end{array}$$

16. $$\begin{array}{l} \neg a \vee \neg(b \wedge c) \\ \neg(\neg a \vee (f \vee h)) \\ f \Leftrightarrow \neg c \\ \hline \therefore \neg(b \vee h) \end{array}$$

17. $$\begin{array}{l} \neg(c \vee d) \\ d \Leftrightarrow (e \vee f) \\ \neg a \Rightarrow (c \vee f) \\ \hline \therefore a \end{array}$$

18. $$\begin{array}{l} (a \Leftrightarrow b) \Rightarrow c \\ \neg(c \vee a) \\ \hline \therefore b \end{array}$$

19. $$\begin{array}{l} x \Leftrightarrow \neg y \\ (y \vee z) \Rightarrow t \\ \neg(t \vee w) \\ \hline \therefore p \Rightarrow x \end{array}$$

20. $$\begin{array}{l} (a \vee b) \Rightarrow (c \vee d) \\ a \Rightarrow \neg c \\ \neg(f \wedge \neg a) \\ f \\ \hline \therefore\ d \end{array}$$

21. $a \Rightarrow \neg b$
$\neg c \Rightarrow b$
$\neg a \Rightarrow \neg c$
$\therefore\ a \Leftrightarrow c$

22. $\neg(a \vee (b \Rightarrow t))$
$(a \wedge c) \vee (w \Rightarrow \neg d)$
$\neg(p \vee t) \Rightarrow d$
$\neg p \Leftrightarrow \neg(t \wedge s)$
$\therefore\ \neg w$

23. $(a \wedge f) \Rightarrow (c \vee g)$
$\neg(c \vee (f \wedge g))$
$f \Leftrightarrow \neg(x \wedge y)$
$\neg(w \Rightarrow x)$
$\therefore\ \neg(a \vee x)$

24. $p \Leftrightarrow (q \Rightarrow r)$
$\neg(p \vee (s \Rightarrow t))$
$z \Rightarrow w$
$\neg(r \vee t) \Rightarrow \neg(s \wedge w)$
$\therefore\ \neg z$

25. $(a \Rightarrow b) \Rightarrow \neg(c \Rightarrow d)$
$\neg(a \vee f)$
$\therefore\ \neg(d \vee f)$

26. $f \Rightarrow (\neg g \Rightarrow \neg f)$
$\neg(h \Rightarrow g)$
$\neg(h \wedge w)$
$a \Rightarrow (s \wedge w)$
$\therefore\ \neg(a \vee f)$

27. $p \vee q$
$q \Rightarrow r$
$r \Rightarrow (s \Rightarrow \neg t)$
$(\neg s \Rightarrow u) \wedge (u \Rightarrow v)$
$\therefore\ (\neg p \wedge \neg v) \Rightarrow \neg t$

28. $(p \wedge s) \Rightarrow (t \vee w)$
$\neg t \Leftrightarrow \neg(m \wedge o)$
$\neg(w \vee (\neg s \vee m))$
$\neg a \Rightarrow p$
$\therefore\ a$

P11. Escriba en lógica simbólica y construya demostraciones de los siguientes argumentos.

1. Platón o Demócrito creían en la teoría de las formas. Platón hubiese creído en la teoría de las formas solo si él no hubiera sido un atomista, y Demócrito hubiese sido un atomista solo si él no hubiese creído en la teoría de las formas. Demócrito fue un atomista. Por lo tanto, Platón no fue atomista.
2. Si fumo o bebo en exceso, no duermo bien, y si no duermo o no como bien, entonces me siento pésimo. Si me siento pésimo, no hago ejercicio y no estudio suficiente. Fumo demasiado, por lo tanto no estudio mucho.
3. Si la mente y el cerebro son idénticos, entonces el cerebro es una entidad física si y solo si la mente lo es. Si la mente es una entidad física, entonces los pensamientos son una entidad material. Los pensamientos no son materiales, pero el cerebro es una entidad física. Por lo tanto, la mente y el cerebro no son lo mismo.
4. Encontraré un trabajo cuando me gradúe, solo si estoy bien preparado. Para estar bien preparado necesito leer y escribir extremadamente bien y tener un buen conocimiento técnico. Voy a leer y escribir extremadamente bien si y solo si tomo muchos cursos de humanidades, pero si tomo muchos cursos de humanidades, no tomaré muchos cursos técnicos. Si no tomo muchos cursos técnicos no tendré un buen conocimiento técnico. Por lo tanto, no encontraré un buen trabajo cuando me gradúe.
5. Si mi gata está enferma, ella estuvo peleando o comió muchos ratones. Ella hubiera peleado solo si hubiese sido atacada, y ella hubiese sido atacada solo si el gato de mi vecina o el perro del jardinero hubiesen estado afuera. El gato de mi vecina sale solo si el día está soleado, y el perro del jardinero sale solo si el día está cálido. Hoy no estuvo ni cálido ni soleado, pero mi gata está enferma. Por consiguiente ella comió muchos ratones.
6. Si los Monetaristas están en lo cierto, entonces la inflación aumenta si y solo si el ingreso de dinero crece muy rápido. Si los Keynesianos tienen razón, entonces hay

un aumento en la inflación si y solo si decrece la cesantía. Si los Liberales tienen razón, la inflación crece si y solo si el gobierno gasta más de lo debido. El ingreso de dinero crece muy rápido solo si los impuestos son muy bajos, y el gobierno gasta más de lo debido si y solo si los impuestos son muy bajos. La cesantía no decrece y los impuestos no son muy bajos, pero la inflación crece. Por lo tanto ni los monetaristas, ni los Keynesianos, ni los Liberales tienen razón.

P12. Traduzca al Cálculo Proposicional y determine la validez usando reglas de inferencia

Si la ciudadanía romana hubiera sido una garantía de los derechos civiles, los romanos habrían gozado de libertad religiosa. Si los romanos hubieran gozado de libertad religiosa, no se habría perseguido a los primeros cristianos. Pero los primeros cristianos fueron perseguidos. Por consiguiente, la ciudadanía romana no puede haber sido una garantía de los derechos civiles.

P13. Dos personas se dicen del mismo tipo si ambas dicen la verdad o ambas mienten. Tenemos tres personas, Aladino, Bertoldo y Ceferino, y sabemos que :

- Aladino dice: "Bertoldo miente".
- Bertoldo dice: "Aladino y Ceferino son del mismo tipo".

¿Ceferino miente o dice la verdad?

P14. Construya una demostración para cada uno de los siguientes argumentos:

1. $$\begin{array}{l} (\neg a \vee \neg b) \Rightarrow \neg c \\ \hline \therefore\ c \Rightarrow a \end{array}$$

2. $$\begin{array}{l} (d \wedge e) \Rightarrow \neg f \\ f \vee (g \wedge w) \\ d \Rightarrow e \\ \hline \therefore\ d \Rightarrow g \end{array}$$

3. $$\begin{array}{l} p \Rightarrow q \\ (p \wedge q) \Rightarrow r \\ p \Rightarrow (r \Rightarrow s) \\ (r \wedge s) \Rightarrow t \\ \hline \therefore p \Rightarrow t \end{array}$$

4. $$\begin{array}{l} w \Rightarrow x \\ (w \Rightarrow y) \Rightarrow (z \vee x) \\ (w \wedge x) \Rightarrow y \\ \neg z \\ \hline \therefore\ x \end{array}$$

5. $$\begin{array}{l} (a \vee b) \Rightarrow \neg c \\ d \Rightarrow (\neg f \wedge \neg g) \\ \hline \therefore (a \vee d) \Rightarrow \neg(c \wedge f) \end{array}$$

6. $$\begin{array}{l} a \Rightarrow (b \Rightarrow c) \\ (c \wedge d) \Rightarrow e \\ f \Rightarrow \neg(d \Rightarrow e) \\ \hline \therefore a \Rightarrow (b \Rightarrow \neg f) \end{array}$$

7. $$\begin{array}{l} (a \vee b) \Rightarrow (a \wedge b) \\ \hline \therefore a \Leftrightarrow b \end{array}$$

8. $$\begin{array}{l} a \vee b \\ \neg a \vee \neg b \\ \hline \therefore \neg(a \Leftrightarrow b) \end{array}$$

9. $$\begin{array}{l} p \Rightarrow s \\ s \Rightarrow \neg(b \wedge d) \\ \neg b \Rightarrow t \\ \neg(d \Rightarrow t) \\ \hline \therefore \neg p \end{array}$$

10. $$\begin{array}{l} a \Rightarrow (b \vee c) \\ c \Rightarrow (d \Leftrightarrow f) \\ d \wedge \neg f \\ b \Rightarrow f \\ \hline \therefore \neg a \end{array}$$

11. $$\begin{array}{l} (a \wedge b) \vee (\neg a \wedge \neg b) \\ \hline \therefore a \Leftrightarrow b \end{array}$$

12. $$\begin{array}{l} a \Rightarrow (b \vee c) \\ e \Rightarrow (c \vee p) \\ \neg c \\ \hline \therefore \neg(b \vee p) \Rightarrow \neg(a \vee e) \end{array}$$

13. $$\begin{array}{l} c \Rightarrow (d \Rightarrow \neg c) \\ c \Leftrightarrow d \\ \hline \therefore \neg c \wedge \neg d \end{array}$$

14. $$\begin{array}{l} a \Leftrightarrow \neg(b \vee c) \\ b \Leftrightarrow (d \wedge \neg e) \\ \neg(e \wedge a) \\ \hline \therefore a \Rightarrow \neg d \end{array}$$

15. $$\begin{array}{l} f \Leftrightarrow \neg(z \wedge y) \\ \neg(g \vee z) \Rightarrow \neg h \\ \neg(f \wedge h) \vee y \\ \hline \therefore f \Rightarrow (h \Rightarrow g) \end{array}$$

16. $(a \vee b) \Rightarrow \neg(f \wedge d)$
$\neg(a \wedge \neg d)$
$\neg f \Rightarrow \neg(c \wedge d)$
$\therefore \neg(a \wedge c)$

17. $(a \vee d) \Rightarrow w$
$\neg(b \vee c)$
$r \Leftrightarrow (c \wedge t)$
$\neg r \Leftrightarrow a$
$\therefore\ \neg(w \Rightarrow c)$

18. $\neg a \vee c$
$t \Rightarrow (s \wedge \neg b)$
$s \Leftrightarrow \neg(d \vee c)$
$\neg a \Rightarrow (e \Rightarrow (b \vee c)$
$\therefore\ t \Rightarrow \neg(d \vee e)$

P15. Construya demostraciones para los siguientes teoremas.

1. $(\neg p \Rightarrow (\neg q \Rightarrow \neg r)) \Rightarrow (r \Rightarrow (p \vee q))$
2. $(p \Rightarrow (q \Rightarrow (r \wedge s))) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow s))$
3. $(p \Rightarrow (p \wedge q)) \vee (q \Rightarrow (p \wedge q))$
4. $\neg((p \Leftrightarrow \neg q) \wedge \neg(p \vee q))$
5. $(p \Leftrightarrow \neg q) \Leftrightarrow \neg(p \Leftrightarrow q)$
6. $((p \vee q) \Rightarrow (p \wedge q)) \Leftrightarrow (p \Leftrightarrow q)$
7. $((p \vee q) \Rightarrow (r \wedge s)) \Rightarrow (\neg s \Rightarrow \neg p)$
8. $p \Rightarrow (\neg p \Rightarrow q)$
9. $(p \Rightarrow q) \Rightarrow ((p \Rightarrow (q \Rightarrow r)) \Rightarrow (p \Rightarrow r))$
10. $(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$

Capítulo 3

Lógica de primer orden

Hasta ahora hemos visto como la lógica proposicional resulta bastante útil. Pero supongamos que tenemos el siguiente argumento: "Los gatos son mamíferos y Felix es un gato, por lo tanto Felix es un mamífero", sin duda al escucharlo nos parece que el argumento es correcto, pero si tratamos de modelarlo con lógica proposicional, vemos que no podemos concluir nada, ya que las tres proposiciones involucradas son simples ("Los gatos son mamíferos", "Felix es un gato" y "Felix es un mamífero"). De este modo para poder hacer este argumento necesitaremos de una herramienta más poderosa que es la lógica de predicados.

Si ponemos atención nos damos cuenta que lo importante se encuentra en el predicado de estas proposiciones lógicas, es decir, lo importante es "es un mamífero", y "es un gato". Sin embargo, los predicados no son proposiciones lógicas porque el valor de verdad de las proposiciones lógicas que usan estos predicados depende del sujeto. Por ejemplo, si yo digo "los gatos son mamíferos" es verdadero, pero si digo "las gallinas son mamíferos" es falso. Entonces definimos lo que llamamos un predicado o una función proposicional.

Para modelar estos problemas necesitamos introducir la lógica de predicados. Comencemos con algunas definiciones básicas.

Definición 3.1. En lógica, el dominio de discurso, también llamado universo de discurso, o simplemente dominio, es el conjunto (no vacío) de objetos acerca de los cuales se habla en un determinado contexto.

Dependiendo del dominio de discurso, una misma proposición podrá ser verdadera o falsa. Por ejemplo, al decir "todos son amigos", si se está hablando acerca de un pequeño grupo de personas, la proposición quizás sea verdadera, pero si se está hablando acerca de todo el mundo, entonces es falsa.

Definición 3.2. Una *función proposicional o predicado* es una función cuyo dominio es alguna potencia de un Dominio de Discurso y su recorrido es $\{V, F\}$, es decir es una función tal que si reemplazamos la variable por un elemento del dominio de discurso obtenemos una proposición lógica

Ejemplos:

- Dominio de discurso: $\mathbb{N}$, $i(x) = x$ es impar.
- Dominio de discurso: Personas, $n(x) = x$ tiene el pelo negro.
- Dominio de discurso: Personas, $h(x, y) = x$ es hermano de y.
- Dominio de discurso: Personas, $p(x, y) = x$ es el padre de y.

Otro elemento que se utiliza en la lógica de predicados son los cuantificadores, que nos dicen cuántos elementos de un dominio de discurso cumplen una función proposicional. Aquí estudiaremos dos cuantificadores:

1. **Cuantificador Universal** ($\forall x\ p(x)$) significa que todos los elementos del dominio de discurso cumplen la propiedad p. Ejemplo:
    - $(\forall x\ i(x))$: para todo x, x es impar.
    - $(\forall x\ n(x))$: para todo x, x tiene el pelo negro.
2. **Cuantificador Existencial** ($\exists x\ p(x)$) significa que al menos uno de los elementos del dominio de discurso cumple la propiedad p. Ejemplo:
    - $(\exists x\ i(x))$: existe al menos un x tal que x es impar.
    - $(\exists x\ n(x))$: existe al menos un x tal que x tiene el pelo negro.

Definición 3.3. En una expresión del tipo $(\forall x\ A)$ o $(\exists x\ A)$ la variable x se conoce como variable de cuantificación, y la fórmula A como ámbito o recorrido de la cuantificación.

Definición 3.4. Una variable x está ligada si está en el ámbito de un cuantificador que la tiene como variable de cuantificación. En caso contrario, la variable está libre.

3.1. Formas bien formadas

Para definir cuando una fórmula es bien formada debemos definir algunos conceptos previos.

1. **Dominio de discurso.** D.
2. **Variables:** x, y, z, etc. En general se usan las últimas letras del abecedario en minúsculas.
3. **Cuantificadores:** $\forall, \exists$.
4. **Conectivos lógicos:** $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \veebar$.
5. **Igualdad:** $=$.
6. **Paréntesis:** $()$.

7. **Funcionales n-arios:** $+, -, \cdot$, etc. $f : D^n \to D$

8. **Predicados n-arios**. $p : D^n \to \{V, F\}$

Definición 3.5. Un término se define como:

1. Toda variable es un término.

2. Si $t_1, \ldots, t_n$ son términos y f es un funcional n-ario entonces: $f(t_1, \ldots, t_n)$ es un término.

Por ejemplo son términos: $f(x, y) = x - y$, $f(x, f(z, y))$.

Note que una constante es un caso especial de función, tal que no importa cual sea el argumento se obtiene el mismo resultado, por lo tanto una constante también es un término.

Definición 3.6. Una fórmula atómica se define como $p(t_1, \ldots, t_n)$, donde $t_1, \ldots, t_n$ son términos y p es un predicado n-ario.

Definición 3.7. Una fórmula es una fórmula bien formada si:

1. Es una fórmula atómica.

2. Es la negación, conjunción, disyunción, implicancia, equivalencia o disyunción excluyente de fórmulas bien formadas.

$$\begin{aligned}
A \text{ es una fórmula bien formada} &\implies \neg A \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \wedge B) \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \vee B) \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \Rightarrow B) \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \Leftrightarrow B) \text{ es una fórmula bien formada}\\
A \text{ y } B \text{ son fórmulas bien formadas} &\implies (A \veebar B) \text{ es una fórmula bien formada}
\end{aligned}$$

3. Es la cuantificación de una variable libre de una fórmula bien formada. $(\forall x\ \alpha(x))$ o $(\exists x\ \alpha(x))$.

3.2. Lógica de predicados Monádica

Definición 3.8. Una *proposición singular* es una proposición que se obtiene al instanciar una función proposicional en un elemento particular del dominio de discurso.

Ejemplo: Usando las proposiciones anteriores:

- $i(5)$: 5 es impar

- n(Lili) : Lili tiene el pelo negro.
- h(Pedro,Juan) : Pedro es hermano de Juan.
- p(Diego,Pedro) : Diego es el padre de Pedro.

Otra forma de transformar una función proposicional en una proposición lógica es usar cuantificadores.

Definición 3.9. Una *proposición cuantificada simple* es una proposición que se obtiene al afirmar que algunos o todos de los elemento del dominio de discurso hacen verdadera la función proposicional.

Ejemplo: Todos tienen un amigo, Hay perros.

Como vimos en el ejemplo “los gatos son mamíferos”, no siempre el sujeto de una función proposicional es reemplazado por un elemento del dominio de discurso o cuantificado, es así como aparecen las proposiciones categóricas.

Definición 3.10. Una *proposición categórica* es una proposición que se obtiene al instanciar una función proposicional en un subconjunto del dominio de discurso.

Ejemplo: Los gatos son mamíferos.

De este modo podemos ver que las funciones proposicionales son la base de la lógica de predicados, ya que tanto las proposiciones singulares como categóricas no son más que una función proposicional en la se reemplaza la variable por un elemento del dominio de discurso o un subconjunto de este.

3.2.1. Lenguaje natural a lógica simbólica de primer orden

Para trabajar en este tema usaremos algunos predicados.

$p(x)$: x está en P $s(x)$: x está en S $q(x)$: x está en Q

Para las proposiciones singulares pasar del lenguaje natural a la lógica simbólica es muy simple basta con identificar el predicado, que es la función proposicional y reemplazar la variable por un elemento del dominio de discurso como se observa en la Tabla 3.1.

Tabla 3.1: Del lenguaje natural a la lógica de predicados en proposiciones singulares.

Lenguaje natural	**Fórmula**
a está en P	$p(a)$
a no está en P	$\neg p(a)$

Ejemplos:

1. Leon Tolstoy era ruso.

   $r(x)$: x era ruso.

   $r(\text{Leon Tolstoy})$

2. La Guerra y la paz es una novela.

   $n(x)$: x es una novela.

   $n(\text{La Guerra y la Paz})$

3. La luna tiene una órbita elíptica.

   $o(x)$: x tiene una órbita elíptica.

   $o(\text{La luna})$

4. Ángela es feliz.

   $f(x)$: x es feliz.

   $f(\text{Ángela})$

También podríamos simbolizar proposiciones compuestas.

1. Si Juan juega básquetbol o fútbol y Pedro juega ambos, entonces el entrenador estará feliz.

   $f(x)$: x juega fútbol.
   $b(x)$: x juega básquetbol.
   $h(x)$: x estará feliz.

   $$\{[b(\text{Juan}) \vee f(\text{Juan})] \wedge [f(\text{Pedro}) \wedge b(\text{Pedro})]\} \Rightarrow h(\text{el entrenador})$$

2. Si Juan y María van al cine, entonces a menos que Juan prepare el almuerzo ninguno tendrá algo para comer.

   $p(x)$: x va al cine.
   $a(x)$: x prepara el almuerzo.
   $c(x)$: x tiene algo para comer

   $$(p(\text{Juan}) \wedge p(\text{María})) \Rightarrow [\neg a(\text{Juan}) \Rightarrow (\neg c(\text{Juan}) \wedge c(\text{María}))]$$

En el caso de las proposiciones cuantificadas simples, debemos tomar en cuenta los cuantificadores. Los cuantificadores como "todos" y "algunos" constituyen uno de los elementos básicos de la lógica de predicados. El rol de un cuantificador es decirnos para cuántos elementos del dominio de discurso la función proposicional toma el valor verdadero. Se ubica siempre al inicio de la función proposicional y al utilizarse tenemos una proposición lógica. Los paréntesis indican el rango de acción de cada cuantificador.

- Cuantificador existencial: $(\exists x\ p(x))$ indica que a algún elemento del dominio de discurso hace que $p(x)$ sea verdadera.

- Cuantificador universal: $(\forall x\ p(x))$ indica que todos y cada uno de los elementos del dominio de discurso cumple la propiedad.

La simbolización para las proposiciones cuantificadas lo podemos resumir en la Tabla 3.2.

Tabla 3.2: Del lenguaje natural a la lógica de predicados en proposiciones cuantificadas.

Lenguaje natural	**Fórmulas**
Todos están en P Nadie está fuera de P	$(\forall x\ p(x))$ $\neg(\exists x\ \neg p(x))$
Algunos están en P No todos están fuera de P	$(\exists x\ p(x))$ $\neg(\forall x\ \neg p(x))$
Todos están fuera de P Nada está en P	$(\forall x\ \neg p(x))$ $\neg(\exists x\ p(x))$
Algunos están fuera P No todos están en P	$(\exists x\ \neg p(x))$ $\neg(\forall x\ p(x))$

Ejemplos:

- Todo tiene un propósito.

  $(p(x) : x$ tiene un propósito, $(\forall x\ p(x)))$

- Todo es hermoso a su manera.

  $(h(x) : x$ es hermoso a su manera, $(\forall x\ h(x)))$

- Cualquier cosa es mejor que una guerra.

  $(g(x) : x$ es mejor que una guerra, $(\forall x\ g(x)))$

- Cada cosa es única.

  $(u(x) : x$ es único, $(\forall x\ u(x)))$

- Hay hoyos negros en el universo.

  $(n(x) : x$ es un hoyo negro, $(\exists x\ n(x)))$

- Hay al menos un billete en mi bolsillo.

  $(b(x) : x$ es un billete en mi bolsillo, $(\exists x\ b(x)))$

- Hay muchas traducciones de la biblia.

  $(t(x) : x$ es una traducción de la Biblia, $(\exists x\ t(x)))$

- Algunas cosas son misteriosas.

  $(m(x) : x$ es misterioso, $(\exists x\ m(x)))$

- Nada limpia como Lysol.

  ($l(x)$: x limpia como Lysol, $\neg(\exists x\ l(x))$)

- No hay vagabundos felices.

  ($v(x)$: x es un vagabundo feliz, $\neg(\exists x\ v(x))$)

- Los demonios no existen.

  ($d(x)$: x es un demonio, $\neg(\exists x\ d(x))$)

- Nada es claro.

  ($c(x)$: x es claro, $\neg(\exists x\ c(x))$)

- No hay tazas voladoras.

  ($v(x)$: x es una taza voladora, $\neg(\exists x\ v(x))$)

- Nada tiene sentido.

  ($s(x)$: x tiene sentido, $\neg(\exists x\ s(x))$)

- No tengo nada

  ($a(x)$: x me pertenece, $\neg(\exists x\ a(x))$)

- No todo es bello

  ($b(x)$: x es bello, $\neg(\forall x\ b(x))$)

- No todas las cosas están compuestas por átomos.

  ($a(x)$: x está compuesto por átomos, $\neg(\forall x\ a(x))$)

Notemos que:

$$\begin{aligned}
\neg(\exists x\ p(x)) &\iff (\forall x\ \neg p(x)) \\
\neg(\forall x\ p(x)) &\iff (\exists x\ \neg p(x)) \\
\neg(\exists x\ \neg p(x)) &\iff (\forall x\ p(x)) \\
\neg(\forall x\ \neg p(x)) &\iff (\exists x\ p(x))
\end{aligned}$$

En el caso de proposiciones categóricas este procedimiento se vuelve más complicado. Si observamos este tipo de proposiciones, podemos decir que el conjunto S es el sujeto y P es la propiedad que cumplen. Observemos el diagrama de Venn de la Figura 3.1, las proposiciones categóricas las podemos clasificar en cuatro tipos.

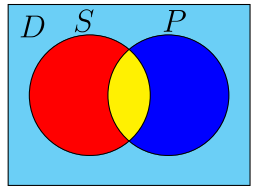


Figura 3.1: Diagrama de Venn

1. **"Algunos S están en P"**, esto quiere decir que la región de color amarillo tiene al menos un elemento. Esto significa que hay elementos del dominio que están en S y también en P. Para simbolizar usaremos: $(\exists x\ s(x) \wedge p(x))$. Ejemplo:

   Algunas manzanas son verdes. ($m(x)$: x es manzana, $v(x)$: x es verde, $(\exists x\ m(x) \wedge v(x)))$

2. **"Algunos S no están en P"**, esto quiere decir que la región de color rojo tiene al menos un elemento. Esto significa que hay elementos del dominio que están en S, pero no están P. Para simbolizar usaremos: $(\exists x\ s(x) \wedge \neg p(x))$. Ejemplo:

   Algunos barcos no tienen velas. ($b(x)$: x es un barco, $v(x)$: x tiene velas, $(\exists x\ b(x) \wedge \neg v(x)))$

3. **"Ningún S está en P"**, esto quiere decir que la región de color amarillo no tiene elementos. Esto significa que si un elemento del dominio está en S entonces no está P. Para simbolizar usaremos: $(\forall x\ s(x) \Rightarrow \neg p(x))$. Ejemplo:

   Ningún adulto hace pataletas. ($a(x)$: x es adulto, $p(x)$: x hace pataletas, $(\forall x\ a(x) \Rightarrow \neg p(x)))$

4. **"Todos los S están en P"**, esto quiere decir que el color rojo no tiene elementos y, por lo tanto $S \subseteq P$. Esto significa que si un elemento del dominio está en S entonces está P. Para simbolizar usaremos: $(\forall x\ s(x) \Rightarrow p(x))$. Ejemplo:

   Todos los cactus tienen espinas. ($c(x)$: x es un cactus, $e(x)$: x tiene espinas, $(\forall x\ c(x) \Rightarrow e(x)))$

Ahora veamos que pasa cuando tenemos negaciones de estas proposiciones categóricas.

- "No hay elementos S en P", claramente esta es una negación de una proposición categórica del tipo "algunos S están en P". Por lo tanto sería la negación de $(\exists x\ s(x) \wedge p(x))$. Pero ya vimos que $\neg(\exists x\ \phi(x)) \iff (\forall x\ \neg\phi(x))$. Entonces:

$$\begin{aligned}
\neg(\exists x\ s(x) \wedge p(x)) &\iff (\forall x\ \neg(s(x) \wedge p(x))) \\
&\iff (\forall x\ \neg s(x) \vee \neg p(x)) \\
&\iff (\forall x\ s(x) \Rightarrow \neg p(x))
\end{aligned}$$

  Esto corresponde a una proposición categórica del tercer tipo.

- "No hay elementos de S que no están en P", es una negación de una proposición categórica del tipo "algunos S no están en P". Por lo tanto sería la negación de $(\exists x\ s(x) \wedge \neg p(x))$. Entonces:

$$\begin{aligned}\neg(\exists x\ s(x) \wedge \neg p(x)) &\iff (\forall x\ \neg(s(x) \wedge \neg p(x)))\\ &\iff (\forall x\ \neg s(x) \vee p(x))\\ &\iff (\forall x\ s(x) \Rightarrow p(x))\end{aligned}$$

  Esto corresponde a una proposición categórica del cuarto tipo.

- "Algunos S están en P", en este caso está es la negación del tercer tipo de proposiciones categóricas y es evidente que corresponde a una proposición categórica del primer tipo.

$$\begin{aligned}\neg(\forall x\ s(x) \Rightarrow \neg p(x)) &\iff (\exists x\ \neg(s(x) \Rightarrow \neg p(x)))\\ &\iff (\exists x\ s(x) \wedge p(x))\end{aligned}$$

- "No todos los S están en P" es la negación de "Todos los S están en P". Por lo tanto:

$$\begin{aligned}\neg(\forall x\ s(x) \Rightarrow p(x)) &\iff (\exists x\ \neg(s(x) \Rightarrow p(x)))\\ &\iff (\exists x\ s(x) \wedge \neg p(x))\end{aligned}$$

  Esto corresponde a una proposición categórica del segundo tipo.

En la Tabla 3.3 tenemos un resumen para pasar desde lenguaje natural a lógica de predicados y vice versa en proposiciones categóricas.

Ejemplos:

1. Todas las plantas tienen clorofila.
2. Las ballenas son mamíferos.
3. Un alce no es de confianza.
4. A algunos estudiantes no les gusta el álgebra.
5. No todas las plantas tienen flores.
6. No hay ratones en el vecindario.
7. No hay peces que vivan en la laguna de los patos.
8. Solo los ciudadanos pueden votar.

Tabla 3.3: Del lenguaje natural a la lógica de predicados en proposiciones categóricas

Lenguaje natural	**Fórmulas**
Todos los S están en P Solo los P están en S No hay S que no están en P	$(\forall x\ s(x) \Rightarrow p(x))$ $\neg(\exists x\ s(x) \wedge \neg p(x))$
Algunos S están en P No todos los S no están en P	$(\exists x\ s(x) \wedge p(x))$ $\neg(\forall x\ s(x) \Rightarrow \neg p(x))$
Ningún S está en P No hay S que esté en P	$(\forall x\ s(x) \Rightarrow \neg p(x))$ $\neg(\exists x\ s(x) \wedge p(x))$
Algunos S no están en P No todos los S están en P	$(\exists x\ s(x) \wedge \neg p(x))$ $\neg(\forall x\ s(x) \Rightarrow p(x))$
Los S que están en P están en Q Los S si están en P estarán en Q	$(\forall x\ s(x) \wedge p(x) \Rightarrow q(x))$ $(\forall x\ s(x) \Rightarrow (p(x) \Rightarrow q(x)))$
Ningún S está en P a menos que esté en Q	$(\forall x\ s(x) \Rightarrow (\neg q(x) \Rightarrow \neg p(x)))$ $(\forall x\ s(x) \Rightarrow (p(x) \Rightarrow q(x)))$ $\neg(\exists x\ s(x) \wedge \neg(p(x) \Rightarrow q(x)))$ $\neg(\exists x\ s(x) \wedge p(x) \wedge \neg q(x)))$

9. Solo los niños hacen pataletas.
10. Solo los que compran boletos pueden ganar la lotería.
11. No solo a los niños les gustan los cuentos de hadas.
12. No hubo nadie que no comiera.

Sujetos y predicados complejos

En este caso, seguiremos la misma técnica que usamos con proposiciones compuestas, es decir, vamos a identificar la estructura principal y luego desglosaremos hasta llegar a expresiones simples.

1. Los rinocerontes tienen mal carácter y atacan si son molestados.
2. Los elefantes no tienen mal carácter y no atacarán a menos que sean provocados o atemorizados.
3. Perros y gatos son buenas mascotas.
4. Algunos perros y gatos tienen pedigrí.
5. Algunos gatos blancos con ojos azules son parte siameses.
6. Los osos con crías son peligrosos si se aproximan a ellos.
7. Algunos profesores sin un segundo empleo son felices, pero no prósperos

8. Ningún gato siamés que está bien alimentado es tranquilo o no es amistoso.

9. Ningún Pastor Alemán es bravo a menos que sea maltratado o esté enfermo.

3.2.2. Reglas de inferencia

Instancia Universal (I.U.)

$$\frac{(\forall x\ p(x))}{\therefore\ p(a)}$$

Esta regla nos dice que si sabemos que una cierta propiedad se cumple para todos los elementos del dominio, podemos tener la certeza que la función proposicional instanciada en cualquier elemento del dominio es verdadera

Los gatos son mamíferos y Felix es un gato, por lo tanto Felix es un mamífero.

1)	$(\forall x\ g(x) \Rightarrow m(x))$	
2)	$g(\text{Felix})$	
	$\therefore\ m(\text{Felix})$	
3)	$g(\text{Felix}) \Rightarrow m(\text{Felix})$	I.U. 1
4)	$m(\text{Felix})$	M.P. 2 y 3

Instancia Existencial (I.E.)

$$\frac{(\exists x\ p(x))}{\therefore\ p(a)}$$

En esta regla debemos tener mucho cuidado, porque a simple vista parece que es lo mismo que la instancia universal, pero no es así.

Cuando hacemos una instancia existencial, tenemos que tener en cuenta que estamos instanciando en un valor particular, que no tiene porqué ser el mismo que el de otra instancia existencial, en ningún caso en el que se instanció un $\forall$.

Hay que tener mucho cuidado en las instancias existenciales, ya que se suele cometer el siguiente error.

1)	$(\exists x\ o(x) \wedge n(x))$	
2)	$(\exists x\ g(x) \wedge n(x))$	
	$\therefore\ (\exists x\ o(x) \wedge g(x) \wedge n(x))$	
3)	$o(a) \wedge n(a)$	I.E. 1
4)	$g(a) \wedge n(a)$	I.E. 2 ¡¡¡ERROR!!!

No podemos instanciar en a las dos proposiciones ya que es un valor que existe y no tiene porqué ser el mismo valor en ambos casos. Si pensamos en qué puede modelar este argumento, podría ser: “Hay osos negros y algunos gatos son negros, por lo tanto hay osos que son gatos negros”. Claramente, a pesar de que las premisas son verdaderas, este argumento es falso, ya que la conclusión es falsa.

Es frecuente que al hacer una demostración se instancie dos cuantificadores existenciales en el mismo elemento, pero esto no es correcto, en este caso se debería hacer:

1) $(\exists x\ o(x) \wedge n(x))$
2) $(\exists x\ g(x) \wedge n(x))$

$\therefore\ (\exists x\ o(x) \wedge g(x) \wedge n(x))$

3) $o(a) \wedge n(a)$ — I.E. 1
4) $g(b) \wedge n(b)$ — I.E. 2

Pero esto no nos llevará a concluir lo que se planteaba, ya que esa conclusión es falsa.

Generalización Existencial (G.E.)

$$\frac{p(a)}{\therefore\ (\exists x\ p(x))}$$

En este caso podemos decir que si tenemos un elemento del dominio de discurso para el cual la función proposicional es verdadera, entonces podemos asegurar que existe al menos un elemento para el cual la proposición es verdadera.

1) $(\forall x\ p(x) \Rightarrow a(x))$
2) $(\exists x\ p(x) \wedge q(x))$

$\therefore\ (\exists x\ q(x) \wedge a(x))$

3) $p(b) \wedge q(b)$ — I.E. 2 (b es el valor para el cual se cumple (2))
4) $p(b) \Rightarrow a(b)$ — I.U. 1 (como (1) se cumple $\forall x$, se cumple para b)
5) $p(b)$ — Simp. 3
6) $q(b)$ — Simp. 3
7) $a(b)$ — M.P. 4 y 5
8) $q(b) \wedge a(b)$ — Conj. 6 y 7
9) $(\exists x\ q(x) \wedge a(x))$ — G.E. 8

Generalización Universal (G.U.)

Sea a cualquiera
$\vdots$
$p(a)$

$\therefore\ (\forall x\ p(x))$

El caso de la generalización Universal es sin duda el más complicado, para estar seguros de poder generalizar algo a todos los elementos del dominio, debemos estar seguros que todos los elementos cumplen la propiedad.

Para esto usaremos un marcador, pondremos en alguna parte del argumento un marcador en el que diremos "sea a cualquiera" esto quiere decir que entre este marcador y su descarga si una función proposicional es instanciada en a, debemos estar seguros que esa función proposicional se cumple para todo elemento del dominio. Luego, al hacer la descarga podemos generalizar esta propiedad a todos los elementos del dominio.

1) $(\forall x\ g(x) \Rightarrow m(x))$
2) $(\forall x\ m(x) \Rightarrow l(x))$

$\therefore\ (\forall x\ g(x) \Rightarrow l(x))$

3) Sea a cualquiera
4) $g(a) \Rightarrow m(a)$ — I.U. 1
5) $m(a) \Rightarrow l(a)$ — I.U. 2
6) $g(a) \Rightarrow l(a)$ — S.H. 4 y 5
7) $(\forall x\ g(x) \Rightarrow l(x))$ — G.U. 6

Ejemplos de demostraciones:

1)	$(\forall x\ (f(x) \vee g(x)) \Rightarrow h(x))$	
2)	$(\forall x\ h(x) \Rightarrow (i(x) \wedge s(x)))$	
	$\therefore\ (\forall x\ f(x) \Rightarrow s(x))$	
3)	Sea a cualquiera	
4)	$(f(a) \vee g(a)) \Rightarrow h(a)$	I.U. 1
5)	$h(a) \Rightarrow (i(a) \wedge s(a))$	I.U. 2
6)	Supongamos $f(a)$	Suposición D.C.
7)	$f(a) \vee g(a)$	Ad. 6
8)	$h(a)$	M.P. 4 y 7
9)	$i(a) \wedge s(a)$	M.P. 5 y 8
10)	$s(a)$	Simp. 9
11)	$f(a) \Rightarrow s(a)$	D.C. 6–10
12)	$(\forall x\ f(x) \Rightarrow s(x))$	G.U. 11

1)	$m(r) \wedge c(r)$	
2)	$(\forall x\ c(x) \Rightarrow e(x))$	
	$\therefore\ (\exists x\ m(x) \wedge e(x))$	
3)	$c(r) \Rightarrow e(r)$	I.U. 2 r/x
4)	$c(r)$	Simp. 1
5)	$m(r)$	Simp. 1
6)	$e(r)$	M.P. 3 y 4
7)	$m(r) \wedge e(r)$	Conj. 5 y 6
8)	$(\exists x\ m(x) \wedge e(x))$	G.E. 7

3.2.3. Reglas de Reemplazo

1. **Negación $\forall$ (Neg. $\forall$):** $\neg(\forall x\ p(x)) \iff (\exists x\ \neg p(x))$
2. **Negación $\exists$ (Neg. $\exists$):** $\neg(\exists x\ p(x)) \iff (\forall x\ \neg p(x))$
3. $((\forall x\ p(x)) \wedge (\forall x\ q(x))) \iff (\forall x\ p(x) \wedge q(x))$

1)	$(\forall x\ p(x)) \wedge (\forall x\ q(x))$	Suposición D.C.
2)	$(\forall x\ p(x))$	Simp. 1
3)	$(\forall x\ q(x))$	Simp. 1
4)	Sea x cualquiera	
5)	$p(x)$	I.U. 2
6)	$q(x)$	I.U. 3
7)	$p(x) \wedge q(x)$	Conj. 5 y 6
8)	$(\forall x\ p(x) \wedge q(x))$	G.U. 7
9)	$((\forall x\ p(x)) \wedge (\forall x\ q(x))) \Rightarrow (\forall x\ p(x) \wedge q(x))$	D.C. 1–8
10)	$(\forall x\ p(x) \wedge q(x))$	Suposición D.C.
11)	Sea x cualquiera	
12)	$p(x) \wedge q(x)$	I.U. 10
13)	$p(x)$	Simp. 10
14)	$(\forall x\ p(x))$	G.U.13
15)	Sea x cualquiera	
16)	$p(x) \wedge q(x)$	I.U. 10
17)	$q(x)$	Simp. 16

18)	$(\forall x\ q(x))$	G.U. 17
19)	$(\forall x\ p(x)) \wedge (\forall x\ q(x))$	Conj. 14 y 18
20)	$(\forall x\ p(x) \wedge q(x)) \Rightarrow ((\forall x\ p(x)) \wedge (\forall x\ q(x)))$	D.C. 10–19
21)	$(\forall x\ p(x) \wedge q(x)) \Leftrightarrow ((\forall x\ p(x)) \wedge (\forall x\ q(x)))$	Conj. 9 y 20+Bicon.

4. $((\exists x\ p(x)) \vee (\exists x\ q(x))) \iff (\exists x\ p(x) \vee q(x))$

$$\begin{aligned}
(\exists x\ p(x) \vee q(x)) &\iff \neg\neg(\exists x\ p(x) \vee q(x))\\
&\iff \neg(\forall x\ \neg p(x) \wedge \neg q(x))\\
&\iff \neg((\forall x\ \neg p(x)) \wedge (\forall x\ \neg q(x)))\\
&\iff \neg(\forall x\ \neg p(x)) \vee \neg(\forall x\ \neg q(x)))\\
&\iff (\exists x\ p(x)) \vee (\exists x\ q(x)))
\end{aligned}$$

5. $(Q_x x\ p(x) \wedge (Q_y y\ q(x,y))) \iff (Q_x x (Q_y y\ p(x) \wedge q(x,y)))$ donde: $Q_x, Q_y \in \{\forall, \exists\}$
Haremos la demostración con dos $\forall$ y veremos que al cambiar los cuantificadores no hay gran diferencia:

1)	$(\forall x\ p(x) \wedge (\forall y\ q(x,y)))$	Suposición D.C.
2)	Sea z cualquiera	
3)	$p(z) \wedge (\forall y\ q(z,y))$	I.U. 1
4)	$p(z)$	Simp. 3
5)	$(\forall y\ q(z,y))$	Simp. 3
6)	Sea w cualquiera	
7)	$q(z,w)$	I.U. 5
8)	$p(z) \wedge q(z,w)$	Conj. 4 y 7
9)	$(\forall y\ p(z) \wedge q(z,y))$	G.U. 8
10)	$(\forall x(\forall y\ p(x) \wedge q(x,y)))$	G.U. 9
11)	$(\forall x\ p(x) \wedge (\forall y\ q(x,y))) \Rightarrow (\forall x(\forall y\ p(x) \wedge q(x,y)))$	D.C. 1–10
12)	$(\forall x(\forall y\ p(x) \wedge q(x,y)))$	Suposición D.C.
13)	Sea z cualquiera	
14)	Sea w cualquiera	
15)	$p(z) \wedge q(z,w)$	I.U. 12
16)	$q(z,w)))$	Simp. 15
17)	$(\forall y\ q(z,w))$	G.U. 16
18)	$p(z) \wedge q(z,a)$	I.U. 12
19)	$p(z)$	Simp. 18
20)	$p(z) \wedge (\forall y\ q(z,w))$	Conj. 17 y 19
21)	$(\forall x\ p(z) \wedge (\forall y\ q(z,w)))$	G.U. 20
22)	$(\forall x(\forall y\ p(x) \wedge q(x,y))) \Rightarrow (\forall x\ p(z) \wedge (\forall y\ q(z,w)))$	D.C. 12–21
23)	$(\forall x\ p(x) \wedge (\forall y\ q(x,y))) \Leftrightarrow (\forall x(\forall y\ p(x) \wedge q(x,y)))$	Conj. 11 y 22

6. $(Q_x x\ p(x) \vee (Q_y y\ q(x,y))) \iff (Q_x x(Q_y y\ p(x) \vee q(x,y)))$ donde: $Q_x, Q_y \in \{\forall, \exists\}$

$$(Q_x x\ p(x) \vee (Q_y y\ q(x,y))) \iff \neg\neg(Q_x x\ p(x) \vee (Q_y y\ q(x,y)))$$

Denotamos por $\bar{Q}$ el cuantificador opuesto, es decir $(Q = \forall \Rightarrow \bar{Q} = \exists)$ y $(Q = \exists \Rightarrow \bar{Q} = \forall)$

$$\begin{aligned}
(Q_x x\ p(x) \vee (Q_y y\ q(x,y))) &\iff \neg(\bar{Q}_x x\ \neg p(x) \wedge \neg(Q_y y\ q(x,y))) \\
&\iff \neg(\bar{Q}_x x\ \neg p(x) \wedge (\bar{Q}_y y\ \neg q(x,y))) \\
&\iff \neg(\bar{Q}_x x(\bar{Q}_y y\ \neg p(x) \wedge \neg q(x,y))) \\
&\iff \neg(\bar{Q}_x x \neg(Q_y y\ p(x) \vee q(x,y))) \\
&\iff \neg\neg(Q_x x(Q_y y\ p(x) \vee q(x,y))) \\
&\iff (Q_x x(Q_y y\ p(x) \vee q(x,y)))
\end{aligned}$$

Notar que:

$$\begin{aligned}
((\forall x\ p(x)) \vee (\forall x\ q(x))) &\implies (\forall x\ p(x) \vee q(x)) \\
(\exists x\ p(x) \wedge q(x)) &\implies ((\exists x\ p(x)) \wedge (\exists x\ q(x)))
\end{aligned}$$

Para probar estas tautologías probamos la segunda y a partir de esta deducimos la primera:

1)	$(\exists x\ p(x) \wedge q(x))$	Suposición D.C.
2)	$p(a) \wedge q(a)$	I.E. 1
3)	$p(a)$	Simp. 2
4)	$q(a)$	Simp. 2
5)	$(\exists x\ p(x))$	G.E. 3
6)	$(\exists x\ q(x))$	G.E. 4
7)	$(\exists x\ p(x)) \wedge (\exists x\ q(x))$	Conj. 6 y 6
8)	$(\exists x\ p(x) \wedge q(x)) \Rightarrow (\exists x\ p(x)) \wedge (\exists x\ q(x))$	D.C. 1–7

Para probar la primera. Por lo ya demostrado:

1)	$(\exists x\ \neg p(x) \wedge \neg q(x)) \Rightarrow ((\exists x\ \neg p(x)) \wedge (\exists x\ \neg q(x)))$	Propiedad anterior
2)	$\neg((\exists x\ \neg p(x)) \wedge (\exists x\ \neg q(x))) \Rightarrow \neg(\exists x\ \neg p(x) \wedge \neg q(x))$	Cont. 1
3)	$(\neg(\exists x\ \neg p(x)) \vee \neg(\exists x\ \neg q(x))) \Rightarrow (\forall x\ \neg(\neg p(x) \wedge \neg q(x)))$	L.M.+Neg. 2
4)	$((\forall x\ p(x)) \vee (\forall x\ q(x))) \Rightarrow (\forall x\ p(x) \vee q(x))$	L.M.+Neg. 3

Ejemplos:

1)	$\neg(\forall x\ f(x) \Rightarrow (g(x) \vee h(x)))$	
2)	$(\forall x\ b(x) \Rightarrow g(x))$	
	$\therefore\ \neg(\forall x\ f(x) \Rightarrow b(x))$	
3)	$(\exists x\ f(x) \wedge \neg(g(x) \vee h(x)))$	Neg. 1
4)	$f(a) \wedge \neg(g(a) \vee h(a))$	I.E. 3
5)	$f(a) \wedge \neg g(a) \wedge \neg h(a)$	L.M. 4
6)	$f(a)$	Simp. 5
7)	$\neg g(a)$	Simp. 5
8)	$b(a) \Rightarrow g(a)$	I.U. 2 a/x
9)	$\neg b(a)$	M.T. 7 y 8
10)	$f(a) \wedge \neg b(a)$	Conj. 6 y 9
11)	$(\exists x\ f(x) \wedge \neg b(x))$	G.E. 10
12)	$\neg(\forall x\ f(x) \Rightarrow b(x))$	Neg. 11

1)	$(\forall x\ (f(x) \wedge g(x)) \Rightarrow (h(x) \vee \neg(i(x) \vee j(x))))$	
2)	$\neg(\exists x\ f(x) \wedge \neg g(x))$	
3)	$\neg(\exists x\ h(x) \wedge \neg(i(x) \wedge \neg z(x)))$	
	$\therefore\ \neg(\exists x\ f(x) \wedge \neg(h(x) \Leftrightarrow i(x)))$	
4)	$(\forall x\ f(x) \Rightarrow g(x))$	Neg. 2
5)	$(\forall x\ h(x) \Rightarrow (i(x) \wedge \neg z(x)))$	Neg. 3
6)	Sea a cualquiera	
7)	$(f(a) \wedge g(a)) \Rightarrow (h(a) \vee \neg(i(a) \vee j(a)))$	I.U. 1
8)	$f(a) \Rightarrow g(a)$	I.U. 4
9)	$h(a) \Rightarrow (i(a) \wedge \neg z(a))$	I.U. 5
10)	Supongamos $f(a)$	Suposición D.C.
11)	$g(a)$	M.P. 8 y 10
12)	$f(a) \wedge g(a)$	Conj. 10 y 11
13)	$h(a) \vee \neg(i(a) \vee j(a))$	M.P. 7 y 12
14)	$h(a) \vee (\neg i(a) \wedge \neg j(a))$	L.M. 13
15)	$(h(a) \vee \neg i(a)) \wedge (h(a) \vee \neg j(a))$	Dist. 14
16)	$h(a) \vee \neg i(a)$	Simp. 15
17)	$i(a) \Rightarrow h(a)$	Cond. 16
18)	Supongamos $h(a)$	Suposición D.C.
19)	$i(a) \wedge \neg z(a)$	M.P. 9 y 18
20)	$i(a)$	Simp. 19
21)	$h(a) \Rightarrow i(a)$	D.C. 18–20
22)	$(h(a) \Rightarrow i(a)) \wedge (i(a) \Rightarrow h(a))$	Conj. 17 y 21
23)	$h(a) \Leftrightarrow i(a)$	Bicon. 22
24)	$f(a) \Rightarrow (h(a) \Leftrightarrow i(a))$	D.C. 10–23
25)	$(\forall x\ f(x) \Rightarrow (h(x) \Leftrightarrow i(x))$	G.U. 24

1)	$(\forall x\ f(x) \Rightarrow g(x))$	
2)	$(\forall x\ g(x)) \Rightarrow (\forall x\ h(x))$	
	$\therefore\ (\forall x\ f(x)) \Rightarrow (\forall x\ h(x))$	
3)	Supongamos $(\forall x\ f(x))$	Suposición D.C.
4)	Sea a cualquiera	
5)	$f(a)$	I.U. 3
6)	$f(a) \Rightarrow g(a)$	I.U. 1
7)	$g(a)$	M.P. 5 y 6
8)	$(\forall x\ g(x))$	G.U. 7
9)	$(\forall x\ h(x))$	M.P. 2 y 8
10)	$(\forall x\ f(x)) \Rightarrow (\forall x\ h(x))$	D.C. 3–9

1)	$(\forall x\ f(x)) \vee (\forall x\ \neg g(x))$	
2)	$(\forall x\ f(x) \Rightarrow j(x))$	
3)	$\neg(\exists x\ h(x) \wedge j(x))$	
	$\therefore\ \neg(\forall x\ \neg h(x)) \Rightarrow \neg(\exists x\ g(x))$	
4)	Supongamos $\neg(\forall x\ \neg h(x))$	Suposición D.C.
5)	$(\exists x\ h(x))$	Neg. 4
6)	$h(a)$	I.E. 5
7)	$(\forall x\ h(x) \Rightarrow \neg j(x))$	Neg. 3
8)	$h(a) \Rightarrow \neg j(a)$	I.U. 7
9)	$\neg j(a)$	M.P. 6 y 8
10)	$f(a) \Rightarrow j(a)$	I.U. 2
11)	$\neg f(a)$	M.T. 9 y 10
12)	$(\exists x\ \neg f(x))$	G.E. 11
13)	$\neg(\forall x\ f(x))$	Neg. 12
14)	$(\forall x\ \neg g(x))$	S.D. 1 y 13
15)	$\neg(\exists x\ g(x))$	Neg. 14
16)	$\neg(\forall x\ \neg h(x)) \Rightarrow \neg(\exists x\ g(x))$	D.C. 4–15

3.3. Lógica de predicados relacional

Ya hemos estudiado el modelo de lógica de predicados monádica, pero aún no podemos simbolizar todo lo que queremos. Analicemos el siguiente argumento:

Hay personas a las que no les gustan los animales. Los gatos son animales. Por lo tanto, hay personas a quienes no le gustan los gatos.

Todos estaremos de acuerdo en que el argumento está correcto, sin embargo no podemos simbolizarlo con lógica monádica. Si trabajamos con lógica monádica el argumento queda como:

$p(x)$: x es persona
$l(x)$: a x le gustan los animales
$q(x)$: a x le gustan los gatos
$a(x)$: x es un animal
$g(x)$: x es un gato

$(\exists x\ p(x) \wedge \neg l(x))$
$(\forall x\ g(x) \Rightarrow a(x))$
$\therefore\ (\exists x\ p(x) \wedge \neg q(x))$

Claramente no podremos demostrar este argumento, entonces necesitamos usamos la lógica relacional.

En el caso de lógica relacional los predicados involucran al menos dos elementos del dominio de discurso. Algunos ejemplos de predicados son:

- $a(x, y)$: x es más alto que y.

- $l(x, y)$: x ama a y.
- $h(x, y)$: x es hermano de y.
- $p(x, y)$: x es el padre de y.
- $e(x, y, z)$: x está entre y y z.
- $t(x, y, z)$: x habló con y acerca de z.
- $i(x, y, z)$: x presentó a y con z.
- $f(x, y, z, w)$: x está más lejos de y que z de w.

3.3.1. Simbolización

La primera forma de simbolizar es reemplazar las variables con nombres y obtenemos una proposición singular.

Ejemplos:

- $a(\text{Pedro}, \text{Juan})$: Pedro es más alto que Juan.
- $l(\text{Juan}, \text{María})$: Juan ama a María.
- $h(\text{Juan}, \text{Diego})$: Juan es hermano de Diego.
- $p(\text{Diego}, \text{Pedro})$: Diego es el padre de Pedro.
- $e(\text{Pedro}, \text{Juan}, \text{Diego})$: Pedro está entre Juan y Diego.
- $t(\text{Pedro}, \text{Juan}, \text{Diego})$: Pedro habló con Juan acerca de Diego.
- $i(\text{Pedro}, \text{Juan}, \text{Diego})$: Pedro presentó a Juan con Diego.
- $f(\text{Concepción}, \text{Arica}, \text{Santiago}, \text{Antofagasta})$: Concepción está más lejos de Arica que Santiago de Antofagasta.

La segunda forma es cuantificar una de las variables.

Ejemplo:

- $(\exists x\ l(x, \text{Juan}))$: alguien ama a Juan.
- $(\exists x\ l(\text{Juan}, x))$: Juan ama a alguien.
- $(\forall x\ l(x, \text{Juan}))$: Todos aman a Juan.
- $(\forall x\ l(\text{Juan}, x))$: Juan ama a todos.
- $\neg(\exists x\ l(x, \text{Juan}))$: Nadie ama a Juan.

- $\neg(\exists x\ l(\text{Juan}, x))$: Juan no ama a alguien.
- $\neg(\forall x\ l(x, \text{Juan}))$: No todos aman a Juan.
- $\neg(\forall x\ l(\text{Juan}, x))$: Juan no ama a todos.

Ahora si cuantificamos las dos variable tendremos seis posibles combinaciones, ya que el orden en el que se usan los cuantificadores es muy importante, además debemos considerar las negaciones:

- $(\forall x(\forall y\ l(x, y)))$: Todos aman a todos.
- $(\forall x(\exists y\ l(x, y)))$: Todos aman a alguien.
- $(\exists x(\forall y\ l(x, y)))$: Hay alguien que ama a todos.
- $(\exists x(\exists y\ l(x, y)))$: Alguien ama a alguien.
- $(\forall y(\exists x\ l(x, y)))$: Todos tienen alguien que los ama.
- $(\exists y(\forall x\ l(x, y)))$: Alguien es amado por todos.
- $\neg(\forall x(\forall y\ l(x, y)))$: No todos aman a todos.
- $\neg(\forall x(\exists y\ l(x, y)))$: No todos aman a alguien.
- $\neg(\exists x(\forall y\ l(x, y)))$: Ninguno ama a todos.
- $\neg(\exists x(\exists y\ l(x, y)))$: Ninguno ama a alguien.
- $\neg(\forall y(\exists x\ l(x, y)))$: No todos tienen alguien que los ama.
- $\neg(\exists y(\forall x\ l(x, y)))$: Ninguno es amado por todos.

Notemos que no hemos considerado $(\exists y\ (\exists x\ r(x, y)))$ ni $(\forall y\ (\forall x\ r(x, y)))$, esto no ha sido un error, ni un olvido, en realidad no las hemos considerado porque ya tienen una expresión equivalente:

$$\begin{aligned} (\exists y\ (\exists x\ r(x, y))) &\iff ((\exists x\ (\exists y\ r(x, y)))) \\ (\forall y\ (\forall x\ r(x, y))) &\iff ((\forall x\ (\forall y\ r(x, y)))) \end{aligned}$$

Demostremos estas propiedades:

1)	Supongamos $(\exists y\ (\exists x\ r(x, y)))$	Suposición D.C.
2)	$(\exists x\ r(x, b))$	I.E. 1
3)	$r(a, b)$	I.E. 2
4)	$(\exists y\ r(a, y))$	G.E. 3
5)	$(\exists x\ (\exists y\ r(x, y)))$	G.E. 4
6)	$(\exists y\ (\exists x\ r(x, y))) \Rightarrow (\exists x\ (\exists y\ r(x, y)))$	D.C. 1–5

7)	Supongamos $(\exists x\ (\exists y\ r(x,y)))$	Suposición D.C.
8)	$(\exists y\ r(a,y))$	I.E. 7
9)	$r(a,b)$	I.E. 8
10)	$(\exists x\ r(x,b))$	G.E. 9
11)	$(\exists y\ (\exists x\ r(x,y)))$	G.E. 10
12)	$(\exists x\ (\exists y\ r(x,y))) \Rightarrow (\exists y\ (\exists x\ r(x,y)))$	D.C. 7–11
13)	$(\exists y\ (\exists x\ r(x,y))) \Leftrightarrow (\exists x\ (\exists y\ r(x,y)))$	Bicon. 6 y 12

$$\begin{aligned}(\forall y\ (\forall x\ r(x,y))) &\iff \neg\neg(\forall y\ (\forall x\ r(x,y))) \iff \neg(\exists y\ \neg(\forall x\ r(x,y)))\\ &\iff \neg(\exists y\ (\exists x\ \neg r(x,y)))\end{aligned}$$

Por la propiedad anterior

$$\begin{aligned}(\forall y\ (\forall x\ r(x,y))) &\iff \neg(\exists x\ (\exists y\ \neg r(x,y))) \iff \neg(\exists x\ \neg(\forall y\ r(x,y)))\\ &\iff (\forall x\ (\forall y\ r(x,y)))\end{aligned}$$

Por último tendremos proposiciones categóricas donde las variables pueden ser reemplazadas por todos o algunos elementos de un subconjunto del dominio de discurso. En estos casos lo importante es ir instanciando paso a paso y de esa manera no entrar en confusiones.

En todos los casos debemos considerar que podemos tener relación con algunos elementos de una clase o con todos los elementos de una clase, en cada caso usaremos las reglas de las proposiciones categóricas para realizar la simbolización.

Ejemplos:

1. Algunos perros usan un collar.

   $p(x)$: x es un perro. $u(x,y)$: x usa y $c(x)$: x es un collar

   $(\exists x\ x$ es un perro $\wedge\ x$ usa un collar$)$

   $(\exists x\ p(x) \wedge (\exists y\ y$ es un collar $\wedge\ x$ usa $y)$

   $(\exists x\ p(x) \wedge (\exists y\ c(y) \wedge u(x,y)))$

2. A los amigos de Germán les gusta la cerveza.

   $a(x,y)$: x es amigo de y. $l(x,y)$: a x le gusta y. $c(x)$: x es cerveza

   $(\forall x\ x$ es amigo de Germán $\Rightarrow$ a x le gusta la cerveza$)$

   a x le gusta la cerveza : $(\forall y\ c(y) \Rightarrow l(x,y))$

   $(\forall x\ a(x, \text{Germán}) \Rightarrow (\forall y\ c(y) \Rightarrow l(x,y)))$

3. Algunos perros con dueños que no los alimentan cazan ratones

   $p(x)$: x es una persona. $d(x)$: x es un perro. $r(x)$: x es un ratón.
   $d(x,y)$: x es dueño de y $c(x,y)$: x caza a y $a(x,y)$: x alimenta a y

   $(\exists x\ x$ es un perro con un dueño que no lo alimenta $\wedge\ x$ caza ratones

   $(\exists x\ x$ es un perro $\wedge\ x$ tiene un dueño que no lo alimenta $\wedge (\exists y\ r(y) \wedge c(x,y)))$

   $(\exists x\ p(x) \wedge (\exists y\ y$ es dueño de x y no lo alimenta$) \wedge (\exists y\ r(y) \wedge c(x,y)))$

   $(\exists x\ p(x) \wedge (\exists y\ y$ es dueño de $x \wedge y$ no alimenta a $x) \wedge (\exists y\ r(y) \wedge c(x,y)))$

   $(\exists x\ p(x) \wedge (\exists y\ d(y,x) \wedge \neg a(y,x)) \wedge (\exists y\ r(y) \wedge c(x,y)))$

4. Algunos profesores con estudiantes brillantes no ponen malas notas.
   $p(x)$: x es profesor $\quad e(x)$: x es estudiante $\quad b(x)$: x es brillante
   $m(x)$: x es mala nota $\quad d(x,y)$: x pone y $\quad t(x,y)$: x enseña a y

   ($\exists x$ x es un profesor $\wedge$ x enseña a estudiantes brillantes $\wedge$ x no pone malas notas)
   ($\exists x$ $p(x) \wedge (\exists y$ y es un estudiante $\wedge$ y es brillante $\wedge$ x enseña a $y) \wedge x$ no pone malas notas)
   ($\exists x$ $p(x) \wedge (\exists y$ $e(y) \wedge b(y) \wedge t(x,y)) \wedge \neg(\exists y$ y es mala nota $\wedge$ x pone y))
   $(\exists x\ p(x) \wedge (\exists y\ e(y) \wedge b(y) \wedge t(x,y)) \wedge \neg(\exists y\ m(y) \wedge d(x,y)))$

5. Los estudiantes brillantes con buenas notas obtienen una beca.
   $e(x)$: x es estudiante $\quad b(x)$: x es brillante $\quad g(x)$: x tiene buenas notas
   $s(x)$: x es una beca $\quad o(x,y)$: x obtiene y

   ($\forall x$ x es un estudiante brillante con buenas notas $\Rightarrow$ x obtiene una beca)
   ($\forall x$ (x es un estudiante $\wedge$ x es brillante $\wedge$ x tiene buenas notas) $\Rightarrow$ x obtiene una beca)
   ($\forall x$ $(e(x) \wedge b(x) \wedge g(x)) \Rightarrow (\exists y$ y es una beca $\wedge$ x obtiene y))
   $(\forall x\ (e(x) \wedge b(x) \wedge g(x)) \Rightarrow (\exists y\ s(y) \wedge o(x,y)))$

6. Ningún estudiante que no obtiene buenas notas, obtiene una beca o se gradúa con honores.
   $e(x)$: x es estudiante $\quad g(x)$: x tiene buenas notas $\quad h(x)$: x se gradúa con honores
   $s(x)$: x es una beca $\quad o(x,y)$: x obtiene y

   $\neg$($\exists x$ x es un estudiante que no tiene buenas notas $\wedge$ x obtiene una beca o se gradúa con honores)
   $\neg$($\exists x$ x es un estudiante $\wedge$ x no tiene buenas notas $\wedge$ x obtiene una beca o se gradúa con honores)
   $\neg$($\exists x$ $e(x) \wedge \neg g(x) \wedge$ (x obtiene una beca $\vee$ x se gradúa con honores))
   $\neg(\exists x\ e(x) \wedge \neg g(x) \wedge ((\exists y\ s(y) \wedge o(x,y)) \vee h(x)))$

7. Los estudiantes que leen libros disfrutan algunos de sus cursos y aprenden algo.
   $e(x)$: x es estudiante $\quad l(x)$: x es un libro $\quad c(x)$: x es un curso
   $a(x,y)$: x aprende y $\quad r(x,y)$: x lee y $\quad d(x,y)$: x disfruta y
   $t(x,y)$: x toma y

   ($\forall x$ x es un estudiante que lee libros $\Rightarrow$ x disfruta algunos de sus cursos y aprende algo)
   ($\forall x$ (x es un estudiante $\wedge$ x lee libros) $\Rightarrow$ (x disfruta algunos de sus cursos $\wedge$ x aprende algo))
   ($\forall x$ $(e(x) \wedge (\exists y$ y es un libro $\wedge$ x lee $y)) \Rightarrow ((\exists y$ y es un curso que toma $x \wedge x$ disfruta $y) \wedge (\exists y$ x aprende y)))
   $(\forall x\ (e(x) \wedge (\exists y\ l(y) \wedge r(x,y))) \Rightarrow ((\exists y\ c(y) \wedge t(x,y) \wedge d(x,y)) \wedge (\exists y\ a(x,y))))$

8. No todos los estudiantes disfrutan todos sus cursos
   $e(x)$: x es estudiante $\quad c(x)$: x es un curso $\quad d(x,y)$: x disfruta y
   $t(x,y)$: x toma y

   $\neg$todos los estudiantes disfrutan todos sus cursos
   $\neg$($\forall x$ x es un estudiante $\Rightarrow$ x disfruta todos sus cursos)
   $\neg$($\forall x$ $e(x) \Rightarrow (\forall y$ y es un curso que x toma $\Rightarrow$ x disfruta y))
   $\neg$($\forall x$ $e(x) \Rightarrow (\forall y$ [y es un curso $\wedge$ x toma y] $\Rightarrow d(x,y)))$
   $\neg(\forall x\ e(x) \Rightarrow (\forall y\ [c(y) \wedge t(x,y)] \Rightarrow d(x,y)))$

9. Ningún estudiante a quien no le agrada ninguno de sus profesores le gusta alguno de sus cursos.

$e(x)$: x es estudiante	$p(x)$: x es profesor	$c(x)$: x es un curso
$l(x,y)$: a x le agrada/gusta y	$t(x,y)$: x toma y	$s(x,y)$: x enseña a y

$\neg(\exists x$ x es un estudiante a quien no le agrada ninguno de sus profesores $\wedge$ x le gusta alguno de sus cursos)

$\neg(\exists x$ (x es un estudiante $\wedge$ a x no le agrada ninguno de sus profesores) $\wedge$ ($\exists y$ y es un curso que x toma $\wedge$ a x le agra

$\neg(\exists x\ (e(x) \wedge \neg(\exists y$ y es profesor de x $\wedge$ a x le agrada $y)) \wedge (\exists y\ c(y) \wedge t(x,y) \wedge l(x,y)))$

$\neg(\exists x\ (e(x) \wedge \neg(\exists y\ p(y) \wedge s(y,x) \wedge l(x,y)) \wedge (\exists y\ c(y) \wedge t(x,y) \wedge l(x,y)))$

En todos los casos descritos anteriormente, la idea es ir cuantificando, instanciando o categorizando las variables de una en una. En la Tabla 3.9 vemos un resumen utilizando las funciones proposicionales $r(x,y)$: x se relaciona con y, $s(x)$: x está en S y $t(x)$: x está en T.

3.3.2. Demostraciones

Para hacer las demostraciones con lógica de predicados relacional, no necesitamos más reglas de inferencia, las que ya conocemos nos entregan todas las herramientas para trabajar con estas reglas.

Veamos algunos ejemplos:

1.

1)	$(\exists x\ p(x) \wedge (\forall y\ d(y) \Rightarrow \neg l(x,y)))$	
2)	$(\forall x\ u(x) \Rightarrow d(x))$	
	$\therefore\ (\exists x\ p(x) \wedge (\forall y\ u(y) \Rightarrow \neg l(x,y)))$	
3)	$p(a) \wedge (\forall y\ d(y) \Rightarrow \neg l(a,y))$	I.E. 1 a/x
4)	$p(a)$	Simp. 3
5)	$(\forall y\ d(y) \Rightarrow \neg l(a,y))$	Simp. 3
6)	Sea z cualquiera	
7)	$d(z) \Rightarrow \neg l(a,z)$	I.U. 5 z/y
8)	$u(z) \Rightarrow d(z)$	I.U. 2 z/x
9)	$u(z) \Rightarrow \neg l(a,z)$	S.H. 7 y 8
10)	$(\forall y\ u(y) \Rightarrow \neg l(a,y))$	G.U. 9
11)	$p(a) \wedge (\forall y\ u(y) \Rightarrow \neg l(a,y))$	Conj. 4 y 10
12)	$(\exists x\ p(x) \wedge (\forall y\ u(y) \Rightarrow \neg l(x,y)))$	G.E. 11

2.

1)	$(\forall x\ p(x) \Rightarrow (\exists y\ f(y,x)))$	
2)	$(\forall x\ (\forall y\ f(y,x) \Rightarrow l(y,x)))$	
	$\therefore\ (\forall x\ p(x) \Rightarrow (\exists y\ l(y,x)))$	
3)	Sea z cualquiera	
4)	$p(z) \Rightarrow (\exists y\ f(y,z))$	I.U. 1 z/x
5)	Supongamos $p(z)$	Suposición D.C.
6)	$(\exists y\ f(y,z))$	M.P. 4 y 5
7)	$f(a,z)$	I.E. 6 a/y
8)	$(\forall y\ f(y,z) \Rightarrow l(y,z))$	I.U. 2 z/x
9)	$f(a,z) \Rightarrow l(a,z)$	I.U. 8 a/y
10)	$l(a,z)$	M.P. 7 y 9
11)	$(\exists y\ l(y,z))$	G.E. 10
12)	$p(z) \Rightarrow (\exists y\ l(y,z))$	D.C. 5–11
13)	$(\forall x\ p(x) \Rightarrow (\exists y\ l(y,x)))$	G.U. 12

Tabla 3.9: Del lenguaje natural a la lógica de predicados en proposiciones con varias variables

Lenguaje natural	**Fórmulas**
a se relaciona con b	$r(a,b)$
a no se relaciona con b	$\neg r(a,b)$
Algo se relaciona con a	$(\exists x\ r(x,a))$
a se relaciona con algo	$(\exists x\ r(a,x))$
Todo se relaciona con a	$(\forall x\ r(x,a))$
a se relaciona con todo	$(\forall x\ r(a,x))$
Nada se relaciona con a	$\neg(\exists x\ r(x,a))$
a no se relaciona con algo	$\neg(\exists x\ r(a,x))$
No todo se relaciona con a	$\neg(\forall x\ r(x,a))$
a no se relaciona con todo	$\neg(\forall x\ r(a,x))$
Algo se relaciona con algo	$(\exists x \exists y\ r(x,y))$
Algo se relaciona con todo	$(\exists x \forall y\ r(x,y))$
Todo se relaciona con algo	$(\forall x \exists y\ r(x,y))$
Todo se relaciona con todo	$(\forall x \forall y\ r(x,y))$
Todo tiene algo que se relaciona con él	$(\forall y \exists x\ r(x,y))$
Hay algo con lo que todo se relaciona	$(\exists y \forall x\ r(x,y))$
Nada se relaciona con algo	$\neg(\exists x \exists y\ r(x,y))$
Nada se relaciona con todo	$\neg(\exists x \forall y\ r(x,y))$
No todo se relaciona con algo	$\neg(\forall x \exists y\ r(x,y))$
No todo se relaciona con todo	$\neg(\forall x \forall y\ r(x,y))$
No todo tiene algo que se relaciona con él	$\neg(\forall y \exists x\ r(x,y))$
No hay algo con lo que todo se relaciona	$\neg(\exists y \forall x\ r(x,y))$
Algunos S se relacionan con algunos T	$(\exists x\ s(x) \wedge (\exists y\ t(y) \wedge r(x,y)))$ $(\exists x\ (\exists y\ s(x) \wedge t(y) \wedge r(x,y)))$
Algunos S se relacionan con todos los T	$(\exists x\ s(x) \wedge (\forall y\ t(y) \Rightarrow r(x,y)))$
Todos los S se relacionan con algunos T	$(\forall x\ s(x) \Rightarrow (\exists y\ t(y) \wedge r(x,y)))$
Todos los S se relacionan con todos los T	$(\forall x\ s(x) \Rightarrow (\forall y\ t(y) \Rightarrow r(x,y)))$ $(\forall x\ (\forall y\ (s(x) \wedge t(y)) \Rightarrow r(x,y)))$
Hay elementos de T tal que todos los S se relacionan con ellos	$(\exists y\ t(y) \wedge (\forall x\ s(x) \Rightarrow r(x,y)))$
Todos los T tienen algún S que se relaciona con ellos	$(\forall y\ t(y) \Rightarrow (\exists x\ s(x) \wedge r(x,y)))$
Ningún S se relaciona con algún T	$\neg(\exists x\ s(x) \wedge (\exists y\ t(y) \wedge r(x,y)))$ $\neg(\exists x\ (\exists y\ s(x) \wedge t(y) \wedge r(x,y)))$
Ningún S se relaciona con todos los T	$\neg(\exists x\ s(x) \wedge (\forall y\ t(y) \Rightarrow r(x,y)))$
No todos los S se relacionan con algún T	$\neg(\forall x\ s(x) \Rightarrow (\exists y\ t(y) \wedge r(x,y)))$
No todos los S se relacionan con todos los T	$\neg(\forall x\ s(x) \Rightarrow (\forall y\ t(y) \Rightarrow r(x,y)))$ $\neg(\forall x\ (\forall y\ (s(x) \wedge t(y)) \Rightarrow r(x,y)))$
No hay elementos de T tal que todos los S se relacionan con ellos	$\neg(\exists y\ t(y) \wedge (\forall x\ s(x) \Rightarrow r(x,y)))$
No todos los T tienen algún S que se relaciona con ellos	$\neg(\forall y\ t(y) \Rightarrow (\exists x\ s(x) \wedge r(x,y)))$

3.

1)	$(\forall x\ [f(x) \wedge \neg g(x)] \Rightarrow \neg(\exists y\ t(y,x) \wedge h(x,y)))$	
2)	$\neg(\exists x\ f(x) \wedge g(x))$	
3)	$(\forall x\ (\forall y\ h(x,y) \Rightarrow z(x,y)) \Rightarrow g(x))$	
	$\therefore\ (\forall x\ f(x) \Rightarrow (\exists y\ \neg[t(y,x) \vee z(x,y)]))$	
4)	$(\forall x\ f(x) \Rightarrow \neg g(x))$	Neg. 2
5)	Sea w cualquiera	
6)	$[f(w) \wedge \neg g(w)] \Rightarrow \neg(\exists y\ t(y,w) \wedge h(w,y))$	I.U. 1 w/x
7)	$f(w) \Rightarrow \neg g(w)$	I.U. 4 w/x
8)	$(\forall y\ h(w,y) \Rightarrow z(w,y)) \Rightarrow g(w)$	I.U. 3 w/x
9)	Supongamos $f(w)$	Suposición D.C.
10)	$\neg g(w)$	M.P. 7 y 9
11)	$f(w) \wedge \neg g(w)$	Conj. 9 y 10
12)	$\neg(\exists y\ t(y,w) \wedge h(w,y))$	M.P. 6 y 11
13)	$\neg(\forall y\ h(w,y) \Rightarrow z(w,y))$	M.T. 8 y 10
14)	$(\exists y\ h(w,y) \wedge \neg z(w,y))$	Neg. 13
15)	$h(w,a) \wedge \neg z(w,a)$	I.E. 14 a/y
16)	$(\forall y\ t(y,w) \Rightarrow \neg h(w,y))$	Neg. 12
17)	$t(a,w) \Rightarrow \neg h(w,a)$	I.U. 16 a/y
18)	$h(w,a)$	Simp. 15
19)	$\neg z(w,a)$	Simp. 15
20)	$\neg t(a,w)$	M.T. 17 y 18
21)	$\neg t(a,w) \wedge \neg z(w,a)$	Conj. 19 y 20
22)	$\neg(t(a,w) \vee z(w,a))$	Neg. 21
23)	$(\exists y\ \neg(t(y,w) \vee z(w,y)))$	G.E. 22
24)	$f(w) \Rightarrow (\exists y\ \neg(t(y,w) \vee z(w,y)))$	D.C. 9–23
25)	$(\forall x\ f(x) \Rightarrow (\exists y\ \neg(t(y,x) \vee z(x,y))))$	G.U. 24

4.

1)	$(\exists x\ (\forall y\ f(x,y)))$	
	$\therefore\ (\forall y\ (\exists x\ f(x,y)))$	
2)	$(\forall y\ f(a,y))$	I.E. 1 a/x
3)	Sea z cualquiera	
4)	$f(a,z)$	I.U. 2 z/y
5)	$(\exists x\ f(x,z))$	G.E. 4
6)	$(\forall y\ (\exists x\ f(x,z)))$	G.U. 5

5. Probemos que $(\forall x\ (\forall y\ f(x,y))) \Rightarrow (\forall x\ (\exists y\ f(x,y)))$

1)	Supongamos $(\forall x\ (\forall y\ f(x,y)))$	Suposición D.C.
2)	Sea w cualquiera	
3)	$(\forall y\ f(w,y))$	I.U. 1 w/x
4)	$f(w,a)$	I.U. 3 a/y
5)	$(\exists y\ f(w,y))$	G.E. 4
6)	$(\forall x\ (\exists y\ f(x,y)))$	G.U. 5
7)	$(\forall x\ (\forall y\ f(x,y))) \Rightarrow (\forall x\ (\exists y\ f(x,y)))$	D.C. 1–6

6. Probemos que $(\forall x\ (\exists y\ f(x,y)) \Rightarrow (\exists z\ f(x,z)))$

1)	Sea w cualquiera	
2)	Supongamos $(\exists y\ f(w,y))$	Suposición D.C.
3)	$f(w,a)$	I.E. 2 a/y
4)	$(\exists z\ f(w,z))$	G.E. 3
5)	$(\exists y\ f(w,y)) \Rightarrow (\exists z\ f(w,z))$	D.C. 2–4
6)	$(\forall x\ (\exists y\ f(x,y)) \Rightarrow (\exists z\ f(x,z)))$	G.U. 5

3.4. Lógica de predicados con relaciones de igualdad

Por último, estudiamos el caso cuando el sujeto no es una categoría del dominio de discurso, si no que ciertos individuos especificados a través de predicados, también estudiaremos casos cuando un número específico de elementos cumple una cierta propiedad. En estos casos debemos usar las relaciones igualdad. La igualdad es una relación que conocemos bien y nos parce totalmente natural, por lo tanto las reglas de inferencia nuevas que tendremos aquí nos parecerán bastante obvias.

3.4.1. Simbolización

Lo primero que estudiamos son los casos donde identificamos dos elementos del dominio de discurso como uno sólo, para esto utilizamos un predicado conocido que es la igualdad. POr ejemplo:

1. Superman es Clark Kent (Superman = Clark Kent)
2. Buffalo Bill fue William Cody (Buffalo Bill = William Cody)

O podríamos tener formas negadas.

1. El Congreso no es la Casa de Gobierno (Congreso $\neq$ Casa de Gobierno)
2. Peter Parker no es Ironman (Peter Parker $\neq$ Ironman)

Un segundo tipo de proposiciones lógicas que debemos considerar son las las excepciones y las expresiones del tipo "solo a cumple p". Por ejemplo:

- Todos vinieron a la fiesta excepto Juan.
  $f(x)$: x vino a la fiesta.
  $$\neg f(\text{Juan}) \wedge (\forall x x \neq \text{Juan} \Rightarrow f(x))$$
- Todos están enfermos excepto Pedro y Juan.
  $e(x)$: x está enfermo.
  $$\neg e(\text{Pedro} \wedge \neg e(\text{Juan})) \wedge (\forall x\ (x \neq \text{Juan} \wedge x \neq \text{Pedro}) \Rightarrow e(x))$$
- Todos los perros excepto Cachupin saben nadar.
  $p(x) x$ es perro, $n(x)$: x sabe nadar.
  $$\neg n(\text{Cachupin}) \wedge (\forall x\ (p(x) \wedge x \neq \text{Cachupin}) \Rightarrow n(x))$$

- No sé si Diego está enfermo, pero todos los demás lo están.

$$(\forall x\ x \neq \text{Diego} \Rightarrow e(x))$$

- Nadie está enfermo excepto Juan
- Solo Juan está enfermo

$$(\forall x\ x \neq \text{Juan} \Rightarrow \neg e(x)) \wedge e(\text{Juan})$$

- Ningún perro excepto Cachupin come ratones.
- Cachupin es el único perro que come ratones.

$$(\forall x\ (p(x) \wedge x \neq \text{Cachupin}) \Rightarrow \neg c(x)) \wedge c(\text{Cachupin})$$

Otra posibilidad es decir que un número determinado de elementos del dominio cumple una cierta propiedad. Aquí podemos distinguir 3 casos:

1. Cuando decimos que hay al menos n elementos que cumplen la propiedad. Ejemplo:

   a) Hay al menos dos enfermos.

   $$(\exists x\ (\exists y\ e(x) \wedge e(y) \wedge x \neq y))$$

   b) Hay al menos un gato que maulla.

   $$(\exists x\ g(x) \wedge m(x))$$

   c) Hay al menos dos perros que comen ratones.

   $$(\exists x\ (\exists y\ p(x) \wedge p(y) \wedge c(x) \wedge c(y) \wedge x \neq y))$$

   d) Hay al menos tres enfermos.

   $$(\exists x\ (\exists y\ (\exists z\ e(x) \wedge e(y) \wedge e(z) \wedge x \neq y \wedge x \neq z \wedge y \neq z)))$$

2. Cuando hay a lo más n elementos que cumplen la propiedad. Ejemplo:

   a) Hay a lo más un enfermo.

   $$(\forall x\ (\forall y\ (e(x) \wedge e(y)) \Rightarrow x = y))$$

   b) A lo más una gato maulla.

   $$(\forall x\ (\forall y\ (g(x) \wedge m(x) \wedge g(y) \wedge m(y)) \Rightarrow x = y))$$

c) Hay a lo más dos perros que comen ratones.

$$(\forall x\ (\forall y\ (\forall z\ (p(x) \wedge c(x) \wedge p(y) \wedge c(y) \wedge p(z) \wedge c(z)) \Rightarrow (x = y \vee x = z \vee y = z))))$$

3. Cuando hay exactamente n elementos que cumplen la propiedad. Este caso podemos verlo como la conjunción de los dos anteriores, pero también podemos usar una expresión equivalente que es la que estudiaremos a continuación. Ejemplo:

   a) María tiene un único hijo. ($h(x)$: x es hijo de María)

   $$(\exists! x\ h(x))$$

   La expresión anterior es correcta, pero no podemos trabajar directamente con eso en una demostración, ya que no sabemos que hacer con "!". Una expresión útil es:

   $$(\exists x\ h(x) \wedge (\forall y\ h(y) \Rightarrow x = y))$$

   b) Hay exactamente dos perros que comen ratones.

   $$(\exists x\ (\exists y\ p(x) \wedge c(x) \wedge p(y) \wedge c(y) \wedge x \neq y \wedge (\forall z\ (p(z) \wedge c(z)) \Rightarrow (z = x \vee z = y))))$$

Por último tenemos el caso cuando un elemento determinado del dominio cumple una propiedad, pero para describir ese elemento no usamos su nombre propio si no que una descripción inequívoca del mismo. Por ejemplo:

1. El esposo de Lili tiene el pelo negro. ($e(x)$: x es el esposo de Lili, $n(x)$: x tiene el pelo negro.)

   $$(\exists x\ e(x) \wedge (\forall y\ e(y) \Rightarrow x = y) \wedge n(x))$$

La Tabla 3.12 muestra un resumen de la simbolización con relaciones de igualdad.

3.4.2. Reglas de inferencia

- **Reflexividad (Refl.)** $(\forall x\ x = x)$.
- **Simetría (Sim.)** $(\forall x\ (\forall y\ (x = y) \Leftrightarrow (y = x)))$
- **Transitividad (Tran.)** $(\forall x\ (\forall y\ (\forall z\ ((x = y) \wedge (y = z)) \Rightarrow (x = z))))$
- **Negación de =.** $(\forall x\ (\forall y\ \neg(x = y) \Leftrightarrow (x \neq y)))$
- **Sustitución (Sust.)** $\begin{array}{l} a = b \\ p(b) \\ \hline \therefore\ p(a) \end{array}$

Ejemplos:

Tabla 3.12: Del lenguaje natural a la lógica de predicados en proposiciones con igualdad

Lenguaje natural	**Fórmulas**
a es igual a b a es lo mismo que b a es b	$a = b$
a no es igual a b a no es lo mismo que b a no es b	$a \neq b$
Solo a está en P	$p(a) \land (\forall x\ x \neq a \Rightarrow \neg p(x))$
Solo $a_1, \ldots, a_n$ está en P	$\bigwedge_{i=1}^{n} p(a_i) \land (\forall x\ \bigwedge_{i=1}^{n} x \neq a_i \Rightarrow \neg p(x))$
Todos excepto a están en P	$\neg p(a) \land (\forall x\ x \neq a \Rightarrow p(x))$
a es el mejor en P	$p(a) \land (\forall x\ (p(x) \land x \neq a) \Rightarrow r(a, x))$
Hay al menos n elementos en P	$(\exists x_1 \ldots \exists x_n\ \bigwedge_{i=1}^{n} p(x_i) \land \bigwedge_{i \neq j} x_i \neq x_j)$
Hay a lo más n elementos en P	$(\forall x_1 \ldots \forall x_n \forall x_{n+1}\ \bigwedge_{i=1}^{n+1} p(x_i) \Rightarrow \bigvee_{i \neq j} x_i = x_j)$
Hay exactamente n elementos en P	$\left(\exists x_1 \ldots \exists x_n\ \bigwedge_{i=1}^{n} p(x_i) \land \bigwedge_{i \neq j} x_i \neq x_j \land (\forall y\ p(y) \Rightarrow \bigvee_{i=1}^{n} y = x_i)\right)$
El elemento que cumple S está en P	$(\exists x\ s(x) \land (\forall y\ s(y) \Rightarrow x = y) \land p(x))$

1.

1)	$\phi(a)$	
2)	$\neg\phi(b)$	
	$\therefore\ a \neq b$	
3)	Supongamos $a = b$	Suposición R.A.
4)	$\phi(b)$	Sust. 1 y 3
5)	$\phi(b) \land \neg\phi(b)$	Conj. 2 y 4 $\rightarrow\leftarrow$
6)	$a \neq b$	R.A. 3–5

2.

1)	$(\exists x\ m(x) \land s(x) \land (\forall y\ (m(y) \land s(y)) \Rightarrow x = y) \land d(x))$	
2)	$(\exists x\ m(x) \land s(x) \land (\forall y\ (m(y) \land s(y)) \Rightarrow x = y) \land k(j, x))$	
	$\therefore\ (\exists x\ d(x) \land k(j, x))$	
3)	$m(a) \land s(a) \land (\forall y\ (m(y) \land s(y)) \Rightarrow a = y) \land d(a)$	I.E. 1 a/x
4)	$m(a) \land s(a)$	Simp. 3
5)	$(\forall y\ (m(y) \land s(y)) \Rightarrow a = y)$	Simp. 3
6)	$d(a)$	Simp. 3
7)	$m(b) \land s(b) \land (\forall y\ (m(y) \land s(y)) \Rightarrow b = y) \land k(j, b)$	I.E. 2 b/x
8)	$m(b) \land s(b)$	Simp. 7
9)	$(m(b) \land s(b)) \Rightarrow a = b$	I.U. 5
10)	$a = b$	M.P. 8 y 9
11)	$k(j, b)$	Simp. 7
12)	$k(j, a)$	Sust. 10 y 11
13)	$d(a) \land k(j, a)$	Conj. 6 y 12
14)	$(\exists x\ d(x) \land k(j, x))$	G.E. 13

3.

1)	$(\forall x\ a(x) \Rightarrow b(x))$	
2)	$(\forall x\ b(x) \Rightarrow c(x))$	
3)	$(\forall x\ (\forall y\ (\forall z\ (c(x) \wedge c(y) \wedge c(z)) \Rightarrow (x = y \vee x = z \vee y = z))))$	
4)	$(\exists x\ (\exists y\ a(x) \wedge a(y) \wedge x \neq y))$	
	$\therefore\ (\exists x\ (\exists y\ b(x) \wedge b(y) \wedge x \neq y \wedge (\forall z\ b(z) \Rightarrow (z = x \vee z = y))))$	
5)	$a(\alpha) \wedge a(\beta) \wedge \alpha \neq \beta$	I.E. 4 $\alpha/x, \beta/y$
6)	$a(\alpha)$	Simp. 5
7)	$a(\beta)$	Simp. 5
8)	$\alpha \neq \beta$	Simp. 5
9)	$a(\alpha) \Rightarrow b(\alpha)$	I.U. 1 α/x
10)	$a(\beta) \Rightarrow b(\beta)$	I.U. 1 β/x
11)	$b(\alpha)$	M.P. 6 y 9
12)	$b(\beta)$	M.P. 7 y 10
13)	$b(\alpha) \Rightarrow c(\alpha)$	I.U. 2 α/x
14)	$b(\beta) \Rightarrow c(\beta)$	I.U. 2 β/x
15)	$c(\alpha)$	M.P. 11 y 13
16)	$c(\beta)$	M.P. 12 y 14
17)	$(\forall z\ (c(\alpha) \wedge c(\beta) \wedge c(z)) \Rightarrow (\alpha = \beta \vee \alpha = z \vee \beta = z))$	I.U. 3 $\alpha/x, \beta/y$
18)	Sea w cualquiera	
19)	$(c(\alpha) \wedge c(\beta) \wedge c(w)) \Rightarrow (\alpha = \beta \vee \alpha = w \vee \beta = w)$	I.U. 18 w/z
20)	Supongamos $b(w)$	Suposición D.C.
21)	$b(w) \Rightarrow c(w)$	I.U. 2 w/x
22)	$c(w)$	M.P. 20 y 21
23)	$c(\alpha) \wedge c(\beta) \wedge c(w)$	Conj. 15 y 16 y 22
24)	$\alpha = \beta \vee \alpha = w \vee \beta = w$	M.P. 19 y 23
25)	$\alpha = w \vee \beta = w$	S.D. 8 y 24
26)	$b(w) \Rightarrow (\alpha = w \vee \beta = w)$	D.C. 20–25
27)	$(\forall z\ b(z) \Rightarrow (\alpha = z \vee \beta = z))$	G.U. 26
28)	$b(\alpha) \wedge b(\beta) \wedge \alpha \neq \beta \wedge (\forall z\ b(z) \Rightarrow (\alpha = z \vee \beta = z))$	Conj. 11, 12 y 27 y8
29)	$(\exists x\ (\exists y\ b(x) \wedge b(y) \wedge x \neq y \wedge (\forall z\ b(z) \Rightarrow (x = z \vee y = z))))$	G.E. 28

4. $f(a) \Leftrightarrow (\forall x\ x = a \Rightarrow f(x))$

1)	Supongamos $f(a)$	Suposición D.C.
2)	Sea z cualquiera	
3)	Supongamos $z = a$	Suposición D.C.
4)	$f(z)$	Sust. 1 y 3
5)	$z = a \Rightarrow f(z)$	D.C. 3–4
6)	$(\forall x\ x = a \Rightarrow f(x))$	G.U. 5
7)	$f(a) \Rightarrow (\forall x\ x = a \Rightarrow f(x))$	D.C. 1–6
8)	Supongamos $(\forall x\ x = a \Rightarrow f(x))$	Suposición D.C.
9)	$a = a \Rightarrow f(a)$	I.U. 8
10)	$a = a$	Refl.
11)	$f(a)$	M.P. 9 y 10
12)	$(\forall x\ x = a \Rightarrow f(x)) \Rightarrow f(a)$	D.C. 8–11
13)	$f(a) \Leftrightarrow (\forall x\ x = a \Rightarrow f(x))$	Bicon. 7 y 12

5. $(\forall x\ (\forall y\ \neg(f(x) \Rightarrow f(y)) \Rightarrow x \neq y))$

1)	Sean x e y cualesquiera	
2)	Supongamos $\neg(f(x) \Rightarrow f(y))$	Suposición D.C.
3)	$f(x) \wedge \neg f(y)$	Neg. 2
4)	Supongamos $x = y$	Suposición R.A.
5)	$f(x) \wedge \neg f(x)$	Sust. 3 y 4 $\rightarrow\leftarrow$
6)	$x \neq y$	R.A. 4–5
7)	$\neg(f(x) \Rightarrow f(y)) \Rightarrow x \neq y$	D.C. 2–6
8)	$(\forall x\ (\forall y\ \neg(f(x) \Rightarrow f(y)) \Rightarrow x \neq y))$	G.U. 7

3.5. Formas normales de Prenex y Skolem

Definición 3.11. Se dice que una fórmula está en forma normal Prenexa (FNP) si es de la forma:

$$(Q_1 x_1\, Q_2 x_2 \ldots Q_n x_n\ M)$$

donde: $Q_i \in \{\forall, \exists\}$ y M es una fórmula sin cuantificadores.

La secuencia $Q_1 x_1\, Q_2 x_2 \ldots Q_n x_n$ se denomina prefijo y M es la matriz de la fórmula.

Teorema 3.1. *Cualquier fórmula tiene un equivalente en forma normal Prenexa.*

Para llevar una fórmula a FNP se puede seguir el siguiente algoritmo:

1. Renombrar las variables que tienen distinto cuantificador.
2. Eliminar $\Rightarrow$ y $\Leftrightarrow$.
3. Aplicar reglas de reemplazo de modo que las negaciones solo afecten a fórmulas atómicas.
4. Pasar los cuantificadores al inicio de la fórmula.

Ejemplo: $(\forall x\ (h(x) \vee f(x)) \Rightarrow [(\forall y\ r(y)) \Rightarrow (\forall y\ s(y))])$

$$(\forall x\ (h(x) \vee f(x)) \Rightarrow [(\forall y\ r(y)) \Rightarrow (\forall y\ s(y))])$$
$$(\forall x\ (h(x) \vee f(x)) \Rightarrow [(\forall y\ r(y)) \Rightarrow (\forall z\ s(z))])$$
$$(\forall x\ \neg(h(x) \vee f(x)) \vee [\neg(\forall y\ r(y)) \vee (\forall z\ s(z))])$$
$$(\forall x\ \neg(h(x) \vee f(x)) \vee [(\exists y\ \neg r(y)) \vee (\forall z\ s(z))])$$
$$(\forall x\ (\exists y\ (\forall z\ \neg(h(x) \vee f(x)) \vee \neg r(y) \vee s(z))))$$

Definición 3.12. Diremos que un literal es una fórmula atómica o la negación de una fórmula atómica.

Definición 3.13. Una fórmula P está en forma normal conjuntiva (FNC) si tiene la forma $P_1 \wedge \cdots \wedge P_n$ siendo $n \geq 1$ y cada P_i es una disyunción de literales.

Definición 3.14. Una fórmula P está en forma normal disyuntiva (FND) si tiene la forma $P_1 \wedge \cdots \wedge P_n$ siendo $n \geq 1$ y cada P_i es una conjunción de literales.

Definición 3.15. Una fórmula está en forma normal conjuntiva Prenexa si está en forma normal Prenexa y su matriz está en forma normal conjuntiva.

$$(\forall x\ (\exists y\ (\forall z\ \neg(h(x) \vee f(x)) \vee \neg r(y) \vee s(z))))$$
$$(\forall x\ (\exists y\ (\forall z\ (\neg h(x) \wedge \neg f(x)) \vee \neg r(y) \vee s(z))))$$
$$(\forall x\ (\exists y\ (\forall z\ (\neg h(x) \vee \neg r(y) \vee s(z)) \wedge (\neg f(x) \vee \neg r(y) \vee s(z)))))$$

Definición 3.16. Una fórmula cerrada está en forma normal de Skolem (FNS) si está en forma normal conjuntiva Prenexa y todos los cuantificadores son universales.

Para transformar una forma normal conjuntiva Prenexa en una forma normal de Skolem, se usa el algoritmo de Skolemización.

1. Se busca el primer cuantificador existencial de izquierda a derecha. Si no se encuentra finalizar.
2. Si el cuantificador existencial está al principio, es decir es de la forma $\exists x\ F(x)$, se suprime la variable cuantificada reemplazándola por una constante, la fórmula queda como $F(a)$.
3. Si existen n cuantificadores universales antes del cuantificador existencial, es decir es de la forma $(\forall x_1 \ldots \forall x_n \exists y\ \ F(x_1, \ldots, x_n, y))$, se reemplaza la variable cuantificada por una función de las n variables anteriores. Esto queda de la forma: $(\forall x_1 \ldots \forall x_n\ F(x_1, \ldots, x_n, f(x_1, \ldots, x_n)))$.
4. Volver al paso 1.

Teorema 3.2. *Dada cualquier fórmula en lógica de predicados, se puede encontrar una forma normal de Skolem equisatisfacible.*

Demostración. En primer lugar vemos que si la fórmula se satisface, su Skolemización también lo hará. Como ya se ha visto toda fórmula en lógica de predicados puede escribirse como una forma normal conjuntiva prenexa equivalente. Si suprimimos los cuantificadores utilizando el algoritmo de Skolemización, tenemos dos opciones:

- La fórmula $(\exists x\ F(x))$ se reemplaza por $F(a)$. $(\exists x\ F(x))$ es satisfacible cuando existe un valor constante del dominio de discurso que satisface F. Si llamamos a esta constante a, como a no tiene una valor asignado, entonces $F(a)$ será satisfacible.
- La fórmula $(\forall x_1 \ldots \forall x_n \exists y\ \ F(x_1, \ldots, x_n, y))$ se reemplaza por $(\forall x_1 \ldots \forall x_n\ \ F(x_1, \ldots, x_n, f(x_1, \ldots, x_n)))$. Lo que tenemos en este caso es una valor y que satisface $F(x_1, \ldots, x_n, y)$ que depende de los valores de $x_1, \ldots, x_n$, esto es exactamente reemplazar y por $f(x_1, \ldots, x_n)$.

Ahora vemos la recíproca. Si la Skolemización es de la forma $F(x, f(x))$, si la expresión $F(x, f(x))$ es satisfacible, luego que para cada x en el dominio de discurso existe un elemento $f(x)$ en el dominio de discurso, tal que $F(x, f(X))$ es verdadera y esto es lo mismo que $\forall x \exists y\ F(x, y)$. Claramente esta misma idea se puede extender a más variables. Por último, si la Skolemización es de la forma $F(x, a)$ haciendo una generalización existencial podemos concluir $(\exists x \forall y F(x, y))$ ■

$$(\forall x\ (\exists y\ (\forall z\ (\neg h(x) \vee \neg r(y) \vee s(z)) \wedge (\neg f(x) \vee \neg r(y) \vee s(z)))))$$
$$(\forall x\ (\forall z\ (\neg h(x) \vee \neg r(g(x)) \vee s(z)) \wedge (\neg f(x) \vee \neg r(g(x)) \vee s(z))))$$

Definición 3.17. Una fórmula está en forma normal clausal si está en forma normal de Skolem y se suprimen todos cuantificadores universales y las conjunciones se reemplazan por comas.

Ejemplo:

$$(\forall x\ (\forall z\ (\neg h(x) \vee \neg r(g(x)) \vee s(z)) \wedge (\neg f(x) \vee \neg r(g(x)) \vee s(z))))$$
$$\{\neg h(x) \vee \neg r(g(x)) \vee s(z), \neg f(x) \vee \neg r(g(x)) \vee s(z)\}$$

3.6. Método de resolución

El método de resolución en lógica de predicados es una generalización del utilizado en lógica proposicional. En lógica de predicados utilizaremos la forma normal clausal para representar las clausulas y el método de unificación de manera de poder igualar términos y aplicar las resolventes.

3.6.1. Sustitución

La sustitución es un método que permite instanciar variables, de este modo, sentamos las bases para aplicar el método de unificación, que se requiere para la resolución.

Definición 3.18. Una sustitución σ es un conjunto finito de la forma $\{v_1/t_1, v_2/t_2, \ldots, v_n/t_n\}$ donde v_i son variables y t_i es un término distinto de v_i y las variables $v_1, \ldots, v_n$ son distintas entre sí.

Diremos que una sustitución es básica si los términos t_i no contienen variables.

Definición 3.19. Una expresión es un término, un literal o una conjunción o disyunción de literales. Una expresión simple es un término o un átomo.

Definición 3.20. Dadas $\sigma = \{v_1/t_1, v_2/t_2, \ldots, v_n/t_n\}$ una sustitución y E una expresión, se define la instancia de E por σ, denotada por $\sigma(E)$ como la expresión que resulta de sustituir cada variable v_i por el término t_i. Si $\sigma(E)$ no contiene variables, entonces $\sigma(E)$ es una instancia básica de E.

Definición 3.21. Sean $\sigma_1 = \{x_1/t_1, x_2/t_2, \ldots, x_m/t_m\}$ y $\sigma_2 = \{y_1/s_1, y_2/s_2, \ldots, y_n/s_n\}$ dos sustituciones, entonces la composición de sustituciones es la sustitución:

$$\sigma_1 \circ \sigma_2 = \{x_1/\sigma_2(t_1), x_2/\sigma_2(t_2), \ldots, x_m/\sigma_2(t_m)\} \cup \{y_1/s_1, y_2/s_2, \ldots, y_n/s_n\}$$

3.6.2. Unificación

Definición 3.22. Dado un conjunto de expresiones $C = \{E_1, \ldots, E_n\}$ y una sustitución ω. Se dice que σ es un unificador para C si $\sigma(E_1) = \cdots = \sigma(E_n)$.

Definición 3.23. Dado un conjunto de expresiones $C = \{E_1, \ldots, E_n\}$ y σ un unificador. Se dice que ω es un unificador más general, si para cualquier otro unificador ω' existe una sustitución σ tal que $\omega' = \omega \circ \sigma$

Con objeto de encontrar el unificador más general de dos términos se han propuesto numerosos algoritmos siendo el más conocido el de Robinson. El algoritmo de unificación de Robinson data del año 1965. La claridad del método utilizado por el algoritmo lo hace muy útil, tanto desde un punto de vista didáctico como desde un punto de vista de implementación. Vamos a exponer el método en un cuadro general y posteriormente lo aplicaremos a varios ejemplos.

Tomemos dos términos que no sean iguales. Eso significa que habrá alguna diferencia entre ellos. Esta diferencia puede hallarse en el nombre de la función, en el número de argumentos, o en alguno de los argumentos.

Si la diferencia está en el nombre de la función, el primer par de discordancia es la pareja formada por los dos términos. Si está en el número de argumentos, al igual que antes, el primer par de discordancia resulta ser el formado por los dos términos considerados.

En cambio, si coinciden en las funciones y en el número de argumentos, el primer par de discordancia debe ser buscado entre sus argumentos empezando a considerar éstos de izquierda a derecha. Se busca en el primer argumento, y si aquí no lo hubiera, se busca en el segundo,…Es evidente que al final se debe encontrar este par de discordancia pues hemos partido de dos términos distintos.

Como se ve, hemos dado una definición recursiva de lo que es un par de discordancia.

Sean E y F dos términos que queremos unificar. Consideramos inicialmente $\sigma_0 = \{\}$ una sustitución vacía, es decir, que no cambia ninguna variable. Dado que vamos a realizar un proceso iterativo, consideramos inicialmente $E_0 = \sigma_0(E)$ y $F_0 = \sigma_0(F)$. En cada iteración k del algoritmo se realizan los siguientes pasos:

1. *a*) Si $E_k = F_k$ entonces las cláusulas E y F son unificables y un unificador de máxima generalidad es $\sigma = \sigma_k \circ \ldots \sigma_0$. Además, el término E_k es el término unificado. En este caso el proceso termina aquí.

   b) Si $E_k \neq F_k$ entonces se busca el primer par de discordancia entre E_k y F_k. Sea esteD_k.

2. Si D_k contiene una variable y un término (pueden ser dos variables y una de ellas hace de término) pasamos al siguiente paso. En otro caso los términos no son unificables y terminamos el proceso.

3. Si la variable aparece en el término se produce un *occur check* por lo que E y F no unifican y terminamos. Si esto no ocurre pasamos al siguiente paso.

4. Construimos una nueva sustitución que vincule la variable con el término de D_k. Sea esta sustitución σ_{k+1}. Construimos ahora dos nuevos términos $E_{k+1} = \sigma_{k+1}(E_k)$ y $F_{k+1} = \sigma_{k+1}(F_k)$ y volvemos al paso 1.

Ejemplo:

Sea $E = \{P(x, x), P(y, f(y))\}$

- **Paso 1:** $k = 0, \sigma_0 = \varepsilon$, $E_0 = P(x, x)$, $F_0 = P(y, f(y))$, $D_0 = \{x, y\}$.
- **Paso 2:** Selecciona $v = x$, $t = y$.
- **Paso 3:** x no aparece en y.
- **Paso 4:** $\sigma_1 = \{x/y\}$, $k = 1$, $\sigma_1(E_0) = P(y, y)$, $\sigma_1(F_0) = P(y, f(y))$.
- **Paso 1:** $k = 1,$, $E_1 = P(y, y)$, $F_1 = P(y, f(y))$, $D_1 = \{y, f(y)\}$
- **Paso 2:** Selecciona $v = y$, $t = f(y)$.
- **Paso 3:** *ocurr check*, no es unificable.

Sea $E = \{P(x, f(y, y)), P(f(z, z), f(x, x))\}$

- **Paso 1:** $k = 0, \sigma_0 = \varepsilon$, $E_0 = P(x, f(y, y))$, $F_0 = P(f(z, z), f(x, x))$, $D_0 = \{x, f(z, z)\}$.
- **Paso 2:** Selecciona $v = x$, $t = f(z, z)$.
- **Paso 3:** x no aparece en $f(z, z)$
- **Paso 4:** $\sigma_1 = \{x/f(z, z)\}$, $k = 1$, $\sigma_1(E_0) = P(f(z, z), f(y, y))$, $\sigma_1(F_0) = P(f(z, z), f(f(z, z), f(z, z)))$.
- **Paso 1:** $k = 1$, $E_1 = P(f(z, z), f(y, y))$, $F_1 = P(f(z, z), f(f(z, z), f(z, z)))$, $D_1 = \{y, f(z, z)\}$
- **Paso 2:** Selecciona $v = y$, $t = f(z, z)$.
- **Paso 3:** y no aparece en $f(z, z)$
- **Paso 4:** , $\sigma_2 = \{y/f(z, z)\}$, $\sigma_2(E_1) = P(f(z, z), f(f(z, z), f(z, z)))$, $\sigma_2(F_1) = P(f(z, z), f(f(z, z), f(z, z)))$.
- **Paso 1:** $k = 2$, $E_2 = F_2 = P(f(z, z), f(f(z, z), f(z, z)))$. El algoritmo termina con el término unificado $P(f(z, z), f(f(z, z), f(z, z)))$ y la unificación más general $\sigma_2 \circ \sigma_1 = \{x/f(z, z), y/f(z, z)\}$

3.6.3. Algoritmo de Resolución

Al igual que en el caso de la lógica proposicional el método de resolución no es más que un caso particular de una reducción al absurdo, donde:

- Se utiliza una única regla de inferencia, la resolvente.
- Las instancias se realizan mediante una sustitución que permite unificar dos fórmulas atómicas con el objetivo de utilizar la regla de la resolvente.
- Tanto las premisas como la negación de la conclusión se expresan en forma normal clausal, ya que esta permite usar la regla de inferencia de la resolvente

Ejemplo:Usaremos como ejemplo el problema 12.28 del listado de ejercicios:

$$\begin{array}{l} ((\exists x\ f(x)) \vee (\exists x\ g(x))) \Rightarrow (\exists x\ \neg h(x)) \\ (\forall x\ h(x) \vee p(x)) \\ \neg(\exists x\ p(x) \wedge q(x)) \\ \hline \therefore\ (\forall x\ q(x)) \Rightarrow (\forall x\ \neg f(x)) \end{array}$$

Lo primero es transformar cada Premisa y la negación de la conclusión en forma normal clausal, utilizando nombres de variables distintos en cada forma normal.

Premisa 1:

$$\begin{aligned} ((\exists x\ f(x)) \vee (\exists x\ g(x))) \Rightarrow (\exists x\ \neg h(x)) &\Leftrightarrow ((\exists x_1\ f(x_1)) \vee (\exists y_1\ g(y_1))) \Rightarrow (\exists z_1\ \neg h(z_1)) \\ &\Leftrightarrow \neg((\exists x_1\ f(x_1)) \vee (\exists y_1\ g(y_1))) \vee (\exists z_1\ \neg h(z_1)) \\ &\Leftrightarrow (\neg(\exists x_1\ f(x_1)) \wedge \neg(\exists y_1\ g(y_1))) \vee (\exists z_1\ \neg h(z_1)) \\ &\Leftrightarrow ((\forall x_1\ \neg f(x_1)) \wedge (\forall y_1\ \neg g(y_1))) \vee (\exists z_1\ \neg h(z_1)) \\ &\Leftrightarrow (\forall x_1\ (\forall y_1\ \exists z_1\ (\neg f(x_1) \wedge \neg g(y_1)) \vee \neg h(z_1)) \\ &\Leftrightarrow (\forall x_1\ (\forall y_1\ \exists z_1\ (\neg f(x_1) \vee \neg h(z_1)) \wedge (\neg g(y_1) \vee \neg h(z_1))) \end{aligned}$$

Skolemización:

$$\stackrel{\text{FNS}}{=} (\forall x_1\ (\forall y_1\ (\neg f(x_1) \vee \neg h(a(x_1, y_1))) \wedge (\neg g(y_1) \vee \neg h(a(x_1, y_1)))$$

Forma normal clausal:

$$\stackrel{\text{FNCl}}{=} \{\neg f(x_1) \vee \neg h(a(x_1, y_1)), \neg g(y_1) \vee \neg h(a(x_1, y_1))\}$$

Premisa 2:

$$(\forall x\ h(x) \vee p(x)) \Leftrightarrow (\forall x_2\ h(x_2) \vee p(x_2)) \stackrel{\text{FNCl}}{=} \{h(x_2) \vee p(x_2)\}$$

Premisa 3:

$$\neg(\exists x\ p(x) \wedge q(x)) \Leftrightarrow \neg(\exists x_3\ p(x_3) \wedge q(x_3)) \Leftrightarrow (\forall x_3\ \neg p(x_3) \vee \neg q(x_3)) \stackrel{\text{FNCl}}{=} \{\neg p(x_3) \vee \neg q(x_3)\}$$

Negación Conclusión:

$$\begin{aligned}
\neg[(\forall x\ q(x)) \Rightarrow (\forall x\ \neg f(x))] &\Leftrightarrow (\forall x\ q(x)) \wedge \neg(\forall x\ \neg f(x)) \\
&\Leftrightarrow (\forall x\ q(x)) \wedge (\exists x\ f(x)) \\
&\Leftrightarrow (\forall x_4\ q(x_4)) \wedge (\exists y_4\ f(y_4)) \\
&\Leftrightarrow (\forall x_4\ \exists y_4\ q(x_4) \wedge f(y_4))
\end{aligned}$$

Skolemización:

$$\stackrel{\text{FNS}}{=} (\forall x_4\ q(x_4) \wedge f(b(x_4)))$$

Forma normal clausal:

$$\stackrel{\text{FNCl}}{=} \{q(x_4), f(b(x_4))\}$$

Ahora aplicamos la resolución:

1)	$\neg f(x_1) \vee \neg h(a(x_1, y_1))$	
2)	$\neg g(y_1) \vee \neg h(a(x_1, y_1))$	
3)	$h(x_2) \vee p(x_2)$	
4)	$\neg p(x_3) \vee \neg q(x_3)$	
5)	$q(x_4)$	
6)	$f(b(x_4))$	
7)	$\neg p(x_3)$	Res. 4 y 5 $\sigma = \{x_4/x_3\}$
8)	$h(x_2)$	Res. 3 y 7 $\sigma = \{x_3/x_2\}$
9)	$\neg f(x_1)$	Res. 1 y 8 $\sigma = \{x_2/a(x_1, y_1)\}$
10)	$\varnothing$	Res. 6 y 9 $\sigma = \{x_1/b(x_4)\}$

3.7. Ejercicios

P1. Escriba en lógica simbólica las siguientes proposiciones:

$l(x)$: x es gratis	$a(x)$: x es un ángel	$e(x)$: x es malvado
$u(x)$: x es un unicornio	$b(x)$: x es hermoso	$g(x)$: x es bueno
$d(x)$: x es un demonio	$j(x)$: x es divertido	$c(x)$: x es cierto
$s(x)$: x es usual	$n(x)$: x termina	$h(x)$: x ayuda
$m(x)$: x es significativo		

1. Nada es gratis.
2. Carlos no es un ángel.
3. No todo es malvado.
4. No existen los unicornios.
5. Todo es hermoso.
6. Los demonios no existen.
7. Hay cosas que no son divertidas.
8. Nada es cierto.
9. Nada es inusual.
10. No es verdad que Andrés es malvado.
11. Todo termina.
12. Nada ayudará.
13. Cecilia ayudará.
14. No todo es significativo.
15. La ruta 66 termina.
16. No es verdad que Guillermo no es bueno.
17. El Universo no está llegando a su fin.

P2. Usando las funciones proposicionales del ejercicio anterior, escriba en lenguaje natural (Recuerde que es importante que, la proposición se lea como se usa en lenguaje natural y no como una traducción término a término)

1. $\neg(\exists x\ a(x))$
2. $\forall x\ \neg e(x)$
3. $\neg(\forall x\ b(x))$
4. $\exists x\ \neg c(x)$
5. $\neg(\exists x\ b(x))$
6. $\exists x\ \neg s(x)$
7. $\exists x\ d(x)$
8. $\forall x\ \neg j(x)$
9. $\neg(\forall x\ \neg a(x))$
10. $\neg(\exists x\ \neg j(x))$
11. $\neg(\forall x\ n(x))$
12. $\exists x\ j(x)$
13. $\neg(\forall x\ h(x))$
14. $\forall x\ \neg m(x)$
15. $\neg(\exists x\ \neg h(x))$
16. $\exists x\ \neg g(x)$
17. $\neg(\forall x\ \neg g(x))$
18. $\neg(\forall x\ c(x))$
19. $\neg(\exists x\ \neg n(x))$
20. $\neg(\exists x\ \neg\neg j(x))$

P3. Escriba en lógica simbólica las siguientes proposiciones:

$b(x)$: x es bonito	$v(x)$: x es valioso
$a(x)$: x es apreciado	$w(x)$: x está en la basura
$d(x)$: x deberá descartarse	$g(x)$: x es una buena persona
$e(x)$: x es una persona que defrauda a sus padres	$h(x)$: x va al cielo
$r(x)$: x es una persona que está aquí	$p(x)$: x aprueba el examen
$m(x)$: x se atrasa	$o(x)$: x es chismoso

1. Algo bonito es valioso
2. No todas las cosas bonitas son apreciadas
3. Hay cosas valiosas en la basura
4. Nada bello debería descartarse
5. Solo las cosas que deberían descartarse

están en la basura.

6. A veces las personas buenas no son bellas.
7. Ninguna persona que defrauda a sus padres es una buena persona.
8. Solo los buenos van al cielo
9. Nadie aquí irá al cielo
10. No todos los presentes reprobaron el examen.
11. Solo los que no están aquí se retrasaron.
12. Las personas buenas no son chismosas.
13. Ninguna persona buena no es apreciada.
14. No todas las cosas valiosas deberían no ser descartadas
15. Hay cosas bellas que no son apreciadas.
16. Los chismosos no son apreciados
17. Las únicas personas que no irán al cielo son las que están aquí.
18. No todos los presentes son menospreciados.
19. No hay nadie aquí que no sea hermoso.

P4. Escriba en lógica simbólica las siguientes proposiciones:

$a(x)$: x es un animal	$b(x)$: x ladra	$c(x)$: x es un gato
$d(x)$: x es un perro	$e(x)$: x come comida de gatos	$f(x)$: x tiene pelaje
$g(x)$: x tiene buenos sentidos	$i(x)$: x come insectos	$m(x)$: x es un mamífero
$n(x)$: x come ratones	$o(x)$: x maúlla	$r(x)$: x es un reptil
$s(x)$: x es una serpiente	$t(x)$: x es bonito	

1. Los gatos tienen pelaje.
2. No todos los animales ladran.
3. Los perros, a veces, comen comida de gatos.
4. Los reptiles no tienen pelaje.
5. Algunas cosas con pelaje no son gatos.
6. No todos los gatos comen comida de gatos.
7. Solo los gatos maúllan.
8. Algunos gatos comen insectos.
9. Hay gatos que no comen ratones.
10. Lo que no es peludo es un reptil.
11. No todo lo que come insectos es un reptil.
12. Los reptiles comen insectos.
13. Los gatos no ladran
14. No hay perros que no ladran.
15. Solo los mamíferos tienen pelaje.
16. No todos los perros carecen de buenos sentidos.
17. Algunos reptiles carecen de buenos sentidos.
18. No hay gatos que no sean bonitos.
19. Algunos reptiles son hermosos.
20. Las serpientes comen ratones.
21. No solo las serpientes comen ratones.
22. No todas las cosas bellas tienen buenos sentidos.
23. No todo lo que tiene buenos sentidos es bello.
24. Solo los que maúllan comen comida de gatos.
25. Algo que come comida de gatos maúlla.

P5. Usando las funciones proposicionales del ejercicio anterior, escriba en lenguaje natural.

1. $\neg(\forall x\ c(x) \Rightarrow n(x))$
2. $\exists x\ d(x) \wedge \neg b(x)$
3. $\neg(\exists x\ c(x) \wedge b(x))$
4. $\forall x\ r(x) \Rightarrow i(x)$
5. $\neg(\forall x\ r(x) \Rightarrow s(x))$
6. $\neg(\exists x\ m(x) \wedge \neg f(x))$
7. $\neg(\forall x\ s(x) \Rightarrow \neg g(x))$
8. $\exists x\ d(x) \wedge \neg g(x)$
9. $\forall x\ r(x) \Rightarrow \neg e(x)$
10. $\neg(\exists x\ s(x) \wedge \neg r(x))$

P6. Escriba en lógica simbólica las siguientes proposiciones:

$p(x)$: x es una pintura	$j(x)$: x es de José
$b(x)$: x es hermosa	$v(x)$: x es valiosa
$g(x)$: x está enmarcada en oro	$d(x)$: x está decorado con diamantes
$s(x)$: x es una escultura	$h(x)$: x es de Hernán
$u(x)$: x tiene unicornios	$a(x)$: x es admirada por los críticos
$l(x)$: x le gusta al público/ es amado por el público	$c(x)$: x es comprensible
$m(x)$: x tiene monstruos	

1. Algunas pinturas de José son bellas pero no valiosas.
2. Ninguna pintura de Hernán es valiosa a menos que este enmarcada en oro.
3. Todas las pintura de José son valiosas si están enmarcadas en oro y decoradas con diamantes.
4. No todas las pinturas y esculturas de José son bellas y valiosas.
5. Ninguna pintura de José o Hernán es bella o valiosa a menos que contenga unicornios.
6. No todas las pinturas de Hernán que tienen unicornios, son admiradas por los críticos y amadas por el público.
7. Algunas pinturas de José que contienen unicornios, son incomprensibles y son admiradas por los críticos si y solo si no le gustan al público.
8. Algunas pinturas de Hernán o José que no tienen unicornios o monstruos, son amadas por el público si y solo si son valiosas, pero incomprensibles.
9. Ninguna pintura de Hernán o José es comprensible a menos que sea hermosa y tenga unicornios o sea valiosa y enmarcada en oro.
10. Las pinturas y esculturas de Hernán y José que son hermosas solo si contienen unicornios y valiosas solo si están decoradas con diamantes, no son admiradas por los críticos a menos que al público no le gusten.

P7. Escriba en lógica simbólica las siguientes proposiciones:

$b(x)$: x es un ejecutivo	$c(x)$: x consulta un abogado
$l(x)$: x quebranta/rompe la ley	$m(x)$: x es millonario
$t(x)$: x paga impuestos	$p(x)$: x es político
$e(x)$: x es reelecto	$s(x)$: x debería ir al psiquiatra
$a(x)$: x abusa del poder	$r(x)$: x es respetado
$i(x)$: x es impugnado	$u(x)$: x fue demandado
$v(x)$: x vota en conciencia	

1. No todos los ejecutivos que consultan un abogado han quebrantado la ley.
2. Algunos ejecutivos son millonarios, pero no pagan impuestos.
3. Los políticos que no pagan sus impuestos no serán reelectos.
4. Los ejecutivos que pagan impuestos, pero no consultan abogados deberían ir al psiquiatra.
5. Ningún político que ha quebrantado la ley y abusa del poder será respetado o reelecto.
6. Los políticos que quebrantan la ley o abusan del poder serán impugnados.
7. Ningún político que paga impuestos y no abusa del poder será impugnado.
8. Los políticos millonarios que pagan impuestos, no quebrantan la ley y no son demandados serán reelectos.
9. Algunos políticos no son reelectos aunque ellos son respetados y no han sido impugnados ni demandados.

P8. De al menos tres fórmulas equivalentes para las siguientes proposiciones.

1. Ningún político será reelecto a menos que sea respetado y vote en conciencia.
2. Un ejecutivo consultará un abogado solo si es millonario o ha quebrantado la ley.
3. Ningún político será impugnado o demandado, si paga sus impuestos y no rompe la ley.
4. No todos los políticos que rompen la ley y no pagan sus impuestos son demandados o impugnados.
5. Ningún político o ejecutivo consulta un abogado a menos que haya quebrantado la ley, abusado del poder o sea millonario, y haya sido demandado.

P9. Escriba en lógica simbólica las siguientes proposiciones:

$p(x):$ x es político	$r(x):$ x es respetado	$e(x):$ x es reelecto
$a(x):$ x abusa del poder	$i(x):$ x es impugnado	$m(x):$ x es millonario
$v(x):$ x vota en conciencia	$h(x):$ x es honesto	$b(x):$ x acepta sobornos
$l(x):$ x miente	$s(x):$ x es una persona	j: Juan
r: Ricardo		

1. Hay políticos que abusan del poder y otros que no.
2. No todos los políticos que son millonarios abusan del poder.
3. Si los políticos votaran en conciencia, ellos no serían impugnados.
4. Si todos lo políticos votaran en conciencia, ninguno sería impugnado.
5. Algunos políticos que no votan en conciencia son respetados y reelectos.
6. Ningún político acepta sobornos o ningún político es respetado.
7. Los políticos son respetados si y solo si ellos no aceptan sobornos.

8. Si Juan no es honesto entonces no hay políticos honestos.
9. Juan no acepta sobornos, pero él abusa del poder y será impugnado.
10. Si Ricardo no acepta sobornos o abusa de su poder entonces él no será impugnado y será reelecto.
11. Si Juan y Ricardo aceptan sobornos entonces no todos los políticos son honestos.
12. Juan aceptará un soborno solo si todos los políticos aceptan sobornos.
13. Alguien miente o Juan y Ricardo aceptan sobornos.
14. Hay políticos que aceptan sobornos o mienten y ellos serán impugnados

P10. Usando las funciones proposicionales del ejercicio anterior, escriba en lenguaje natural.

1. $(\exists x\ h(x) \wedge p(x)) \Rightarrow \neg b(j)$
2. $\neg(\forall x\ p(x) \Rightarrow h(x)) \wedge \neg(\forall x\ p(x) \Rightarrow \neg h(x))$
3. $\neg(\exists x\ p(x) \wedge r(x)) \Rightarrow (\exists x\ p(x) \wedge b(x))$
4. $\neg(b(j) \vee b(r)) \Rightarrow ((m(j) \wedge m(r)) \vee (h(j) \wedge h(r)))$
5. $(\neg r(j) \wedge \neg e(j)) \Rightarrow (a(j) \vee \neg h(j) \vee \neg m(j))$
6. $(\forall x\ p(x) \wedge h(x) \Rightarrow r(x)) \vee (\exists x\ p(x) \wedge h(x) \wedge \neg e(x))$
7. $(\forall x\ p(x) \wedge \neg h(x) \wedge b(x) \Rightarrow m(x) \wedge \neg r(x) \wedge \neg v(x))$
8. $\neg(\exists x\ p(x) \wedge v(x)) \Rightarrow \neg(\exists x\ p(x) \wedge (r(x) \vee e(x)))$
9. $\neg(\exists x\ p(x) \wedge l(x) \wedge r(x)) \wedge \neg(\forall x\ p(x) \wedge l(x) \wedge b(x) \Rightarrow \neg e(x))$
10. $((b(j) \wedge a(r)) \vee (l(r) \wedge \neg v(j)) \Rightarrow (\neg(\exists x\ p(x) \wedge h(x)) \vee (\exists x\ s(x) \wedge l(x)))$

P11. De una interpretación para explicar porque los siguientes pares de fórmulas no significan lo mismo.

1. $(\forall x\ f(x) \vee g(x))$ y $(\forall x\ f(x)) \vee (\forall x\ g(x))$
2. $(\exists x\ f(x) \wedge g(x))$ y $(\exists x\ f(x)) \wedge (\exists x\ g(x))$
3. $(\forall x\ f(x)) \Rightarrow (\forall x\ g(x))$ y $(\forall x\ f(x) \Rightarrow g(x))$
4. $\neg(\exists x\ f(x) \wedge g(x))$ y $(\exists x\ \neg(f(x) \wedge g(x)))$
5. $\forall x(\exists y\ g(x,y))$ y $\exists y(\forall x\ g(x,y))$

P12. Demuestre usando reglas de inferencia y técnicas de demostración.

1. $$\begin{array}{l} (\forall x\ c(x) \Rightarrow d(x)) \\ (\forall x\ e(x) \Rightarrow \neg d(x)) \\ \hline \therefore\ (\forall x\ e(x) \Rightarrow \neg c(x)) \end{array}$$

2. $$\begin{array}{l} (\forall x\ f(x) \Rightarrow \neg g(x)) \\ (\exists x\ h(x) \wedge g(x)) \\ \hline \therefore\ \neg(\forall x\ h(x) \Rightarrow f(x)) \end{array}$$

3. $$\begin{array}{l} (\forall x\ k(x) \Rightarrow l(x)) \\ (\forall x\ (k(x) \wedge l(x)) \Rightarrow m(x)) \\ \hline \therefore\ (\forall x\ k(x) \Rightarrow m(x)) \end{array}$$

4. $$\begin{array}{l} (\forall x\ s(x) \Rightarrow (t(x) \Rightarrow u(x))) \\ (\forall x\ u(x) \Rightarrow (v(x) \wedge w(x))) \\ \hline \therefore\ (\forall x\ (s(x) \wedge t(x)) \Rightarrow v(x)) \end{array}$$

5. $(\forall x\ t(x) \Rightarrow (f(x) \wedge d(x)))$
$\neg(\forall x\ t(x) \Rightarrow \neg b(x))$
$\therefore\ \neg(\forall x\ d(x) \Rightarrow \neg b(x))$

6. $(\forall x\ (a(x) \vee b(x)) \Rightarrow (c(x) \wedge d(x)))$
$(\forall x\ (c(x) \vee d(x)) \Rightarrow (a(x) \wedge b(x)))$
$\therefore\ (\forall x\ a(x) \Leftrightarrow c(x))$

7. $\neg(\exists x\ f(x) \wedge g(x))$
$(\forall x\ z(x) \Rightarrow (g(x) \vee h(x)))$
$(\exists x\ f(x) \wedge z(x))$
$\therefore\ \neg(\forall x\ f(x) \Rightarrow \neg h(x))$

8. $(\forall x\ (b(x) \vee w(x)) \Rightarrow ((a(x) \vee f(x)) \Rightarrow s(x)))$
$\therefore\ (\forall x\ (b(x) \wedge f(x)) \Rightarrow s(x))$

9. $(\forall x\ c(x) \Rightarrow (f(x) \vee n(x)))$
$(\forall x\ f(x) \Rightarrow b(x))$
$\neg(\forall x\ c(x) \Rightarrow b(x))$
$\therefore\ \neg(\forall x\ c(x) \Rightarrow \neg n(x))$

10. $(\exists x\ c(x) \wedge (\neg s(x) \Rightarrow (v(x) \vee w(x))))$
$(\forall x\ v(x) \Rightarrow \neg c(x))$
$\neg(\exists x\ w(x) \wedge c(x))$
$\therefore\ (\exists x\ s(x) \wedge \neg w(x))$

11. $\neg(\exists x\ f(x) \wedge \neg(g(x) \wedge h(x)))$
$(\forall x\ (g(x) \vee s(x)) \Rightarrow z(x))$
$\neg(\exists x\ z(x) \wedge a(x))$
$\therefore\ (\forall x\ f(x) \Rightarrow \neg a(x))$

12. $(\forall x\ f(x) \Rightarrow (b(x) \Leftrightarrow \neg t(x)))$
$\neg(\forall x\ f(x) \Rightarrow (b(x) \vee c(x)))$
$\neg(\exists x\ t(x) \wedge \neg(d(x) \Rightarrow c(x)))$
$\therefore\ (\exists x\ f(x) \wedge \neg(c(x) \vee d(x)))$

13. $\neg(\exists x\ (a(x) \wedge b(x)) \wedge \neg c(x))$
$\neg(\exists x\ a(x) \wedge \neg b(x))$
$(\forall x\ c(x) \Rightarrow \neg(s(x) \vee t(x)))$
$\therefore\ \neg(\exists x\ a(x) \wedge t(x))$

14. $(\forall x\ (a(x) \vee b(x)) \Rightarrow (g(x) \wedge \neg h(x)))$
$(\forall x\ g(x) \Rightarrow h(x))$
$(\forall x\ (d(x) \wedge e(x)) \Rightarrow b(x))$
$\neg(\exists x\ p(x) \wedge \neg e(x))$
$\therefore\ \neg(\exists x\ p(x) \wedge (a(x) \vee d(x)))$

15. $\neg(\exists x\ a(x) \wedge b(x))$
$\neg(\exists x\ a(x) \wedge \neg c(x))$
$\neg(\forall x\ a(x) \Rightarrow (f(x) \vee g(x)))$
$(\forall x\ h(x) \Rightarrow g(x))$
$\therefore\ \neg(\forall x\ c(x) \Rightarrow (b(x) \vee h(x)))$

16. $(\forall x\ (a(x) \vee b(x)) \Rightarrow \neg(g(x) \wedge \neg h(x)))$
$\neg(\exists x\ a(x) \wedge d(x))$
$\neg(\exists x\ h(x) \wedge \neg d(x))$
$(\forall x\ f(x) \Rightarrow (g(x) \Leftrightarrow w(x)))$
$\therefore\ \neg(\exists x\ a(x) \wedge f(x) \wedge w(x))$

17. $(\forall x\ a(x) \Leftrightarrow \neg c(x))$
$\neg(\exists x\ s(x) \wedge c(x) \wedge e(x) \wedge \neg(a(x) \vee b(x)))$
$\therefore\ \neg(\exists x\ e(x) \wedge \neg b(x) \wedge s(x) \wedge \neg a(x))$

18. $(\forall x\ (a(x) \Leftrightarrow b(x)) \Rightarrow (c(x) \Rightarrow (z(x) \vee w(x))))$
$\neg(\exists x\ c(x) \wedge (e(x) \Rightarrow w(x)))$
$\neg(\exists x\ e(x) \wedge c(x) \wedge z(x))$
$(\exists x\ c(x) \wedge (\neg b(x) \Leftrightarrow \neg(d(x) \Rightarrow z(x))))$
$\neg(\exists x\ c(x) \wedge \neg(w(x) \vee d(x)))$
$\therefore\ \neg(\forall x\ a(x) \Rightarrow z(x))$

19. $\neg(\exists x\ p(x) \wedge q(x) \wedge (r(x) \Leftrightarrow t(x)))$
$(\forall x\ (p(x) \Leftrightarrow \neg s(x)) \vee (a(x) \Rightarrow b(x)))$
$\neg(\exists x\ a(x) \wedge \neg s(x))$
$\neg(\exists x\ q(x) \wedge \neg(p(x) \vee t(x)))$
$(\forall x\ (p(x) \Leftrightarrow r(x)) \Rightarrow a(x))$
$\therefore\ (\forall x\ q(x) \Rightarrow (t(x) \vee b(x)))$

20. $(\forall x\ f(x) \Rightarrow g(x))$
$\neg((\exists x\ g(x)) \vee (\exists x\ h(x)))$
$\therefore \neg(\exists x\ f(x))$

21. $(\forall x\ f(x) \Rightarrow \neg g(x)) \Rightarrow (\forall x\ f(x) \Rightarrow \neg h(x))$
$\therefore (\exists x\ f(x) \wedge h(x)) \Rightarrow (\exists x\ f(x) \wedge g(x))$

22. $(\forall x\ (f(x) \vee g(x)) \Rightarrow h(x))$
$(\forall x\ h(x)) \Rightarrow (\forall x\ s(x))$
$\therefore (\forall x\ f(x)) \Rightarrow (\forall x\ s(x))$

23. $(\forall x\ f(x)) \vee (\forall x\ g(x))$
$(\forall x\ f(x) \Rightarrow h(x))$
$\therefore (\exists x\ \neg g(x)) \Rightarrow (\forall x\ h(x))$

24. $(\exists x\ f(x)) \Rightarrow (\forall x\ g(x) \vee h(x))$
$(\forall x\ f(x) \Rightarrow \neg g(x))$
$\therefore \neg(\exists x\ h(x)) \Rightarrow (\forall x \neg f(x))$

25. $(\exists x\ f(x)) \Rightarrow (\forall x\ h(x) \Rightarrow \neg j(x))$
$\neg(\exists x\ s(x) \wedge \neg j(x))$
$\therefore (\forall x\ f(x)) \Rightarrow \neg(\exists x\ h(x) \wedge s(x))$

26. $(\forall x\ f(x) \Rightarrow g(x)) \Rightarrow (\forall x\ f(x) \Rightarrow h(x))$
$(\exists x\ f(x) \wedge \neg h(x))$
$(\exists x\ \neg g(x)) \Rightarrow \neg(\forall x\ j(x))$
$\therefore (\exists x\ \neg j(x))$

27. $\neg((\forall x\ f(x)) \vee (\exists x\ g(x)))$
$(\forall x\ h(x) \Rightarrow f(x))$
$((\exists x\ \neg h(x)) \wedge (\forall x\ s(x))) \Rightarrow (\exists x\ g(x))$
$\therefore\ (\exists x\ \neg s(x))$

28. $((\exists x\ f(x)) \vee (\exists x\ g(x))) \Rightarrow (\exists x\ \neg h(x))$
$(\forall x\ h(x) \vee p(x))$
$\neg(\exists x\ p(x) \wedge q(x))$
$\therefore\ (\forall x\ q(x)) \Rightarrow (\forall x\ \neg f(x))$

29. $\neg((\exists x\ \neg f(x)) \wedge (\exists x\ g(x) \wedge \neg h(x)))$
$(\forall x\ h(x)) \Rightarrow \neg(\exists x\ z(x) \wedge w(x))$
$\neg(\forall x\ w(x) \Rightarrow f(x))$
$\therefore\ \neg(\exists x\ \neg z(x)) \Rightarrow \neg(\forall x\ g(x))$

P13. Demuestre los siguientes teoremas:

1. $(\forall x\ f(x) \Rightarrow g(x)) \implies (\neg(\forall x\ g(x)) \Rightarrow \neg(\forall x\ f(x)))$
2. $\neg(\exists x\ f(x) \wedge g(x)) \implies ((\forall x\ f(x)) \Rightarrow \neg(\exists x\ g(x))$
3. $\neg((\exists x\ f(x)) \vee (\exists x\ \neg g(x))) \implies (\forall x\ f(x) \Rightarrow h(x))$
4. $(\forall x\ f(x) \Rightarrow \neg(g(x) \vee h(x))) \implies \neg(\exists x\ f(x) \wedge h(x))$

P14. Simbolice y demuestre:

1. Médicos y abogados son profesionales bien pagados. Ningún médico bien pagado come en McDonald's y ningún profesional compra ropa en Mercado Persa. Por lo tanto ningún médico compra ropa en el Mercado Persa o come en McDonald's.
2. Cualquiera que repara su propio auto es muy hábil y ahorra mucho dinero en reparaciones. Algunas personas que reparan su auto tienen trabajos de poca importancia. Por lo tanto algunas personas con trabajo de poca importancia son muy hábiles.
3. Algunos Oficiales de policía están obligados a tener un segundo trabajo. Nadie que tiene dos trabajos puede estar completamente alerta en su trabajo. Un policía que no está completamente alerta comete errores de juicio. De modo que algunos policías cometen errores de juicio.
4. Algunos jóvenes que cometen delitos menores son enviados a la cárcel, y los jóvenes en la cárcel están expuestos a toda clase de criminales. Un joven expuesto a toda clase de criminales quedará resentido y aprenderá mas técnicas para cometer crímenes. Cualquier persona que aprende más técnicas para cometer crímenes es una amenaza para la sociedad si está resentido. Por lo tanto, algunos jóvenes que cometen delitos menores se convertirán en una amenaza para la sociedad.

P15. Escriba en lógica simbólica las siguientes proposiciones:

1. $l(x,y)$: x ama a y, $b(x,y)$: x es el hermano de y,
$s(x,y)$: x es la hermana de y, $p(x,y,z)$: x presenta a y con z.

1.1) Ema no ama a nadie.
1.2) No todos aman a Juan.
1.3) Juan no ama a Ema.
1.4) Nadie ama a Ricardo.
1.5) Nadie ama a todos.
1.6) No todos aman a alguien.
1.7) Juan tiene hermanos.
1.8) Ema no tiene hermanas.
1.9) Nadie presento a Andrés con Marta.
1.10) Andrés no le presentó alguien a Carla.
1.11) Juan no fue presentado a alguien por Ema.
1.12) No todos fallaron en presentar a Ricardo con Ema.
1.13) No todos presentan personas.
1.14) Andrés se presentó él mismo con Ema.

2. $s(x)$: x es estudiante
   $c(x)$: x es una historieta
   $r(x, y)$: x lee y
   $f(x)$: x es profesor/a.
   $w(x)$: x es íntegro
   $e(x, y)$: x escribe y
   $b(x)$: x es un libro
   $g(x)$: x obtiene un buen título
   $l(x, y)$: x escucha a y
   $h(x, y)$: x es profesor de y
   $p(x)$: x es poesía
   $a(x, y, z)$: x asigna y a z

2.1) Todos los estudiantes leen algún libro.
2.2) Algunos estudiantes leen libros e historietas.
2.3) Los estudiantes no leen todos los libros.
2.4) Los estudiantes no solo leen historietas.
2.5) Algunos estudiantes que no leen libros obtendrán buenos títulos.
2.6) Algunos estudiantes escuchan a algunos de sus profesores.
2.7) No todos los estudiantes que no leen libros obtendrán buenos títulos.
2.8) No hay estudiantes que no escuchen a algunos de sus profesores.
2.9) No todos los estudiantes escuchan a todos sus profesores.
2.10) Un estudiante que no lee ni libros ni historietas no será íntegro.
2.11) Algunos estudiantes leen algunos libros asignados por sus profesores.
2.12) Cualquier estudiante que lea todos los libros asignados por sus profesores será integro y obtendrá un buen título.
2.13) Algunos estudiantes escriben poesía.
2.14) Todos los estudiantes leen algo de poesía.
2.15) Algunos estudiantes íntegros que no obtienen un buen título, leen y escriben poesía.
2.16) No todos los estudiantes que leen todas las historietas no leen libros.

P16. Usando las abreviaciones del ejercicio 15.2 escriba en lenguaje natural.

1. $\neg(\forall x\ s(x) \Rightarrow (\exists y\ c(y) \wedge r(x, y)))$
2. $(\exists x(\exists y\ f(x) \wedge s(y) \wedge h(x, y) \wedge l(x, y)))$
3. $\neg(\forall x\ f(x) \Rightarrow (\forall y\ s(y) \wedge h(x, y) \Rightarrow l(x, y))$
4. $\neg(\exists x\ f(x) \wedge \neg(\exists y\ s(y) \wedge h(x, y) \wedge l(x, y)))$

5. $(\forall x\ s(x) \wedge (\forall y\ f(y) \wedge h(x,y) \Rightarrow l(x,y)) \Rightarrow (\exists z\ b(z) \wedge r(x,z) \wedge g(x)))$
6. $(\exists x\ f(x) \wedge (\exists y\ b(y) \wedge e(x,y)) \wedge \neg(\exists z\ p(z) \wedge e(x,z)))$
7. $\neg(\exists x\ b(x) \wedge (\forall y s(y) \Rightarrow r(y,x)))$
8. $(\exists x\ p(x) \wedge (\forall y\ s(y) \Rightarrow \neg e(x,y)))$
9. $(\forall x\ (s(x) \vee f(x)) \wedge (\exists y\ p(y) \wedge e(x,y)) \Rightarrow w(x) \wedge \neg(\exists z\ c(x) \wedge r(x,z)))$
10. $(\exists x\ f(x) \wedge (\forall y\ (p(y) \wedge \neg e(x,y)) \Rightarrow \neg r(x,y)))$
11. $(\forall x\ s(x) \wedge (\exists y\ c(y) \wedge r(x,y)) \wedge \neg(\exists z\ (b(z) \vee p(z)) \wedge r(x,z) \Rightarrow \neg(g(x) \vee w(x)))$

P17. Lleve a clausulas las proposiciones del ejercicio anterior.

P18. Demuestre usando reglas de inferencia, reglas de reemplazo y métodos de demostración.

1. $$\begin{array}{l} (\forall x\ e(x) \Rightarrow (\forall y\ f(y) \Rightarrow g(x,y))) \\ (\exists x\ e(x) \wedge (\exists y\ \neg g(x,y))) \\ \hline \therefore\ \neg(\forall x\ f(x)) \end{array}$$

2. $$\begin{array}{l} (\forall x\ o(x) \Rightarrow (\forall y\ r(y) \Rightarrow \neg l(x,y))) \\ (\forall x\ o(x) \Rightarrow (\exists y\ h(y) \wedge l(x,y))) \\ (\exists x\ o(x)) \\ \hline \therefore\ (\exists x\ h(x) \wedge \neg r(x)) \end{array}$$

3. $$\begin{array}{l} (\forall x(\exists y\ d(y) \wedge k(y,x)) \Rightarrow (\forall z\ a(z) \Rightarrow h(x,z))) \\ (\forall x(\forall y\ f(x,y) \Rightarrow \neg h(x,y))) \\ \neg(\forall x\ a(x) \Rightarrow \neg d(x)) \\ (\forall x\ c(x) \Rightarrow (\forall y\ k(y,x))) \\ \hline \therefore\ (\forall x\ c(x) \Rightarrow (\exists y\ d(y) \wedge \neg f(x,y))) \end{array}$$

4. $$\begin{array}{l} (\forall x\ d(x) \Rightarrow m(x)) \\ (\forall x\ [p(x) \wedge (\exists y\ m(y) \wedge w(x,y))] \Rightarrow g(x)) \\ (\exists x\ p(x) \wedge o(x) \wedge (\exists y\ n(y) \wedge d(y) \wedge w(x,y))) \\ \hline \therefore\ (\exists x\ p(x) \wedge o(x) \wedge g(x)) \end{array}$$

5. $$\begin{array}{l} (\exists x\ p(x) \wedge (\forall y\ s(y) \Rightarrow t(x,y))) \\ (\forall x\ [p(x) \wedge \neg(\forall y\ w(y) \Rightarrow a(y,x))] \Rightarrow (\forall z\ b(x,z) \Rightarrow s(z))) \\ (\forall x\ p(x) \Rightarrow \neg(\exists y\ w(y) \wedge (t(x,y) \vee a(y,x)))) \\ \hline \therefore\ (\exists x\ p(x) \wedge (\forall y\ w(y) \Rightarrow \neg(a(y,x) \vee b(x,y))) \end{array}$$

6. $$\begin{array}{l} (\forall x\ a(x) \wedge \neg(\forall y\ d(x,y) \Rightarrow r(x,y)) \Rightarrow (\forall z\ t(z,x) \Rightarrow w(z))) \\ \neg(\exists x\ (\exists y\ t(y,x) \wedge \neg d(x,y))) \\ \neg(\forall x\ a(x) \Rightarrow (\forall y\ t(y,x) \Rightarrow r(x,y)))) \\ \hline \therefore\ (\exists x\ w(x)) \end{array}$$

P19. Simbolice usando las siguientes funciones proposicionales:

1.
$d(x,y)$:	x vence a y	$a(x)$:	x es albino
$e(x,y)$:	x es enemigo de y	$f(x)$:	x es un pez
$f(x,y)$:	x es amigo de y	$m(x)$:	x es un mamífero
$s(x,y)$:	x es más rápido que y	$p(x)$:	x es una persona
$m(x,y)$:	x es más cruel que y	$w(x)$:	x es una ballena
$z(x,y)$:	x teme a y	$n(x)$:	x es un animal
$b(x,y)$:	x es mejor navegante que y	$s(x)$:	x lanza un chorro
$q(x)$:	x está en el barco	$g(x)$:	x es un dios

(Ind. Dios y El Diablo, cuando están escritos con mayúscula son nombres propios y por lo tanto elementos del dominio de discurso)

1.1) Moby Dick es una ballena.

1.2) Una ballena es un mamífero.

1.3) Moby Dick es enemiga de Ahab.

1.4) Moby Dick no es El Diablo.

1.5) Ishmael no es albino.

1.6) Ishmael es amigo de Moby Dick.

1.7) Ishmael no es Dios.

1.8) Moby Dick no es un pez.

1.9) Moby Dick vence a Ahab.

1.10) Ahab es más cruel que El Diablo.

1.11) Ishmael es amigo de todas las personas

1.12) Ahab no es enemigo de Ishmael.

1.13) Moby Dick es albina.

1.14) Nadie es más cruel que Ahab.

1.15) Ahab es más cruel que todas las personas.

1.16) Dios no es una ballena.

1.17) El Diablo no es amigo de nadie.

1.18) Ahab no tiene amigos.

1.19) Ishmael no vence a Ahab.

1.20) Dios no es El Diablo.

1.21) Todos excepto Ahab temen a Moby Dick.

1.22) Nadie excepto Ahab puede vencer a Moby Dick.

1.23) Moby Dick es la única ballena albina.

1.24) Solo Ishmael es amigo de Moby Dick.

1.25) Nadie es más cruel que Ahab excepto el Diablo.

1.26) Todas las ballenas, excepto Moby Dick son amigas de Ahab.

1.27) Moby Dick es la ballena más rápida.

1.28) Ahab es la persona más cruel.

1.29) Ningún animal excepto las ballenas lanzan chorros.

1.30) Ishmael es el mejor navegante en el barco.

1.31) Ahab tiene al menos dos enemigos.

1.32) Hay un dios.

1.33) Moby Dick tiene exactamente dos amigos.

1.34) Hay al menos dos ballenas albinas.

2.
$c(x)$:	x es un diputado	$n(x)$:	x es de Dakota del Norte
$d(x)$:	x es una deidad	$p(x)$:	x es un planeta
$b(x)$:	x es un edificio	$l(x)$:	x está en la manzana

2.1) Hay al menos tres diputados de Dakota del Norte.

2.2) Hay a lo mas tres edificios en la manzana.

2.3) Hay exactamente tres formas de deidad.

2.4) Hay al menos cinco planetas.

3.

$b(x)$:	x es un libro	$t(x)$:	x está en la mesa
$n(x)$:	x es una novela	$c(x)$:	x es un edificio del capitolio
$i(x,y)$:	x está en y	$p(x)$:	x es un conductor de Pony Express
$b(x,y)$:	x es más valiente que y	$o(x)$:	x es huérfano
$f(x,y)$:	x es más rápido que y	$f(x)$:	x era famoso
$m(x)$:	x es un hombre	$s(x)$:	x creó Pony Express
$b(x)$:	x era un hombre de negocios	$l(x)$:	x perdió mucho dinero

3.1) El libro en la mesa es una novela.

3.2) El libro en la mesa es La Guerra y la Paz.

3.3) El edificio del capitolio está en Washington DC.

3.4) El conductor de Pony Express más valiente fue Billy Tate, quien era huérfano.

3.5) El conductor de Pony express más rápido fue Bob Haslam.

3.6) El único estudiante de la clase que no se expresa claramente es Andrés.

3.7) Andrés es el peor estudiante de la clase.

3.8) Andrés es el único perro de la clase.

3.9) Trufa es el único estudiante que no tiene identificación.

3.10) Trufa es el estudiante más pequeño de la clase.

3.11) Todos los estudiantes excepto Trufa y Andrés dieron su último examen.

3.12) A todos los estudiantes excepto Trufa les agrada Andrés.

3.13) Los únicos estudiantes en la clase que no leen bien son Trufa y Andrés.

3.14) Trufa es el estudiante menos obediente de la clase.

3.15) Trufa es el único gato en la clase.

3.16) Hay al menos un gato y un único perro en la clase.

3.17) Hay al menos dos estudiantes en la clase que no leen bien.

3.18) Hay a lo más un estudiante en la clase que maulla.

3.19) Hay a lo más dos estudiantes que no pasarán.

3.20) Hay dos estudiantes que necesitan un tutor.

3.21) Al menos tres estudiantes en la clase obtendrán una A.

3.22) Al menos cuatro estudiantes pasarán.

3.23) No más de dos estudiantes obtendrán una B.

3.24) No es verdad que a lo más dos estudiantes obtendrán una A.

3.25) No es verdad que al menos tres estudiantes no pasarán.

3.26) El estudiante más obediente en la clase obtendrá una A.

P20. Construya demostraciones para:

1. $(\forall x\ f(x) \wedge (\exists y f(y) \wedge x \neq y) \Rightarrow (p(x,b) \vee p(b,x))$
   $f(a) \wedge f(b)$
   $g(a) \wedge \neg g(b)$
   ____
   $\therefore p(a,b) \vee p(b,a)$

2. $(\exists x\ p(x) \land (\forall y\ p(y) \Rightarrow x = y) \land (x = a))$
   $p(b) \lor p(c)$
   $\therefore a = b \lor a = c$

3. $(\exists x\ p(x) \land (\forall y\ p(y) \Rightarrow x = y) \land (\exists z\ q(z) \land (\forall w\ q(w) \Rightarrow z = w) \land z = x))$
   $q(a)$
   $\therefore (\forall x\ p(x) \Rightarrow x = a)$

4. $(\exists x \exists y \exists z\ f(x) \land f(y) \land f(z) \land x \neq y \land x \neq z \land y \neq z)$
   $(\exists x\ f(x) \land g(x) \land (\forall y\ f(y) \land g(y) \Rightarrow x = y))$
   $(\forall x\ \neg g(x) \Rightarrow h(x))$
   $\therefore (\exists x \exists y\ h(x) \land h(y) \land x \neq y)$

5. $(\exists x \exists y \exists z\ f(x) \land f(y) \land f(z) \land x \neq y \land x \neq z \land y \neq z)$
   $(\forall x\ f(x) \Rightarrow g(x))$
   $(\forall x \forall y \forall z \forall w\ (g(x) \land g(y) \land g(z) \land g(w)) \Rightarrow (x = y \lor x = z \lor x = w \lor y = z \lor y = w \lor z = w))$
   $\therefore (\exists x \exists y \exists z\ f(x) \land f(y) \land f(z) \land x \neq y \land x \neq z \land y \neq z \land (\forall w\ f(w) \Rightarrow (w = x \lor w = y \lor w = z)))$

6. $f(a) \iff (\exists x\ f(x) \land x = a)$

7. $(\exists x (\forall y\ f(y) \Leftrightarrow x = y)) \iff (\exists x\ f(x) \land (\forall y\ f(y) \Leftrightarrow x = y))$

8. $(\forall x \forall y \forall z\ (x = y \land y = z) \Rightarrow x = z)$

9. $(\forall x \forall y \forall z \forall w\ (x = y \land y = z \land z = w) \Rightarrow x = w)$

10. $((\exists x\ f(x)) \land (\forall x \forall y\ (f(x) \land f(y)) \Rightarrow x = y)) \iff (\exists x\ f(x) \land (\forall y\ f(y) \Rightarrow x = y))$

Capítulo 4

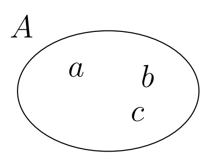
Conjuntos

Definición 4.1. Un conjunto es una colección de objetos arbitrarios.

Estos objetos son completamente arbitrarios no necesitan tener algún tipo de relación entre ellos, no existe ninguna restricciones para los elemento de un conjunto.

Hay varias maneras de representar un conjunto:

1. **Diagrama:** Este sirve solo cuando los objetos pueden representarse por una figura y tienen una cantidad relativamente pequeña de elementos que permita una correcta visualización. Por ejemplo:



2. **Por extensión:** al igual que los diagramas solo es útil con pocos elementos, la ventaja respecto al diagrama es que permite ser escrito en una línea de texto. Por ejemplo:
$$A = \{a, b, c\}$$

3. **Por comprensión:** permite describir conjuntos grandes, incluso infinitos, pero los elementos del conjunto deben estar relacionados por alguna propiedad que permita describirlos. Es decir, su descripción es de la forma:

$$\{x : p(x)\}$$

donde $p(x)$ es una forma proposicional unaria.

Por ejemplo:

$$A = \{x : x \text{ es una de las tres primeras letras del abecedario}\}$$

Ejemplos de conjuntos:

1. $\mathbb{N}$
2. $\mathbb{Z}$
3. $\mathbb{Q}$
4. $\mathbb{R}$

4. $A = \{x : x \text{ es una letra del abecedario}\}$
5. $B = \{x : x \text{ es una letra del alfabeto griego}\}$
6. $C = \{x : x \text{ es un alumno de esta clase}\}$
7. $D = \{x : x \text{ es cualquier cosa o persona en esta sala}\}$

La proposición $a \in A$ es verdadera si el elemento "a" está en el conjunto "A".

La proposición $a \notin A$ corresponde a la negación de $a \in A$.

Por notación, los conjuntos se denotan con letras mayúsculas y los elementos con letras minúsculas.

Por ejemplo, si usamos los conjuntos de los ejemplos anteriores.

1. $\text{g} \in A$
2. $7 \notin B$
3. $5 \in \mathbb{N}$
4. $\text{Superman} \notin C$
5. $\text{Lili} \in D$
6. $\pi \notin \mathbb{Z}$

En los conjuntos no importa el orden ni la repetición de elementos, es decir:

$$A = \{a, b, c\} = \{a, b, c, a\} = \{b, c, a\} = \{b, c, a, c, c\}$$
$$\mathbb{Q} = \left\{q : \left(\exists n\ \exists d\ n \in \mathbb{Z} \wedge d \in \mathbb{N} \wedge q = \frac{n}{d}\right)\right\}$$

Definición 4.2. El conjunto vacío, denotado por $\varnothing$, es el conjunto que no tiene elementos.

Observación 4.1. Otra manera de denotar el conjunto vacío es $\{\ \}$.

El conjunto $\{\varnothing\}$ no es el conjunto vacío, este corresponde a un conjunto que tiene como elemento al conjunto vacío.

La forma proposicional $x \in \varnothing$ es siempre falsa. De este modo se establece que $(\forall x\ x \notin \varnothing)$.

Definición 4.3. El conjunto universo, denotado por $\mathbf{U}$, es el conjunto que tiene todos los elementos.

Es decir, la forma proposicional $x \in \mathbf{U}$ es siempre verdadera. De este modo se establece que $(\forall x\ x \in \mathbf{U})$

Observación 4.2. Claramente la definición del conjunto universo, depende del problema que se esté abordando, este conjunto universo es el dominio de discurso de nuestro problema.

Definición 4.4. Diremos que un conjunto es un síngleton si tiene un único elemento.

4.1. Relaciones entre conjuntos

Definición 4.5. Diremos que los conjuntos A y B son iguales si tienen exactamente los mismos elementos y lo denotamos por $A = B$. Es decir:

$$(\forall x\ x \in A \iff x \in B)$$

En caso contrario diremos que A es distinto de B y lo denotaremos por $A \neq B$

Algunas propiedades de la igualdad que son fáciles de verificar son:

1. $A = A$

   Demostración.

1)	Sea x cualquiera	
2)	$x \in A \Leftrightarrow x \in A$	Tautología
3)	$(\forall x\ x \in A \Leftrightarrow x \in A)$	G.U. 2
4)	$A = A$	Def. $=$

■

2. $A = B \iff B = A$

   Demostración.

1)	$A = B$	Suposición D.C.
2)	$(\forall x\ x \in A \Leftrightarrow x \in B)$	Def. $=$
3)	Sea x cualquiera	
4)	$x \in A \Leftrightarrow x \in B$	I.U. 2
5)	$x \in B \Leftrightarrow x \in A$	Conm. 4
6)	$(\forall x\ x \in B \Leftrightarrow x \in A)$	G.U. 5
7)	$B = A$	Def. $=$
8)	$A = B \Rightarrow B = A$	D.C. 1–7

■

3. $(A = B \wedge B = C) \implies A = C$

   Demostración.

1)	$A = B \wedge B = C$	Suposición D.C.
2)	$A = B$	Simp. 1
3)	$B = C$	Simp. 1
4)	$(\forall x\ x \in A \Leftrightarrow x \in B)$	Def. $=$ 2
5)	$(\forall x\ x \in B \Leftrightarrow x \in C)$	Def. $=$ 3
6)	Sea x cualquiera	
7)	$x \in A \Leftrightarrow x \in B$	I.U. 4
8)	$x \in B \Leftrightarrow x \in C$	I.U. 5
9)	$x \in A \Leftrightarrow x \in C$	S.H. 4 y 5
10)	$(\forall x\ x \in A \Leftrightarrow x \in C)$	G.U. 9
11)	$A = C$	Def. $=$ 10
12)	$(A = B \wedge B = C) \Rightarrow A = C$	D.C. 1–11

∎

4. $A \neq B \implies (\exists x\ (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B))$

   Demostración.

1)	$A \neq B$	Suposición D.C.
2)	$\neg(\forall x\ x \in A \Leftrightarrow x \in B)$	Def. $=$ 1
3)	$(\exists x\ \neg(x \in A \Leftrightarrow x \in B))$	Neg. 2
4)	$(\exists x\ \neg((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)))$	Bicon. 3
5)	$(\exists x\ (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A))$	Neg. 4
6)	$A \neq B \Rightarrow (\exists x\ (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B))$	D.C. 1–5

∎

Definición 4.6. Diremos que un conjunto A es un subconjunto de B, si todos los elementos de A también son elementos de B, y lo denotamos por $A \subseteq B$. Es decir:

$$A \subseteq B \iff (\forall x\ x \in A \Rightarrow x \in B)$$

Otra forma de decir que $A \subseteq B$ es decir que A está incluido (o contenido) en el conjunto B.

Propiedades:

1. $A \subseteq A$

   Demostración.

1)	Sea x cualquiera	
2)	$x \notin A \vee x \in A$	Tautología
3)	$x \in A \Rightarrow x \in A$	Cond. 2
4)	$(\forall x\ x \in A \Rightarrow x \in A)$	G.U. 3
5)	$A \subseteq A$	Definición de $\subseteq$

∎

2. $\varnothing \subseteq A$

   Demostración.

1)	$(\forall x\ x \notin \varnothing)$	Def. $\varnothing$
2)	Sea x cualquiera	
3)	$x \notin \varnothing$	I.U. 1
4)	$x \notin \varnothing \vee x \in A$	Ad. 3
5)	$x \in \varnothing \Rightarrow x \in A$	Cond. 4
6)	$(\forall x\ x \in \varnothing \Rightarrow x \in A)$	G.U. 5
7)	$\varnothing \subseteq A$	Def. $\subseteq$ 6

∎

3. $(A \subseteq B \wedge B \subseteq A) \implies A = B$

   Demostración.

1)	$A \subseteq B \wedge B \subseteq A$	Suposición D.C.
2)	$A \subseteq B$	Simp. 1
3)	$B \subseteq A$	Simp. 1
4)	$(\forall x\ x \in A \Rightarrow x \in B)$	Def. $\subseteq$ 2
5)	$(\forall x\ x \in B \Rightarrow x \in A)$	Def. $\subseteq$ 3
6)	Sea x cualquiera	
7)	$x \in A \Rightarrow x \in B$	I.U. 4
8)	$x \in B \Rightarrow x \in A$	I.U. 5
9)	$x \in A \Leftrightarrow x \in B$	Bicon. 7 y 8
10)	$(\forall x\ x \in A \Leftrightarrow x \in B)$	G.U. 9
11)	$A = B$	Def. $=$ 10
12)	$(A \subseteq B \wedge B \subseteq A) \implies A = B$	D.C. 1–11

■

4. $(A \subseteq B \wedge B \subseteq C) \implies A \subseteq C$

Demostración.

1)	$A \subseteq B \wedge B \subseteq C$	Suposición D.C.
2)	$A \subseteq B$	Simp. 1
3)	$B \subseteq C$	Simp. 1
4)	$(\forall x\ x \in A \Rightarrow x \in B)$	Def. $\subseteq$ 2
5)	$(\forall x\ x \in B \Rightarrow x \in C)$	Def. $\subseteq$ 3
6)	Sea x cualquiera	
7)	$x \in A \Rightarrow x \in B$	I.U. 4
8)	$x \in B \Rightarrow x \in C$	I.U. 5
9)	$x \in A \Rightarrow x \in C$	S.H. 7 y 8
10)	$(\forall x\ x \in A \Rightarrow x \in C)$	G.U. 9
11)	$A \subseteq C$	Def. $\subseteq$ 10
12)	$(A \subseteq B \wedge B \subseteq C) \implies A \subseteq C$	D.C. 1–11

■

Definición 4.7. El conjunto de las partes de A, denotado por $\mathcal{P}(A)$, es el conjunto cuyos elementos son todos los subconjuntos de A. Es decir:

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

Ejemplo: $A = \{a, b, c\}$, $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

Observación 4.3. Debemos notar que los elementos del conjunto $\mathcal{P}(A)$ son conjuntos.

4.2. Operaciones entre conjuntos

Definición 4.8. Se define la diferencia entre el conjunto A y el conjunto B, denotada por $A \setminus B$ como los elementos del conjunto A que no pertenecen al conjunto B. Es decir:

$$A \setminus B = \{x : x \in A \wedge x \notin B\}$$

O equivalentemente:

$$(\forall x\ x \in A \setminus B \Leftrightarrow (x \in A \wedge x \notin B))$$

Propiedades:

1. $A \setminus \varnothing = A$

   Demostración.

1)	$(\forall x\ x \in A \setminus \varnothing \Leftrightarrow (x \in A \wedge x \notin \varnothing))$	Def. $\setminus$
2)	Sea x cualquiera	
3)	$x \in A \setminus \varnothing \Leftrightarrow (x \in A \wedge \underbrace{x \notin \varnothing}_{V})$	I.U. 1
4)	$x \in A \setminus \varnothing \Leftrightarrow x \in A$	Taut. 3
5)	$(\forall x\ x \in A \setminus \varnothing \Leftrightarrow x \in A)$	G.U. 4
6)	$A \setminus \varnothing = A$	Def. = 5

■

2. $A \setminus \mathbf{U} = \varnothing$

   Demostración.

1)	$(\forall x\ x \in A \setminus \mathbf{U} \Leftrightarrow (x \in A \wedge x \notin \mathbf{U}))$	Def. $\setminus$
2)	Sea x cualquiera	
3)	$x \in A \setminus \mathbf{U} \Leftrightarrow (x \in A \wedge \underbrace{x \notin \mathbf{U}}_{F})$	I.U. 1
4)	$x \in A \setminus \mathbf{U} \Leftrightarrow F$	Taut. 3
5)	$x \in \varnothing \Leftrightarrow F$	Def. $\varnothing$
6)	$x \in A \setminus \mathbf{U} \Leftrightarrow x \in \varnothing$	4 y 5
7)	$(\forall x\ x \in A \setminus \mathbf{U} \Leftrightarrow x \in \varnothing)$	G.U. 6
8)	$A \setminus \mathbf{U} = \varnothing$	Def. = 7

■

3. $\varnothing \setminus A = \varnothing$

   Demostración.

1)	$(\forall x\ x \in \varnothing \setminus A \Leftrightarrow (x \in \varnothing \wedge x \notin A))$	Def. $\setminus$
2)	Sea x cualquiera	
3)	$x \in \varnothing \setminus A \Leftrightarrow (\underbrace{x \in \varnothing}_{F} \wedge x \notin A)$	I.U. 1
4)	$x \in \varnothing \setminus A \Leftrightarrow F$	Tautología 3
5)	$x \in \varnothing \Leftrightarrow F$	Tautología
6)	$x \in \varnothing \setminus A \Leftrightarrow x \in \varnothing$	4 y 5
7)	$(\forall x\ x \in \varnothing \setminus A \Leftrightarrow x \in \varnothing)$	I.U. 6
8)	$\varnothing \setminus A = \varnothing$	Def. = 7

■

4. $A \setminus A = \varnothing$

   Demostración.

1)	$(\forall x\ x \in A \setminus A \Leftrightarrow (x \in A \wedge x \notin A))$	Def. $\setminus$
2)	Sea x cualquiera	
3)	$x \in A \setminus A \Leftrightarrow (x \in A \wedge x \notin A)$	I.U. 1
4)	$x \in A \setminus A \Leftrightarrow F$	Tautología 3

5)	$x \in \varnothing \Leftrightarrow F$	Def. $\varnothing$
6)	$x \in A \setminus A \Leftrightarrow x \in \varnothing$	4 y 5
7)	$(\forall x\ x \in A \setminus A \Leftrightarrow x \in \varnothing)$	I.U. 6
8)	$A \setminus A = \varnothing$	Def. = 7

■

Un caso particular importante es la diferencia con el conjunto universo. De este modo se define el complemento de un conjunto A, denotado por A^c como la diferencia entre el conjunto universo y A. Es decir:

$$A^c = \mathbf{U} \setminus A$$

Lo que es equivalente a;

$$A^c = \{x : x \notin A\}$$

O:

$$(\forall x\ x \in A^c \Leftrightarrow x \notin A)$$

Propiedades:

1. $\varnothing^c = \mathbf{U}$

   Demostración.

1)	$(\forall x\ x \notin \varnothing)$	Def. $\varnothing$
2)	$(\forall x\ x \in \mathbf{U}))$	Def. $\mathbf{U}$
3)	Sea x cualquiera	
4)	$x \notin \varnothing$	I.U. 1
5)	$x \in \varnothing^c$	Def. $\varnothing^c$ 4
6)	$x \in \mathbf{U}$	I.U. 2
7)	$x \in \varnothing^c \Leftrightarrow x \in \mathbf{U}$	5 y 6
8)	$(\forall x\ x \in \varnothing^c \Leftrightarrow x \in \mathbf{U})$	G.U. 7
9)	$\varnothing^c = \mathbf{U}$	Def. = 8

■

2. $\mathbf{U}^c = \varnothing$

   Demostración.

1)	$(\forall x\ x \notin \varnothing)$	Def. $\varnothing$
2)	$(\forall x\ x \in \mathbf{U}))$	Def. $\mathbf{U}$
3)	Sea x cualquiera	
4)	$x \notin \varnothing$	I.U. 1
5)	$x \in \mathbf{U}$	I.U. 2
6)	$x \notin \varnothing \Leftrightarrow x \in \mathbf{U}$	4 y 5
7)	$x \in \varnothing \Leftrightarrow x \notin \mathbf{U}$	Taut. 6
8)	$x \in \varnothing \Leftrightarrow x \in \mathbf{U}^c$	Def. $\mathbf{U}^c$
9)	$(\forall x\ x \in \varnothing \Leftrightarrow x \in \mathbf{U}^c)$	G.U. 8
10)	$\varnothing = \mathbf{U}^c$	Def. = 9

■

3. $(A^c)^c = A$

   Demostración.

1)	Sea x cualquiera	
2)	$x \in A \Leftrightarrow x \in A$	Taut.
3)	$\neg\neg(x \in A) \Leftrightarrow x \in A$	D.N. 2
4)	$\neg(x \notin A) \Leftrightarrow x \in A$	Def. $\notin$ 3
5)	$\neg(x \in A^c) \Leftrightarrow x \in A$	Def. A^c 4
6)	$x \notin A^c \Leftrightarrow x \in A$	Def. $\notin$ 5
7)	$x \in (A^c)^c \Leftrightarrow x \in A$	Def. $(A^c)^c$ 6
8)	$(\forall x\ x \in (A^c)^c \Leftrightarrow x \in A)$	G.U. 7
9)	$(A^c)^c = A$	Def $=$ 8

■

Definición 4.9. Se define la unión del conjunto A y el conjunto B, denotada por $A \cup B$, como:

$$A \cup B = \{x : x \in A \vee x \in B\}$$

O equivalentemente:

$$(\forall x\ x \in A \cup B \Leftrightarrow (x \in A \vee x \in B))$$

Definición 4.10. Se define la intersección del conjunto A y el conjunto B, denotada por $A \cap B$, como:

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

O equivalentemente:

$$(\forall x\ x \in A \cap B \Leftrightarrow (x \in A \wedge x \in B))$$

Propiedades:

1. Conmutatividad: $A \cup B = B \cup A$
   $A \cap B = B \cap A$

   Demostración.

1)	$(\forall x\ x \in A \cup B \Leftrightarrow (x \in A \vee x \in B))$	Def. $A \cup B$
2)	$(\forall x\ x \in B \cup A \Leftrightarrow (x \in B \vee x \in A))$	Def. $B \cup A$
3)	Sea x cualquiera	
4)	$x \in A \cup B \Leftrightarrow (x \in A \vee x \in B)$	I.U. 1
5)	$x \in A \cup B \Leftrightarrow (x \in B \vee x \in A)$	Conm. 4
6)	$x \in B \cup A \Leftrightarrow x \in B \cup A$	I.U. 2
7)	$x \in A \cup B \Leftrightarrow x \in B \cup A$	5 y 6
8)	$(\forall x\ x \in A \cup B \Leftrightarrow x \in B \cup A)$	G.U. 7
9)	$A \cup B = B \cup A$	Def. $=$ 8

■

2. Asociatividad: $(A \cup B) \cup C = A \cup (B \cup C)$
   $(A \cap B) \cap C = A \cap (B \cap C)$

   Demostración.

1)	$(\forall x\ x \in (A\cup B)\cup C \Leftrightarrow (x \in (A\cup B) \vee x \in C))$	Def. $\cup$
2)	$(\forall x\ x \in A\cup (B\cup C) \Leftrightarrow (x \in A \vee x \in B\cup C))$	Def. $\cup$
3)	Sea x cualquiera	
4)	$x \in (A\cup B)\cup C \Leftrightarrow (x \in (A\cup B) \vee x \in C)$	I.U. 1
5)	$x \in (A\cup B)\cup C \Leftrightarrow ((x \in A \vee x \in B) \vee x \in C)$	Def. $\cup$ 4
6)	$x \in (A\cup B)\cup C \Leftrightarrow (x \in A \vee (x \in B \vee x \in C))$	Asoc. 5
7)	$x \in (A\cup B)\cup C \Leftrightarrow (x \in A \vee x \in B\cup C)$	Def. $\cup$ 6
8)	$x \in (A\cup B)\cup C \Leftrightarrow x \in A\cup (B\cup C)$	Def. $\cup$ 7
9)	$x \in A\cup (B\cup C) \Leftrightarrow (x \in A \vee x \in B\cup C)$	I.U. 2
10)	$x \in (A\cup B)\cup C \Leftrightarrow x \in A\cup (B\cup C)$	8 y 9
11)	$(\forall x\ x \in (A\cup B)\cup C \Leftrightarrow x \in A\cup (B\cup C))$	G.U. 9
12)	$(A\cup B)\cup C = A\cup (B\cup C)$	Def. $=$ 11

■

3. Distributividad: $A\cup (B\cap C) = (A\cup B)\cap (A\cup C)$
   $A\cap (B\cup C) = (A\cap B)\cup (A\cap C)$

4. $A\cup \varnothing = A$

   Demostración.

1)	$(\forall x\ x \in A\cup\varnothing \Leftrightarrow (x \in A \vee \underbrace{x \in \varnothing}_{F}))$	Def. $\cup$
2)	$(\forall x\ x \in A\cup\varnothing \Leftrightarrow x \in A)$	Tautología
3)	$A\cup\varnothing = A$	Def. $=$

■

5. $A\cup \mathbf{U} = \mathbf{U}$

6. $A\cap \varnothing = \varnothing$

7. $A\cap \mathbf{U} = A$

8. $A\cup A^c = \mathbf{U}$

9. $A\cap A^c = \varnothing$

10. Leyes de De Morgan: $(A\cup B)^c = A^c\cap B^c$
    $(A\cap B)^c = A^c\cup B^c$

    Demostración.

Sea x cualquiera
$x \in A\cup B \Leftrightarrow (x \in A \vee x \in B)$
$x \notin A\cup B \Leftrightarrow \neg(x \in A \vee x \in B)$
$x \notin A\cup B \Leftrightarrow (x \notin A \wedge x \notin B)$
$x \in (A\cup B)^c \Leftrightarrow (x \in A^c \wedge x \in B^c)$
$x \in (A\cup B)^c \Leftrightarrow (x \in A^c \cap B^c)$
$(\forall x\ x \in (A\cup B)^c \Leftrightarrow (x \in A^c \cap B^c))$
$(A\cup B)^c = A^c\cap B^c$

■

11. $A \setminus B = A \cap B^c$

Demostración.

$$\begin{array}{ll}
(\forall x\ x \in A \setminus B \Leftrightarrow x \in A \land x \notin B) & \text{Def. } \setminus \\
(\forall x\ x \in A \setminus B \Leftrightarrow x \in A \land x \in B^c) & \text{Def. } B^c \\
(\forall x\ x \in A \setminus B \Leftrightarrow x \in A \cap B^c) & \text{Def. } \cap \\
A \setminus B = A \cap B^c & \text{Def. } =
\end{array}$$

■

12. $A \subseteq A \cup B,\ B \subseteq A \cup B$
    $A \cap B \subseteq A,\ A \cap B \subseteq B$

Un abuso de notación comúnmente utilizado es:

$$\begin{aligned}
(\forall x \in A, p(x)) &\iff (\forall x\ x \in A \Rightarrow p(x)) \\
(\exists x \in A, p(x)) &\iff (\exists x\ x \in A \land p(x))
\end{aligned}$$

Las negaciones son consistente con lo visto hasta ahora:

$$\begin{aligned}
\neg(\forall x \in A, p(x)) &\iff \neg(\forall x\ x \in A \Rightarrow p(x)) \\
&\iff (\exists x\ \neg(x \in A \Rightarrow p(x)) \\
&\iff (\exists x\ x \in A \land \neg p(x)) \\
&\iff (\exists x \in A, \neg p(x))
\end{aligned}$$

$$\begin{aligned}
\neg(\exists x \in A, p(x)) &\iff \neg(\exists x\ x \in A \land p(x)) \\
&\iff (\forall x\ \neg(x \in A \land p(x)) \\
&\iff (\forall x\ x \notin A \lor \neg p(x)) \\
&\iff (\forall x\ x \in A \Rightarrow \neg p(x)) \\
&\iff (\forall x \in A, \neg p(x))
\end{aligned}$$

4.3. Principio de inducción

La inducción matemática es un importante método de demostración en las matemáticas discretas. En esta primera parte veremos como la inducción las recurrencias y la recursividad son esencialmente lo mismo.

Ejemplo 4.1 (Torres de Hanoi)**.** El juego consiste en tres postes verticales, en uno de los postes se apila un número determinado de discos perforados por su centro (elaborados de madera), que determinará la complejidad de la solución. Los discos se apilan sobre uno de los postes en tamaño decreciente de abajo a arriba. No hay dos discos iguales, y todos ellos están apilados de mayor a menor radio –desde la base del poste hacia arriba– en uno de los postes, quedando los otros dos postes vacíos. El juego consiste en pasar todos los discos desde el poste ocupado (es decir, el que posee la torre) a uno de los otros postes vacíos. Para realizar este objetivo, es necesario seguir tres simples reglas:

1. Solo se puede mover un disco cada vez y para mover otro los demás tienen que estar en postes.
2. Un disco de mayor tamaño no puede estar sobre uno más pequeño que él mismo.
3. Solo se puede desplazar el disco que se encuentre arriba en cada poste.

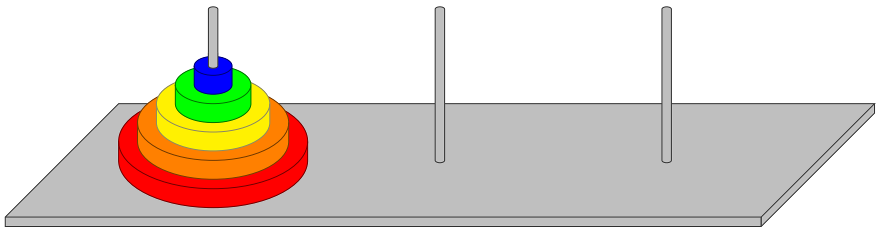


Figura 4.1: Torres de Hanoi

Supongamos que tenemos solo un disco. El problema resulta trivial. Lo mismo si tenemos dos, pero que pasa si tenemos n discos ¿cómo podemos encontrar la secuencia de movimientos que nos da la solución? Una manera de solucionarlo es con un procedimiento recursivo, sabemos resolverlo para $n = 1$, supondremos que sabemos que hacer en el caso $n - 1$ y a partir de esto encontraremos la solución.

Aquí hay varias preguntas que podemos hacer:¿Es posible hacerlo? y si esto es posible ¿Cómo lo hago? ¿Cuánto tiempo toma?

Procedimiento Hanoi(n: número de discos, i: torre de inicio, f: torre final)

```
if n = 1 then
    Mover disco de Torre i a torre f;
else
    m ⟵ Torre que no es i ni f;
    Hanoi(n − 1, i, m);
    Mover disco de Torre i a torre f;
    Hanoi(n − 1, m, f);
end
```

Este procedimiento recursivo funciona, pero ¿cómo podemos justificar que funciona? la razón es el principio de inducción.

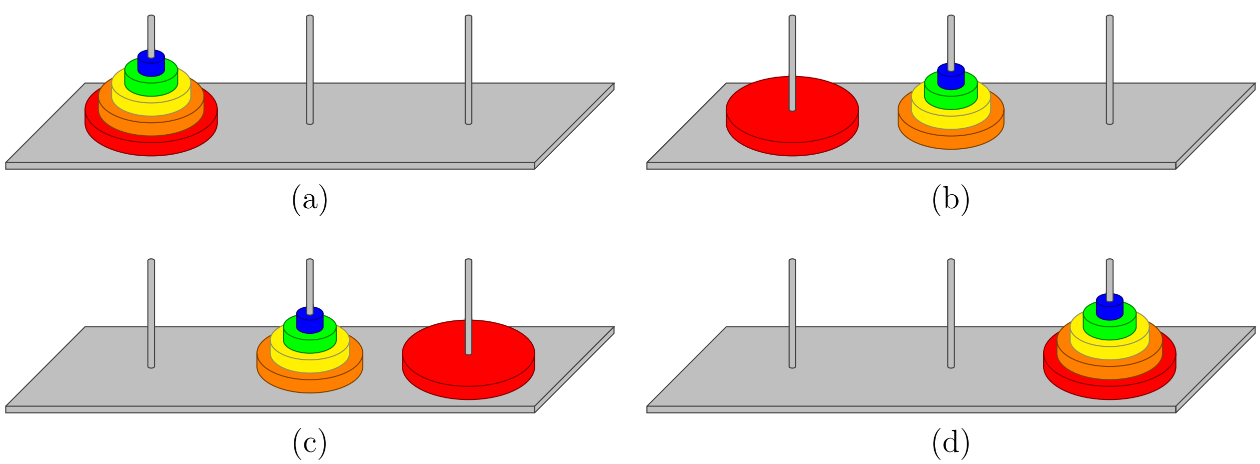


Figura 4.2: Solución Torres de Hanoi

Definición 4.11. Un conjunto S se dice inductivo si y solo si:

1. $1 \in S$
2. $\forall n \in S,\ n \in S \Rightarrow (n+1) \in S$

Observación 4.4. Todo conjunto inductivo incluye a $\mathbb{N}$

Teorema 4.1 (Teorema fundamental de Inducción Matemática)**.** *Sea $P(n)$ una función proposicional cuyo dominio de discurso es $\mathbb{N}$. Si $P(n)$ satisface las siguientes dos condiciones:*

1. *$P(1)$ es verdadera.*
2. *$(\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))$*

Entonces $\forall n \in \mathbb{N}, P(n)$ es verdadera.

Demostración. Sea K el conjunto de todos los enteros positivos para el cual $P(n)$ es cierta. Es decir:

$$K = \{k \in \mathbb{N} : P(k) \text{ es verdadera}\}$$

De 1 se observa que $1 \in K$.

De 2 se observa que $k \in K \Rightarrow (k+1) \in K$.

Por tanto K es un conjunto inductivo, de aquí, tomando en cuenta la Observación 4.4 $\mathbb{N} \subseteq K$. Y, por la definición de K, se sabe que $K \subseteq \mathbb{N}$. Por lo tanto, $K = \mathbb{N}$, es decir $P(n)$ es cierta para todo $n \in \mathbb{N}$. ■

En algunos casos también es útil considerar una segunda forma del teorema de inducción que es la siguiente:

Teorema 4.2. *Sea $P(n)$ una función proposicional cuyo dominio de discurso es $\mathbb{N}$. Si $P(n)$ satisface las siguientes dos condiciones:*

1. *$P(k)$ es verdadera.*
2. *$(\forall n \geq k, P(n) \Rightarrow P(n+1))$*

Entonces $\forall n \geq k, P(n)$ es verdadera.

4.3.1. Demostraciones por inducción

El método de demostración por inducción utiliza tres pasos.

1. **Base de inducción.** Se verifica que $P(1)$ es verdadera.
2. **Hipótesis de inducción.** Se supone que $P(n)$ es verdadero. Usualmente denotaremos la hipótesis de inducción por Ⓗ.
3. **Caso $n+1$.** Se prueba que $P(n) \Rightarrow P(n+1)$

Podemos probar que el algoritmo `Hanoi` funciona y que demora $2^n - 1$ pasos. Primero veamos que funciona:

Base. Si $n = 1$ el procedimiento `Hanoi` funciona sin problemas ya que considera la entrada "if".

Hipótesis de inducción. El procedimiento `Hanoi` funciona para n.

Paso inductivo. Veamos que para $n \geq 1$, `Hanoi`$(n{+}1, i, f)$ funciona. Como $n{+}1 > 1$ el procedimiento entra a "else", por hipótesis de inducción el procedimiento `Hanoi`(n, i, m) funciona correctamente, claramente podemos mover el disco más grande a la posición vacía y nuevamente por hipótesis de inducción `Hanoi`(n, m, f) funciona.

Ahora, veamos que h_n que es el número de movimientos para mover n discos en las torres de Hanoi es $2^n - 1$. Primero, observemos que:

$$\begin{aligned} h_1 &= 1 \\ h_n &= h_{n-1} + 1 + h_{n-1} = 2h_{n-1} + 1 \end{aligned}$$

Para calcular este número nos gustaría poder hacerlo sin tener que "adivinar" y luego comprobar por inducción, más adelante veremos una técnica para calcular esta recurrencia, pero de momento nos quedaremos con la adivinanza. Siguiendo la ecuación de recurrencia vemos que:

$$\begin{aligned} h_1 &= 1 = 2^1 - 1 \\ h_2 &= 2(1) + 1 = 2 + 1 = 3 = 2^2 - 1 \\ h_3 &= 2(2+1) + 1 = 2^2 + 2 + 1 = 7 = 2^3 - 1 \\ h_4 &= 2(2^2 + 2 + 1) + 1 = 2^3 + 2^2 + 2 + 1 = 15 = 2^4 - 1 \\ h_5 &= 2(2^3 + 2^2 + 2 + 1) + 1 = 2^4 + 2^3 + 2^2 + 2 + 1 = 31 = 2^5 - 1 \\ h_6 &= 2(2^4 + 2^3 + 2^2 + 2 + 1) = 2^5 + 2^4 + 2^3 + 2^2 + 2 + 1 = 63 = 2^6 - 1 \end{aligned}$$

Como vemos una conjetura que podemos hacer es que: $h_n = 1 + 2 + 2^2 + \cdots + 2^{n-1}$, sin embargo, no podemos calcular este valor de una manera simple, esto ya lo haremos más adelante. Entonces, por el momento podemos probar la "adivinanza" que hemos hecho, es decir, probemos que $h_n = 2^n - 1$.

Base. Si $n = 1$, $h_1 = 1 = 2^1 - 1$.

Hipótesis de inducción. $h_n = 2^n - 1$.

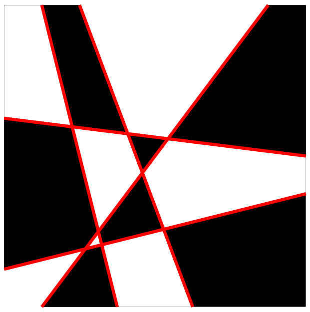
Paso inductivo. Caso $n + 1$.

$$h_{n+1} = 2h_n + 1 \overset{\text{Ⓗ}}{=} 2(2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1.$$

Veamos algunos ejemplos.

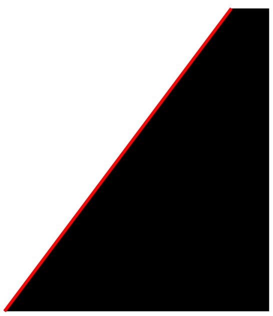
Ejemplo 4.2. Sea XY el plano real $\mathbb{R}^2$. Pruebe que si se trazan rectas en el plano, se puede hacer una bicoloración del plano, es decir, cada región acotada por rectas se puede pintar de un color de manera que las regiones adyacentes tengan un color diferente, además para lograr este objetivo basta con utilizar 2 colores.

Ejemplo:



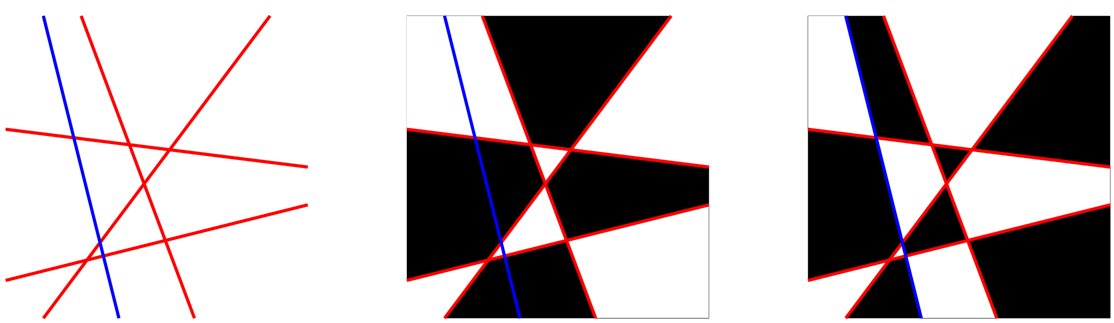
Hagamos una demostración por inducción.

Base. Si tenemos una recta no es difícil hacerlo ya que el plano queda dividido en dos regiones cada una de las cuales se pinta de un color diferente.



Hipótesis de inducción: Si tenemos n rectas sobre el plano XY, podemos hacer una bicoloración del plano.

Paso inductivo: Supongamos que tenemos $n+1$ rectas sobre el pano.



Plano XY con $n+1$ rectas | **Hipótesis de inducción:** Bicoloración del plano con n rectas | Bicoloración del plano con $n+1$ rectas.

Figura 4.3: Bicoloración con $n+1$ rectas

Como se aprecia en la Figura 4.3 cuando tenemos $n+1$ rectas en el plano hacemos una bicoloración con n, lo que es posible por hipótesis de inducción luego a un lado de la recta nueva invertimos la bicoloración. De este modo las regiones adyacentes por la nueva recta tienen coloraciones diferentes y a cada lado de la recta se mantiene una coloración adecuada.

Ejemplo 4.3. Comiendo chocolates en un tren al sur. En un tren al sur va un grupo de matemáticos a una conferencia comiendo chocolates. Cuando comienza el viaje se avisa que los baños del tren no estarán disponibles durante el viaje y que si alguien necesita hacer uso de ellos deberá bajarse en una estación. Cuando pasa el inspector controlando los boletos le dice al grupo de matemáticos: "Sugiero a quien necesite lavarse que baje en la siguiente estación". Debido a esto todos miran la cara del resto de la comitiva para saber quienes tienen la cara sucia, pero como todos son muy tímidos, no se atreven a preguntarle a otro si tienen la cara sucia ellos mismos y tampoco tienen un espejo.

Pruebe que si hay n matemáticos con la cara sucia, todos bajan en el n-ésima estación a lavarse la cara.

Base. Si hay exactamente un pasajero con la cara sucia, este sabrá que es el único que la tiene sucia, ya que el no ve a nadie más con la cara sucia y dada la sugerencia del inspector, sabe que hay alguien con la cara sucia, por lo tanto debe ser él y baja en la primera estación.

Hipótesis de inducción: Si hay n matemáticos con la cara sucia los n se bajan en la n-ésima estación a lavarse la cara.

Paso inductivo: Primero veamos que pasa si hay 2, ambos ven a otra persona con la cara sucia, por lo tanto creen que la sugerencia era para esa otra persona. Pero, cuando esa persona no se baja en la primera estación a lavarse, se dan cuenta que debe haber alguien más, ya que esa persona pensó que era otro. De modo que él también debe tener la cara sucia, y de ese modo ambos se bajan en la segunda estación.

Si hay 3, cada uno de ellos ve a otras 2 personas con la cara sucia, por lo tanto creen que la sugerencia era para esos 2. Pero, cuando ellos no se bajan en la segunda estación a lavarse, se dan cuenta que debe haber alguien más, ya que esos dos, también veían a otros dos. De modo que él también debe tener la cara sucia, y de ese modo se bajan los tres en la tercera estación.

Supongamos que hay $n+1$ matemáticos con la cara sucia, cada uno de ellos ve a otros n que tienen la cara sucia, ninguno de ellos sabe que tiene la cara sucia, por lo tanto piensan que solo los otros n tienen que bajarse y cuando no se bajan en la n-ésima estación se dan cuenta que hay uno más con la cara sucia, y ese debe ser él mismo, por lo tanto todos se bajan en estación $n+1$

Ejemplo 4.4. En este ejemplo mostraremos una demostración por inducción que está mal hecha. La idea es que ustedes vean la demostración y descubran que se hizo mal. Esto se trata de demostrar que todos los lápices de una caja son del mismo color.

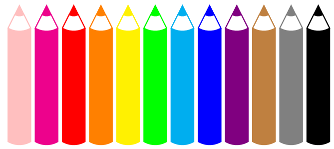


Figura 4.4: Caja de lápices de colores

Base. Si la caja de colores tiene exactamente un lápiz, entonces todos los lápices son del mismo color.

Hipótesis de inducción: Si una caja contiene exactamente n lápices todos son del mismo color.

Paso inductivo: Si tenemos una caja con $n+1$ lápices. Consideramos los n primeros, por hipótesis de inducción estos son del mismo color, luego consideramos los n últimos, nuevamente por hipótesis de inducción son todos del mismo color (ver Figura 4.5), luego como el primero tiene el mismo color que los $n-1$ del medio y el último también, los $n+1$ deben ser del mismo color.

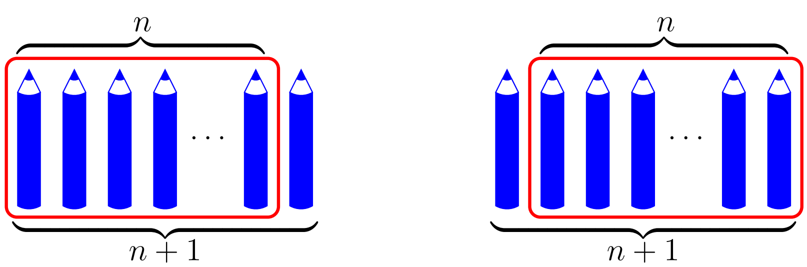


Figura 4.5: Paso inductivo

Claramente al observar la Figura 4.4 vemos que esta demostración tiene un error, pero ¿cuál es?

Revisemos paso a paso, la base de la inducción está bien, si consideramos una caja con un único lápiz la proposición se cumple. La hipótesis de inducción es eso, una hipótesis, por lo tanto puedo plantear "cualquier cosa". De este modo llegamos al paso inductivo que es donde debe encontrarse el error.

Recordemos que el Teorema 4.1 en su segunda condición pide: $(\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))$, la demostración que se presentó es válida solo cuando $n \geqslant 2$, pero no funciona para $n = 1$, ya que en ese caso el dibujo es el que se presenta en la Figura 4.6 y en este caso $n - 1 = 0$ por lo tanto no hay elementos "en el medio" para generar la igualdad entre el primero y el último.

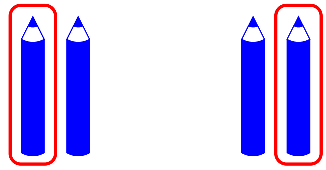


Figura 4.6: Paso inductivo para $n = 1$

4.4. Cardinalidad

Definición 4.12. Dado A un conjunto, se define su cardinal como la cantidad de elementos que tiene el conjunto. Sea esta cantidad finita o infinita. El cardinal de A se denota por $|A|$.

Por ejemplo:

$A = \{a, e, i, o, u\}\,, |A| = 5$

$|\mathbb{N}| = \infty$

Teorema 4.3. *Sean A y B dos conjuntos disjuntos finitos, entonces $|A \uplus B| = |A| + |B|$.*

Demostración.

Por inducción sobre $|B|$

Base. Si $|B| = 0$, entonces $B = \varnothing$, luego $A \cap B = \varnothing$. Por lo tanto;

$$|A \uplus B| = |A \uplus \varnothing| = |A| = |A| + 0 = |A| + |B|$$

Hipótesis de inducción. Si $|B| \leqslant n$ y $A \cap B = \varnothing$, entonces $|A \cup B| = |A| + |B|$.

Paso inductivo. Sea $|B| = n + 1$ y $A \cap B = \varnothing$. Sea $b \in B$:

$$|A \cup B| = |A \cup ((B \setminus \{b\}) \cup \{b\})| = |(A \cup (B \setminus \{b\})) \cup \{b\}\,|$$

Por hipótesis de inducción:

$$|A \cup B| = |A \cup (B \setminus \{b\})| + |\,\{b\}\,| = |A| + |(B \setminus \{b\})| + |\,\{b\}\,| = |A| + |B \setminus \{b\}) \cup \{b\}\,| = |A| + |B|$$

■

Corolario 4.4. *Dados dos conjuntos A y B finitos tal que $A \subseteq B$, entonces $|B \setminus A| = |B| - |A|$*

Demostración. Primero probemos que $B = (B \setminus A) \uplus A$.

$$(B \setminus A) \cup A = (B \cap A^c) \cup A = (B \cup A) \cap (A^c \cup A) = (B \cup A) \cap \mathbf{U} = (B \cup A) \overset{*}{=} B$$
$$(B \setminus A) \cap A = (B \cap A^c) \cap A = B \cap (A^c \cap A) = B \cap \varnothing = \varnothing$$

Nos falta demostrar (*).

P.D.Q. $A \subseteq B \Rightarrow A \cup B = B$

1)	Supongamos $A \subseteq B$	Suposición D.C.
2)	$(\forall x\ x \in A \Rightarrow x \in B)$	Def. $\subseteq$ 1
3)	Sea x cualquiera	
4)	$x \in B \Rightarrow x \in B$	Tautología
5)	$x \in A \Rightarrow x \in B$	I.U. 2
6)	Supongamos $x \in A \cup B$	Suposición D.C.
7)	$x \in A \vee x \in B$	Def. $\cup$ 6
8)	$x \in B$	Dil. 4, 5 y 6
9)	$x \in A \cup B \Rightarrow x \in B$	D.C. 6–8
10)	$(\forall x\ x \in A \cup B \Rightarrow x \in B)$	G.U. 9
11)	$A \cup B \subseteq B$	Def. $\subseteq$ 10
12)	$B \subseteq A \cup B$	Propiedad de $\subseteq$
13)	$A \cup B = B$	Propiedad de $\subseteq$
14)	$A \subseteq B \Rightarrow A \cup B = B$	D.C. 1–13

Por teorema anterior $|B| = |B \setminus A| + |A|$, de aquí concluimos que:

$$|B \setminus A| = |B| - |A|$$

■

Corolario 4.5. *Dados dos conjuntos finitos A y B tal que $A \subseteq B$, $|A| \leqslant |B|$.*

Demostración. $0 \leqslant |B \setminus A| = |B| - |A|$, luego:

$$0 \leqslant |B| - |A|$$

Por lo tanto,

$$|A| \leqslant |B|$$

■

Corolario 4.6. *Dados A y B dos conjuntos finitos. $|A \cup B| = |A| + |B| - |A \cap B|$.*

Demostración. Primero probemos que $A \cup B = A \uplus (B \setminus A)$

$$\begin{aligned} A \cup (B \setminus A) &= A \cup (B \cap A^c) = (A \cup B) \cap (A \cup A^c) = (A \cup B) \cap \mathbf{U} = A \cup B \\ A \cap (B \setminus A) &= A \cap (B \cap A^c) = (A \cap A^c) \cap B = \varnothing \cap B = \varnothing \end{aligned}$$

En segundo lugar probemos que $B = (B \setminus A) \uplus (A \cap B)$

$$\begin{aligned} (B \setminus A) \cup (A \cap B) &= (B \cap A^c) \cup (B \cap A) = B \cap (A^c \cup A) = B \cap \mathbf{U} = B \\ (B \setminus A) \cap (A \cap B) &= (B \cap A^c) \cap (B \cap A) = B \cap (A^c \cap A) = B \cap \varnothing = \varnothing \end{aligned}$$

$$|A \cup B| = |A \uplus (B \setminus A)| = |A| + |B \setminus A| \tag{4.1}$$

Pero $|B| = |B \setminus A| + |A \cap B|$, luego:

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{4.2}$$

■

Teorema 4.7. *Si A es un conjunto tal que $|A|$ es finito, entonces:*

$$|\mathcal{P}(A)| = 2^{|A|}$$

Demostración. Demostremos este resultado por inducción sobre el cardinal de A.

Base. Si $|A| = 0$, entonces $|\mathcal{P}(A)| = |\{\varnothing\}| = 1 = 2^0$.

Hipótesis de inducción. Si $A = \{a_0, a_1, \ldots, a_{n-1}\}$ entonces $|\mathcal{P}(A)| = 2^n$.

Paso inductivo. Sea $A' = \{a_0, a_1, \ldots, a_n\}$ y $A = \{a_0, a_1, \ldots, a_{n-1}\}$, entonces:

$$
\begin{aligned}
&|\mathcal{P}(A')| = |\{B : B \subseteq A'\}| = |\{B : B \subseteq A' \wedge a_n \in B\} \cup \{B : B \subseteq A' \wedge a_n \notin B\}| \\
&|\mathcal{P}(A')| = |\{B : B \subseteq A' \wedge a_n \in B\}| + |\{B : B \subseteq A' \wedge a_n \notin B\}| \\
&|\mathcal{P}(A')| = |\{B \cup \{a_n\} : B \subseteq A\}| + |\{B : B \subseteq A\}| \\
&|\mathcal{P}(A')| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1} \\
&|\mathcal{P}(A')| = 2^{|A'|}
\end{aligned}
$$

■

En el caso de los conjuntos infinitos determinar su cardinal es un poco más complicado, pues existen distintos tipos de infinito. Como un adelanto podemos mencionar que $|\mathbb{N}| \neq |\mathbb{R}|$, sin embargo $|\mathbb{N}| = |\mathbb{Q}|$. Este tema lo tocaremos cuando revisemos los conceptos de funciones.

4.5. Familias de conjuntos

Dado un conjunto de índices I, no necesariamente finito, y una familia de conjuntos A_i, $i \in I$, se definen:

$$\bigcup_{i \in I} A_i = \{x : (\exists i \in I, x \in A_i)\}, \qquad \bigcap_{i \in I} A_i = \{x : (\forall i \in I, x \in A_i)\}$$

Una familia de conjuntos A_i, $i \in I$ es una partición de un conjunto X si:

1. $\bigcup_{i \in I} A_i = X$
2. $(\forall i \in I, A_i \neq \varnothing)$
3. $(\forall i, j \in I, i \neq j \Rightarrow A_i \cap A_j = \varnothing)$

4.6. Producto cartesiano

Definición 4.13. Se define el producto cartesiano entre A y B, denotado por $A \times B$, como:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

Notar que: $A \times B \neq B \times A$ excepto en el caso en que $A = B$

Esta definición puede extenderse al caso de un producto cartesiano de más de dos conjuntos. Esto es:

$$\bigtimes_{i=1}^{n} A_i = A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i\}$$

Si todos los conjuntos $A_i = A$ entonces se hace el abuso de notación:

$$\bigtimes_{i=1}^{n} A = A^n$$

Propiedades:

Si A y B son conjuntos finitos

$$|A \times B| = |A| \cdot |B|$$

Y si los conjuntos A_i con $i \in \{1, \ldots, n\}$ son finitos:

$$|\bigtimes_{i=1}^{n} A_i| = \prod_{i=1}^{n} |A_i|$$

4.7. Ejercicios

P1. Determine el valor de verdad de cada una de las siguientes proposiciones. Justifique.

1. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}: \quad x^2 + y^2 \geq 0$
2. $\forall \varepsilon > 0, \forall x \in \mathbb{R}, \exists y \in \mathbb{R}: |x - y| \leq \varepsilon$
3. $\forall \varepsilon > 0, \exists y \in \mathbb{R}, \forall x \in \mathbb{R}: |x - y| > \varepsilon$
4. $(A \times B)^c = A^c \times B^c$
5. $\mathcal{P}(A^c) = \mathcal{P}(A)^c$
6. $(\forall A: A \cap B = \varnothing) \Longrightarrow B = \varnothing$
7. $X = Y \Longleftrightarrow (\forall A: X \cup A = Y \cap A)$

P2. Pruebe, usando equivalencias lógicas, las siguientes proposiciones.

1. $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$
2. $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C)$
3. $A \cup B = A \cap C \Longrightarrow B \subseteq A \;\wedge\; A \subseteq C$
4. $A \subseteq B \Longleftrightarrow A \cup B = B$
5. $A \subseteq B \Longleftrightarrow A \cap B = A$
6. $A \cap B = \varnothing \Longleftrightarrow \mathcal{P}(A) \cap \mathcal{P}(B) = \{\varnothing\}$

P3. Pruebe, usando propiedades de conjuntos, las siguientes proposiciones.

1. $(A \setminus C) \setminus (B \setminus C) = (A \setminus B) \setminus C$
2. $(A \cap B) \setminus (A \cap C) = (A \cap B) \setminus (A^c \cup C)$
3. $[A \setminus (B \setminus A)] \cup [(B \setminus A) \setminus A] = A \cup B$
4. $A \cap C = \varnothing \Longrightarrow (A \setminus B) \setminus C = A \setminus (B \setminus C)$

P4. Demuestre las siguientes propiedades del producto Cartesiano de conjuntos.

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
3. $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$
4. $A \times B = \bigcup_{b \in B} (A \times \{b\})$
5. $B \times \bigcup_{i \in I} A_i = \bigcup_{i \in I} (B \times A_i)$
6. $B \times \bigcap_{i \in I} A_i = \bigcap_{i \in I} (B \times A_i)$

P5. Dada $\{A_i\}_{i\in\mathbb{N}}$ una familia de conjuntos, se define la familia $\{B_j\}_{j\in\mathbb{N}}$ por:

$$B_1 = A_1 \quad \wedge \quad B_k = A_k \setminus \bigcup_{i=1}^{k-1} A_i,\ \forall k \geq 2.$$

Pruebe que :

1. $\bigcup_{j\in\mathbb{N}} B_j = \bigcup_{i\in\mathbb{N}} A_i$
2. $(\forall i, j \in \mathbb{N},\ i \neq j \Rightarrow B_i \cap B_j = \varnothing)$

P6. Un conjunto $M \subseteq \mathcal{P}(E)$ se denomina un *álgebra* de las partes de E si verifica las siguientes propiedades:

i) $E \in M$,

ii) $(\forall A, B \in M, A \cup B \in M)$,

iii) $(\forall A \in M, (E \setminus A) \in M)$.

Se pide:

1. Demostrar que $\varnothing \in M$
2. Demostrar que si $A,\ B \in M$, entonces $A \cap B \in M$
3. Sea $E = \{1, 2, 3, 4\}$ y sea $M = \{\varnothing, E, \{1\}, \{2\}, \{1, 2\}, \{3, 4\}\}$ ¿Es M un álgebra? Si no lo es, agregue el menor número de conjuntos para que lo sea.

P7. Para la familia de conjuntos $\{A_i\}_{i\in\mathbb{N}}$ encuentre $\bigcup_{i\in\mathbb{N}} A_i$ y $\bigcap_{i\in\mathbb{N}} A_i$ en cada caso. Justifique su respuesta.

1. $A_i = \{1, 2, 3, \ldots, 2i + 1\},\ \forall i \in \mathbb{N}$
2. $A_i = \left[-1 - \frac{1}{i}, 1 - \frac{1}{i}\right],\ \forall i \in \mathbb{N}$
3. $A_i = \left]-\frac{1}{i}, \frac{1}{i}\right[\ \forall i \in \mathbb{N}$
4. $A_i = \mathbb{R} \setminus [0, i],\ \forall i \in \mathbb{N}$

P8. Defina una familia de conjuntos $\{A_i\}_{i\in\mathbb{N}}$ de elementos distintos (i.e. $\forall i, j \in \mathbb{N},\ i \neq j$, $A_i \neq A_j$) tal que verifique las condiciones dadas en cada caso.

1. $\bigcup_{i\in\mathbb{N}} A_i = [0, +\infty[,\quad \bigcap_{i\in\mathbb{N}} A_i = [0, 1]$
2. $\bigcup_{i\in\mathbb{N}} A_i =]0, +\infty[,\quad \bigcap_{i\in\mathbb{N}} A_i = \varnothing$
3. $\bigcup_{i\in\mathbb{N}} A_i = \mathbb{R},\quad \bigcap_{i\in\mathbb{N}} A_i = \{1\}$
4. $\bigcup_{i\in\mathbb{N}} A_i = \mathbb{R},\quad \bigcap_{i\in\mathbb{N}} A_i = \mathbb{Q}$

P9. Pruebe que:

1. $(\exists x,\ p_1(x) \vee p_2(x) \vee \cdots \vee p_n(x)) \Longleftrightarrow [(\exists x,\ p_1(x)) \vee (\exists x,\ p_2(x)) \vee \cdots \vee (\exists x,\ p_n(x))]$
2. $(\forall x,\ p_1(x) \wedge p_2(x) \wedge \cdots \wedge p_n(x)) \Longleftrightarrow [(\forall x,\ p_1(x)) \wedge (\forall x,\ p_2(x)) \wedge \cdots \wedge (\forall x,\ p_n(x))]$

P10. Pruebe que:

1. $\left(\bigcup_{i=1}^{n} A_i\right)^c = \bigcap_{i=1}^{n} A_i^c$
2. $\left(\bigcap_{i=1}^{n} A_i\right)^c = \bigcup_{i=1}^{n} A_i^c$
3. $\neg\left(\bigvee_{i=1}^{n} p_i\right) \Longleftrightarrow \bigwedge_{i=1}^{n} \neg p_i$
4. $\neg\left(\bigwedge_{i=1}^{n} p_i\right) \Longleftrightarrow \bigvee_{i=1}^{n} \neg p_i$

P11. Dada la sucesión $(a_n)_{n\in\mathbb{N}}$.

1. Sea $x_1 = a_1$, y sea $x_i = a_i + x_{i-1}, \forall i \geq 2$. Pruebe que:

$$x_n = \sum_{i=1}^{n} a_i, \forall n \geq 1$$

2. Sea $u_1 = a_1$, $u_i = a_i + \frac{1}{u_{i-1}}, \forall i \geq 2$. La sucesión $(u_n)_{n\in\mathbb{N}_+}$, se dice bien definida si la sucesión $(a_n)_{n\in\mathbb{N}_+}$ es tal que $u_n \neq 0, \forall n \in \mathbb{N}_+$. Sea $(q_n)_{n\in\mathbb{N}_+}$ definida por:

$$\begin{aligned} q_1 &= a_1 \\ q_2 &= a_2 a_1 + 1, \\ q_i &= a_i q_{i-1} + q_{i-2}, \quad \forall i \geq 3. \end{aligned}$$

   Pruebe que si $(u_n)_{n\in\mathbb{N}}$ está bien definida, $u_i = \frac{q_i}{q_{i-1}}, \forall i \geq 2$

P12. Pruebe que: $\forall n \in \mathbb{N}, n > 5 \Rightarrow 2^n > n^2$

P13. Demuestre que:

1. $\forall n \in \mathbb{N}, n \neq 1 \wedge n \neq 3, n$ puede expresarse como suma de 2's y 5's.
2. $\forall n \in \mathbb{N}, n \geq 14, n$ puede expresarse como suma de 3's y 8's.

P14. Pruebe por inducción que:

1. 5 divide a $n^5 - n$
2. 6 divide a $(n^3 + 5n)$
3. 57 divide a $7^{n+2} + 8^{2n+1}$
4. 8 divide a $3^{2n} + 7$
5. 3 divide a $2^{2n} - 1$
6. $x - y$ divide a $x^{2n-1} - y^{2n-1}$

P15. Dada una familia de conjuntos $\{A_i\}_{i=0}^{n}$. Pruebe que:

$$\left|\bigcup_{i=0}^{n} A_i\right| \leq \sum_{i=0}^{n} |A_i|, \quad \forall n \geq 2$$

Capítulo 5

Relaciones binarias

Definición 5.1. Dado un producto cartesiano $A \times B$ una relación binaria $\mathcal{R}$ es un subconjunto del producto cartesiano $A \times B$.

	a	b	c	d	e
1	$(1, a)$	$(1, b)$	$(1, c)$	$(1, d)$	$(1, e)$
2	$(2, a)$	$(2, b)$	$(2, c)$	$(2, d)$	$(2, e)$
3	$(3, a)$	$(3, b)$	$(3, c)$	$(3, d)$	$(3, e)$
4	$(4, a)$	$(4, b)$	$(4, c)$	$(4, d)$	$(4, e)$

$$\mathcal{R} = \{(1, c), (2, b), (2, d), (3, e), (4, c)\}$$
$$(a, b) \in \mathcal{R} \iff a \,\mathcal{R}\, b$$

5.1. Representación de una relación binaria

Como sabemos una relación binaria es un subconjunto de un producto cartesiano por lo tanto podemos utilizar las representaciones de conjuntos y algunas específicas de una relación binaria.

- **Diagrama:** Dados dos conjuntos finitos $A = \{a_1, \ldots, a_m\}$ y $B = \{b_1, \ldots, b_n\}$ se representa la relación binaria $\mathcal{R}$ como:

$\mathcal{R}$	b_1	b_2	$\ldots$	b_n
a_1	$\times$			$\times$
a_2		$\times$		
$\vdots$				
a_m		$\times$		$\times$

  Donde, ponemos el símbolo $\times$ en el recuadro (a_i, b_j) si y solo si $a_i \,\mathcal{R}\, b_j$.

- **Por extensión:** En este caso se listan los pares ordenados que pertenecen a la relación. Claramente solo sirve si la relación es un conjunto finito, aunque los conjuntos A y B podrían ser infinitos.

$$\mathcal{R} = \{(a_1, b_1), (a_1, b_n), (a_2, b_2), \ldots, (a_m, b_2), (a_m, b_n)\}$$

- **Por comprensión**: se usa una función proposicional de dos variables para describir la relación:
$$\mathcal{R} = \{(x, y) \in A \times B : p(x, y)\}$$

- **Expresiones lógicas:** Es lo mismo que la representación por comprensión, simplemente se usa la representación lógica de la igualdad de conjuntos:
$$(\forall x \in A, \forall y \in B, x\,\mathcal{R}\,y \Leftrightarrow p(x, y))$$
Como usualmente conocemos de antemano los conjuntos A y B, no se escriben los cuantificadores, es decir:
$$x\,\mathcal{R}\,y \Leftrightarrow p(x, y)$$

- **Forma matricial:** Si tenemos dos conjuntos finitos $A = \{a_1, \ldots, a_m\}$ y $B = \{b_1, \ldots, b_n\}$. Se define la matriz $M_{\mathcal{R}} \in \mathcal{M}_{m\times n}(\{0, 1\})$ tal que $m_{i,j} = 1 \Leftrightarrow a_i\,\mathcal{R}\,b_j$

Ejemplo 5.1. Dados $A = \{a, b, c\}, \mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ consideremos una relación binaria en $A \times \mathcal{P}(A)$

$\mathcal{R}$	$\varnothing$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	$\{a, b, c\}$
a		$\times$			$\times$	$\times$		$\times$
b			$\times$		$\times$		$\times$	$\times$
c				$\times$		$\times$	$\times$	$\times$

$\longrightarrow$ Diagrama de una relación binaria

Por extensión:
$$\begin{aligned}\mathcal{R} = \{&(a, \{a\}), (a, \{a, b\}), (a, \{a, c\}), (a, \{a, b, c\}), (b, \{b\}), (b, \{a, b\}),\\ &(b, \{b, c\}), (b, \{a, b, c\}), (c, \{c\}), (c, \{a, c\}), (c, \{b, c\}), (c, \{a, b, c\})\}\end{aligned}$$

Por comprensión:
$$\mathcal{R} = \{(x, X) : x \in A \wedge X \subseteq A \wedge x \in X\}$$

Utilizando expresiones lógicas:
$$x\,\mathcal{R}\,X \iff x \in X$$

O utilizando la representación matricial definimos la matriz representante de la relación $\mathcal{R}$ en $A \times \mathcal{P}(A)(A)$ como: $M_R \in \mathcal{M}_{3\times 8}(\{0, 1\})$:
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

5.2. Relaciones binarias homogéneas

Definición 5.2. Una relación binaria $\mathcal{R}$ en $A \times B$ se dice homogénea si $A = B$. En caso contrario será heterogénea. Para denotar una relación homogénea $\mathcal{R}$ en el conjunto A, usaremos $(A, \mathcal{R})$.

Ejemplo 5.2. Supongamos $A = \{\text{Personas}\}$. A continuación tenemos una lista de relaciones homogéneas en distintos conjuntos.

1. $(A, \mathcal{R}_1)$ donde $a\,\mathcal{R}_1\,b \iff a$ es hermano de b.
2. $(A, \mathcal{R}_2)$ donde $a\,\mathcal{R}_2\,b \iff a$ es antepasado de b.
3. $(A, \mathcal{R}_3)$ donde $a\,\mathcal{R}_3\,b \iff a$ tiene la misma nacionalidad de b.
4. $(A, \mathcal{R}_4)$ donde $a\,\mathcal{R}_4\,b \iff a$ es amigo de b.
5. $(\mathbb{N}, |)$ donde $n \,|\, m \iff \frac{m}{n} \in \mathbb{N}$ (n divide a m).
6. $(\mathbb{Z}, =_{\text{mód } p})$ donde $n =_{\text{mód } p} m \iff (\exists k \in \mathbb{Z}, (m - n = k \cdot p))$.
7. $(\mathbb{R}, \leqslant)$
8. $(\mathbb{R}, >)$
9. $(\mathbb{R}, =_{\cos})$ donde $x =_{\cos} y \iff \cos(x) = \cos(y)$

5.2.1. Clasificación de relaciones homogéneas

Dada una relación binaria homogénea $(A, \mathcal{R})$, diremos que:

1. $\mathcal{R}$ es refleja si y solo si $(\forall x \in A, x\,\mathcal{R}\,x)$.

   Ejemplo: $(A, \mathcal{R}_3), (\mathbb{N}, |), (\mathbb{Z}, =_{\text{mód } p}), (\mathbb{R}, \leqslant), (\mathbb{R}, =_{\cos})$

   Hagamos la demostración para $(\mathbb{N}, |)$.

1)	Sea $n \in \mathbb{N}$ cualquiera	
2)	$\frac{n}{n} = 1 \in \mathbb{N}$	
3)	$n \,|\, n$	Def. $\|$ 2
4)	$(\forall n \in \mathbb{N}, n \,|\, n)$	G.U. 3
5)	$(\mathbb{N}, |)$ es simétrica	Def. relación simétrica

2. $\mathcal{R}$ es simétrica si y solo si $(\forall x, y \in A, x\,\mathcal{R}\,y \implies y\,\mathcal{R}\,x)$.

   Ejemplo: $(A, \mathcal{R}_1), (A, \mathcal{R}_3), (A, \mathcal{R}_4), (\mathbb{Z}, =_{\text{mód } p}), (\mathbb{R}, =_{\cos})$

   Veamos la demostración para $(\mathbb{Z}, =_{\text{mód } p})$:

1)	Sean $x, y \in \mathbb{Z}$ cualesquiera	
2)	Supongamos $x =_{\text{mód } p} y$	Suposición D.C.

3)	$(\exists k \in \mathbb{Z}, (x-y) = k \cdot p)$	Def. $=_{\text{mód } p}$ 2
4)	$k_* \in \mathbb{Z} \wedge (x-y) = k_* \cdot p$	I.E. 3
5)	$k_* \in \mathbb{Z}$	Simp. 4
6)	$(x-y) = k_* \cdot p$	Simp. 4
7)	$(y-x) = (-k_*) \cdot p$	6
8)	$-k_* \in \mathbb{Z}$	5
9)	$-k_* \in \mathbb{Z} \wedge (y-x) = (-k_*) \cdot p$	Conj. 7 y 8
10)	$(\exists k \in \mathbb{Z}, (y-x) = k \cdot p)$	G.E. 9
11)	$y =_{\text{mód } p} x$	Def. $=_{\text{mód } p}$ 10
12)	$x =_{\text{mód } p} y \Rightarrow y =_{\text{mód } p} x$	D.C. 2–11
13)	$(\forall x, y \in \mathbb{Z}, x =_{\text{mód } p} y \Rightarrow y =_{\text{mód } p} x)$	G.U. 12
14)	$(\mathbb{Z}, =_{\text{mód } p})$ es simétrica	Def. relación simétrica 13

3. $\mathcal{R}$ es antisimétrica si y solo si $(\forall x, y \in A, (x \,\mathcal{R}\, y \wedge y \,\mathcal{R}\, x) \implies x = y)$.

   Ejemplo: $(A, \mathcal{R}_2), (\mathbb{N}, |), (\mathbb{R}, \leqslant), (\mathbb{R}, >)$.

   Demostremos para $(\mathbb{N}, |)$:

1)	Sean $n, m \in \mathbb{N}$ cualesquiera	
2)	Supongamos $n \,|\, m \wedge m \,|\, n$	Suposición D.C.
3)	$n \,|\, m$	Simp. 2
4)	$m \,|\, n$	Simp. 2
5)	$\frac{n}{m} \in \mathbb{N}$	Def. | 3
6)	$(\exists k \in \mathbb{N}, n = km)$	Def. 5
7)	$\frac{m}{n} \in \mathbb{N}$	Def. | 4
8)	$(\exists k \in \mathbb{N}, m = kn)$	Def. 7
9)	$k_1 \in \mathbb{N} \wedge n = k_1 m$	I.E. 6
10)	$k_2 \in \mathbb{N} \wedge m = k_2 n$	I.E. 8
11)	$k_1 \in \mathbb{N}$	Simp. 9
12)	$n = k_1 m$	Simp. 9
13)	$k_2 \in \mathbb{N}$	Simp. 10
14)	$m = k_2 n$	Simp. 10
15)	$n = k_2 k_1 n$	Sust. 12 y 14
16)	$k_2 k_1 = 1$	Propiedades de $\mathbb{N}$
17)	$k_1 = k_2 = 1$	Propiedades de $\mathbb{N}$
18)	$n = m$	Sust. 12 y 17
19)	$(n \,|\, m \wedge m \,|\, n) \Rightarrow n = m$	D.C. 2–18
20)	$(\forall n, m \in \mathbb{N}, (n \,|\, m \wedge m \,|\, n) \Rightarrow n = m)$	G.U. 19
21)	$(\mathbb{N}, |)$ es antisimétrica	Def. relación antisimétrica 20

4. $\mathcal{R}$ es transitiva si y solo si $(\forall x, y, z \in A, (x \,\mathcal{R}\, y \wedge y \,\mathcal{R}\, z) \implies x \,\mathcal{R}\, z)$.

   Ejemplo: $(A, \mathcal{R}_1), (A, \mathcal{R}_2), (A, \mathcal{R}_3), (\mathbb{N}, |), (\mathbb{R}, \leqslant), (\mathbb{R}, >), (\mathbb{R}, =_{\cos})$

   Veamos el caso $(\mathbb{Z}, =_{\text{mód } p})$:

1)	Sean $n, m, l \in \mathbb{Z}$ cualesquiera	
2)	Supongamos $n =_{\text{mód } p} m \wedge m =_{\text{mód } p} l$	Suposición D.C.
3)	$n =_{\text{mód } p} m$	Simp. 2
4)	$m =_{\text{mód } p} l$	Simp. 2
5)	$(\exists k \in \mathbb{Z}, n - m = kp)$	Def. $=_{\text{mód } p}$ 3
6)	$(\exists k \in \mathbb{Z}, m - l = kp)$	Def. $=_{\text{mód } p}$ 4
7)	$k_1 \in \mathbb{Z} \wedge n - m = k_1 p$	I.E. 5
8)	$k_2 \in \mathbb{Z} \wedge m - l = k_2 p$	I.E. 6

9)	$k_1 \in \mathbb{Z}$	Simp. 7
10)	$n - m = k_1 p$	Simp. 7
11)	$k_2 \in \mathbb{Z}$	Simp. 8
12)	$m - l = k_2 p$	Simp. 8
13)	$n - l = (k_1 + k_2)p$	Sumando 10 y 12
14)	$(k_1 + k_2) \in \mathbb{Z}$	Propiedades de $\mathbb{Z}+$ 9 y 11
15)	$(k_1 + k_2) \in \mathbb{Z} \wedge n - l = (k_1 + k_2)p$	Conj. 13 y 15
16)	$(\exists k \in \mathbb{Z}, n - l = kp)$	G.E. 15
17)	$n =_{\text{mód } p} l$	Def. $=_{\text{mód } p}$ 16
18)	$(n =_{\text{mód } p} m \wedge m =_{\text{mód } p} l) \Rightarrow n =_{\text{mód } p} l$	D.C. 2–17
19)	$(\forall n, m, l \in \mathbb{Z}, (n =_{\text{mód } p} m \wedge m =_{\text{mód } p} l) \Rightarrow n =_{\text{mód } p} l)$	G.U. 18
20)	$(\mathbb{Z}, =_{\text{mód } p})$ es transitiva	Def. relación transitiva 19

Definición 5.3. Diremos que una relación binaria homogénea es una relación de orden, si es refleja, antisimétrica y transitiva.

Ejemplos de relaciones de orden: $(\mathbb{R}, \leqslant)$, $(\mathbb{N}, |)$.

Definición 5.4. Diremos que una relación de orden $(A, \preccurlyeq)$ es total si:

$$(\forall a, b \in A, (a \preccurlyeq b) \vee (b \preccurlyeq a)).$$

En caso contrario diremos que se trata de una relación de orden parcial

$(\mathbb{R}, \leqslant)$ es relación de orden total y $(\mathbb{N}, |)$ es relación de orden parcial.

Definición 5.5. Diremos que una relación binaria homogénea es una relación de equivalencia, si es refleja, simétrica y transitiva.

Ejemplos: $(A, \mathcal{R}_3)$, $(\mathbb{Z}, =_{\text{mód } p})$, $(\mathbb{R}, =_{\cos})$

Definición 5.6. Dada una relación de equivalencia $(A, \sim)$ y $a \in A$ se define la clase de equivalencia de a como:

$$[a]_\sim = \{x \in A : x \sim a\}$$

Propiedades:

1. $x \not\sim y \implies [x]_\sim \cap [y]_\sim = \varnothing$

   Demostración.

1)	Supongamos $x \not\sim y \wedge [x]_\sim \cap [y]_\sim \neq \varnothing$	Suposición R.A.
2)	$x \not\sim y$	Simp. 1
3)	$[x]_\sim \cap [y]_\sim \neq \varnothing$	Simp. 1
4)	$(\exists z \; z \in [x]_\sim \cap [y]_\sim)$	Def. $\varnothing$ 3
5)	$a \in [x]_\sim \cap [y]_\sim$	I.E. 3
6)	$a \in [x]_\sim \wedge a \in [y]_\sim$	Def. $\cap$ 5
7)	$a \sim x \wedge a \sim y$	Def. $\sim$ 6
8)	$x \sim a \wedge a \sim y$	Def. Relación simétrica 7
9)	$x \sim y$	Def. Relación transitiva 8
10)	$x \not\sim y \wedge x \sim y$	Conj. 2 y 9 $\to\leftarrow$
11)	$x \not\sim y \implies [x]_\sim \cap [y]_\sim = \varnothing$	R.A. 1–10

■

2. $x \sim y \implies [x]_\sim = [y]_\sim$

Demostración.

1)	Supongamos $x \sim y$	Suposición D.C.
2)	Sea z cualquiera	
3)	Supongamos $z \in [x]$	Suposición D.C.
4)	$z \sim x$	Def. Clase de equivalencia 3
5)	$z \sim x \wedge x \sim y$	Conj. 1 y 4
6)	$z \sim y$	Def. Transitividad de $\sim$ 5
7)	$z \in [y]_\sim$	Def. Clase de equivalencia 6
8)	$z \in [x]_\sim \Rightarrow z \in [y]_\sim$	D.C. 3–7
9)	Supongamos $z \in [y]_\sim$	Suposición D.C.
10)	$z \sim y$	Def. Clase de equivalencia 9
11)	$y \sim x$	Def. Simetría $\sim$ 1
12)	$z \sim y \wedge y \sim x$	Conj. 10 y 11
13)	$z \sim x$	Def. Transitividad de $\sim$ 12
14)	$z \in [x]_\sim$	Def. Clase de equivalencia 13
15)	$z \in [y]_\sim \Rightarrow z \in [x]_\sim$	D.C. 9–14
16)	$z \in [x]_\sim \Leftrightarrow z \in [y]_\sim$	Conj.+Bicon. 8 y 15
17)	$(\forall z\ z \in [x]_\sim \Leftrightarrow z \in [y]_\sim)$	G.U. 16
18)	$[x]_\sim = [y]_\sim$	Def. = 17
19)	$x \sim y \Rightarrow [x]_\sim = [y]_\sim$	D.C. 1–18

■

De este modo vemos que el conjunto de clases de equivalencia de una relación de equivalencia en A, genera una partición del conjunto A.

Definición 5.7. Dada una relación de equivalencia $(A, \sim)$ definimos el espacio cociente como:

$$A_\sim = \{[x]_\sim : x \in A\}$$

Ejemplo 5.3. Calculemos las clases de equivalencia de la relación $(\mathbb{Z}, =_{\text{mód } p})$.

$$\begin{aligned}
[0]_p &= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, (n-0) = k \cdot p\} \\
&= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = k \cdot p\} \\
[1]_p &= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, (n-1) = k \cdot p\} \\
&= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = k \cdot p + 1\} \\
[2]_p &= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, (n-2) = k \cdot p\} \\
&= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = k \cdot p + 2\} \\
[3]_p &= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, (n-3) = k \cdot p\} \\
&= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = k \cdot p + 3\} \\
&\vdots \\
[p-1]_p &= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, (n-(p-1)) = k \cdot p\} \\
&= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = k \cdot p + (p-1)\}
\end{aligned}$$

Recordemos que al dividir cualquier número entero n por un natural p obtenemos un resto $r \in \{0, \ldots, p-1\}$. De este modo se cumple que:

$$(\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, \exists r \in \{0, \ldots, p-1\}, n = k \cdot p + r)$$

De este modo la relación $(\mathbb{Z}, =_{\text{mód } p})$ tiene p clases de equivalencia. Generalmente, estas clases toman como representante los elemento en $\{0, \ldots, p-1\}$, pero en realidad podría usarse cualquier otro. Por ejemplo: $[0]_p = [p]_p$, $[-1]_p = [p-1]_p = [4p-1]_p$.

Notemos que en este caso el espacio cociente es: $\{[i]_p\}_{i=0}^{p-1}$.

Ejemplo 5.4. Calculemos las clases de equivalencia de $(\mathbb{R}, =_{\cos})$. Recordemos la gráfica de la función coseno: Así vemos que $(\forall x \in [0, \pi])$ podemos definir la clase de equivalencia de x como:

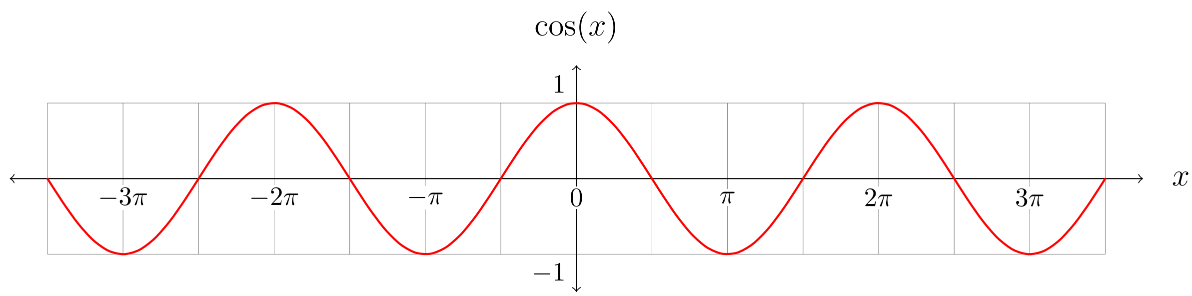


Figura 5.1: Función coseno

$$[x]_{\cos} = \{y \in \mathbb{R} : (\exists k \in \mathbb{Z}, y = x + 2\pi k \vee y = -x + 2\pi k)\}$$

De este modo la partición de $\mathbb{R}$ es: $\{[x]_{\cos}\}_{x \in [0,\pi]}$

5.3. Ejercicios

P1. Estudie y clasifique las siguientes relaciones:

1. $x \mathcal{R} y \iff \max\{x,y\} \leq 2$, en $\mathbb{N}$.
2. $x \mathcal{R} y \iff \max\{x,y\} = 20$, en $\mathbb{N}$.
3. $x \mathcal{R} y \iff \mathrm{MCD}\{x,y\} \neq 1$, en $\mathbb{N}$.
4. $x \mathcal{R} y \iff x^2+y^2 \leq 1$, en $\mathbb{R}$.
5. $X \mathcal{R} Y \iff X \subseteq Y^c$, en $\mathcal{P}(\mathbb{N})$.
6. $X \mathcal{R} Y \iff XY = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, en $\mathcal{M}_{2\times 2}(\{0,1\})$.

P2. Se define la relación $\mathcal{R}$ en $\mathbb{R} \setminus \{0\}$ como:

$$x \mathcal{R} y \iff \frac{x}{y} \in A, \text{ donde } A \subseteq \mathbb{R}.$$

1. Probar que $\mathcal{R}$ es relación de equivalencia si $A = \mathbb{R}$. Encuentre la clase de equivalencia de $\frac{1}{3}$.
2. Probar que $\mathcal{R}$ es relación de orden si $A = \mathbb{N}$. Determine si el orden es total o parcial.

P3. Sea $\{a,b\}^*$ el conjunto de todas las palabras que se escriben con a's y b's. Por ejemplo, $aabb$, $abab$, $abaa$, etc.

Suponga que cada vez que tiene el término ab usted puede borrarlo de este modo:

$$\begin{aligned} \underline{ab}bbaaa &\longrightarrow bbaaa \\ \underline{ababab} &\longrightarrow \text{palabra vacía} \\ \underline{ab}a\underline{ab}a\underline{ab} &\longrightarrow aa \end{aligned}$$

Estudie la relación:

$\forall w, u \in \{a,b\}^*,\ w \mathcal{R} u \iff$ al eliminar todos los términos ab se obtiene en ambos casos la misma palabra

P4. Sean $\mathcal{R}_1, \mathcal{R}_2$ dos relaciones sobre un conjunto E. Se define las relaciones $\mathcal{R}_1 \cap \mathcal{R}_2$ y $\mathcal{R}_1 \cup \mathcal{R}_2$ por:

$$\begin{aligned} x\,(\mathcal{R}_1 \cap \mathcal{R}_2)\,y &\iff x \mathcal{R}_1 y \wedge x \mathcal{R}_2 y \\ x\,(\mathcal{R}_1 \cup \mathcal{R}_2)\,y &\iff x \mathcal{R}_1 y \vee x \mathcal{R}_2 y \end{aligned}$$

Estudie las propiedades de $\mathcal{R}_1 \cap \mathcal{R}_2$ y $\mathcal{R}_1 \cup \mathcal{R}_2$ en base a las propiedades de $\mathcal{R}_1$ y $\mathcal{R}_2$.

P5. Sea X un conjunto no vacío y $\mathcal{P}$ el conjunto de todas las particiones finitas de X. Es decir, los elementos de $\mathcal{P}$ son las particiones $\{A_i\}_{i=1}^n$ donde $n \in \mathbb{N}$. Se define la relación $\preccurlyeq$ en $\mathcal{P}$ como sigue:

$$\{A_i\}_{i=1}^n \preccurlyeq \{B_j\}_{j=1}^m \iff (\forall j \in \{1,\ldots,m\}, \exists i \in \{1,\ldots,n\}, B_j \subseteq A_i)$$

1. Pruebe que $\preccurlyeq$ es relación de orden.

2. Muestre que si $|X| > 3$, entonces $\leq$ es relación de orden parcial.

P6. Sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones en E conjunto no vacío. Se definen las relaciones: $\mathcal{R}^{-1}$ y $\mathcal{R} \circ \mathcal{S}$ como: $\forall a, b \in E$:

$$\begin{aligned} a\mathcal{R}^{-1}b &\iff b\,\mathcal{R}\,a, \\ a(\mathcal{R} \circ \mathcal{S})b &\iff \exists c \in E,\ a\,\mathcal{R}\,c \ \wedge \ c\,\mathcal{S}\,b. \end{aligned}$$

Pruebe que:

1. Si $\mathcal{R}$ y $\mathcal{S}$ son relaciones de equivalencia, entonces $\mathcal{R} \circ \mathcal{S}$ es relación de equivalencia si y solo si $\mathcal{R} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{R}$.
2. Si $\mathcal{R}$ y $\mathcal{S}$ son relaciones de equivalencia, entonces $\mathcal{R} \cap \mathcal{S}$ es relación de equivalencia.
3. Si $\mathcal{R}$ y $\mathcal{S}$ son relaciones de equivalencia, entonces $\mathcal{R} \cup \mathcal{S}$ no necesariamente es relación de equivalencia.
4. Si $\mathcal{R}$ es relación de orden total, entonces $\mathcal{R}^{-1}$ es también relación de orden total.

P7. Diremos que una relación R homogénea sobre X es completa si existe $A \subseteq X$ tal que $R = A^2$. Muestre que si R es completa entonces R es simétrica y transitiva.

P8. Sea R una relación homogénea sobre X. Una relación homogénea se dice asimétrica si $\forall a, b \in X, a\,\mathcal{R}\,b \implies b \not\mathcal{R} a$. Además, se define $\mathrm{Id}_X = \{(x, x) : x \in X\}$

1. Muestre que R es asimétrica si y solo si $R \cap R^{-1} = \varnothing$.
2. Muestre que R es antisimétrica si y solo si $R \cap R^{-1} \subseteq \mathrm{Id}_X$.
3. Concluya que toda relación asimétrica es antisimétrica, y dé un ejemplo de una relación antisimétrica pero no asimétrica.

Capítulo 6

Funciones

Definición 6.1. Una función f del conjunto A en el conjunto B es una relación en $A \times B$ tal que:

$$(\forall x \in A, \exists! y \in B, x \, \mathcal{R} \, y)$$

Si f es una función de A en B lo denotamos por: $\begin{aligned} f : A &\to B \\ x &\to f(x) \end{aligned}$.

Diremos que A es el dominio de la función y B es el codominio de la función.

De este modo, una función f es tal que:

$$(\forall x \in A, \exists! y \in B, y = f(x))$$

o equivalentemente,

$$(\forall x \in A, \exists y \in B, y = f(x) \wedge (\forall z \in B, z = f(x) \Rightarrow z = y))$$

Diremos que dos funciones $f : A \to B$ y $g : A \to B$ son iguales ($f = g$) si:

$$(\forall x \in A, f(x) = g(x))$$

6.1. Representación de una función

Para definir una función podemos hacerlo de diferentes maneras.

1. Si el dominio de la función es finito podemos definirla por medio de una tabla:

x	$f(x)$
a_1	$f(a_1)$
a_2	$f(a_2)$
$\vdots$	$\vdots$
a_n	$f(a_n)$

A veces para ahorrar espacio la tabla se puede escribir de manera horizontal.

x	a_1	a_2	$\ldots$	a_n
$f(x)$	$f(a_1)$	$f(a_2)$	$\ldots$	$f(a_n)$

2. También podemos definir una función a través de una fórmula como una regla de asignación. Por ejemplo: $f : \mathbb{N} \to \mathbb{N}$
$$x \to x^2 + 1$$

Para visualizar las funciones existen varios métodos, sin embargo para cada uno de ellos se requieren algunas condiciones extra.

1. Si el dominio y co-dominio son conjuntos finitos, lo suficientemente pequeños para tener una representación en un diagrama, podemos poner ambos diagramas y unir un elemento del dominio con su imagen por una flecha:

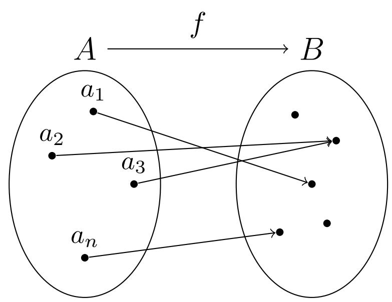


Figura 6.1: Representación de una función en un diagrama

2. También podemos representar con un gráfico. Esta es la visualización más usada para funciones, es útil incluso con conjuntos infinitos, ya que al menos permite visualizar grosso modo el comportamiento de la función. En este caso en el eje horizontal o abscisa se representa el dominio de la función y en el eje vertical u ordenada se representa el co-dominio de la función. De este modo, se dibujan los pares ordenados $(x, f(x))$ en el plano que forman ambos ejes. Esta representación se hace con un punto en los casos discretos. En el caso continuo, se observa como una línea. No entraremos en detalle de lo que significa continuidad porque eso es todo un tema, de modo que nos quedamos con la intuición. Dependiendo del tipo de función también pueden utilizarse barras en vez de puntos. En la Figura 6.2 podemos ver ejemplos de gráficos de funciones.

6.2. Imagen y pre-imagen

Definición 6.2. Dada $f : A \to B$ y $X \subseteq A$, diremos que el conjunto imagen de X por f es:

$$f(X) = \{y \in B : (\exists x \in X, f(x) = y)\}$$

Análogamente, la imagen de un elemento $x \in A$ se define como: $f(x) \in B$.

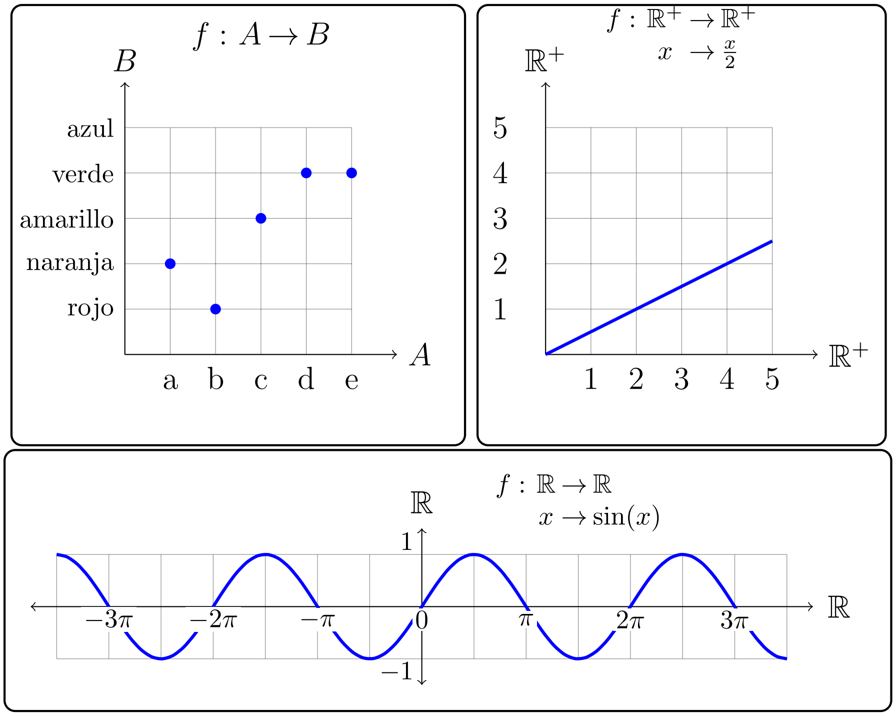


Figura 6.2: Ejemplos de gráficos de funciones

Definición 6.3. Dada $f : A \to B$ se define el recorrido de f como la imagen del conjunto A, es decir, $f(A)$.

Definición 6.4. Dada $f : A \to B$ una función y $Y \subseteq B$ se define la pre-imagen o imagen recíproca de Y como:

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}$$

Análogamente, la pre-imagen de un elemento $y \in B$ es el conjunto:

$$f^{-1}(y) = \{x \in A : f(x) = y\}$$

6.2.1. Propiedades

1. $f^{-1}(B) = A$

   Demostración. Por definición:

   $$f^{-1}(B) = \{x \in A : f(x) \in B\} \subseteq A$$

   luego, debemos demostrar que $A \subseteq f^{-1}(B)$

1)	Sea x cualquiera	
2)	Supongamos $x \in A$	Suposición D.C.
3)	$f(x) \in B$	Def. f
4)	$x \in A \wedge f(x) \in B$	Conj. 2 y 3
5)	$x \in f^{-1}(B)$	Def. $f^{-1}(B)$ 4
6)	$x \in A \Rightarrow x \in f^{-1}(B)$	D.C. 2–5
7)	$(\forall x\ x \in A \Rightarrow x \in f^{-1}(B))$	G.U. 6
8)	$A \subseteq f^{-1}(B)$	Def. $\subseteq$ 7

■

2. $f(A) \subseteq B$

   Demostración.

$$f(A) = \{y \in B : (\exists x \in A, y = f(x))\} \subseteq B$$

■

3. $\forall X, X' \subseteq A, X \subseteq X' \implies f(X) \subseteq f(X')$

   Demostración.

Supongamos $X \subseteq X'$
$(\forall x\ x \in X \Rightarrow x \in X')$
Sea y cualquiera
Supongamos $y \in f(X)$
$(\exists x\ x \in X \wedge y = f(x))$
$x_* \in X \wedge y = f(x_*)$
$x_* \in X$
$x_* \in X'$
$y = f(x_*)$
$x_* \in X' \wedge y = f(x_*)$
$(\exists x\ x \in X' \wedge y = f(x))$
$y \in f(X')$
$y \in f(X) \Rightarrow y \in f(X')$
$(\forall y\ y \in f(X) \Rightarrow y \in f(X'))$
$f(X) \subseteq f(X')$
$X \subseteq X' \Rightarrow f(X) \subseteq f(X')$

■

4. $\forall Y, Y' \subseteq B, Y \subseteq Y' \implies f(Y)^{-1} \subseteq f^{-1}(Y')$

   Demostración.

Supongamos $Y \subseteq Y'$
$(\forall y\ y \in Y \Rightarrow y \in Y')$
Sea x cualquiera
Supongamos $x \in f(Y)^{-1}$
$x \in A \wedge f(x) \in Y$
$x \in A$
$f(x) \in Y$
$f(x) \in Y \Rightarrow f(x) \in Y'$
$f(x) \in Y'$
$x \in A \wedge f(x) \in Y'$
$x \in f(Y')^{-1}$
$x \in f(Y)^{-1} \Rightarrow x \in f(Y')^{-1}$
$(\forall x\ x \in f(Y)^{-1} \Rightarrow x \in f(Y')^{-1})$
$f(Y)^{-1} \subseteq f(Y')^{-1}$
$Y \subseteq Y' \Rightarrow f(Y)^{-1} \subseteq f(Y')^{-1}$

■

5. $\forall X, X' \subseteq A, f(X \cup X') = f(X) \cup f(X')$

   Demostración.

Sea y cualquiera
$y \in f(X \cup X') \Leftrightarrow y \in B \wedge (\exists x\ x \in X \cup X' \wedge f(x) = y)$
$y \in f(X \cup X') \Leftrightarrow y \in B \wedge (\exists x\ (x \in X \vee x \in X') \wedge f(x) = y)$

$y \in f(X \cup X') \Leftrightarrow y \in B \wedge (\exists x\ (x \in X \wedge f(x) = y) \vee (x \in X' \wedge f(x) = y))$
$y \in f(X \cup X') \Leftrightarrow y \in B \wedge [(\exists x\ x \in X \wedge f(x) = y) \vee (\exists x\ x \in X' \wedge f(x) = y)]$
$y \in f(X \cup X') \Leftrightarrow y \in B \wedge (x \in f(X) \vee x \in f(X'))$
$y \in f(X \cup X') \Leftrightarrow y \in B \wedge x \in f(X) \cup f(X')$
$(\forall y\ y \in f(X \cup X') \Leftrightarrow y \in B \wedge x \in f(X) \cup f(X'))$
$f(X \cup X') \subseteq f(X) \cup f(X'))$

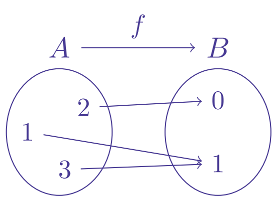
■

6. $\forall Y, Y' \subseteq B, f^{-1}(Y \cup Y') = f^{-1}(Y) \cup f^{-1}(Y')$
7. $\forall X, X' \subseteq A, f(X \cap X') \subseteq f(X) \cap f(X')$

Demostración.

Sea y cualquiera
Supongamos $y \in f(X \cap X')$
$y \in B \wedge (\exists x\ x \in X \cap X' \wedge f(x) = y)$
$y \in B$
$(\exists x\ x \in X \cap X' \wedge f(x) = y)$
$(\exists x\ x \in X \wedge x \in X' \wedge f(x) = y)$
$(\exists x\ (x \in X \wedge f(x) = y) \wedge (x \in X' \wedge f(x) = y))$
$(\exists x\ x \in X \wedge f(x) = y) \wedge (\exists x\ x \in X' \wedge f(x) = y)$
$y \in B \wedge (\exists x\ x \in X \wedge f(x) = y) \wedge y \in B \wedge (\exists x\ x \in X' \wedge f(x) = y)$
$y \in f(X) \wedge y \in f(X')$
$y \in f(X) \cap f(X')$
$y \in f(X \cap X') \Rightarrow y \in f(X) \cap f(X')$
$(\forall y\ y \in f(X \cap X') \Rightarrow y \in f(X) \cap f(X'))$
$f(X \cap X') \subseteq f(X) \cap f(X'))$

La igualdad no se da, un ejemplo de esto es:



X	$f(X)$
$\{1,2\}$	$\{0,1\}$
$\{2,3\}$	$\{0,1\}$
$\{2\}$	$\{0\}$

$\Longrightarrow\ f(\{1,2\}) \cap f(\{2,3\}) = \{0,1\} \neq \{0\} = f(\{2\})$

■

8. $\forall Y, Y' \subseteq B, f^{-1}(Y \cap Y') = f^{-1}(Y) \cap f^{-1}(Y')$
9. $\forall X \subseteq A, X \subseteq f^{-1}(f(X))$

Demostración.

Sea x cualquiera
Supongamos $x \in X$
$f(x) \in f(X)$
$f(x) = f(x)$
$f(x) \in f(X) \wedge f(x) = f(x)$
$(\exists y\ y \in f(X) \wedge y = f(x))$
$x \in f^{-1}(f(X))$
$x \in X \Rightarrow x \in f^{-1}(f(X))$
$(\forall x\ x \in X \Rightarrow x \in f^{-1}(f(X)))$
$X \subseteq f^{-1}(f(X))$

■

10. $\forall Y \subseteq B, f(f^{-1}(Y)) \subseteq Y$

6.3. Clasificación de funciones

Definición 6.5. Una función $f : A \to B$ se dice inyectiva si:

$$(\forall x, x' \in A, f(x) = f(x') \implies x = x')$$

Algunas funciones inyectivas son:

1. $\exp : \mathbb{R} \to \mathbb{R}$
2. $\tan : \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\to \mathbb{R}$
3. $\ln : \mathbb{R}^+ \to \mathbb{R}$
4. $f_{a,b} : \mathbb{R} \to \mathbb{R}$
   $x \to ax + b$

No son inyectivas

1. $\sin : \mathbb{R} \to \mathbb{R}$
2. $g_{a,b} : \mathbb{R} \to \mathbb{R}$
   $x \to a(x-b)^2$
3. $\tan : \mathbb{R} \setminus \left\{\frac{\pi}{2} + n\pi : n \in \mathbb{Z}\right\} \to \mathbb{R}$

Definición 6.6. Una función $f : A \to B$ se dice sobreyectiva o epiyectiva si:

$$(\forall y \in B, \exists x \in A, f(x) = y)$$

Son funciones sobreyectivas:

1. $\tan : \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\to \mathbb{R}$
2. $f_{a,b} : \mathbb{R} \to \mathbb{R}$
   $x \to ax + b$
3. $\tan : \mathbb{R} \setminus \left\{\frac{\pi}{2} + n\pi : n \in \mathbb{Z}\right\} \to \mathbb{R}$
4. $\tan : \mathbb{R} \setminus \left\{\frac{\pi}{2} + n\pi : n \in \mathbb{Z}\right\} \to \mathbb{R}$
5. $\ln : \mathbb{R}^+ \to \mathbb{R}$
6. $\exp : \mathbb{R} \to \mathbb{R}^+$

No son sobreyectivas:

1. $\exp : \mathbb{R} \to \mathbb{R}$
2. $g_{a,b} : \mathbb{R} \to \mathbb{R}$
   $x \to a(x-b)^2$

3. $\sin : \mathbb{R} \to \mathbb{R}$

Definición 6.7. Una función $f : A \to B$ se dice biyectiva si es inyectiva y sobreyectiva.

$$(\forall y \in B, \exists x \in A, f(x) = y \wedge (\forall z \in A, f(z) = f(x) \Rightarrow x = z))$$

Son biyectivas:

1. $\exp : \mathbb{R} \to \mathbb{R}^+$
2. $\ln : \mathbb{R}^+ \to \mathbb{R}$
3. $\tan : \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\to \mathbb{R}$
4. $f_{a,b} : \mathbb{R} \to \mathbb{R}$
   $x \to ax + b$

Proposición 6.1. *Si $f : A \to B$ es biyectiva existe una función de B en A que denominaremos la inversa de f, denotada por f^{-1}, tal que f^{-1} es biyectiva y:*

$$(\forall x \in A, f^{-1}(f(x)) = x) \wedge (\forall y \in B, f(f^{-1}(y)) = y)$$

Demostración. En primer lugar debemos probar que existe la función $f^{-1} : B \to A$. Para esto debemos probar que $(\forall y \in B, \exists! x \in A, f^{-1}(y) = x)$

Como f biyectiva $(\forall y \in B, \exists x \in A, f(x) = y \wedge (\forall z\ f(z) = f(x) \Rightarrow x = z))$, esto es equivalente a $(\forall y \in B, \exists! x \in A, f(x) = y)$. De este modo para cada y se define $f^{-1}(y) = x$ tal que $f(x) = y$.

Ahora,

Sea $x \in A$ cualquiera	Sea $y \in B$ cualquiera
$f(x) = y$	$f^{-1}(y) = x$
$f(x) = y \implies f^{-1}(y) = x$	$f^{-1}(y) = x \implies f(x) = y$
$f^{-1}(y) = x$	$f(x) = y$
$f^{-1}(f(x)) = x$	$f(f^{-1}(y)) = y$
$(\forall x \in A, f^{-1}(f(x)) = x)$	$(\forall y \in B, f(f^{-1}(y)) = y)$

■

6.4. Composición de funciones

Definición 6.8. Sean $f : A \to B$ y $g : B \to C$ dos funciones, se define la composición de f y g, como la función:

$$\begin{aligned} g \circ f : A &\to C \\ x &\to (g \circ f)(x) = g(f(x)) \end{aligned}$$

Proposición 6.2. *Dadas $f : A \to B$, $g : B \to C$ y $h : C \to D$ funciones, se cumple que:*

1. *Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.*
2. *Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.*
3. *Si f y g son biyectivas, entonces $g \circ f$ es biyectiva. Además,*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

4. $h \circ (g \circ f) = (h \circ g) \circ f$.

Demostración.

1. Demostremos que si f y g son inyectivas, entonces $g \circ f$ es inyectiva.

$$
\begin{array}{l}
\text{Supongamos } f \text{ y } g \text{ son inyectivas} \\
(\forall x, x' \in A, f(x) = f(x') \Rightarrow x = x') \\
(\forall y, y' \in B, g(y) = g(y') \Rightarrow y = y') \\
\quad \text{Sean } x, x' \in A' \text{ cualesquiera} \\
\quad f(x) = f(x') \Rightarrow x = x' \\
\quad g(f(x)) = g(f(x')) \Rightarrow f(x) = f(x') \\
\quad g(f(x)) = g(f(x')) \Rightarrow x = x' \\
(\forall x, x' \in A, g(f(x)) = g(f(x')) \Rightarrow x = x') \\
(\forall x, x' \in A, g \circ f(x) = g \circ f(x') \Rightarrow x = x') \\
g \circ f \text{ es inyectiva} \\
f \text{ y } g \text{ son inyectivas} \Rightarrow g \circ f \text{ es inyectiva}
\end{array}
$$

2. Demostremos que si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.

$$
\begin{array}{l}
\text{Supongamos } f \text{ y } g \text{ son sobreyectivas} \\
(\forall y \in B, \exists x \in A, f(x) = y) \\
(\forall z \in C, \exists y \in B, g(y) = z) \\
\quad \text{Sean } z \in C \text{ cualquiera} \\
\quad (\exists y \in B, g(y) = z) \\
\quad y_* \in B \wedge g(y_*) = z \\
\quad y_* \in B \\
\quad g(y_*) = z \\
\quad (\exists x \in A, f(x) = y_*) \\
\quad x_* \in A \wedge f(x_*) = y_* \\
\quad x_* \in A \\
\quad f(x_*) = y_* \\
\quad g(f(x_*)) = z \\
\quad x_* \in A \wedge g(f(x_*)) = z \\
\quad (\exists x \in A, g(f(x)) = z) \\
(\forall z \in C, \exists x \in A, g(f(x)) = z) \\
(\forall z \in C, \exists x \in A, g \circ f(x) = z) \\
g \circ f \text{ es sobreyectiva} \\
f \text{ y } g \text{ son sobreyectivaa} \Rightarrow g \circ f \text{ es sobreyectiva}
\end{array}
$$

3. De las 2 propiedades anteriores se deduce esta de manera directa. Solo debemos probar la forma que tiene la inversa de la composición:

1)	Sea $z \in C$ cualquiera	
2)	$z = (g \circ f)(x)$	$g \circ f$ biyectiva
3)	$z = g(f(x))$	Def. $\circ$
4)	$g^{-1}(z) = f(x)$	Def. g^{-1}
5)	$f^{-1}(g^{-1}(z)) = x$	Def. f^{-1}
6)	$(f^{-1} \circ g^{-1})(z) = x$	Def. $\circ$
7)	$(f^{-1} \circ g^{-1})(z) = (g \circ f)^{-1}(z)$	Def. $(g \circ f)^{-1}$
8)	$(\forall z \in (f^{-1} \circ g^{-1})(z) = (g \circ f)^{-1}(z))$	G.U. 7
9)	$f^{-1} \circ g^{-1} = (g \circ f)^{-1}$	Def. $=$

4. Probemos esta última propiedad.

$$\begin{array}{l}
\text{Sea } x \in A \text{ cualquiera} \\
(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) \\
(h \circ (g \circ f))(x) = (h \circ g)(f(x)) \\
(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x) \\
(\forall x \in A, (h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)) \\
h \circ (g \circ f) = (h \circ g) \circ f
\end{array}$$

■

6.5. Funciones y cardinalidad de conjuntos

Primero analicemos el caso de funciones que actúan sobre conjuntos finitos.

Teorema 6.3 (Principio de palomar)**.** *Sean A y B dos conjuntos finitos no vacíos, y $f : A \to B$ una función. Se tiene que:*

1. *Si f es inyectiva entonces $|A| \leq |B|$.*
2. *Si f es sobreyectiva entonces $|A| \geq |B|$.*
3. *Si f es biyectiva entonces $|A| = |B|$.*

Antes de demostrar este teorema demostremos el siguiente lema:

Lema 6.4. *Sea $f : A \to B$ y $X \subseteq A$ un conjunto finito, entonces:*

1. *$|f(X)| \leqslant |X|$*
2. *Si f inyectiva, entonces $|f(X)| = |X|$*

Demostración. Demostremos por inducción sobre el cardinal de X.

Base. Si $|X| = 1$, $X = \{a\}$, $f(X) = \{f(a)\}$ y claramente $|f(X)| = 1$, por lo tanto $|f(X)| \leqslant |X|$ y Si f inyectiva, $|f(X)| = |X|$.

Hipótesis de inducción. Si $|X| = n$ entonces $|f(X)| \leqslant |X|$ y Si f inyectiva, entonces $|f(X)| = |X|$.

Paso inductivo. Sea X tal que $|X| = n + 1$. Sea $a \in X$. Luego:

$$X = (X \setminus \{a\}) \cup \{a\}$$

Luego por propiedad de la imagen de funciones:

$$f(X) = f(X \setminus \{a\}) \cup f(\{a\})$$

Por propiedades de cardinal de conjuntos finitos

$$|f(X)| = |f(X \setminus \{a\})| + |f(\{a\})| - |f(X \setminus \{a\}) \cap f(\{a\})|$$

Como $|X| = n+1$ y $a \in X$, $|X \setminus \{a\}| = n$, luego por hipótesis de inducción $|f(X \setminus \{a\})| \leqslant n$, de aquí:

$$|f(X)| \leqslant n + 1 - |f(X \setminus \{a\}) \cap f(\{a\})| \leqslant n + 1 = |X|$$

Si f inyectiva, $|f(X \setminus \{a\})| = |X \setminus \{a\}| = n$.

$$|f(X)| = n + 1 - |f(X \setminus \{a\}) \cap f(\{a\})|$$

Veamos que si f inyectiva, entonces $f(X \setminus \{a\}) \cap f(\{a\}) = \varnothing$.

1)	Supongamos f inyectiva	Suposición D.C.
2)	Supongamos $f(X \setminus \{a\}) \cap f(\{a\}) \neq \varnothing$	Suposición R.A.
3)	$(\exists y\ y \in f(X \setminus \{a\}) \cap f(\{a\}))$	Def. $\varnothing$
4)	$y_* \in f(X \setminus \{a\}) \cap f(\{a\})$	I.E. 3
5)	$y_* \in f(X \setminus \{a\})$	Def. $\cap$ +Simp. 4
6)	$y_* \in f(\{a\})$	Def. $\cap$ +Simp. 4
7)	$(\exists x\ x \in X \setminus \{a\} \wedge y_* = f(x))$	Def. $f(X \setminus \{a\})$ 5
8)	$(\exists x\ x \in \{a\} \wedge y_* = f(x))$	Def. $f(\{a\})$ 6
9)	$\bar{x} \in X \setminus \{a\} \wedge y_* = f(\bar{x})$	I.E. 7
10)	$\hat{x} \in \{a\} \wedge y_* = f(\hat{x})$	I.E. 8
11)	$f(\bar{x}) = f(\hat{x})$	Simp.+Sust. 9 y 10
12)	$\bar{x} = \hat{x}$	f inyectiva
13)	$\bar{x} \in X \setminus \{a\}$	Simp. 9
14)	$\bar{x} \in X \wedge \bar{x} \notin \{a\}$	Def. $\setminus$ 13
15)	$\bar{x} \notin \{a\}$	Simp. 14
16)	$\bar{x} \neq a$	Def. $\{a\}$ 15
17)	$\hat{x} \in \{a\}$	Simp. 10
18)	$\hat{x} = a$	Def. $\{a\}$ 17
19)	$\bar{x} = a$	Sust. 12 y 18
20)	$\bar{x} = a \wedge \bar{x} \neq a$	Conj. 16 y 19 $\rightarrow\leftarrow$
21)	$f(X \setminus \{a\}) \cap f(\{a\}) = \varnothing$	R.A. 2–20
22)	f inyectiva $\Rightarrow f(X \setminus \{a\}) \cap f(\{a\}) = \varnothing$	

Por lo tanto si f es inyectiva:

$$|f(X)| = n + 1 - 0 = n + 1 = |X|$$

■

Demostración de Teorema 6.3.

1. Por reducción al absurdo.

Supongamos f es inyectiva, A es finito y $\lvert B\rvert < \lvert A\rvert$	
$f(A) \subseteq B$	Por propiedad del conjunto imagen
$\lvert A\rvert = \lvert f(A)\rvert \leqslant \lvert B\rvert < \lvert A\rvert$	Por lema anterior, prop. de $\subseteq$ y suposición
$\lvert A\rvert < \lvert A\rvert$	$\rightarrow\leftarrow$

Si f es inyectiva entonces $|A| \leqslant |B|$.

2. En primer lugar notemos que por lema anterior, si $|X| < \infty$, $|f(X)| \leqslant |X|$. Además, si $f : A \to B$ es sobreyectiva se tiene que: $f(A) = B$, por lo tanto:

$$|A| \geqslant |f(A)| = |B|.$$

3. Esta propiedad es un corolario directo de las dos anteriores.

■

Corolario 6.5. *Sean A y B dos conjuntos finitos no vacíos. $|A| = |B|$ si y solo si existe $f : A \to B$ biyectiva.*

Proposición 6.6. *Sea $f : A \to B$ tal que $|A| = |B|$, ambos conjuntos finitos. Entonces, f es inyectiva si y solo si f es sobreyectiva*

Demostración.

Supongamos $\|A\| = \|B\| < \infty$	Suposición D.C.
Supongamos f inyectiva	Suposición D.C.
$\|f(A)\| = \|A\| = \|B\|$	
$f(A) \subseteq B$	
$f(A) = B$	
f es sobreyectiva	
f inyectiva $\Rightarrow f$ sobreyectiva	D.C.
Supongamos f no inyectiva	Suposición D.C.
$f(A) = \{f(a) : a \in A\}$	
$(\exists x, y \in A, x \neq y \wedge f(x) = f(y))$	
$\|f(A)\| < \|A\| = \|B\|$	
f no sobreyectiva	
f no inyectiva $\Rightarrow f$ no sobreyectiva	D.C.
f inyectiva $\Leftrightarrow f$ sobreyectiva	
$\|A\| = \|B\| < \infty \Rightarrow (f$ inyectiva $\Leftrightarrow f$ sobreyectiva$)$	D.C.

■

De este modo surge la noción de que dos conjuntos tienen el mismo cardinal cuando existe una biyección entre ellos. Formalicemos lo anterior:

Definición 6.9. Dados dos conjuntos A y B (no necesariamente finitos) diremos que tienen igual cardinal si existe una función biyectiva $f : A \to B$.

Proposición 6.7. *La relación tener igual cardinal es una relación de equivalencia.*

Demostración.

- Refleja: Sea $f : A \to A$ tal que $f(x) = x$, claramente f es biyectiva, luego $|A| = |A|$.
- Simétrica: Si $|A| = |B|$, entonces existe $f : A \to B$ biyectiva, luego existe $f^{-1} : B \to A$ biyectiva, de donde se concluye que $|B| = |A|$.
- Transitiva: Si $|A| = |B|$ y $|B| = |C|$, se tiene que existe $f : A \to B$ y $g : B \to C$ biyectivas, luego $g \circ f : A \to C$ también es biyectiva, por lo tanto $|A| = |C|$.

■

Definición 6.10. Sean A y B dos conjuntos. Si existe $f : A \to B$ inyectiva, entonces $|A| \leq |B|$.

Proposición 6.8. *La relación $|\cdot| \leq |\cdot|$ cumple que*

1. $|A| \leq |A|$

2. $|A| \leq |B| \wedge |B| \leq |C| \implies |A| \leq |C|$
3. $|A| \leq |B| \wedge |B| \leq |A| \implies |A| = |B|$

Demostración. De estas 3 proposiciones la única que no es evidente es (3), sin embargo no la demostraremos ya que esta demostración escapa a las herramientas que usamos en esta asignatura. ■

Estas definiciones se cumplen en el caso finito, como vimos en el principio del palomar. Veamos que pasa en el caso infinito.

Ejemplo 6.1. Sea $2\mathbb{N} = \{2n \in \mathbb{N} : n \in \mathbb{N}\}$ y $f : \mathbb{N} \to 2\mathbb{N}$ tal que $f(n) = 2n$. Claramente la función f es biyectiva luego $|\mathbb{N}| = |2\mathbb{N}|$, esto contradice nuestra intuición ya que $2\mathbb{N} \subsetneq \mathbb{N}$. El cardinal de $\mathbb{N}$ lo llamaremos aleph cero

De aquí concluimos que $|\mathbb{N}|$ y $|2\mathbb{N}|$ tienen el mismo tipo de infinito.

Después de ver este ejemplo, surge la pregunta natural, ¿existe más de un tipo de infinito? La respuesta, es sí, y este es un tema muy complicado y con muchas aristas que van a las bases de la matemática. Dada la naturaleza de este curso, no entraremos en grandes detalles, pero es relevante que al menos distingamos dos tipos de infinito: los infinitos numerables y los infinitos no numerables.

Definición 6.11. Diremos que el conjunto A es numerable si tiene cardinal finito o tiene cardinal aleph cero.

Teorema 6.9. *Sea $\{A_i\}_{i\in\mathbb{N}}$ una familia de conjuntos numerables, entonces $\bigcup_{i\in\mathbb{N}} A_i$ es numerable.*

Demostración. No haremos una demostración formal, pero usaremos la intuición. En este caso consideramos que si podemos asegurar poner todos los elemento de la familia de conjuntos en una secuencia, entonces la familia de conjuntos tiene a lo más el cardinal de $\mathbb{N}$. Para construir esa secuencia se utiliza el siguiente esquema de la Figura 6.3. ■

$$
\begin{array}{lllllll}
A_1 = \{a_1^1, & a_2^1, & a_3^1, & a_4^1, & a_5^1, & \cdots\} \\
A_2 = \{a_1^2, & a_2^2, & a_3^2, & a_4^2, & a_5^2, & \cdots\} \\
A_3 = \{a_1^3, & a_2^3, & a_3^3, & a_4^3, & a_5^3, & \cdots\} \\
A_4 = \{a_1^4, & a_2^4, & a_3^4, & a_4^4, & a_5^4, & \cdots\} \\
A_5 = \{a_1^5, & a_2^5, & a_3^5, & a_4^5, & a_5^5, & \cdots\} \\
\quad\ \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}
$$

$$\bigcup_{i\in\mathbb{N}} A_i = \{\, a_1^1,\ a_2^1,\ a_1^2,\ a_3^1,\ a_2^2,\ a_1^3,\ a_4^1,\ a_3^2,\ a_2^3,\ a_1^4,\ a_5^1,\ a_4^2,\ a_3^3,\ a_2^4,\ a_1^5, \ldots\}$$

Figura 6.3: Secuencia de elementos de la unión numerable de conjuntos numerables

Como corolario de este teorema se tiene que:

Corolario 6.10.

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{N}^k| = |\mathbb{Z}^k| = |\mathbb{Q}^k|$$

Otro conjunto conocido que nos interesa su cardinal es $\mathbb{R}$. Para esto observemos que $\tan : \left]-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right[\to \mathbb{R}$ es una función biyectiva, por lo tanto $\mathbb{R}$ tiene el mismo cardinal que $\left]-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right[$.

Así mismo, si definimos $f : [0,1] \to [a,b]$ como $f(x) = \frac{b-1}{a}x + 1$, vemos que f es biyectiva por lo tanto todos los intervalos de $\mathbb{R}$ tienen el mismo cardinal que $\mathbb{R}$.

Un último punto que debemos estudiar es si el cardinal de $\mathbb{R}$ es numerable o no.

Teorema 6.11. $\mathbb{R}$ *no es numerable.*

Demostración. Supongamos que el cardinal de $[0,1]$ es numerable, entonces existe $f : \mathbb{N} \to [0,1]$ biyectiva. Usando representación binaria, cada $x \in [0,1]$ podemos escribirlo como $x = 0.a_1a_2a_3\ldots$, donde $a_i \in \{0,1\}$. Luego:

$$\begin{aligned} f(1) &= 0.a_{1,1}a_{1,2}a_{1,3}\ldots \\ f(2) &= 0.a_{2,1}a_{2,2}a_{2,3}\ldots \\ f(3) &= 0.a_{3,1}a_{3,2}a_{3,3}\ldots \\ &\vdots \end{aligned}$$

Sea $\varepsilon = 0.\varepsilon_1\varepsilon_2\ldots$ tal que $\varepsilon_i = 1 - a_{i,i}$. Claramente ε no es la imagen de ningún n, luego f no es sobreyectiva y por lo tanto f no es biyectiva, lo que genera una contradicción. De esto concluimos que $|\mathbb{N}| \neq |[0,1]| = |\mathbb{R}|$. ■

Veamos ahora que $|\mathcal{P}(\mathbb{N})| = |[0,1]|$. Sea $f : \mathcal{P}(\mathbb{N}) \to [0,1]$ definida por: $f(A) = 0.a_1^A a_2^A a_3^A \ldots$ donde $a_i^A = 0$ si $i \notin A$ y $a_i^A = 1$ si $i \in A$. Es fácil ver que f es biyectiva y por lo tanto $|\mathcal{P}(\mathbb{N}) = |[0,1]| = |\mathbb{R}|$.

6.6. Ejercicios

P1. Sea $\mathbb{Z}_p$ el conjunto cociente de las congruencias modulo p. Estudie para $p = 2, 3, 4, 5$, la función:

$$\begin{aligned} f_r : \mathbb{Z}_p &\to \mathbb{Z}_p, \\ [x] &\to f_r([x]) = [r \cdot x] \end{aligned}$$

donde $r \in \{1, \ldots, p-1\}$.

(Indicación: Considere cierta la identidad de Bézout que dice que: "a y b son coprimos si y solo si $\exists u, v \in \mathbb{Z}, au + bv = 1$")

1. Pruebe que f está bien definida
2. Demuestre que, p es primo si y solo si $\forall r \in \{1, \ldots, p-1\}$, f_r es biyectiva.
   (Indicación: Considere cierta la identidad de Bézout que dice que: "a y b son coprimos si y solo si $(\exists u, v \in \mathbb{Z}, au + bv = 1)$")

P2.

1. Sean A y B conjuntos no vacíos, $g : A \to A$ y $h : B \to B$. Pruebe que:

   $$\begin{aligned} f : A \times B &\to A \times B \\ (x, y) &\to (g(x), h(y)) \end{aligned}$$

   es biyectiva si y solo si g y h lo son.
2. Sea,

   $$\begin{aligned} f_r : \mathbb{Z}_p \times \mathbb{Z}_p &\to \mathbb{Z}_p \times \mathbb{Z}_p \\ ([x], [y]) &\to ([x] \cdot [r], [y] + [r]) \end{aligned}$$

   donde $[x] \cdot [r] = [x \cdot r]$ y $[x] + [r] = [x + r]$.
   Pruebe que p es primo si y solo si $\forall r \in \{1, \ldots, p-1\}$, f_r es biyectiva.
3. Sea

   $$\begin{aligned} g : \mathbb{Z}_p \times \mathbb{Z}_p &\to \mathbb{Z}_p \\ ([x], [y]) &\to \max\{[x], [y]\} \end{aligned}$$

   donde $\max\{[x], [y]\} = \{\max\{\hat{x}, \hat{y}\} : \hat{x} \in [x], \hat{y} \in [y] \text{ y } \hat{x}, \hat{y} \in \{0, \ldots, p-1\}\}$.
   Encuentre $A \subseteq \mathbb{Z}_p \times \mathbb{Z}_p$ tal que $g \circ f_r|_A$ es biyectiva $(1 \leq r < p)$

P3. Sea $\mathcal{R}$ una relación asociada a $R \subseteq A \times B$. Sea además:

$$\begin{aligned} \tilde{\mathcal{R}} : A &\to \mathcal{P}(B) \\ x &\to \tilde{\mathcal{R}}(x) = \{y \in B : x \, \mathcal{R} \, y\} \end{aligned}$$

Demuestre que la función.

$$\begin{aligned} H : \mathcal{P}(A \times B) &\to \mathcal{F}(A, \mathcal{P}(B)) \quad \text{es inyectiva} \\ R \quad &\to \tilde{\mathcal{R}} \end{aligned}$$

donde $\mathcal{F}(A, \mathcal{P}(B)) = \{ f : A \to \mathcal{P}(B) \}$

P4. Demuestre que existen dos personas en el mundo con el mismo número de cabellos.

P5. Para cada par de números reales a y b se define:

$$\begin{aligned} f_{ab} : \mathbb{R} &\to \mathbb{R} \\ x &\to f_{ab}(x) = ax + b. \end{aligned}$$

1. Muestre que $f_{1b} \circ f_{a0} = f_{ab}$.
2. Para $a \neq 0$, pruebe que f_{ab} es biyectiva.
3. Para $a \neq 0$, calcule f_{ab}^{-1}.

P6. Sea $f : X \to Y$, $g : Y \to Z$. Sea $A \subseteq X$, pruebe que:

$$(g \circ f)|_A = g \circ (f|_A)$$

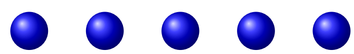
donde $\begin{aligned} f|_A : A &\to Y, \\ x &\to f|_A(x) = f(x) \end{aligned}$ y $\begin{aligned} (g \circ f)|_A : A &\to Z, \\ x &\to (g \circ f)|_A(x) = (g \circ f)(x) \end{aligned}$

P7. Sea $f : X \to Y$. Pruebe que f es inyectiva si y solo si $\forall A, B \subseteq X$, $f(A \cap B) = f(A) \cap f(B)$.

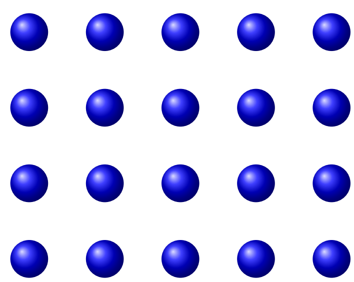
Capítulo 7

Técnicas de conteo

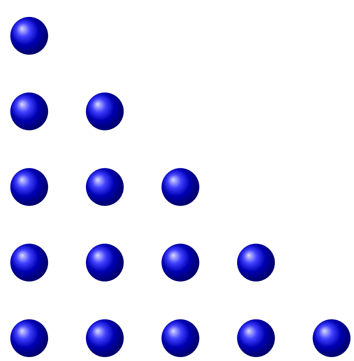
Seguramente, todos piensan que saben contar, pero a veces la tarea puede ser un poco más complicada de lo que parece a simple vista. Por ejemplo si pregunto ¿Cuántas pelotitas hay aquí?



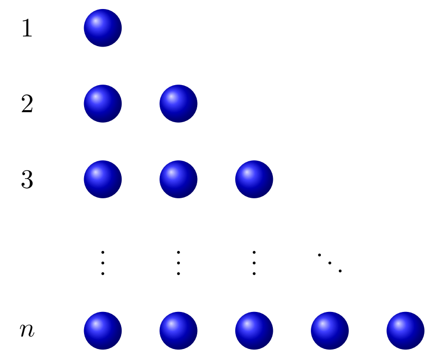
Por cierto, todos contestarán 5 pelotitas después de haberlas contado una a una. Pero si pregunto ¿Cuántas pelotitas hay aquí?



En este caso, contestarán 20, pero seguramente nadie contó las pelotitas una por una, para llegar a esta conclusión simplemente contaron 4 en vertical, 5 en horizontal y al realizar el producto de estos números obtuvieron 20. Bueno, pero que pasa si les pido contar:



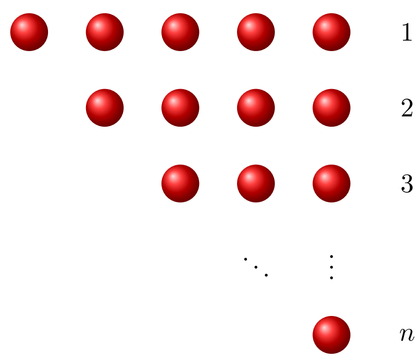
Aquí, nuevamente, parece que tendremos que contar exhaustivamente todas las pelotitas una por una y llegar a la conclusión que hay 15 pelotitas. Pero esto es muy poco eficiente, además, qué pasa ahora si lo que tengo es algo como esto:



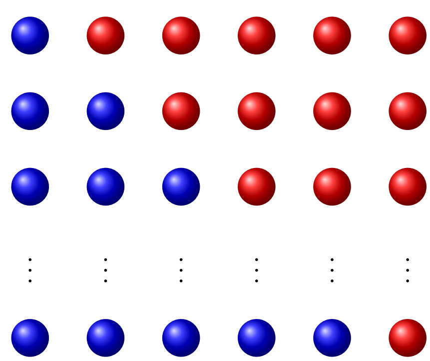
Es decir, quiero contar paramétricamente, en este caso mi cuenta depende de un parámetro n y dependiendo de su valor es el resultado que obtengo. En este caso quiero conocer la suma:

$$1 + 2 + 3 + \cdots + n$$

Una manera de calcular esta suma es ver las cosas desde otro ángulo. Si miramos el dibujo a continuación, vemos que tenemos la misma cantidad de pelotitas que antes, pero en otra posición.



De este modo si juntamos ambos dibujos tendremos:



Al verlo de este modo, tenemos un rectángulo y obtenemos que:

$$2(1 + 2 + 3 + \cdots + n) = n(n+1)$$
$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Pero, qué pasa si ahora queremos conocer la suma de los cuadrados de los n primeros enteros, o la suma de las n primeras potencias de 2 u otro número, tenemos que utilizar otro tipo de técnicas y para eso comenzamos por introducir el concepto de sumatoria.

7.1. Sumatorias

Definición 7.1.

$$\sum_{i=k}^{n} a_i = \begin{cases} a_k & \text{Si } k = n, \\ \sum\limits_{i=n}^{k} a_i & \text{Si } k > n, \\ \sum\limits_{i=k}^{n-1} a_i + a_n & \text{Si } k < n. \end{cases}$$

Intuitivamente,

$$\sum_{i=k}^{n} a_i = a_k + a_{k+1} + \cdots + a_n.$$

Propiedades de las sumatorias

1. Si $n > k$, $\sum\limits_{i=k}^{n} a_i = a_k + \sum\limits_{i=k+1}^{n} a_i$.

   Demostración.

   Base. Si $n = k+1$,

   $$\sum_{i=k}^{k+1} a_i = \sum_{i=k}^{k} a_i + a_{k+1} = a_k + a_{k+1} = a_k + \sum_{i=k+1}^{k+1} a_i$$

   Hipótesis de inducción. $\sum\limits_{i=k}^{n} a_i = a_k + \sum\limits_{i=k+1}^{n} a_i$.

   Paso inductivo.

   $$\sum_{i=k}^{n+1} a_i = \sum_{i=k}^{n} a_i + a_{n+1} \overset{\text{H}}{=} a_k + \sum_{i=k+1}^{n} a_i + a_{n+1} = a_k + \sum_{i=k+1}^{n+1} a_i.$$

   ■

2. $\sum\limits_{i=k}^{n} a_i = \sum\limits_{i=k}^{l} a_i + \sum\limits_{i=l+1}^{n} a_i, \quad l \in \{k, \ldots, n-1\}$.

   Demostración. Por inducción sobre l

   Base. si $l = k$,

   $$\sum_{i=k}^{n} a_i \overset{1}{=} a_k + \sum_{i=k+1}^{n} a_i = \sum_{i=k}^{k} a_i + \sum_{i=k+1}^{n} a_i$$

   Hipótesis de inducción. $\sum\limits_{i=k}^{n} a_i = \sum\limits_{i=k}^{l} a_i + \sum\limits_{i=l+1}^{n} a_i$

Paso inductivo. Caso $l+1$,

$$\sum_{i=k}^{n} a_i \overset{\text{Ⓗ}}{=} \sum_{i=k}^{l} a_i + \sum_{i=l+1}^{n} a_i \overset{1}{=} \sum_{i=k}^{l} a_i + a_{l+1} + \sum_{i=l+2}^{n} a_i = \sum_{i=k}^{l+1} a_i + \sum_{i=l+2}^{n} a_i$$

■

3. $\sum_{i=k}^{n} \lambda = (n-k+1)\lambda.$

Demostración.

Base. Si $n=k$,

$$\sum_{i=k}^{k} \lambda = \lambda = 1 \cdot \lambda = (k-k+1)\lambda.$$

Hipótesis de inducción. $\sum_{i=k}^{n} \lambda = (n-k+1)\lambda$

Paso inductivo. Caso $n+1$,

$$\sum_{i=k}^{n+1} \lambda = \sum_{i=k}^{n} \lambda + \lambda \overset{\text{Ⓗ}}{=} (n-k+1)\lambda + \lambda = (n+1-k+1)\lambda.$$

■

4. $\sum_{i=k}^{n} \lambda a_i = \lambda \sum_{i=k}^{n} a_i.$

Demostración.

Base. Si $n=k$,

$$\sum_{i=k}^{k} \lambda a_i = \lambda a_k = \lambda \sum_{i=k}^{k} a_i.$$

Hipótesis de inducción. $\sum_{i=k}^{n} \lambda a_i = \lambda \sum_{i=k}^{n} a_i$

Paso inductivo. Caso $n+1$,

$$\sum_{i=k}^{n+1} \lambda a_i = \sum_{i=k}^{n} \lambda a_i + \lambda a_{n+1} \overset{\text{Ⓗ}}{=} \lambda \sum_{i=k}^{n} a_i + \lambda a_{n+1} = \lambda \left(\sum_{i=k}^{n} a_i + a_{n+1} \right) = \lambda \sum_{i=k}^{n+1} a_i$$

■

5. $\sum_{i=k}^{n} (a_i + b_i) = \sum_{i=k}^{n} a_i + \sum_{i=k}^{n} b_i.$

Demostración.

Base. Si $n = k$,

$$\sum_{i=k}^{k}(a_i + b_i) = a_k + b_k = \sum_{i=k}^{k} a_i + \sum_{i=k}^{k} b_i$$

Hipótesis de inducción. $\sum_{i=k}^{n}(a_i + b_i) = \sum_{i=k}^{n} a_i + \sum_{i=k}^{n} b_i$

Paso inductivo. Caso $n + 1$,

$$\begin{aligned}\sum_{i=k}^{n+1}(a_i + b_i) &= \sum_{i=k}^{n}(a_i + b_i) + a_{n+1} + b_{n+1} \overset{\text{H}}{=} \sum_{i=k}^{n} a_i + \sum_{i=k}^{n} b_i + a_{n+1} + b_{n+1} \\ &= \sum_{i=k}^{n} a_i + a_{n+1} + \sum_{i=k}^{n} b_i + b_{n+1} = \sum_{i=k}^{n+1} a_i + \sum_{i=k}^{n+1} b_i\end{aligned}$$

■

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

Demostración.

$$\sum_{i=k}^{n}(a_i - b_i) = \sum_{i=k}^{n}(a_i + (-1)b_i) = \sum_{i=k}^{n} a_i + \sum_{i=k}^{n}(-1)b_i = \sum_{i=k}^{n} a_i + (-1)\sum_{i=k}^{n} b_i = \sum_{i=k}^{n} a_i - \sum_{i=k}^{n} b_i$$

■

7. $\sum_{i=k}^{n} a_i = \sum_{i=s}^{n-k+s} a_{i-s+k}$ Cambio de variables.

Demostración.

Base. $n = k$

$$\sum_{i=s}^{k-k+s} a_{i-s+k} = \sum_{i=s}^{s} a_{i-s+k} = a_{s-s+k} = a_k = \sum_{i=k}^{k} a_i$$

Hipótesis de inducción. $\sum_{i=k}^{n} a_i = \sum_{i=s}^{n-k+s} a_{i-s+k}$

Paso inductivo.

$$\sum_{i=s}^{n+1-k+s} a_{i-s+k} = \sum_{i=s}^{n-k+s} a_{i-s+k} + a_{(n+1-k+s)-s+k} \overset{\text{H}}{=} \sum_{i=k}^{n} a_i + a_{n+1} = \sum_{i=k}^{n+1} a_i$$

■

8. $\sum_{i=k}^{n}(a_{i+1} - a_i) = a_{n+1} - a_k$ Propiedad Telescópica.

Demostración. Nuevamente por inducción sobre n.

Base. Si $n = k$,

$$\sum_{i=k}^{k}(a_{i+1} - a_i) = a_{k+1} - a_k.$$

Hipótesis de inducción. $\sum_{i=k}^{n}(a_{i+1} - a_i) = a_{n+1} - a_k$.

Paso inductivo. Caso $n + 1$,

$$\sum_{i=k}^{n+1}(a_{i+1} - a_i) = \sum_{i=k}^{n}(a_{i+1} - a_i) + a_{n+2} - a_{n+1} \overset{\text{Ⓗ}}{=} a_{n+1} - a_k + a_{n+2} - a_{n+1} = a_{n+2} - a_k.$$

■

7.2. Coeficientes binomiales

Definición 7.2. Se define $\binom{n}{k}$ como el número de subconjuntos de cardinal k de un conjunto de cardinal n.

Esta cantidad es muy útil para calcular, por ejemplo, las probabilidades de ganar un juego de azar y muchos otros problemas combinatoriales.

Propiedades

1. $\displaystyle\binom{n}{k} = \frac{n!}{k!(n-k)!}$

   Hagamos una deducción de esta fórmula. Supongamos en primer lugar, que debemos elegir una secuencia de k elementos sin repetición ¿De cuántas maneras puedo hacer esto? Bueno, el primer elemento lo puedo elegir de n formas distintas, el segundo de $n - 1$ formas y así sucesivamente el k-ésimo lo puedo elegir de $n - k + 1$ formas distintas. De este modo el número de secuencias (ordenadas) sin repetición de k elementos en un conjunto de n elementos es:

   $$n(n-1)\cdots(n-k+1)$$

   Pero, en este caso no nos interesa el orden en el que aparecen los elementos de modo que debemos dividir esta cantidad por el número de formas de ordenar estos k elementos. Siguiendo la misma lógica anterior: el primer elemento lo puedo elegir de k formas distintas, el segundo de $k-1$ formas y así sucesivamente el k-ésimo lo puedo elegir de una sola forma. Es decir, existen $k!$ ordenes. De este modo concluimos que:

   $$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

   Pero si amplifico esta fracción por $(n-k)!$ obtendremos:

   $$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}\frac{(n-k)!}{(n-k)!} = \frac{n!}{k!(n-k)!}$$

2. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

   Aquí podemos comprobar la fórmula matemáticamente:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!} \\
&= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} \\
&= \frac{(n-1)!}{(k-1)!(n-1-k)!(n-k)} + \frac{(n-1)!}{k(k-1)!(n-1-k)!} \\
&= \frac{(n-1)!}{(k-1)!(n-1-k)!}\left(\frac{1}{n-k} + \frac{1}{k}\right) \\
&= \frac{(n-1)!}{(k-1)!(n-1-k)!} \cdot \frac{k+n-k}{k(n-k)} \\
&= \frac{(n-1)!}{(k-1)!(n-1-k)!} \cdot \frac{n}{k(n-k)} = \frac{n!}{k!(n-k)!} \\
&= \binom{n}{k}
\end{aligned}$$

   Sin embargo, resulta mucho más interesante analizar que significan estos términos. Sin pérdida de generalidad podemos suponer que un conjunto de cardinal n lo podemos describir como:

$$A = \{a_1, a_2, \ldots, a_n\}$$

   Si queremos encontrar todos los subconjuntos de cardinal k podemos considerar que existen dos tipos de subconjuntos de cardinal k:

   a) Los subconjuntos que no contienen a_n. Para tener conjuntos como este basta elegir k elementos en el conjunto $\{a_1, \ldots, a_{n-1}\}$, es decir los conjuntos de este tipo son los subconjuntos de cardinal k de un conjunto de cardinal $n-1$, luego existen $\binom{n-1}{k}$ subconjuntos de este tipo.

   b) Los subconjuntos que contienen a_n. En este caso basta elegir $k-1$ elementos en el conjunto $\{a_1, \ldots, a_{n-1}\}$ y agregar el elemento a_n, de este modo los conjuntos de este tipo son los subconjuntos de cardinal $k-1$ de un conjunto de cardinal $n-1$, luego existen $\binom{n-1}{k-1}$ subconjuntos de este tipo.

   Así haciendo la suma obtenemos que:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

   El cálculo de los coeficientes binomiales con esta recurrencia puede observarse con el Tríangulo de Pascal (ver Figura 7.1).

3. $\binom{n}{k} = \binom{n}{n-k}$

   Demostración. Sin duda hacer el cálculo no resulta complicado:

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

   Pero me parece mucho más interesante ir al significado y darnos cuenta que en realidad es evidente. Si queremos elegir k elementos dentro de un conjunto de n elementos una manera de hacerlo es

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}
$$

$n \backslash k$	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

Figura 7.1: Triángulo de Pascal

elegir los $n-k$ que quedan afuera. Es decir, cada vez que elijo un conjunto de k elementos estoy también eligiendo un conjunto de $n-k$ (los que quedan fuera), luego tenemos una función inyectiva entre los subconjuntos de cardinal k y los de cardinal $n-k$, por lo tanto tenemos la misma cantidad. ■

4. $(a+b)^n = \sum\limits_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$

De esta forma viene el nombre de coeficientes binomiales, ya que son los coeficientes que acompaña a las potencias en la expansión de una potencia de un binomio.

Demostración.

Base. Caso $n = 1$.

$$(a+b)^1 = a + b = a^1 b^0 + a^0 b^1$$

Hipótesis de inducción. $(a+b)^n = \sum\limits_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$

Paso inductivo.

$$(a+b)^{n+1} = (a+b)(a+b)^n \overset{H}{=} (a+b)\sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$
$$(a+b)^{n+1} = a\sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i + b\sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$
$$(a+b)^{n+1} = \sum_{i=0}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^{i+1}$$

Haciendo un cambio de variable en la segunda sumatoria

$$(a+b)^{n+1} = \sum_{i=0}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=1}^{n+1} \binom{n}{i-1} a^{n-(i-1)} b^i$$
$$(a+b)^{n+1} = \sum_{i=0}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=1}^{n+1} \binom{n}{i-1} a^{n+1-i} b^i$$

Separamos el primer término de la primera sumatoria y el último de la segunda para igualar los límites,

$$(a+b)^{n+1} = \binom{n}{0}a^{n+1}b^0 + \sum_{i=1}^{n}\binom{n}{i}a^{n+1-i}b^i + \sum_{i=1}^{n}\binom{n}{i-1}a^{n+1-i}b^i + \binom{n}{n+1-1}a^{n+1-(n+1)}b^{n+1}$$

Como $\binom{n}{0} = \binom{n}{n} = 1 = \binom{n+1}{0} = \binom{n+1}{n+1}$:

$$(a+b)^{n+1} = \binom{n+1}{0}a^{n+1}b^0 + \sum_{i=1}^{n}\left[\binom{n}{i} + \binom{n}{i-1}\right]a^{n+1-i}b^i + \binom{n+1}{n+1}a^{n+1-(n+1)}b^{n+1}$$

Como $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$,

$$(a+b)^{n+1} = \binom{n+1}{0}a^{n+1}b^0 + \sum_{i=1}^{n}\binom{n+1}{i}a^{n+1-i}b^i + \binom{n+1}{n+1}a^{n+1-(n+1)}b^{n+1}$$

$$(a+b)^{n+1} = \sum_{i=0}^{n+1}\binom{n+1}{i}a^{n+1-i}b^i$$

■

5. $2^n = \sum_{i=0}^{n}\binom{n}{i}$

Esto lo podemos demostrar de varias formas. En este caso, después de haber hecho las demostraciones anteriores, lo primero que se nos ocurre es hacer una demostración por inducción similar a la anterior, lo que por cierto resulta.

Base. Caso $n = 1$.

$$2^1 = \binom{1}{0} + \binom{1}{1} = 1 + 1 = 2$$

Hipótesis de inducción. $2^n = \sum_{i=0}^{n}\binom{n}{i}$

Paso inductivo.

$$\sum_{i=0}^{n+1}\binom{n+1}{i} = \binom{n+1}{0} + \sum_{i=1}^{n}\binom{n+1}{i} + \binom{n+1}{n+1}$$

$$\sum_{i=0}^{n+1}\binom{n+1}{i} = \binom{n}{0} + \sum_{i=1}^{n}\left[\binom{n}{i} + \binom{n}{i-1}\right] + \binom{n}{n}$$

$$\sum_{i=0}^{n+1}\binom{n+1}{i} = \binom{n}{0} + \sum_{i=1}^{n}\binom{n}{i} + \sum_{i=1}^{n}\binom{n}{i-1} + \binom{n}{n}$$

$$\sum_{i=0}^{n+1}\binom{n+1}{i} = \sum_{i=0}^{n}\binom{n}{i} + \sum_{i=0}^{n-1}\binom{n}{i} + \binom{n}{n}$$

$$\sum_{i=0}^{n+1}\binom{n+1}{i} = \sum_{i=0}^{n}\binom{n}{i} + \sum_{i=0}^{n}\binom{n}{i}$$

$$\sum_{i=0}^{n+1}\binom{n+1}{i} = 2\sum_{i=0}^{n}\binom{n}{i} \overset{\text{H}}{=} 2 \cdot 2^n = 2^{n+1}$$

Sin embargo, hay maneras mucho más simples de demostrar esta igualdad. La primera es recordar que un conjunto de n elementos tiene exactamente 2^n subconjuntos y que $\binom{n}{i}$ son los subconjuntos de cardinal i de un conjunto de cardinal n, de modo que si sumamos la cantidad de subconjuntos de cada cardinal de un conjunto de cardinal n debemos obtener 2^n.

La segunda forma es aún mas simple, usando la fórmula anterior con $a = b = 1$ obtenemos:

$$\begin{aligned}(1+1)^n &= \sum_{i=0}^{n}\binom{n}{i}1^{n-i}1^i = \sum_{i=0}^{n}\binom{n}{i}1\cdot 1\\ 2^n &= \sum_{i=0}^{n}\binom{n}{i}\end{aligned}$$

Ejemplos de sumatorias

En primer lugar resulta muy interesante calcular la suma de la progresión geométrica, de hecho ya hemos visto que una suma de este tipo aparece en las torres de Hanoi. En este caso haremos el cálculo más general de $\sum_{i=0}^{n} a^i$, donde $a \notin \{0, 1\}$.

$$\sum_{i=0}^{n} a^i = \frac{1-a}{1-a}\sum_{i=0}^{n} a^i = \frac{1}{1-a}\sum_{i=0}^{n}(1-a)a^i = \frac{1}{1-a}\sum_{i=0}^{n}(a^i - a^{i+1})$$

Por propiedad telescópica:

$$\sum_{i=0}^{n} a^i = \frac{a^0 - a^{n+1}}{1-a} = \frac{1-a^{n+1}}{1-a}$$

El caso particular de $a = 2$ nos da:

$$\sum_{i=0}^{n} 2^i = \frac{1-2^{n+1}}{1-2} = \frac{1-2^{n+1}}{-1} = 2^{n+1} - 1$$

Otro caso interesante es $S(k)_n = \sum_{i=1}^{n} i^k$. Ya hemos visto que $S(1)_n = \frac{n(n+1)}{2}$, sin embrago para averiguar este valor hemos tenido que recurrir a astucias más allá de las sumatorias. Veamos ahora si podemos calcular este valor y, de este modo, aprender a calcular los restantes.

$$\begin{aligned}\sum_{i=0}^{n}(i+1)^2 &= \sum_{i=0}^{n}(i^2+2i+1)\\ \sum_{i=1}^{n+1} i^2 &= \sum_{i=0}^{n} i^2 + 2\sum_{i=0}^{n} i + \sum_{i=0}^{n} 1\\ \sum_{i=1}^{n} i^2 + (n+1)^2 &= \sum_{i=1}^{n} i^2 + 2\sum_{i=1}^{n} i + (n+1)\\ (n+1)^2 &= 2\sum_{i=1}^{n} i + (n+1)\\ 2\sum_{i=1}^{n} i &= (n+1)^2 - (n+1) = (n+1)(n+1-1) = n(n+1)\\ \sum_{i=1}^{n} i &= \frac{n(n+1)}{2}\end{aligned}$$

Como vemos tratando de calcular una suma de un grado superior hemos logrado calcular lo que queríamos. La pregunta evidente ahora es ¿podremos calcular $S(2)_n$ usando una técnica similar?

$$\sum_{i=0}^{n}(i+1)^3 = \sum_{i=0}^{n}(i^3 + 3i^2 + 3i + 1)$$

Haciendo un cambio de variables a la izquierda y separando las sumatorias a la derecha obtenemos:

$$\sum_{i=1}^{n+1} i^3 = \sum_{i=0}^{n} i^3 + 3\sum_{i=0}^{n} i^2 + 3\sum_{i=0}^{n} i + \sum_{i=0}^{n} 1$$

Por definición de sumatoria separamos el último término en la izquierda y, por propiedad (1) el primer término en las sumatorias de la derecha, como esos términos son 0, los eliminamos:

$$\begin{aligned}
\sum_{i=1}^{n} i^3 + (n+1)^3 &= \sum_{i=1}^{n} i^3 + 3\sum_{i=1}^{n} i^2 + 3\sum_{i=1}^{n} i + (n+1) \\
(n+1)^3 &= 3\sum_{i=1}^{n} i^2 + 3\sum_{i=1}^{n} i + (n+1) \\
3\sum_{i=1}^{n} i^2 &= (n+1)^3 - 3\sum_{i=1}^{n} i - (n+1) \\
3\sum_{i=1}^{n} i^2 &= (n+1)^3 - 3\frac{n(n+1)}{2} - (n+1) = (n+1)\left((n+1)^2 - \frac{3n}{2} - 1\right) \\
3\sum_{i=1}^{n} i^2 &= (n+1)\left(n^2 + 2n + 1 - \frac{3n}{2} - 1\right) = (n+1)\left(n^2 + 2n - \frac{3n}{2}\right) \\
3\sum_{i=1}^{n} i^2 &= (n+1)\left(n^2 + \frac{n}{2}\right) = n(n+1)\left(n + \frac{1}{2}\right) = \frac{n(n+1)(2n+1)}{2} \\
\sum_{i=1}^{n} i^2 &= \frac{n(n+1)(2n+1)}{6}
\end{aligned}$$

Esto nos da la idea que siguiendo este procedimiento podemos calcular cualquier $S(k)_n$ en tanto conozcamos los anteriores. Sin embargo, esto es muy trabajoso e implica calcular todos los anteriores.

Pero también podemos observar que en ambos casos el resultado es un polinomio de grado $k+1$, es decir, $S(1)_n$ es un polinomio de grado 2 en n y $S(2)_n$ es un polinomio de grado 3. Entonces probemos por inducción sobre k que $S(k)_n$ es un polinomio de grado $k+1$ en n.

Base. La base de la inducción es el cálculo de $S(1)_n$ que ya se realizó.

Hipótesis de inducción. $\forall l \leq k, S(l)_n$ es un polinomio de grado $l+1$. (inducción fuerte).

Paso inductivo.

$$\sum_{i=0}^{n}(i+1)^{k+2} = \sum_{i=0}^{n}\sum_{j=0}^{k+2}\binom{k+2}{j} i^j$$

Haciendo un cambio de variables a la izquierda y, como los límites de la sumatoria al interior no dependen de la variable de la sumatoria al exterior en la sumatoria doble, podemos cambiar el orden de las sumatorias a la derecha, así obtenemos:

$$\sum_{i=1}^{n+1} i^{k+2} = \sum_{j=0}^{k+2} \binom{k+2}{j} \sum_{i=0}^{n} i^j$$

$$\sum_{i=1}^{n} i^{k+2} + (n+1)^{k+2} = \binom{k+2}{0} \sum_{i=0}^{n} i^0 + \sum_{j=1}^{k+1} \binom{k+2}{j} \sum_{i=0}^{n} i^j + \binom{k+2}{k+2} \sum_{i=0}^{n} i^{k+2}$$

$$(n+1)^{k+2} = \sum_{i=0}^{n} 1 + \sum_{j=1}^{k+1} \binom{k+2}{j} \sum_{i=1}^{n} i^j$$

$$\binom{k+2}{k+1} \sum_{i=1}^{n} i^{k+1} = (n+1)^{k+2} - (n+1) - \underbrace{\sum_{j=1}^{k} \binom{k+2}{j} \sum_{i=1}^{n} i^j}_{\substack{\text{combinación lineal de} \\ \text{polinomios de grado } \leq k+1}} = \text{polinomio de grado } k+2$$

Lo mejor de este resultado es que nos permite encontrar cualquier $S(k)_n$ sin necesidad de conocer los anteriores. Por ejemplo si queremos calcular $S(3)_n$ sabemos que esto es un polinomio de grado 4. Luego:

$$S(3)_n = An^4 + Bn^3 + Cn^2 + Dn + E$$

Ahora solo debemos calcular A, B, C, D yE. para esto usamos los primeros términos de la sucesión. Solo para hacer más fácil este cálculo consideramos que $S(3)_n = \sum_{i=0}^{n} i^3$, como el primer término es cero, es exactamente lo mismo que partir desde 1.

$$\begin{aligned}
S(3)_0 &= A0^4 + B0^3 + C0^2 + D0 + E = E = 0 \\
S(3)_1 &= A1^4 + B1^3 + C1^2 + D1 + E = A + B + C + D + E = 1 \\
S(3)_2 &= A2^4 + B2^3 + C2^2 + D2 + E = 16A + 8B + 4C + 2D + E = 9 \\
S(3)_3 &= A3^4 + B3^3 + C3^2 + D3 + E = 81A + 27B + 9C + 3D + E = 36 \\
S(3)_4 &= A4^4 + B4^3 + C4^2 + D4 + E = 256A + 64B + 16C + 4D + E = 100
\end{aligned}$$

Ahora se debe resolver el sistema lineal. Claramente el sistema queda como:

$$\begin{array}{rrrrr} & & & & E = 0 \\ A+ & B+ & C+ & D+ & E = 1 \\ 16A+ & 8B+ & 4C+ & 2D+ & E = 9 \\ 81A+ & 27B+ & 9C+ & 3D+ & E = 36 \\ 256A+ & 64B+ & 16C+ & 4D+ & E = 100 \end{array} \implies \begin{array}{ll} A & = \frac{1}{4} \\ B & = \frac{1}{2} \\ C & = \frac{1}{4} \\ D & = 0 \\ E & = 0 \end{array}$$

Luego,

$$S(3)_n = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2 = \frac{1}{4}n^2(n^2 + 2n + 1) = \frac{n^2(n+1)^2}{4} = \left(\frac{n(n+1)}{2}\right)^2$$

7.3. Recurrencias

Una recurrencia es una sucesión real donde cada término de la secuencia es definido como una función de términos anteriores. En esta parte del curso, estudiaremos algunos casos particulares, para los cuales podemos encontrar una solución.

Hasta este punto ya conocemos la recurrencia de las torres de Hanoi donde.

$$\begin{aligned} h_1 &= 1 \\ h_{n+1} &= 2h_n + 1 \end{aligned}$$

y hemos encontrado una solución para ella, pero lo que buscamos es tener un método que nos permita encontrar esta fórmula cerrada sin tener que adivinar sino que usando un método matemático que nos permita encontrar la solución.

7.3.1. Recurrencias lineales homogéneas

Definición 7.3. Una *recurrencia lineal homogénea de grado k* es una recurrencia definida por:

$$T_n = \sum_{i=1}^{k} a_i T_{n-i}$$

En este punto usaremos espacios vectoriales para construir las demostraciones, un pequeño recordatorio de este tema puede verse en Apéndice B

Teorema 7.1. *Sea $\mathcal{F}_{\mathbb{N}} = \left\{ f : \mathbb{N} \to \mathbb{C} \right\}$ el espacio vectorial de las funciones con dominio en $\mathbb{N}$ y recorrido en $\mathbb{C}$ entonces $\mathcal{F} = \left\{ h \in \mathcal{F}_{\mathbb{N}} : h_n = \sum_{i=1}^{k} a_i h_{n-i} \right\}$ es un subespacio vectorial de $\mathcal{F}_{\mathbb{N}}$ de dimensión k.*

Demostración. En primer lugar probemos que $\vec{0} \in \mathcal{F}$, Esto obviamente es cierto ya que:

$$0 = \vec{0}_n = \sum_{i=1}^{k} a_i \cdot \vec{0}_{n-i} = 0$$

En segundo lugar probemos que $\mathcal{F}$ es cerrado para la suma. Sean $f, g \in \mathcal{F}$:

$$\begin{aligned} f_n &= \sum_{i=1}^{k} a_i f_{n-i} \\ g_n &= \sum_{i=1}^{k} a_i g_{n-i} \end{aligned}$$

sumando ambas ecuaciones obtenemos:

$$\begin{aligned} f_n + g_n &= \sum_{i=1}^{k} a_i f_{n-i} + \sum_{i=1}^{k} a_i g_{n-i} = \sum_{i=1}^{k} (a_i f_{n-i} + a_i g_{n-i}) \\ f_n + g_n &= \sum_{i=1}^{k} a_i (f_{n-i} + g_{n-i}) \\ (f+g)_n &= \sum_{i=1}^{k} a_i (f+g)_{n-i} \end{aligned}$$

Por último, probemos que es cerrado con producto por escalar. Sea $f \in \mathcal{F}$:

$$\begin{aligned} f_n &= \sum_{i=1}^{k} a_i f_{n-i} && / \cdot \alpha \\ \alpha f_n &= \alpha \sum_{i=1}^{k} a_i f_{n-i} = \sum_{i=1}^{k} a_i \alpha f_{n-i} \\ (\alpha f)_n &= \alpha \sum_{i=1}^{k} a_i f_{n-i} = \sum_{i=1}^{k} a_i (\alpha f)_{n-i} \end{aligned}$$

Con esto hemos probado que es espacio vectorial. Para probar que su dimensión es k debemos encontrar k sucesiones linealmente independientes que generen todo el espacio. Sean $e_n^1, \dots, e_n^k$ las sucesiones definidas por:

$$e_j^i = \begin{cases} 1 & j \leq k \wedge i = j \\ 0 & j \leq k \wedge i \neq j \\ \sum_{l=1}^{k} a_l e_{j-l}^i & j > k \end{cases}$$

Como estas sucesiones cumplen la ecuación de recurrencia son elementos de $\mathcal{F}$. Veamos que son linealmente independientes. Supongamos:

$$\sum_{i=1}^{k} a_i e_n^i = \vec{0}$$

Entonces:

$$\forall j \leq k, \sum_{i=1}^{k} a_i e_j^i = 0$$

Pero como $e_j^i \neq 0$ si y solo si $i = j$

$$\forall j \leq k, a_j e_j^j = 0$$

Por lo tanto, $\forall j \leq k, a_j = 0$. Luego estas recurrencias son l.i.

Ahora solo necesitamos probar que cualquier sucesión de $\mathcal{F}$ puede escribirse como una combinación lineal de $e_n^1, \dots, e_n^k$. Sea $f \in \mathcal{F}$ cualquiera, f debe ser tal que:

$$f_j = \begin{cases} b_j & j \leq k \\ \sum_{i=1}^{k} a_i f_{j-i}^j & j > k \end{cases}$$

Claramente:

$$f_j = \sum_{i=1}^{k} b_i e_j^i$$

Luego, $e_n^1, \dots, e_n^k$ es una base de $\mathcal{F}$. ■

De este modo, para encontrar las soluciones de estas recurrencias necesitamos encontrar k sucesiones l.i. que cumplan la ecuación de recurrencia.

En primer lugar, imaginemos que queremos tener una solución de tipo exponencial, de modo que queremos saber para que valores de $q \neq 0$ la función q^n es solución de la ecuación de recurrencia $T_n = \sum_{i=1}^{k} a_i T_{n-i}$. Con esto encontraremos algunas soluciones, si estas son suficientes tenemos nuestra base del espacio vectorial y si no, deberemos seguir buscando.

$$\begin{aligned} q^n &= \sum_{i=1}^{k} a_i q^{n-i} && / : q^{n-k} \\ q^k &= \sum_{i=1}^{k} a_i q^{n-i-n+k} = \sum_{i=1}^{k} a_i q^{k-i} \\ q^k - \sum_{i=1}^{k} a_i q^{k-i} &= 0 \end{aligned}$$

Claramente los valores de q que cumplen esta ecuación son las raíces del polinomio. Llamaremos a este polinomio, polinomio característico. Luego si analizamos cualquier ecuación de recurrencia tendremos soluciones del tipo $T_n = q^n$, donde q es una raíz del polinomio característico. Si todas las soluciones del polinomio tienen multiplicidad algebraica 1, por Teorema Fundamental del Álgebra, obtendremos k soluciones linealmente independientes y, de este modo, tenemos una base del espacio de soluciones.

Ejemplo 7.1.

$$T_n = T_{n-1} + 6T_{n-2}$$

Es una recurrencia lineal homogénea de grado 2, de modo que debemos encontrar dos soluciones linealmente independientes.

Polinomio característico:

$$x^2 - x - 6 = (x-3)(x+2)$$

Luego:

$$T_n = \alpha 3^n + \beta(-2)^n$$

De este modo tenemos todas las soluciones posibles.

Pero ¿qué ocurre si una raíz del polinomio tiene multiplicidad algebraica 2 o más?

Analicemos el caso con multiplicidad algebraica igual a 2. Si tenemos el polinomio característico:

$$x^2 - 2rx + r^2 = 0$$

que proviene de la ecuación:

$$s_n = 2rs_{n-1} - r^2 s_{n-2}$$

tenemos que r es una raíz del polinomio característico con multiplicidad algebraica 2.

De este modo, veamos que le pasa a la ecuación de recurrencia cuando resto a ambos lados rs_{n-1}:

$$\begin{aligned} s_n &= 2rs_{n-1} - r^2 s_{n-2} && / - rs_{n-1} \\ s_n - rs_{n-1} &= 2rs_{n-1} - rs_{n-1} - r^2 s_{n-2} \\ s_n - rs_{n-1} &= rs_{n-1} - r^2 s_{n-2} = r(s_{n-1} - rs_{n-2}) \end{aligned}$$

Considerando $t_n = s_n - rs_{n-1}$, obtenemos:

$$t_n = rt_{n-1}$$

que, por lo ya visto $t_n$tiene como solución $t_n = tr^n$, luego, volviendo a la recurrencia s_n, tenemos:

$$\begin{aligned} s_n - rs_{n-1} &= tr^n \\ s_n &= rs_{n-1} + tr^n \end{aligned}$$

Ahora queremos resolver esta recurrencia que ya no es homogénea, pero sigue siendo lineal y es solo de grado 1, por lo tanto podemos tratar de hacerlo de forma más bien manual.

$$\begin{aligned} s_0 &= s \\ s_1 &= rs_0 + tr \\ s_2 &= rs_1 + tr^2 \\ s_3 &= rs_2 + tr^3 \\ &\vdots \\ s_n &= rs_{n-1} + r^n \end{aligned}$$

Ahora vamos a multiplicar ambos lados de cada ecuación por un factor adecuado y haremos la suma a ambos lados:

$$\begin{aligned} s_0 &= s \\ \frac{1}{r}s_1 &= \frac{1}{r}rs_0 + \frac{1}{r}r = s_0 + t \\ \frac{1}{r^2}s_2 &= \frac{1}{r^2}rs_1 + \frac{1}{r^2}r^2 = \frac{1}{r}s_1 + t \\ \frac{1}{r^3}s_3 &= \frac{1}{r^3}rs_2 + \frac{1}{r^3}r^3 = \frac{1}{r^2}s_2 + t \\ &\vdots \\ \frac{1}{r^n}s_n &= \frac{1}{r^n}rs_{n-1} + \frac{1}{r^n}r^n = \frac{1}{r^{n-1}}s_{n-1} + t \end{aligned}$$

$$\begin{aligned} \cancel{s_0} &= s \\ \cancel{\frac{1}{r}s_1} &= \cancel{s_0} + t \\ \cancel{\frac{1}{r^2}s_2} &= \cancel{\frac{1}{r}s_1} + t \\ \cancel{\frac{1}{r^3}s_3} &= \cancel{\frac{1}{r^2}s_2} + t \\ &\vdots \\ \frac{1}{r^n}s_n &= \cancel{\frac{1}{r^{n-1}}s_{n-1}} + t \end{aligned}$$

Sumando obtenemos:

$$\frac{1}{r^n}s_n = s + tn$$
$$s_n = sr^n + tnr^n$$

Esto corresponde a una combinación lineal de r^n y nr^n tal como lo muestra el Teorema 7.2 que se presenta a continuación. Este teorema no lo demostraremos, simplemente no quedaremos con los argumento que ya hemos dado para llegar a esto.

Definición 7.4. Dada una recurrencia lineal homogénea:

$$T_n = \sum_{i=1}^{k} a_i T_{n-i}$$

Se define el polinomio característico asociado a esta como:

$$x^k - \sum_{i=1}^{k} a_i x^{k-i}$$

Teorema 7.2. *Sean $s_1, \ldots, s_d$, con multiplicidades $m_1, \ldots, m_d$, las raíces del polinomio característico de la recurrencia lineal homogénea T_n, tales que $\sum_{i=1}^{d} m_i = k$. Entonces las funciones:*

$$n^l s_j^n \quad j = 1, \ldots, d, l = 0, \ldots, m_j - 1$$

son una base para el espacio vectorial de soluciones de T_n.

Ejemplo 7.2.

$$T_n = 3T_{n-2} - 2T_{n-3}$$

El polinomio característico es:

$$x^3 - 3x + 2$$

Las raíces de este polinomio son $s_1 = 1$ con multiplicidad 2 y $s_2 = -2$ con multiplicidad 1, ya que $x^3 - 3x + 2 = (x-1)^2(x+2)$.

Luego una base de soluciones es: $\langle 1^n, n1^n, (-2)^n \rangle$, es decir: $\langle 1, n, (-2)^n \rangle$. De este modo cualquier solución de esta recurrencia es una combinación lineal de estas funciones:

$$T_n = \alpha + \beta n + \gamma(-2)^n$$

Números de Fibonacci

Imagine que quiere calcular la población de conejos en un mundo donde:

1. Los conejos son inmortales.
2. Cada pareja de conejos adultos crea una pareja de conejos bebés cada mes.
3. Un conejo bebé alcanza la adultez en un mes.

4. Comienza en el mes 1 con una pareja de conejos bebes.

Llamaremos f_n el número de parejas de conejos en el mes n. Si queremos saber cuántas parejas de conejos tenemos en el mes n una manera de encontrar este valor es decir que:

$$f_n = a_n + b_n$$

donde a_n es el número de parejas de conejos adultos en el mes n y b_n es el número de parejas de conejos bebés en el mes n.

El número de parejas de conejos adultos es el mismo número de parejas de conejos del mes anterior, luego: $a_n = f_{n-1}$. Y el número de parejas de conejos bebés en n es el número de parejas de conejos adultos en $n-1$ es decir $b_n = a_{n-1}$, pero como ya vimos $a_{n-1} = f_{n-2}$. Por lo tanto:

$$f_n = f_{n-1} + f_{n-2}, \qquad f_1 = f_2 = 1$$

Esta recurrencia es la conocida recurrencia de Fibonacci que da origen a los números del mismo nombre. Esta sucesión de números cumple muchas propiedades muy interesantes, pero ahora nos concentraremos en encontrar una fórmula cerrada para la recurrencia.

Los números de Fibonacci son un ejemplo de recurrencia lineal homogénea

$$\begin{aligned}
&f_1 = 1;\\
&f_2 = 1;\\
&f_n = f_{n-1} + f_{n-2}.
\end{aligned}$$

Usemos el método anterior para calcular una fórmula cerrada para los número de Fibonacci.

Primero el polinomio característico es:

$$x^2 = x + 1 \quad \Longleftrightarrow \quad x^2 - x - 1 = 0$$

Las soluciones son:

$$x = \frac{-(-1) \pm \sqrt{(-1)^2 - 4\cdot 1\cdot(-1)}}{2\cdot 1} = \frac{1 \pm \sqrt{5}}{2}$$

Ahora, definimos que $f_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$, luego se debe cumplir que:

$$\begin{aligned}
f_1 &= A\left(\frac{1+\sqrt{5}}{2}\right)^1 + B\left(\frac{1-\sqrt{5}}{2}\right)^1 = 1\\
f_2 &= A\left(\frac{1+\sqrt{5}}{2}\right)^2 + B\left(\frac{1-\sqrt{5}}{2}\right)^2 = 1
\end{aligned}$$

haciendo el cálculo se comprueba que:

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

Una propiedad interesante de los números de Fibonacci es que aparecen en el triángulo de Pascal.

$$f_n = \sum_{i=0}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-1-i}{i}$$

1 1 2 3 5 8

$n \backslash k$	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

$$\begin{aligned}
f_{n-1} + f_{n-2} &= \sum_{i=0}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i} + \sum_{i=0}^{\lceil \frac{n-2}{2} \rceil - 1} \binom{n-3-i}{i} \\
&= \sum_{i=0}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i} + \sum_{i=1}^{\lceil \frac{n-2}{2} \rceil} \binom{n-2-i}{i-1} \\
&= \binom{n-2}{0} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i} + \sum_{i=1}^{\lceil \frac{n-2}{2} \rceil} \binom{n-2-i}{i-1}
\end{aligned}$$

Ahora analizamos dos casos:

1. Caso n par: En este caso $\lceil \frac{n-1}{2} \rceil - 1 = \lceil \frac{n-2}{2} \rceil$ y $\lceil \frac{n-1}{2} \rceil = \lceil \frac{n}{2} \rceil$

$$\begin{aligned}
f_{n-1} + f_{n-2} &= \binom{n-2}{0} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i} + \sum_{i=1}^{\lceil \frac{n-2}{2} \rceil} \binom{n-2-i}{i-1} \\
&= \binom{n-2}{0} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i-1} \\
&= 1 + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \left[\binom{n-2-i}{i} + \binom{n-2-i}{i-1} \right] \\
&= \binom{n-1}{0} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-1-i}{i} \\
&= \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n-1-i}{i}
\end{aligned}$$

2. Caso n impar: En este caso $\lceil \frac{n-1}{2} \rceil = \lceil \frac{n-2}{2} \rceil$ y $\lceil \frac{n-1}{2} \rceil = \lceil \frac{n}{2} \rceil - 1$

$$\begin{aligned}
f_{n-1} + f_{n-2} &= \binom{n-2}{0} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i} + \sum_{i=1}^{\lceil \frac{n-2}{2} \rceil} \binom{n-2-i}{i-1} \\
&= 1 + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil} \binom{n-2-i}{i-1} \\
&= 1 + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-2-i}{i-1} + \binom{n-2-\lceil \frac{n-1}{2} \rceil}{\lceil \frac{n-1}{2} \rceil - 1} \\
&= 1 + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \left[\binom{n-2-i}{i} + \binom{n-2-i}{i-1} \right] + \binom{n-2-(\lceil \frac{n}{2} \rceil - 1)}{\lceil \frac{n-1}{2} \rceil - 1} \\
&= \binom{n-1}{0} + \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-1-i}{i} + \binom{n-1-\lceil \frac{n}{2} \rceil}{\lceil \frac{n-1}{2} \rceil - 1} \\
&= \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 2} \binom{n-1-i}{i} + \binom{n-1-\lceil \frac{n}{2} \rceil}{\lceil \frac{n-1}{2} \rceil - 1}
\end{aligned}$$

Notemos que n es impar entonces $n = 2k+1$, luego:

$$\binom{n-1-\lceil \frac{n}{2} \rceil}{\lceil \frac{n-1}{2} \rceil - 1} = \binom{2k+1-1-(\lceil \frac{2k+1}{2} \rceil)}{\lceil \frac{2k+1-1}{2} \rceil - 1} = \binom{2k-(k+1)}{k-1} = \binom{k-1}{k-1} = 1$$

Y

$$\binom{n-1-(\lceil \frac{n}{2} \rceil - 1)}{\lceil \frac{n}{2} \rceil - 1} = \binom{2k+1-\lceil \frac{2k+1}{2} \rceil}{\lceil \frac{2k+1}{2} \rceil - 1} = \binom{2k+1-(k+1)}{k+1-1} = \binom{k}{k} = 1$$

$$\begin{aligned}
f_{n-1} + f_{n-2} &= \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 2} \binom{n-1-i}{i} + \binom{n-1-\lceil \frac{n}{2} \rceil}{\lceil \frac{n-1}{2} \rceil - 1} \\
&= \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 2} \binom{n-1-i}{i} + \binom{n-1-(\lceil \frac{n}{2} \rceil - 1)}{\lceil \frac{n}{2} \rceil - 1} \\
&= \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n-1-i}{i}
\end{aligned}$$

7.3.2. Recurrencias lineales no homogéneas

Recibe el nombre de ecuación de recurrencia lineal no homogénea de grado k, con coeficientes constantes, una expresión del tipo:

$$t_n = \sum_{i=1}^{k} a_i t_{n-i} + F(n), \qquad a_i \in \mathbb{R}, a_k \neq 0$$

Definición 7.5. Un subespacio vectorial afín B de un espacio vectorial V es un conjunto $B = \{u + a : u \in E\}$, donde $a \in V$, y E es un subespacio vectorial de V.

Teorema 7.3. *Sea* $\mathcal{F}_{\mathbb{N}} = \left\{ f : \mathbb{N}\ \mathbb{C} \rightarrow \right\}$ *el espacio vectorial de las funciones con dominio en* $\mathbb{N}$ *y recorrido en* $\mathbb{C}$ *entonces* $\mathcal{F} = \left\{ h \in \mathcal{F}_{\mathbb{N}} : h_n = \sum\limits_{i=1}^{k} a_i h_{n-i} + F(n) \right\}$ *es un subespacio vectorial afín de* $\mathcal{F}_{\mathbb{N}}$.

Demostración. Sea $\mathcal{F}^{(h)} = \left\{ h \in \mathcal{F}_{\mathbb{N}} : h_n = \sum\limits_{i=1}^{k} a_i h_{n-i} \right\}$ el espacio vectorial de las soluciones de la recurrencia lineal homogénea asociada a la recurrencia no homogénea $h_n = \sum\limits_{i=1}^{k} a_i h_{n-i} + F(n)$.

Sea $h_n^{(p)}$ una solución particular de $h_n = \sum\limits_{i=1}^{k} a_i h_{n-i} + F(n)$. Debemos probar, que $\mathcal{F} = \mathcal{F}^{(h)} + h_n^{(p)}$.

Primero se prueba que $\mathcal{F} \subseteq \mathcal{F}^{(h)} + h_n^{(p)}$. Sea $g_n \in \mathcal{F}$, es decir:

$$g_n = \sum_{i=1}^{k} a_i g_{n-i} + F(n)$$

Además

$$h_n^{(p)} = \sum_{i=1}^{k} a_i h_{n-i}^{(p)} + F(n)$$

Restando ambas ecuaciones obtenemos:

$$g_n - h_n^{(p)} = \sum_{i=1}^{k} a_i (g_{n-i} - h_{n-i}^{(p)}) + (F(n) - F(n)) = \sum_{i=1}^{k} a_i (g_{n-i} - h_{n-i}^{(p)})$$

Luego $g_n - h_n^{(p)}$ cumple la ecuación de recurrencia homogénea, por lo tanto $g_n - h_n^{(p)} \in \mathcal{F}^{(h)}$, lo que implica $g_n \in \mathcal{F}^{(h)} + h_n^{(p)}$.

Ahora analizamos la inclusión $\mathcal{F}^{(h)} + h_n^{(p)} \subseteq \mathcal{F}$. Sea $h_n^{(h)} \in \mathcal{F}^{(h)}$. tenemos que:

$$h_n^{(h)} = \sum_{i=1}^{k} a_i h_{n-i}^{(h)}$$

$$h_n^{(p)} = \sum_{i=1}^{k} a_i h_{n-i}^{(p)} + F(n)$$

Sumando obtenemos:

$$h_n^{(h)} + h_n^{(p)} = \sum_{i=1}^{k} a_i (h_{n-i}^{(h)} + h_{n-i}^{(p)}) + F(n)$$

Luego $h_n^{(h)} + h_n^{(p)} \in \mathcal{F}$. ■

Resolución

La solución general sería: $t_n = t_n^{(h)} + t_n^{(p)}$, donde $t_n^{(h)}$ es la solución de la ecuación de recurrencia lineal homogénea asociada, es decir, la ecuación: $t_n = \sum\limits_{i=1}^{k} a_i t_{n-i}$, $a_i \in \mathbb{R}$, $a_k \neq 0$ y donde $t_n^{(p)}$ es la solución particular que depende de la función $F(n)$. Por lo tanto, los pasos a seguir serían, primero calcular la solución de la ecuación homogénea, calcular una solución particular para $F(n)$ y sumarla a la homogénea, y a continuación aplicar las condiciones iniciales para calcular las constantes. En la siguiente tabla, encontramos cuales son las posibles soluciones particulares:

$\boldsymbol{F(n)}$	$\boldsymbol{t_n}^{(\boldsymbol{p})}$
$p(n)$ (polinomio de grado k)	polinomio de grado k o superior
cb^n(b no es raíz característica)	$C_0 b^n$
$n^t r^n$	$r^n(C_0 + C_1 n + \cdots + C_{t+1} n^{t+1})$
cb^n(b es raíz característica con multiplicidad m)	$kn^m b^n$

Consideraciones:

1. Si $F(n)$ es una combinación lineal de algunas de las funciones de la tabla anterior, su solución particular es la combinación lineal de las soluciones particulares de esas mismas funciones.

2. Si uno de los sumandos de $F(n)$ es el producto de una constante por una solución de la ecuación característica homogénea asociada, entonces es necesario multiplicar la solución particular correspondiente a este sumando por la menor potencia de n, tal que este nuevo producto no sea solución de la ecuación característica homogénea asociada.

Un caso particular de estas recurrencias que es interesante de estudiar es $S(k)_n = \sum_{i=1}^{n} i^k$, para calcular esta suma, se pueden usar las técnicas de recurrencias lineales no homogéneas, planteando el problema como:

$$\begin{aligned} S(k)_1 &= 1 \\ S(k)_n &= S(k)_{n-1} + n^k. \end{aligned}$$

7.3.3. Algunas recurrencias no lineales

La ecuaciones de recurrencia que se obtienen no siempre son lineales, por ejemplo para ordenar un serie de números se pueden usar varios métodos distintos como el método de la burbuja. La burbuja son dos términos de la lista seguidos, j y $j+1$, que se comparan: si el primero es mayor que el segundo sus valores se intercambian. Esta comparación se repite en el centro de los dos bucles, dando lugar a la postre a una lista ordenada, este algoritmo se describe en Algoritmo 7.1.

Puede verse que el número de repeticiones solo depende de n.

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

Otro ejemplo de algoritmo de ordenamiento es mergeSort. Este método fue desarrollado en 1945 por John Von Neumann. Conceptualmente, el ordenamiento por mezcla funciona de la siguiente manera (Algoritmo 7.2):

Algoritmo 7.1: BubbleSort$(a_1, \ldots, a_n)$

for $i \in \{2, \ldots, n\}$ **do**
    for $j \in \{1, \ldots, i-1\}$ **do**
        if $a_j > a_{j+1}$ **then**
            aux $\longleftarrow a_j$;
            $a_j \longleftarrow a_{j+1}$;
            $a_{j+1} \longleftarrow$ aux;
        end
    end
end

1. Si la longitud de la lista es 0 o 1, entonces ya está ordenada. En otro caso:
2. Dividir la lista desordenada en dos sublistas de aproximadamente la mitad del tamaño.
3. Ordenar cada sublista recursivamente aplicando el ordenamiento por mezcla.
4. Mezclar las dos sublistas en una sola lista ordenada.

Algoritmo 7.2: MergeSort$(a_1, \ldots, a_n)$

if $n = 1$ **then**
    return (a_1);
else
    $L_1 \leftarrow$ MergeSort$(a_1, \ldots, a_{\lfloor \frac{n}{2} \rfloor})$;
    $L_2 \leftarrow$ MergeSort$(a_{\lfloor \frac{n}{2} \rfloor + 1}, \ldots, a_n)$;
    $i \leftarrow 1$; $j \leftarrow 1$;
    $L \leftarrow ()$;
    for $k \leftarrow 1$ **to** n **do**
        if $L_1[i] \leqslant L_2[j]$ **then**
            $L[k] \leftarrow L_1[i]$;
            $i \leftarrow i + 1$;
        else
            $L[k] \leftarrow L_2[j]$;
            $j \leftarrow j + 1$;
        end
    end
    return L;
end

En este caso el número de operaciones es:

$$q_n = q_{\lfloor \frac{n}{2} \rfloor} + q_{\lceil \frac{n}{2} \rceil} + n, \qquad q_1 = 1.$$

Si bien es cierto, para hacer el cálculo caso a caso debemos tomar en cuenta todos los casos, podemos tratar de resolver esta recurrencia en un infinidad de casos que nos den una idea de lo que ocurre en el caso general. En este caso consideramos solo los n que son potencia de dos, es decir $n = 2^k$. Al hacer este reemplazo en la ecuación obtenemos:

$$\begin{aligned} q_{2^0} &= 1 \\ q_{2^k} &= q_{\lfloor \frac{2^k}{2} \rfloor} + q_{\lceil \frac{2^k}{2} \rceil} + 2^k = q_{2^{k-1}} + q_{2^{k-1}} + 2^k = 2q_{2^{k-1}} + 2^k \end{aligned}$$

Si consideramos que $a_k = q_{2^k}$, obtenemos:

$$\begin{aligned} a_0 &= 1 \\ a_k &= 2a_{k-1} + 2^k \end{aligned}$$

Y esta recurrencia si podemos resolverla como antes. Luego la solución homogénea es: $a_k^{(h)} = \alpha 2^k$ y la particular de la forma $a_k^{(p)} = \beta k 2^k$.

$$\begin{aligned} \beta k 2^k &= 2\beta(k-1)2^{k-1} + 2^k & / : 2^k \\ \beta k &= \beta(k-1) + 1 \\ \beta &= 1 \end{aligned}$$

De aquí: $a_k = \alpha 2^k + k2^k$, con condición de borde $a_0 = 1$, luego:

$$a_0 = \alpha + 0 = 1$$

Finalmente, $a_k = 2^k + k2^k$, luego $q_{2^k} = 2^k + k2^k$ y haciendo el cambio de variable $n = 2^k$ tenemos que: $q_n = n + n\log_2 n$.

Ahora nos gustaría generalizar este método y esto se logra para algunas recurrencias no lineales realizando un cambio de variables en orden a obtener una recurrencia lineal.

Un caso particular, son las recurrencias del tipo:

$$t_n = \sum_{i=1}^{k} a_i t_{\frac{n}{b^i}} + F(n), \qquad a_i \in \mathbb{R}, a_k \neq 0$$

En estos casos, si bien no obtenemos la fórmula general para cada n, podemos obtener una expresión para las potencias de b y de ese modo tener una estimación en el caso general.

Para esto, se realiza el cambio de variable $n = b^m$. Así:

$$\begin{aligned} t_n &= \sum_{i=1}^{k} a_i t_{\frac{n}{b^i}} + F(n), \qquad a_i \in \mathbb{R}, a_k \neq 0 \\ t_{b^m} &= \sum_{i=1}^{k} a_i t_{\frac{b^m}{b^i}} + F(b^m), \qquad a_i \in \mathbb{R}, a_k \neq 0 \\ t_{b^m} &= \sum_{i=1}^{k} a_i t_{b^{m-i}} + F(b^m), \qquad a_i \in \mathbb{R}, a_k \neq 0 \end{aligned}$$

Si consideramos $u_m = t_{b^m}$ obtenemos

$$u_m = \sum_{i=1}^{k} a_i u_{m-i} + F(b^m), \qquad a_i \in \mathbb{R}, a_k \neq 0$$

Esta última es una recurrencia lineal. Luego resolvemos u_m con las técnicas vistas para recurrencias lineales y luego a partir de esto calculamos t_n.

7.3.4. Algunas recurrencias importantes

	Recurrencia	**Fórmula cerrada**
Progresión aritmética	$\begin{cases} a_0 = a; \\ a_n = a_{n-1} + d. \end{cases}$	$a_n = a + nd$
Progresión geométrica	$\begin{cases} b_0 = b; \\ b_n = rb_{n-1}. \end{cases}$	$b_n = r^n b$
$S_n(k) = \sum_{i=1}^{n} i^k = S_{n-1}(k) + n^k$	$k = 1$	$S_n(1) = \frac{n(n+1)}{2}$
	$k = 2$	$S_n(2) = \frac{n(n+1)(2n+1)}{6}$
	$k = 3$	$S_n(3) = \left(\frac{n(n+1)}{2}\right)^2$

7.4. Ejercicios

P1. Pruebe que si $a \neq 1$, $\sum_{i=1}^{n} i^k a^i = p_k(n)a^n + c$ donde $p_k(n)$ es un polinomio de grado k y c es una constante.

P2. Calcule:

1. $\sum_{i=0}^{n} 2^i$
2. $\sum_{i=1}^{n} i^4$
3. $\sum_{i=1}^{n} i^5$
4. $\sum_{i=1}^{n} \frac{1}{i(i+1)}$
5. $\sum_{i=1}^{n} i(i+2)$

P3. Demuestre que:

1. $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$
2. $2^n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} x^i (2+x)^{n-i}$
3. Calcule: $\sum_{i=0}^{n} 2^i \binom{n}{i}$

P4. Sea $(a_i)_{i\in\mathbb{N}}$ una progresión aritmética. Demuestre que:

$$\sum_{k=1}^{n} \frac{1}{\sqrt{a_{k-1}} + \sqrt{a_k}} = \frac{n}{\sqrt{a_0} + \sqrt{a_n}}$$

P5. Sea $(u_n)_{n\in\mathbb{N}}$ la sucesión de Fibonacci. Demuestre que:

1. $\sum_{i=1}^{n} u_i = u_{n+2} - 1$
2. $\sum_{i=1}^{n} u_{2i-1} = u_{2n}$
3. $\sum_{i=1}^{n} u_{2i} = u_{2n+1} - 1$
4. $\sum_{i=1}^{n} u_i^2 = u_n u_{n+1}$
5. $u_{n+m} = u_{n-1}u_m + u_n u_{m+1}$

P6. Un programa recursivo toma tiempo $T(n)$ en ejecutarse, donde n es el tamaño del problema. Se satisface que: $T(n) = 3T(n-1) - 2T(n-2), \forall n \geq 2$, con $T(0) = 3$ y $T(1) = 7$. Determine un fórmula cerrada para $T(n)$.

P7. Para $n \geq 0$, sea $S = \{1, 2, 3, \ldots, n\}$ y sea a_n el número de subconjuntos de S que no contienen enteros consecutivos. Encuentre y resuelva una relación de recurrencia para a_n.

P8. Suponga que un niño, en cada paso, puede subir un escalón o dos escalones de una escalera. Encuentre y resuelva una relación de recurrencia para f_n, el número de formas distintas en las que el niño puede subir una escalera de n escalones.

P9. Una partícula se mueve de forma horizontal hacia la derecha. Para $n \in \mathbb{N}$ la distancia que recorre la partícula en el $(n+1)$–ésimo segundo es igual a la distancia que recorre en el n–ésimo segundo. Si x_n denota la posición de la partícula al inicio del $(n+1)$–ésimo segundo, encuentre y resuelva una relación de recurrencia para x_n, donde $x_0 = 1$ y $x_1 = 5$.

P10. Encuentre y resuelva una relación de recurrencia para el número de formas de estacionar las motocicletas y los autos pequeños en una fila de n espacios si cada motocicleta requiere un espacio y un auto dos. (Ind. suponga que todas las motocicletas tienen apariencia idéntica, lo mismo que los autos, y que queremos utilizar todos los espacios).

P11. Sea s_n el número de secuencias de n bolitas de color rojo y verde, tal que todas las bolitas tienen una bolita de su mismo color a la izquierda o a la derecha. Por ejemplo, son secuencias permitidas: rrvvv, vvrrvvv, rrrvvrr, rrrr. Son secuencias prohibidas: rvrr, vvrv, rvrvrvrvr. Encuentre una fórmula de recurrencia para s_n.

P12. Sea p_n el número de palabras de largo n escritas en el alfabeto $\{a, b, c\}$ tal que no tienen dos b ni dos c juntas. Encuentre una fórmula de recurrencia para p_n.

P13. Encuentre una fórmula de recurrencia para $|A_n|$, donde:

$$A_n = \left\{ (x_1, \ldots, x_k) : k \in \mathbb{N}, x_i \in \{1, 2, 3\}, \sum_{i=1}^{k} x_i = n \right\}$$

Por ejemplo: $(1, 2, 1) \in A_4$, $(2, 2) \in A_4$, $(1, 2, 1, 3) \in A_7$, etc.

P14. Dado el alfabeto $\{a, b, c\}$, sea T_n el número de palabras de largo n tal que todas las cadenas de a son de largo par. Es decir *baac* es una palabra permitida, pero *baca* no lo es. Encuentre una fórmula de recurrencia para T_n.

P15. Encuentra el término general de las siguientes sucesiones recurrentes no homogéneas:

1. $a_n = a_{n-1} + 6a_{n-2} + 2^n$, $n \geqslant 2$, $a_0 = 0, a_1 = 1$
2. $a_n = 3a_{n-1} + 5 \cdot 7^n$, $n \geqslant 1$, $a_0 = 2$
3. $a_n = 4a_{n-1} - 4a_{n-2} + n$, $n \geqslant 2$, $a_0 = 1, a_1 = 3$
4. $a_n = 3a_{n-1} + 5 \cdot 3^n$, $n \geqslant 1$, $a_0 = 2$
5. $a_n = a_{n-1} + 3n^2$, $n \geqslant 1$, $a_0 = 7$
6. $a_n = 3a_{n-1} - 4a_{n-3} + n^2$, $n \geqslant 3$, $a_0 = 11$, $a_1 = 1$, $a_2 = -1$
7. $a_n = a_{n-2} + 3n + 4$, $n \geqslant 3$, $a_1 = 1$, $a_2 = 6$
8. $a(n) = a(n/2) + 2a(n/4) + 3n$, $a(1) = 1$, $a(2) = 2$
9. $b(n) = b(n/3) + 6b(n/9) + 5n$, $b(1) = 1$, $b(2) = 1$, $b(3) = 2$
10. $t(n) = 2t(n/2) - t(n/4) + n$, $t(1) = 5$, $t(2) = 11$.
11. $t(n) = 4t(n/3) + n^2 - 7n + 5$, $t(1) = 1$
12. $t(n) = t(n/4) + \sqrt{n} + 1$, $t(1) = 1$

Capítulo 8

Grafos

Los grafos son un modelo matemático ampliamente utilizado. Permiten modelar conexiones e interacciones entre distintos entes de un sistema.

Cuando pensamos en un modelo, una buena idea para imaginarnos de que se trata es pensar en un juguete. Cuando pequeños, los niños juegan con autitos, muñecas etc. imitando un comportamiento adulto, son una herramienta que nos permite testear y aprender muchas cosas de una manera segura.

Es así como los modelos matemáticos tienen como objetivo permitir la mejor comprensión de un sistema, ya sea simulando diferentes casos para tratar de encontrar el que presenta un mejor comportamiento o predecir algún evento importante.

Al igual que en el caso de los juguetes, muchas veces estos modelos matemáticos, no se comportan exactamente igual que el sistema real, pero su comportamiento debe ser suficientemente cercano al comportamiento del sistema real de modo que su uso sea de utilidad.

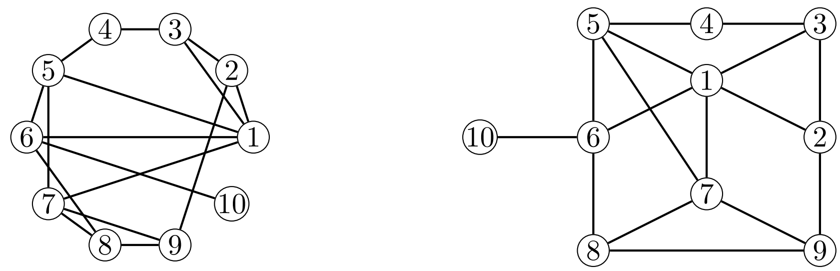
En el caso particular de los grafos, se utilizan como modelo para estudiar redes de transporte en general. El transporte no necesariamente se refiere a personas, puede ser: energía, información, carga, etc.

8.1. Conceptos y nociones fundamentales

Definición 8.1. Un *grafo* es un par ordenado $G = (V, E)$ donde:

- V es un conjunto finito y no vacío, cuyos elementos llamamos *vértices*.
- E conjunto de pares no ordenados de V llamados *aristas*. Dicho de otra forma ($E \subseteq \mathcal{P}(V)$ y $\forall e \in E$, $|e| = 2$)

En la Figura 8.1 vemos un ejemplo de una representación gráfica de un grafo. Note que las aristas, si bien es cierto son subconjuntos de los vértices del grafo, se representan por una línea que une los dos vértices que contiene este subconjunto. Si se usara una línea que rodea ambos grafos, como usualmente se usa para conjuntos, el dibujo sería muy desordenado y no sería fácil de entender. Claramente, la representación gráfica de un grafo no es única, ya que puedo reordenar los vértices en otras posiciones y el grafo podría verse bastante diferente.



$$
\begin{aligned}
G &= (V,E)\\
V &= \{1,2,3,4,5,6,7,8,9,10\}\\
E &= \{\{1,2\},\{1,3\},\{1,5\},\{1,6\},\{1,7\},\{2,3\},\{2,9\},\{3,4\},\\
&\qquad \{4,5\},\{5,6\},\{5,7\},\{6,8\},\{6,10\},\{7,8\},\{7,9\},\{8,9\}\}
\end{aligned}
$$

Figura 8.1: Ejemplo de dos representaciones de un mismo grafo

Notación.

1. $V(G)$ conjunto de vértices en referencia a G.
2. $E(G)$ conjunto de aristas en referencia a G.
3. $\{u,v\} = uv = vu = e \in E(G)$ arista con $u, v \in V(G)$.

Definiciones 8.2. Dado $G = (V,E)$ un grafo, se dice que:

- $e \in E$ es *incidente* a los vértices $u, v \in V$ si $e = uv$.
- $u, v \in V$ son *vértices adyacentes* si $(\exists e \in E, e = uv)$.
- $u, v \in V$ son *independientes* si $uv \notin E$.
- $e, f \in E$ son *aristas adyacentes* si $(\exists u, v, w \in V, e = uv \wedge f = vw)$.
- $u \in V$ es *aislado* si $(\forall v \in V, uv \notin E)$.
- El *orden de un grafo* $G = (V,E)$ es la cantidad de vértices del grafo, es decir, $|V|$.
- El *tamaño de un grafo* $G = (V,E)$ es la cantidad de aristas de un grafo, es decir, $|E|$.

Observación 8.1. Si $G = (V,E)$ es un grafo con $|V| = n$ entonces $|E| \leq \binom{n}{2}$

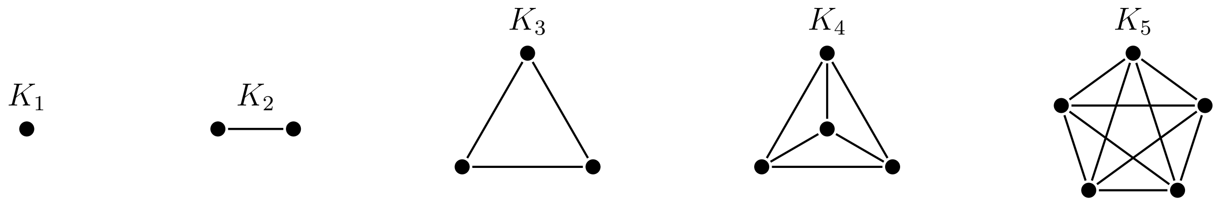


Figura 8.2: Ejemplos de grafo completo

Definición 8.3. Sea $G = (V, E)$ un grafo con $|V| = n$, $n \in \mathbb{N}$. Si $|E| = \binom{n}{2}$, entonces se dice que G es un *grafo completo* y se denota por K_n.

En la Figura 8.2 se observan ejemplos de grafos completos.

Definición 8.4. Sea $G = (V, E)$ un grafo y $v \in V$ se define la *vecindad* de v como:

$$N_G(v) = \{u \in V : uv \in E\} = \{u \in V : u \text{ es vértice adyacente a } v \text{ en } G\}$$

Definición 8.5. Sea $G = (V, E)$ se define el *grado* de $u \in V$ como $d_G(u) := |N_G(u)|$

Definiciones 8.6. Sea $G = (V, E)$ un grafo entonces se define:

- El *grado mínimo* como $\delta(G) := \min\limits_{u \in V} d_G(u)$
- El *grado máximo* como $\Delta(G) := \max\limits_{u \in V} d_G(u)$
- El *grado promedio* como $\dfrac{1}{|V|} \sum\limits_{v \in V} d_G(v)$

Definición 8.7. Si $\delta(G) = \Delta(G) = k$ entonces se dice que G es un grafo k-*regular*.

Notemos que G se dice *regular* si es k-regular para algún $k \in \mathbb{N}$. En la Figura 8.3, vemos ejemplos de grafos regulares.

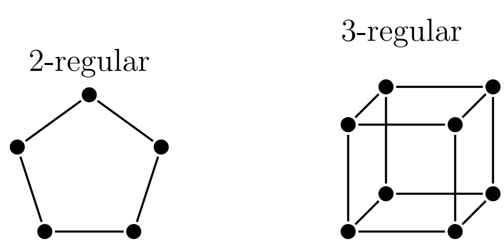
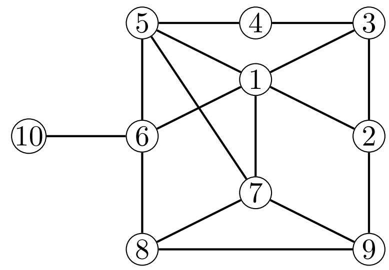


Figura 8.3: Ejemplos de grafos regulares

Definición 8.8. Dado $G = (V, E)$ un grafo, donde $|V| = n$. La secuencia de grados de G es una lista de enteros no negativos $(d_1, d_2, \ldots, d_n)$ con $0 \leq d_1 \leq d_2 \leq \cdots \leq d_n$ tal que si $V = \{v_1, v_2, \ldots, v_n\}$, $\forall i \in \{1, 2, \ldots, n\}, d(v_i) = d_i$.

$G = (V, E)$



Secuencia de grados $= (1, 2, 3, 3, 3, 3, 4, 4, 4, 5)$

Figura 8.4: Ejemplo de secuencia de grados

En la Figura 8.4 vemos un ejemplo de la secuencia de grados de un grafo.

Después de esta larga lista de definiciones llegamos al primer teorema acerca de grafos. Este teorema parece ser muy simple, sin embargo se utiliza mucho para probar una serie de resultados que se estudiarán durante el semestre.

Teorema 8.1. *Sea $G = (V, E)$ un grafo cualquiera, entonces se tiene que:*

$$\sum_{u \in V} d_G(u) = 2|E|$$

Demostración. Por inducción sobre el número de aristas.

Base. Sea G un grafo con una arista. Sea ab la arista del grafo, luego existen solo 2 vértices de grado 1 y el resto de los vértices tiene grado 0. Por lo tanto $\sum\limits_{u \in V(G)} d_G(u) = d_G(a) + d_G(b) = 2$.

Hipótesis de inducción. Si $|E(G)| = m$ entonces $\sum\limits_{u \in V(G)} d_G(u) = 2m$.

Paso inductivo. Sea G un grafo tal que $|E(G)| = m + 1$. Sea ab una arista de G. Consideremos el grafo G' tal que $V(G') = V(G)$ y $E(G') = E(G) \setminus \{ab\}$. El grafo G' es un grafo con m aristas, por lo tanto cumple la hipótesis de inducción. Es decir, $\sum\limits_{u \in V(G')} d_{G'}(u) = 2m$. Pero, como G' es igual a G salvo por la arista ab, tenemos que:

$$d_{G'}(u) = \begin{cases} d_G(u) & \text{si } u \neq a \wedge u \neq b \\ d_G(u) - 1 & \text{si no.} \end{cases}$$

De este modo:

$$\begin{aligned} 2m = \sum_{u \in V(G')} d_{G'}(u) &= \sum_{u \in \{a,b\}} d_{G'}(u) + \sum_{u \in V(G') \setminus \{a,b\}} d_{G'}(u) \\ &= d_G(a) - 1 + d_G(b) - 1 + \sum_{u \in V(G') \setminus \{a,b\}} d_G(u) \\ &= \sum_{u \in V(G)} d_G(u) - 2 \end{aligned}$$

Luego,

$$\sum_{u \in V(G)} d_G(u) = 2m + 2 = 2(m+1) = 2|E(G)|$$

■

Corolario 8.2. *La cantidad de vértices en un grafo que tienen grado impar es par.*

Demostración. Como la suma de los grados es un número par, no puede haber un número impar de vértices de grado impar, ya que si esto fuera así la suma de los grados sería impar. ■

8.2. Subgrafos

Cuando nos enfrentamos a un problema de grafos, muchas veces necesitamos considerar solo una parte de este. Por ejemplo, si que queremos encontrar una ruta óptima entre la universidad y la Plaza de la Independencia, no necesitamos utilizar el grafo con las calles de toda la región, me basta con la comuna de Concepción. Por otro lado, si quiero encontrar una ruta entre Concepción y Santiago, solo necesito las aristas correspondientes a carreteras y no las calles de cada ciudad en el trayecto. Con estos ejemplos vemos que en muchas ocasiones solo necesitamos utilizar una parte del grafo para obtener la información que necesitamos, y por supuesto, el utilizar menos información nos ayuda a hacer un manejo más eficiente de esta.

En esta sección veremos la notación que necesitamos para trabajar con subgrafos.

Definición 8.9. Sea $G = (V, E)$ un grafo, se dice que $G' = (V', E')$ es *subgrafo* de G si G' es un grafo tal que:

- $V' \subseteq V$.
- $E' \subseteq E$.

y se denota como $G' \subseteq G$

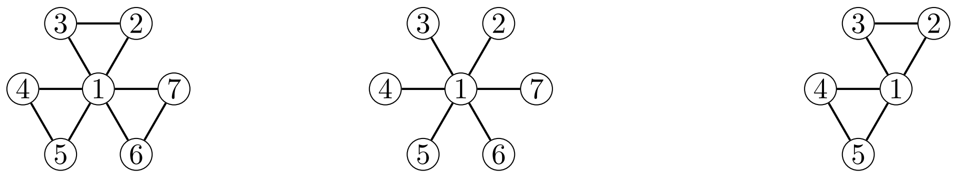
Note que un punto clave de esta definición es el hecho de que G' es un grafo, esto trae como consecuencia que si elijo la arista uv para que esté en el grafo G', entonces tanto el vértice u como el vértice v deben estar en V', ya que si esto no fuera así tendríamos una arista que queda "colgando" y, en ese caso, G' no sería un grafo.

Definiciones 8.10. Sea $G = (V, E)$ y sea $G' \subseteq G$ se define lo siguiente:

- Si $V' = V$ entonces se dice que G' es un *subgrafo generador o recubridor* de G
- Si $E' = \{uv \in E : u, v \in V'\}$ entonces se dice que G' es un *subgrafo inducido* por V' y se denota por $G' = G[V']$

En la Figura 8.5 podemos ver ejemplos de subgrafos recubridores e inducidos.

Definición 8.11. Un subgrafo completo $K_m \subseteq G$ se denomina *clique* en G.



G — Subgrafo recubridor de G — Subgrafo generado por $V' = \{1, 2, 3, 4, 5\}$

Figura 8.5: Ejemplos de subgrafo

8.3. Eliminación y adición de vértices y aristas

En esta sección se define la notación necesaria para agregar y quitar vértices y aristas de un grafo. Esta notación es muy utilizada especialmente cuando realizamos demostraciones por inducción como en el Teorema 8.1 y en general cuando estudiamos algún modelo es frecuente que sea necesario realizar estas operaciones.

Definiciones 8.12. Sea $G = (V, E)$ un grafo

- Si $W \subseteq V$ se define $G - W := G[V \setminus W]$. En particular si $W = \{v\}$ entonces denotaremos $G - W$ como $G - v$.
- Si $F \subseteq E$ se define $G - F := (V, E \setminus F)$. En particular si $F = \{e\}$ entonces denotaremos $G - F$ como $G - e$.
- Si $F \subseteq \{uv : u, v \in V\}$ entonces: $G + F := (V, E \cup F)$.

La Figura 8.6 muestra ejemplos de eliminaciones y adiciones de vértices y aristas en un grafo.

8.4. Isomorfismos

Los isomorfismos de grafos, son una herramienta muy interesante, al igual que en una estructura algebraica con leyes de composición interna, cuando existe un isomorfismo de grafos estos grafos tienen un comportamiento idéntico entre sí, es de algún modo como si fueran el mismo grafo, y por lo tanto, todas las propiedades del grafo se mantienen.

Definición 8.13. Dos grafos G y H se dicen *isomorfos* denotado por $G \cong H$ si $\exists\ \varphi : V(G) \to V(H)$ función biyectiva tal que $uv \in E(G) \Leftrightarrow \varphi(u)\varphi(v) \in E(H)$. Si además $V(G) = V(H)$ se dice que φ es un *automorfismo*.

Observación 8.2. Sea

$$\mathcal{G} = \{G : G \text{ es un grafo}\}$$

La relación $(\mathcal{G}, \cong)$ es una relación de equivalencia.

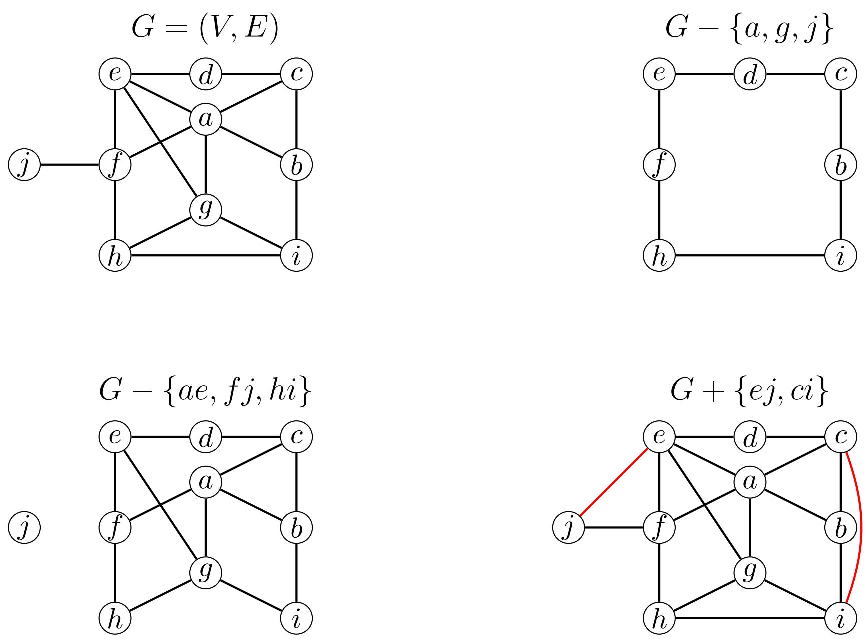
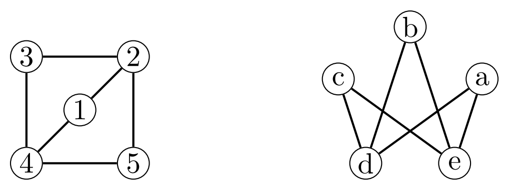


Figura 8.6: Ejemplos de eliminación y adición de vértices y aristas de un grafo



v	$f(v)$
1	a
2	e
3	b
4	d
5	c

Figura 8.7: Ejemplo de grafos isomorfos

Teorema 8.3. *Si $G \cong H$, entonces G y H tienen la misma secuencia de grados.*

Demostración. Primero notemos que como existe $f : V(G) \to V(H)$ biyectiva, se tiene que $|V(G)| = |V(H)|$. Probemos que $(\forall v \in V(G), d_G(v) = d_H(f(v)))$.

$$|N_H(f(v))| = |\{w \in V(H) : wf(v) \in E(H)\}|$$

Como f es biyectiva $(\exists! u \in V(G), w = f(u))$, luego:

$$|N_H(f(v))| = |\{f(u) \in V(H) : f(u)f(v) \in E(H)\}|$$

Como f es un isomorfismo $f(u)f(v) \in E(H) \Leftrightarrow uv \in E(G)$:

$$|N_H(f(v))| = |\{f(u) \in V(G) : uv \in E(G)\}|$$

Nuevamente por biyectividad de f:

$$|N_H(f(v))| = |\{u \in V(G) : uv \in E(G)\}| = |N_G(v)|$$

■

Cabe notar que la recíproca es falsa. Para esto basta ver el ejemplo que se presenta en la Figura 8.8

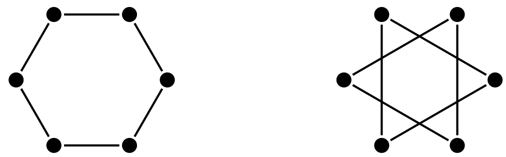


Figura 8.8: Grafos con igual secuencia de grados que no son isomorfos

8.5. Caminos y ciclos

Como ya hemos hablado, los grafos se utilizan mucho como modelo de transporte, es así como se definen los caminos y recorridos en un grafo, como una analogía con el desplazamiento que se produce al transportar algo.

Definiciones 8.14. Dado $G = (V, E)$ un grafo definimos lo siguiente:

- *Recorrido* entre v_0 y v_l como una secuencia ordenada de vértices de G tal que $\forall j \in \{0, \ldots, l-1\}$, $v_j v_{j+1} \in E$.

  La notación al respecto es:

  - Recorrido $R = v_0, v_1, \ldots, v_l$.
  - Vértices de un recorrido $V(R) = \{v_0, v_1, \ldots, v_l\}$.
  - Aristas de un recorrido $E(R) = \{v_j v_{j+1} : j = 0, \ldots, l-1\}$.
  - A los vértices v_0 y v_l se les denomina *vértices externos*.
  - A los vértices $v_1, \ldots, v_{l-1}$ se les denomina *vértices internos*.
  - El *largo de un recorrido* es $l(R) = l$

- Si el recorrido es tal $v_0 = v_l$ entonces lo denominamos *circuito*.

- Si el recorrido no contiene vértices repetidos entonces lo denominamos *camino*.

- Si el circuito no contiene vértices repetidos (excepto por los extremos) entonces lo denominamos *ciclo*.

Observación 8.3. El largo, vértices y aristas de un recorrido es extensible a circuito, camino y ciclo.

Figura 8.9: Ejemplo de recorrido, circuito, camino y ciclo

Proposición 8.4. *Dado un G un grafo cualquiera, si existe un recorrido entre los vértices u y v de G entonces existe un camino entre u y v en G.*

Demostración. Primero vemos una demostración que nos da un algoritmo que nos permite encontrar el camino en cuestión.

Sea $R = v_0 v_1 v_2 \ldots v_l$ un recorrido de u a v, es decir, $v_0 = u$, $v_l = v$ y para todo $i \in \{0, \ldots, l-1\}$, $v_i v_{i+1} \in E(G)$. A partir de esto construimos un algoritmo que nos permita encontrar un camino entre u y v. Vemos que el algoritmo elimina los pedazos del recorrido que vuelven al mismo punto. Una etapa del algoritmo puede observarse en la Figura 8.10.

Algoritmo 8.1: Camino($v_0 \ldots v_l$: recorrido de un grafo)

if $(\forall i, j \in \{0, \ldots, l\}, i \neq j \Rightarrow v_i \neq v_j)$ **then**
  return $v_0 \ldots v_l$;
else
  $i_* \leftarrow \text{mín}\{i \in \{0, \ldots, l-1\} : \exists j > i, v_j = v_i\}$;
  $j_* \leftarrow \text{máx}\{j > i_* : v_j = v_{i_*}\}$;
  return Camino($v_0 \ldots v_{i_*} v_{j_*+1} \ldots v_l$);

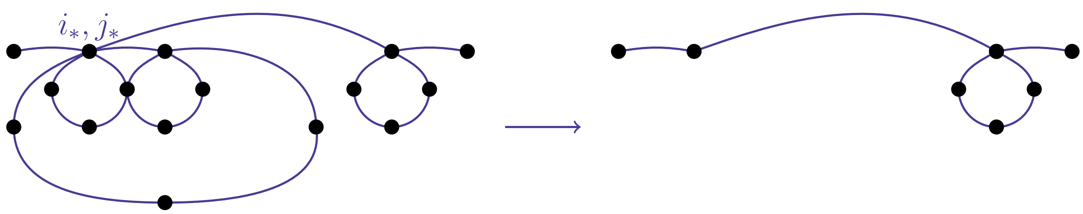


Figura 8.10: Idea de funcionamiento de una etapa de Algoritmo 8.1

También podemos plantear una demostración puramente matemática. Por reducción al absurdo, supongamos que existe un recorrido de u a v, pero no existe un camino. Sea $R = v_0 v_1 v_2 \ldots v_l$ el recorrido más corto entre u y v, que no es un camino, por lo tanto este recorrido tiene vértices repetidos, así podemos definir:

$$i_* = \text{mín}\{i \in \{0, \ldots, l-1\} : \exists j > i, v_j = v_i\}$$
$$j_* = \text{máx}\{j > i_* : v_j = v_{i_*}\}$$

Con estas definiciones obtenemos que $R' = v_0 \ldots v_{i_*} v_{j_*+1} \ldots v_l$ también es un recorrido entre u y v y es más corto que R, por lo que tenemos una contradicción.

■

Proposición 8.5. *Sea $G = (V, E)$ un grafo no trivial entonces existe un camino P tal que $l(P) \geq \delta(G)$ además si $\delta(G) \geq 2$ entonces existe un ciclo c tal que $l(c) \geq \delta(G) + 1$.*

Demostración. Supongamos que $|E| \neq 0$. Sea $P = v_0, v_2, \ldots, v_l$ un camino de largo máximo $l(P) = l$ en G, supongamos que $d_G(v_0) = k$, $k \geq \delta(G)$ como P es un camino de largo máximo $N_G(v_0) \subseteq V(P)$ de lo contrario, el camino P puede ser aumentado, lo que contradice el suponer que P es de largo máximo. Así $l(P) \geq \text{máx}\{i : v_i \in N_G(v_0) \cap V(P)\} \geq \delta(G)$ (ver Figura 8.11).

Además si $\delta(G) \geq 2$ entonces existe $v_i \neq v_1$ tal que $v_i \in N_G(v_0) \cap V(P)$ sea $j = \text{máx}\{i : v_i \in N_G(v_0) \cap V(P)\}$. Luego $C = v_0 v_1 \ldots v_{j-1} v_j v_0$ es un ciclo en G tal que $l(C) = j + 1$ como $N_G(v_0) \subseteq V(C)$ y $d_G(v_0) = |N_G(v_0)| \geq \delta(G)$ tenemos que $l(C) \geq d_G(v_0) + 1 \geq \delta(G) + 1$.

■

Corolario 8.6. *Todo grafo G con $\delta(G) \geq 2$ tiene un ciclo.*

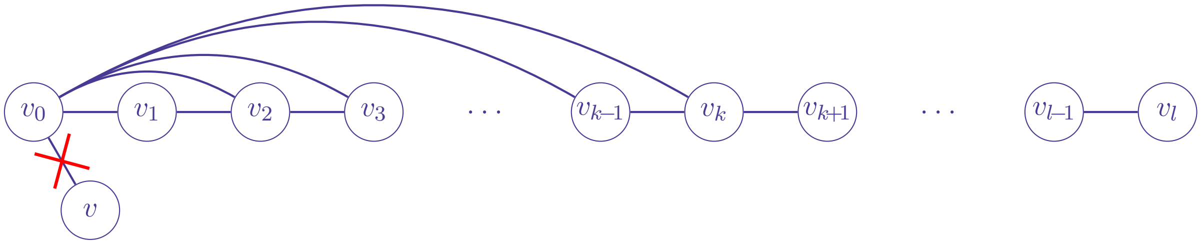


Figura 8.11

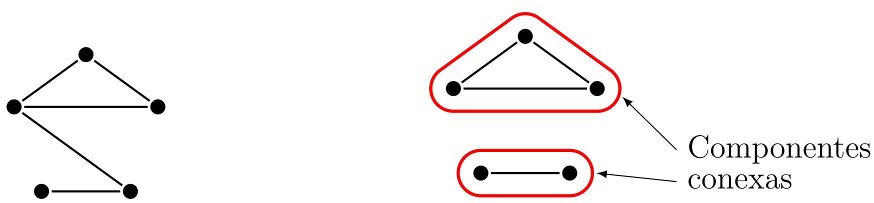
8.6. Conexidad en grafos

Una importante característica de un grafo es su conexidad, es decir, saber si desde cualquier vértice del grafo puedo encontrar un camino hasta otro vértice cualquiera, esta es una característica muy importante en un sistema de transporte, de modo que definiremos formalmente que significa.

Definiciones 8.15. Sea $G = (V, E)$ un grafo:

- G se dice *conexo* si es trivial o $\forall u, v \in V$ existe un camino en G.
- Si G no es conexo se dice *disconexo*.
- Una *componente conexa* de G es un subgrafo maximal en la propiedad de conexidad, es decir, no existe otro subgrafo conexo conteniendo estrictamente a alguna componente conexa. El número de componentes conexas de un grafo G se denota por $k(G)$

Observación 8.4. La conexidad es una invariante en grafos isomorfos.



(a) Grafo conexo (b) Grafo disconexo con 2 componentes conexas

Figura 8.12: Ejemplos de conexidad en grafos

Teorema 8.7. *Un grafo G es conexo si y solo si existe $u \in V(G)$ tal que para todo $v \in V(G)$ existe un camino de u a v.*

Demostración. Si G es conexo entonces si $\forall u, v \in V(G)$ existe un camino de u a v, esto claramente implica que $\exists u \in V(G)$ tal que $\forall v \in V(G)$ existe un camino de u a v (Recuerde que $(\forall x\ p(x)) \implies (\exists x\ p(x))$)

Luego lo que debemos demostrar es la recíproca. Sea $G = (V, E)$ un grafo y $w \in V$ tal que $\forall v \in V(G)$ existe un camino de w a v. Sean $u, v \in V$ cualesquiera, luego existen $P_u = wu_1 \dots u_{l-1}u$ y $P_v = wv_1 \dots v_{l'-1}v$, así obtenemos el recorrido $R_{uv} = uu_{l-1} \dots u_1wv_1 \dots v_{l'-1}v$, luego por Proposición 8.4, existe un camino entre u y v, por lo tanto, como u y v son cualesquiera, $\forall u, v \in V$ existe camino de u a v, que es la definición de conexidad. ∎

8.7. Vértices de corte y puentes

Definiciones 8.16. Sea $G = (V, E)$ un grafo no trivial se define los siguiente:

- Un vértice $v \in V$ se dice *vértice de corte* si el número de componentes conexas de $G - v$ es mayor que el de G.
- Una arista $e \in E$ se dice *puente* si $G - e$ tiene un mayor número de componentes conexas que G.

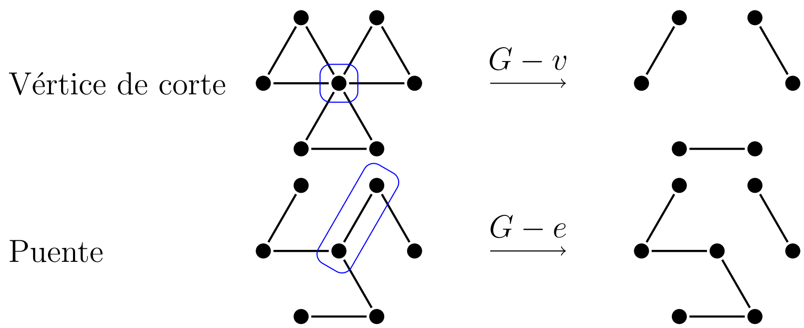


Figura 8.13: Ejemplos vértices de corte y puente

Teorema 8.8. *Dado $G = (V, E)$ un grafo conexo no trivial, G tiene al menos dos vértices que no son de corte.*

Demostración. Sea $P : u_0, u_2, \ldots, u_l$ un camino simple en G de largo máximo. Veamos que u_0 y u_l no son un vértices de corte. Analicemos el caso de u_0, si u_0 fuera vértice de corte existen $u, v \in V(G)$ tal que no existe camino entre u y v en $G - u_0$, de este modo existen $u_*, v_* \in N(u_0)$ tal que hay un camino entre u_* y u, un camino entre v_* y u, pero no hay camino entre u_* y v_*, sin embargo esto es imposible ya que como u_0 es el extremo de un camino más largo $\{u_*, v_*\} \subseteq N(u_0) \subseteq V(P)$, luego existe el camino entre u_* y v_*.

El caso u_l es análogo. ∎

Teorema 8.9 (Caracterización de vértices de corte)**.** *Sea $G = (V, E)$ un grafo conexo y $v \in V$ entonces las siguientes afirmaciones son equivalentes:*

1. *v es vértice de corte.*
2. *$\exists \{U, W\}$ partición de $V \setminus \{v\}$ tal que $\forall u \in U$, $\forall w \in W$; v pertenece a todo camino entre u y w en G.*
3. *$\exists u, w \in V \setminus \{v\}$ con $u \neq w$ tal que todo camino entre u y w contiene a v.*

Demostración.

(1) $\Longrightarrow$ (2) Si G es conexo y $v \in V$ es vértice de corte, entonces $k(G - v) > 1$, sean $G_1, \ldots, G_k$ ($k = k(G - v) > 1$) las componentes conexas de de $G - v$, $U = V(G_1)$ y $W = \bigcup_{i=2}^{k} V(G_i)$. Por reducción al absurdo, supongamos que existen $u \in U$ y $w \in W$ tal que $P = u_1 \ldots u_{l-1} w$ es un camino de u a w que no pasa por v, luego P es un camino de u a w en $G - v$, por lo tanto u y w están en la misma componente conexa de $G - v$ lo que es una contradicción.

(2) $\Longrightarrow$ (3) Si $\exists\{U,W\}$ partición de $V\setminus\{v\}$ tal que $\forall u\in U$, $\forall w\in W$; v pertenece a todo camino entre u y w en G, es claro que dado $u\in U$ y $w\in W$ todo camino entre u y w contiene a v.

(3) $\Longrightarrow$ (1) Si $\exists u,w\in V\setminus\{v\}$ con $u\neq w$ tal que todo camino entre u y w contiene a v, entonces no existe camino de u a w en $G-v$, por lo tanto u y w están en distintas componentes conexas de $G-v$, luego $k(G-v)>1=k(G)$.

■

Teorema 8.10. *Sea G un grafo no trivial conexo entonces $e\in E(G)$ es puente si y solo si e no pertenece a un ciclo de G*

Demostración. Si G es conexo y $e=uv\in E(G)$ es puente si y solo si $k(G-e)>1$, esto significa que u y v están en distintas componentes conexas en $G-e$, lo que es equivalente a que no existe un camino de v a u en $G-e$, esto ocurre si y solo si no existe un ciclo que pase por e en G. ■

8.8. Árboles

Como ya hemos dicho la conexidad es una característica muy importante en un grafo, es esta sección estudiaremos algunos aspectos acerca de los árboles que son grafos conexos minimales, es decir, son conexos, pero si eliminamos cualquier arista del grafo este dejará de serlo.

Definiciones 8.17. Sea $G=(V,E)$ un grafo se define lo siguiente:

- Si G es conexo y sin ciclos decimos que G es un *árbol*.
- Si G es un árbol y $v\in V$ tal que $d_G(v)=1$ decimos que v es una *hoja*.
- Si G no tiene ciclos decimos que G es un *bosque*.

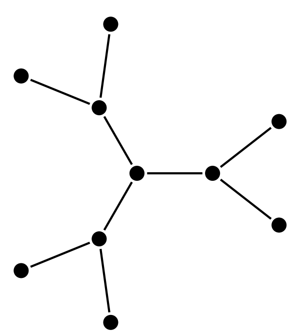


Figura 8.14: Ejemplo de árbol

Teorema 8.11. *Sea $G=(V,E)$ un grafo las siguientes proposiciones son equivalentes:*

1. *G es árbol.*
2. *$\forall u,v\in V$, $\exists!$ camino entre ellos en G.*

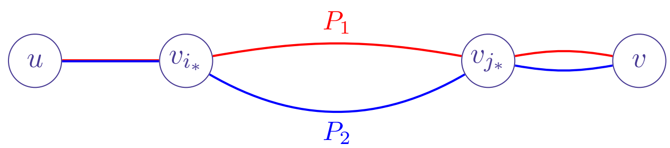
3. *G es conexo y $|E| = |V| - 1$*

4. *G no tiene ciclos y $|E| = |V| - 1$*

Demostración. Esta demostración se hace principalmente pon inducción.

(1) $\implies$ (2) Si G es árbol, es conexo; luego existe un camino entre cualquier par de vértices, solo necesitamos probar que ese camino es único. Por reducción al absurdo, supongamos que existe $u, v \in V(G)$ tal que existen $P_1 = v_0v_1 \dots v_l$ y $P_2 = u_0u_1 \dots u_{l'}$ caminos entre u y v distintos. Sean:

$$\begin{aligned} i_* &= \text{mín}\,\{i \in \{0, \dots, l\} : v_{i+1} \neq u_{i+1}\} \\ j_* &= \text{mín}\,\{j > i_* : \exists k \in \{i_* + 1, \dots, l'\}, v_j = u_k\} \\ k_* &= \text{mín}\,\{k > i_* : v_{j_*} = u_k\} \end{aligned}$$



entonces tenemos el ciclo $C = v_{i_*}v_{i_*+1} \dots v_{j_*}u_{k_*-1} \dots u_{i_*}$, lo que es una contradicción.

(2) $\implies$ (3) Suponemos que $\forall u, v \in V$, $\exists!$ camino entre ellos en G. Demostramos por inducción.

Base. Damos los únicos casos posibles para $|V| \in \{1, 2, 3\}$.

$\lvert V\rvert$	1	2	3
$\lvert E\rvert$	0	1	2
G	●	●——●	●——●——●

Hipótesis de inducción. Si $|V| = n$ y $\forall u, v \in V$, $\exists!$ camino entre ellos en G, entonces G es conexo y $|E| = |V| - 1$.

Paso inductivo. Sea $G' = (V', E')$ tal que $|V'| = n + 1$ y $\forall u, v \in V'$, $\exists!$ camino entre ellos en G'. Veamos que existe un vértice de grado uno. Sea $P = v_0 \dots v_l$ el camino más largo de G'. Como P es el camino más largo $N(v_0) \subseteq V(P)$, luego si $d(v_0) > 1$ existe v_j, $j \neq 1$ tal que $v_0v_j \in E'$ y en ese caso habría dos caminos entre v_0 y v_j, lo que es una contradicción.
Sea $v_* \in V'$ tal que $d_{G'}(v_*) = 1$, luego si $G = G' - v_*$, entonces $\forall u, v \in V(G)$, $\exists!$ camino entre ellos en G; por hipótesis de inducción G es conexo y $|E(G)| = |V(G)| - 1$. Por construcción:

$$\begin{aligned} |V(G)| &= |V'| - 1 \\ |E(G)| &= |E'| - 1 \end{aligned}$$

luego,

$$|E'| - 1 = |V'| - 1 - 1$$

así concluimos:

$$|E'| = |V'| - 1$$

(3) $\implies$ (4) Nuevamente procedemos por inducción.

Base. Aquí basta mirar los mismos dibujos del punto anterior para ver que la base de la inducción se cumple.

Hipótesis de inducción. Si $|V| = n$, G es conexo y $|E| = |V| - 1$, entonces G no tiene ciclos y $|E| = |V| - 1$.

Paso inductivo. Sea $G' = (V', E')$ tal que $|V'| = n + 1$ G' es conexo y $|E'| = |V'| - 1$. Nuevamente queremos quitar un vértice de grado 1 para hacer la inducción, en este caso para probar que el vértice existe usaremos Teorema 8.1.

$$\sum_{v \in V'} d_{G'}(v) = 2|E'|$$

Sea $|H| = \{v \in V' : d_{G'}(v) = 1\}$

$$\sum_{v \in H} \underbrace{d_{G'}(v)}_{=1} + \sum_{v \in V' \setminus H} \underbrace{d_{G'}(v)}_{\geq 2} = 2|E'|$$

luego,

$$|H| + 2|V' \setminus H| \leq 2|E'|$$

Pero como $|E'| = |V'| - 1$ y $|V' \setminus H| = |V'| - |H|$

$$\begin{aligned} |H| + 2(|V'| - |H|) &\leq 2(|V'| - 1) \\ |H| + \cancel{2|V'|} - 2|H| &\leq \cancel{2|V'|} - 2 \\ |H| &\geq 2 \end{aligned}$$

De este modo concluimos que existen al menos dos vértices de grado 1.

Sean $v_* \in V'$ tal que $d_{G'}(v_*) = 1$ y $G = (V, E) = G' - v_*$. $|V| = n$, G es conexo y $|E| = |V| - 1$, luego por hipótesis de inducción G es acíclico. Si G' fuera cíclico, entonces debería haber un ciclo que pase por v_*, pero como $d_{G'}(v_*) = 1$ esto es imposible.

(4) $\Longrightarrow$ (1) Como en los casos anteriores usamos inducción:

Base. Aquí basta mirar los mismos dibujos del punto anterior para ver que la base de la inducción se cumple.

Hipótesis de inducción. Si $|V| = n$, G es acíclico y $|E| = |V| - 1$, entonces G es una árbol (grafo conexo y acíclico).

Paso inductivo. Sea $G' = (V', E')$ tal que $|V'| = n + 1$ G' acíclico y $|E'| = |V'| - 1$. Al igual que antes, queremos verificar que existe un vértice de grado 1. Para esto usamos Corolario 8.6, ya que si todos los vértices de G' tienen grado mayor o igual a 2 el grafo tiene al menos un ciclo, como el grafo es acíclico, debe haber al menos un vértice de grado menor que 2. Podemos obviar el caso de vértices de grado 0, ya que se considera el subgrafo en el que se eliminan estos vértices, por lo tanto debe haber al menos un vértice de grado 1.

Sean $v_* \in V'$ tal que $d_{G'}(v_*) = 1$ y $G = (V, E) = G' - v_*$. $|V| = n$, G es acíclico y $|E| = |V| - 1$, luego por hipótesis de inducción G es conexo. Luego G' es conexo ya que los vértices grado 1 no pueden ser vértices de corte.

■

Corolario 8.12. *Todo árbol no trivial tiene al menos dos hojas.*

Definición 8.18. Sea G un grafo. Un *árbol recubridor* de un grafo G es un subgrafo recubridor de G que es árbol.

Teorema 8.13. *G es conexo si y solo si G tiene un árbol recubridor.*

Demostración. Primero demostremos que si G es conexo entonces tiene un árbol recubridor. Para esto haremos un algoritmo que encuentra el árbol.

Algoritmo 8.2: Arbol(G: grafo conexo)

```
if G es acíclico then
    return G;
else
    e ← Una arista en un ciclo;
    return Arbol(G − e);
```

Claramente, si G tiene ciclos existe la arista e y como e pertenece a un ciclo, por teorema de caracterización de puentes e no es un puente y en consecuencia $G-e$ sigue siendo conexo.

Ahora, si G tiene un grafo recubridor T, entonces T es un subgrafo de G, como T es conexo (ya que es un árbol) existe camino entre cualquier par de vértices. Los caminos de T, también son caminos de G, por lo tanto G es conexo. ∎

8.9. Distancia

Definición 8.19. Sea $G=(V,E)$ un grafo no trivial $\forall x,y\in V$ se define la *distancia* como:

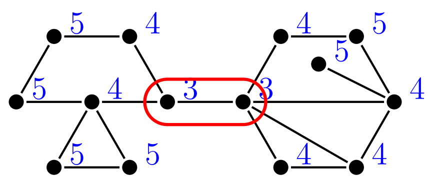
$$d(x,y)=\begin{cases}0 & \text{Si } x=y\\ \text{mín}\{l(P): P \text{ es camino entre } x \text{ e } y\} & \text{Si existe un camino entre } x \text{ e } y\\ +\infty & \text{si no existe camino entre } x \text{ e } y\end{cases}$$

Esta distancia define una métrica, es decir, cumple con las siguientes propiedades:

- $\forall x,y\in V, d(x,y)\geq 0$.
- $d(x,y)=0 \iff x=y$.
- $d(x,y)=d(y,x)$.
- $\forall x,y,z\in V, d(x,y)\leq d(x,z)+d(y,z)$.

Definiciones 8.20. Sea $G=(V,E)$ un grafo conexo no trivial entonces se define (ver Figura 8.15):

- La *excentricidad* de $u\in V$ como $e(u):=\max\limits_{v\in V} d(u,v)$.
- El *diámetro* de G como $D(G):=\max\limits_{u,v\in V} d(u,v)$.



$$D(G) = 5, r(G) = 3$$

Figura 8.15: Excentricidad, radio, diámetro y centro de un grafo

- El *radio* de G como $r(G) := \min_{u \in V} e(u)$.
- El *centro* de G como $Z(G) := \{u \in V : e(u) = r(G)\}$

Proposición 8.14. *Sea G un grafo conexo no trivial entonces se tiene que:*

$$r(G) \leq D(G) \leq 2r(G) \tag{8.1}$$

Demostración.

$$r(G) = \min_{u \in V} e(u) \leq \max_{u \in V} e(u) = \max_{u \in V} \max_{v \in V} d(u, v) = D(G)$$
$$D(G) = \max_{u,v \in V} d(u, v)$$

Sea $w \in Z(G)$, por desigualdad triangular:

$$D(G) \leq \max_{u,v \in V} d(u, w) + d(w, v) = \max_{u \in V} d(u, w) + \max_{v \in V} d(w, v) = e(w) + e(w) = 2r(G)$$

■

8.9.1. Procedimiento de Búsqueda en anchura

Su nombre se debe a que expande uniformemente la frontera entre lo descubierto y lo no descubierto. Llega a los nodos de distancia k, solo tras haber llegado a todos los nodos a distancia $k - 1$.

Dado un vértice fuente s, Breadth-first search sistemáticamente explora los vértices de G para "descubrir" todos los vértices alcanzables desde s. De este modo es capaz de encontrar la componente conexa a la que pertenece el vértice s.

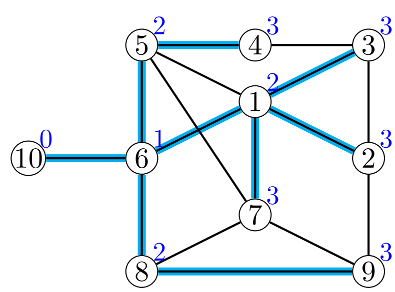
El camino desde s a cada vértice en este recorrido contiene el mínimo número de vértices. Es el camino más corto medido en número de vértices, de este modo se obtiene la distancia (menor número de vértices) desde s a todos los vértices alcanzables. Esta característica permite por ejemplo calcular diámetro y radio de un grafo.

La nomenclatura adicional utilizada es: Q = Estructura de datos cola

El tiempo de ejecución es $O(|V| + |E|)$. Cabe notar, que cada nodo es puesto a la cola una vez y su lista de adyacencia es recorrida una vez también.

Algoritmo 8.3: BFS(G: grafo, s: vértice de G)

```
forall u ∈ V(G) do
    visitado[u] ← Falso;
    distancia[u] ← ∞ ;
    padre[u] ← Null;
visitado[s] ← Verdadero;
distancia[s] ← 0;
encolar(Q, s);
while Q no está vacía do
    u ← extraer(Q);
    forall v ∈ N(u) do
        if visitado[v] = Falso then
            visitado[v] ← Verdadero;
            distancia[v] ← distancia[u] + 1;
            padre[v] ← u;
            encolar(Q, v);
```



$s = 10$

Figura 8.16: Ejemplo de BFS

8.10. Grafos bipartitos

Otra clase de grafos que encontramos frecuentemente son los grafos bipartitos, en estos grafos tenemos una bipartición del conjunto de vértices en que cada elemnto de la partición es un conjunto independiente. Dicho de otra forma:

Definiciones 8.21. Un grafo $G = (V, E)$ se dice:

- *Bipartito* si $\exists \{V_1, V_2\}$ partición de V tal que $\forall uv \in E$, $(u \in V_1 \wedge v \in V_2) \vee (u \in V_2 \wedge v \in V_1)$.
- *Bipartito completo* si $(\forall u \in V_1)(\forall v \in V_2)$, $uv \in E$. Denotado por $K_{k,l}$ donde $|V_1| = k$ y $|V_2| = l$.

Figura 8.17: Ejemplo de grafo bipartito, el color de los vértices indica a que elemento de la partición pertenece el vértice

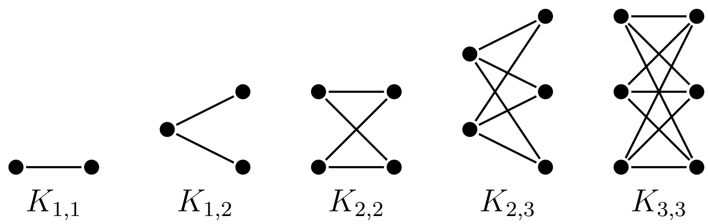


Figura 8.18: Ejemplos de grafos bipartitos completos

Para tener un teorema de caracterización de un grafo bipartito necesitamos demostrar un lema previo.

Lema 8.15. *Todo recorrido cerrado de largo impar en un grafo contiene un ciclo de largo impar.*

Demostración. Por inducción sobre el largo de R.

Base. Sea $R = u_0, u_1, u_2, u_0$ un recorrido cerrado tal que $l(R) = 3$ se observa que $u_0 \neq u_1$, $u_1 \neq u_2$ y $u_0 \neq u_2$. Así R es un ciclo en G de largo tres.

Hipótesis de inducción. Supongamos que el resultado es cierto para todo R recorrido cerrado tal que $l(R) \leq 2k - 1$ impar.

Paso inductivo. Sea $\widetilde{R} : u_0, u_1, \ldots, u_{2k}, u_0$ un recorrido tal que $l(\widetilde{R}) \geq 3$ impar. Si $\widetilde{R}$ no tiene repetición de vértices interiores, entonces $\widetilde{R}$ es un ciclo de largo impar. En caso contrario, sea $u_i = u_j$ un vértice repetido de $\widetilde{R}$ con $i < j$ y consideremos $\widetilde{R_1} : u_i, u_{i+1}, \ldots, u_{j-1}, u_j$ y $\widetilde{R_2} : u_i, u_{i-1}, \ldots, u_0, u_{2k}, u_{2k-1}, \ldots, u_j$ recorridos cerrados donde $l(\widetilde{R_1}) + l(\widetilde{R_2}) = l(\widetilde{R})$ lo que implica que $\widetilde{R_1}$ o $\widetilde{R_2}$ tiene largo impar menor que $2k-1$. Así por hipótesis de inducción tenemos que $\widetilde{R_1}$ o $\widetilde{R_2}$ contiene un ciclo de largo impar lo que implica que existe un ciclo de largo impar en $\widetilde{R}$. ■

Teorema 8.16. *Sea G un grafo no trivial. G es bipartito si y solo si G NO tiene ciclos de largo impar.*

Demostración. $\Rightarrow$) Sea $G = (V, E)$ un grafo bipartito con $\{V_1, V_2\}$ partición, sea $C : u_0, u_1, \ldots, u_{\alpha-1}, u_0 = u_\alpha$ un ciclo tal que $l(C) = \alpha$ en G. Si $u_0 \in V_1$ entonces todos los índices pares están en V_1 y los índices impares están en V_2, como $u_0 = u_\alpha$ entonces α debe ser par. Análogo si $u_0 \in V_2$

$\Leftarrow$) Supongamos que $G = (V, E)$ es conexo y no tiene ciclos de largo impar, es decir, no tiene ciclos o sus ciclos son todos de largo par. Sea $v \in V$ fijo y definamos $V_1 = \{u \in V \setminus \{v\} : d(u, v) \text{ es par}\}$ y

$V_2 = V \setminus V_1 = \{u \in V \setminus \{v\} : d(u,v) \text{ es impar}\} \cup \{v\}$. Probemos que V_1 y V_2 son conjuntos de vértices independientes[1]. Por contradicción sea $y \neq z \in V_1$ tal que $yz \in E$ como $y, z \in V_1$ entonces existe $P_{yv} : y = u_1, u_2, \ldots, u_p = v$ y $P_{vz} : v = w_1, w_2, \ldots, w_q = z$[2] caminos de largo par entre y y v; v y z en G respectivamente.

Luego, $P : y = u_1, u_2, \ldots, u_p = v = w_1, w_2, \ldots, w_q = z, y$ es un recorrido cerrado de largo impar en G y por lema anterior existe ciclo de largo impar en G lo que contradice el supuesto inicial que $G = (V, E)$ no tiene ciclos de largo impar. Así, V_1 es un conjunto de vértices independientes. De manera análoga se prueba que V_2 es un conjunto de vértices independientes lo implica que G es bipartito. ■

En el caso en que $G = (V, E)$ es disconexo se aplica el resultado anterior a cada componente conexa y se agrupan en los conjuntos V_1 y V_2 los vértices de cada componente conexas.

8.11. Grafos planares

Definiciones 8.22. Sea G un grafo se define lo siguiente:

- Se dice que G es *planar* si puede ser dibujado en el plano XY de modo que sus aristas no se intersectan.
- El dibujo de un grafo planar se llama *grafo plano*.
- La región acotada en el grafo plano que son limitadas por ciclos del grafo se denominan *caras*.
- La región no acotada en el grafo plano se llama *cara exterior*.

Ejemplos de grafo planar se observan en la Figura 8.19.

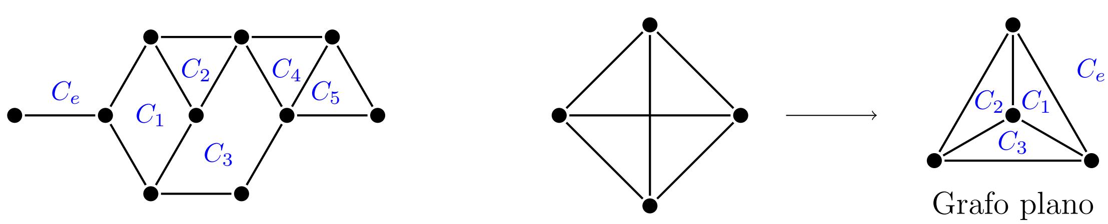


Figura 8.19: Ejemplos de grafo planar

Teorema 8.17 (Fórmula de Euler). *Sea $G = (V, E)$ un grafo conexo, planar, no trivial con f caras entonces:*

$$f = |E| - |V| + 2$$

Demostración. Por inducción sobre el numero de caras.

[1]Si se logra probar que V_1 y V_2 son independientes eso quiere decir que G es bipartito

[2]Se pueden considerar a P_{yv} y P_{vz} los caminos que definen la $d(y, v)$ y $d(v, z)$.

Base. Si el grafo G es conexo, planar y tiene solo una cara, quiere decir que es un árbol ya que si tuviera al menos un ciclo tendría una cara interior y una exterior. Como es un árbol.

$$|E| = |V| - 1$$

sumando a ambos lados $-|V| + 2$ obtenemos:

$$|E| - |V| + 2 = 1 = \text{número de caras.}$$

Hipótesis de inducción. Si $G = (V, E)$ es un grado planar, conexo con f caras, entonces $f = |E| - |V| + 2$

Paso inductivo. Sea $G' = (V', E')$ un grafo planar y conexo con $f + 1$ caras, sea $e \in E'$ una arista que pertenece a un ciclo. Luego, como e no es puente, $G' - e$ es conexo, planar y tiene f caras, entonces:

$$f = |E(G' - e)| - |V(G' - e)| + 2$$

Pero $|V(G' - e)| = |V'|$ y $|E(G' - e)| = |E'| - 1$, luego:

$$\begin{aligned} f &= |E'| - 1 - |V'| + 2 \\ f + 1 &= |E'| - |V'| + 2 \end{aligned}$$

■

Corolario 8.18. *Sea $G = (V, E)$ grafo conexo, planar con f caras entonces:*

$$3f \leq 2|E| \quad y \quad |E| \leq 3|V| - 6$$

Demostración. Sean $c_1, \ldots, c_f$ las caras del grafo y $g(c_i)$ el número de aristas que rodea la cara c_i, cada cara tiene al menos 3 aristas que la rodean, luego:

$$\sum_{i=1}^{f} g(c_i) \geq 3f$$

además, cada arista rodea 1 o 2 caras del grafo, luego cada arista aparece un máximo de 2 veces en la sumatoria:

$$2|E| \geq \sum_{i=1}^{f} g(c_i) \geq 3f$$

Para demostrar la segunda desigualdad, reemplazamos la que ya hemos probado en la fórmula de Euler:

$$\begin{aligned} f &= |E| - |V| + 2 \\ 3f &= 3|E| - 3|V| + 6 \leq 2|E| \\ |E| &\leq 3|V| - 6 \end{aligned}$$

■

Corolario 8.19. *Sea $G = (V, E)$ grafo conexo, planar con f caras, sin ciclos de largo 3 entonces $|E| \leq 2|V| - 4$.*

Demostración. Sean $c_1, \dots, c_f$ las caras del grafo y $g(c_i)$ el número de aristas que rodea la cara c_i, cada cara tiene al menos 4 aristas que la rodean, luego:

$$\sum_{i=1}^{f} g(c_i) \geq 4f$$

además, cada arista rodea 1 o 2 caras del grafo, luego cada arista aparece un máximo de 2 veces en la sumatoria:

$$2|E| \geq \sum_{i=1}^{f} g(c_i) \geq 4f$$
$$|E| \geq 2f$$

Para demostrar la desigualdad, reemplazamos la que ya hemos probado en la fórmula de Euler:

$$\begin{aligned} f &= |E| - |V| + 2 \\ 2f &= 2|E| - 2|V| + 4 \leq |E| \\ |E| &\leq 2|V| - 4 \end{aligned}$$

■

Corolario 8.20. *Sea $G = (V, E)$ grafo conexo, planar, bipartito con f caras entonces $|E| \leq 2|V| - 4$.*

Ahora vemos una caracterización de grafos planares, para esto necesitamos algunas definiciones previas.

Definiciones 8.23. Sea $G = (V, E)$ un grafo no trivial diremos que:

- La arista $uv \in E$ *se subdivide* si es reemplazado en G por un camino de la forma $C : u, w, v$ tal que $l(C) = 2$ con $w \notin V$.

- El grafo $H = (V_H, E_H)$ es una *subdivisión de G en un paso* si $V_H = V \cup \{w\}$ con $w \notin V$ y $E_H = (E - \{uv\}) \cup \{uw, wv\}$

- H es *subdivisión de G* si H es isomorfo a G o si H se obtiene de una sucesión de "subdivisiones de G en un paso"

Teorema 8.21 (Teorema de Kuratowski)**.** *Un grafo es planar si y solo si no contiene ningún subgrafo que sea subdivisión de K_5 o $K_{3,3}$*

No haremos una demostración de este teorema, pero note que K_5 no es planar como consecuencia del Corolario 8.19 y por Corolario 8.20 $K_{3,3}$ no es planar. Además, es fácil ver que hacer una subdivisión no cambia la planaridad del grafo, de todo esto la implicancia hacia la derecha resulta fácil de probar. Sin embargo la recíproca es mucho más compleja de probar y no la demostraremos en este apunte.

8.12. Grafos Eulerianos

Muchos de los primeros conceptos y teoremas de la teoría de grafos surgieron bastante indirectamente, a menudo de matemática recreativa, a través de rompecabezas, juegos o problemas que podrían expresarse en términos de gráficos. El primero de estos problemas fue conocido como el problema de los puentes de Königsberg, que no solo fue resuelto por uno de los matemáticos más famosos de todos los tiempos sino cuya solución se considera el origen de la teoría de grafos y condujo a una importante clase de grafos.

Un problema popular, llamado el problema del puente de Königsberg, pregunta si hay una ruta que cruce cada uno de estos puentes exactamente una vez. La distribución de los puentes de Königsberg puede verse en la Figura 8.20. Aunque durante mucho tiempo se pensó que tal ruta era imposible, el famoso matemático Leonhard Euler (1707-1783) presentó la primera verificación matemática de esta en la Academia de Petersburgo el 26 de agosto de 1735. Al terminar esta sección veremos cuál fue la conclusión a la que llegó Euler.

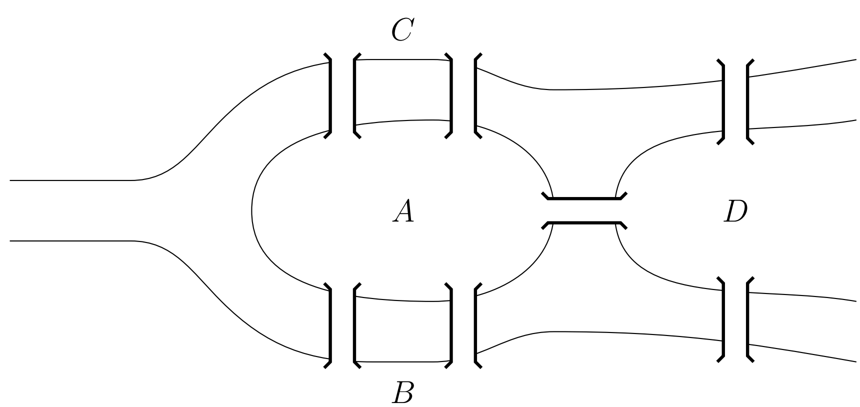


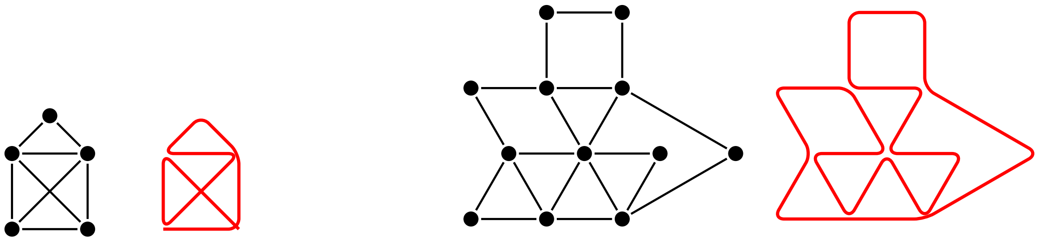
Figura 8.20: Esquema de los puentes de Königsberg

Definiciones 8.24. Dado un grafo G se define lo siguiente:

- Un recorrido en G se dice *recorrido Euleriano* si contiene una y solo una vez cada arista de G.
- Un *circuito Euleriano* es un recorrido Euleriano cerrado.
- Un grafo se dice *Euleriano* si tiene un circuito Euleriano.

Teorema 8.22. *Sea $G = (V, E)$ un grafo sin vértices aislados, las siguientes proposiciones son equivalentes:*

1. *G es Euleriano.*
2. *G es conexo y $\forall u \in V, d(u)$ es par.*



Grafo con recorrido Euleriano   Grafo con circuito Euleriano

Figura 8.21: Ejemplos de grafos con recorrido Euleriano y con circuito Euleriano

3. *G es conexo y E puede ser particionado en ciclos, es decir, $\exists \{E_1, E_2, \ldots, E_k\}$ partición de E tal que $\forall i = 1, 2, \ldots, k \quad E_i$ son las aristas de un ciclo G.*

Demostración.

(1) $\Longrightarrow$ (2) Sea G un grafo Euleriano sin vértices aislados luego $\exists C : x_0, x_1, \ldots, x_p, x_0$ un circuito Euleriano en G se sigue que $V(C) = V$ además $\forall i \in \{0, 1, \ldots, p-1\} \quad p \equiv 0$ se tiene que $x_{i-1}x_i$ y x_ix_{i+1} son aristas en C incidentes al vértice x_i y como C no repite aristas y si x_i aparece k veces en C entonces $d(x_i) = 2k$, es decir, par. Además, para probar la conexidad basta tomar un recorrido al interior del circuito y a partir de eso se tiene un camino entre cualquier par de vértices.

(2) $\Longrightarrow$ (3) Para esto haremos una algoritmo que encuentra la partición de ciclos, ya que la conexidad está dada. Pero antes debemos justificar la existencia de ciclos. Observemos que en un grafo G sin vértices aislados y con todos sus vértices de grado par $\delta(G) \geq 2$ y por Corolario 8.6 el grafo tiene al menos un ciclo.

Algoritmo 8.4: ParticionCiclos(G: grafo con todos sus vértices de grado par)

if G *es un ciclo* **then**
  return $\{E(G)\}$;
else
  $C \leftarrow$ Ciclo de G;
  $G' \leftarrow G - E(C)$;
  $V' \leftarrow$ vértices aislados de G';
  $G'' \leftarrow G' - V'$;
  return $\{E(C)\} \cup$ ParticionCiclos(G'');

Cuando se define el grafo G'' en esta función es claro que este grafo cumple la condición de paridad en los vértices y la ausencia de vértices aislados, por lo tanto se puede ingresar a la función recursivamente

(3) $\Longrightarrow$ (1) Para probar esto construyamos el circuito Euleriano a partir de la partición en ciclos. Sean $C_1, C_2, \ldots, C_k$ una partición en ciclos de G. Como G es conexo, sin pérdida de generalidad puedo suponer que:

$$\forall i \in \{2, \ldots, k\}, C_i = u_0^i \ldots u_{l_i-1}^i u_0^i, \qquad u_0^i \in \bigcup_{j=1}^{i-1} C_j$$

■

Algoritmo 8.5: CircuitoEuleriano($C_1, C_2, \ldots, C_k$: partición en ciclos ordenada)

if $k = 1$ **then**
  return C_1;
else
  $R \leftarrow$ CircuitoEuleriano$(C_1, \ldots, C_{k-1}) = v_0 v_1 \ldots v_l v_0$;
  Sea i_* tal que $v_{i_*} = u_0^k$;
  return $v_0 v_1 \ldots v_{i_*-1} u_0^k \ldots u_{l_i-1}^i u_0^k v_{i_*+1} \ldots v_l v_0$;

Noten que la partición en ciclos no es necesariamente única. En la Figura 8.22 podemos ver dos ejemplos de partición en ciclos para un mismo grafo Euleriano.

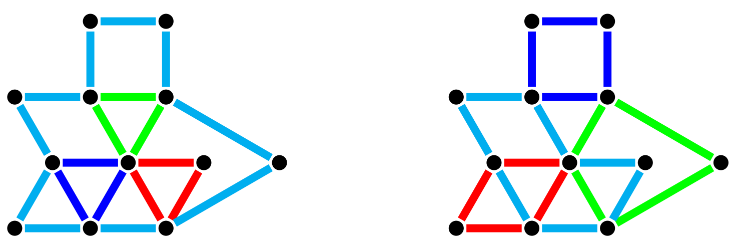


Figura 8.22: Ejemplos de particiones de ciclos de un grafo Euleriano

Corolario 8.23. *Sea G un grafo conexo con exactamente dos vértices de grado impar. Entonces G tiene un recorrido Euleriano que comienza y termina en estos vértices.*

Demostración. Sean u y v los vértices de grado impar, $w \notin V(G)$, luego el grafo $G + w + uw + wv$ es Euleriano, así quitando las aristas uw y wv obtenemos un recorrido Euleriano que comienza en u y termina en v. ∎

Veamos ahora qué pasó con los puentes de Königsberg. El grafo asociado al problema de los puentes de Königsberg podemos verlo en la Figura 8.23 ahí observamos que los vértices A, B, C y D tienen grado impar, por lo tanto, es imposible encontrar un recorrido Euleriano.

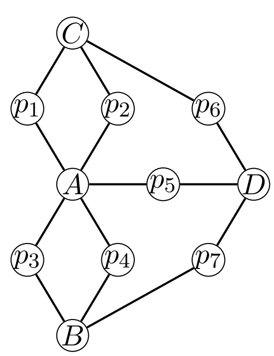


Figura 8.23: Grafo asociado al problema de los puentes de Königsberg

8.13. Grafos Hamiltonianos

Por último vamos a ver los grafos Hamiltonianos. Cuando se plantea este problema, la primera impresión sugiere que se parece al caso Euleriano y que, por lo tanto, debe ser fácil de solucionar. Sin embargo, las apariencias engañan y, saber si existe una caracterización de este tipo de grafos que sea verificable de manera eficiente, es un problema abierto hasta el día de hoy.

Definiciones 8.25. Sea G un grafo se define lo siguiente:

- Un camino que contiene todos los vértices de G se dice *camino Hamiltoniano.*
- Un ciclo que contiene todos los vértices de G se dice *ciclo Hamiltoniano.*
- Un grafo con ciclo Hamiltoniano se dice *grafo Hamiltoniano.*

En la Figura 8.24 podemos observar ejemplos de grafos con camino y ciclo Hamiltoniano.

Grafo con camino Hamiltoniano   Grafo con ciclo Hamiltoniano

Figura 8.24: Ejemplos de grafos con camino Hamiltoniano y ciclo Hamiltoniano

Este problema no es fácil de resolver de modo que no daremos un teorema de caracterización, si no que un condiciones necesarias para que el grafo sea Hamiltoniano y luego un teorema de condiciones suficientes.

Proposición 8.24. *Si G es un grafo Hamiltoniano las siguientes proposiciones son verdaderas:*

1. *G es conexo.*
2. *$\delta(G) \geq 2$.*
3. *G no tiene vértices de corte.*
4. *G no tiene puentes.*
5. *Si G es bipartito $|V(G)|$ es par, más aún $|V_1| = |V_2|$.*

Lema 8.25. *Sea G un grafo de n vértices y $u, v \in V(G)$ no adyacentes tal que $d(u)+d(v) \geq n$ entonces G es Hamiltoniano si y solo si $G + uv$ es Hamiltoniano.*

Demostración. Claramente si G es Hamiltoniano, $G + uv$ es Hamiltoniano. Lo que debemos demostrar es la recíproca. Hacemos una demostración constructiva. Supongamos que $G + uv$ es Hamiltoniano, luego tenemos el ciclo Hamiltoniano $C = u_0u_1 \dots u_{n-1}u_0$, donde $u = u_0$ y $v = u_{n-1}$. Sea $U = \{i \in \{0, \dots, n-1\} : u_{i+1} \in N(u)\}$ y $W = \{i \in \{0, \dots, n-1\} : u_i \in N(v)\}$.

$$|U \cup W| = |U| + |W| - |U \cap W|$$

luego,

$$|U \cap W| = |U| + |W| - |U \cup W| = d(u) + d(v) - |U \cup W| \geq |V| - |U \cup W|$$

como u y v no son adyacentes $n-1 \notin U \cup W$, por lo tanto $|U \cup W| \leq |V| - 1$, de este modo:

$$|U \cap W| \geq |V| - (|V| - 1) = 1$$

Sea $i_* \in U \cap W$, entonces tenemos el ciclo Hamiltoniano $u_0u_1 \dots u_{i_*}u_{n-1}u_{n-2}u_{n-3} \dots u_{i_*+1}u_0$, como $u = u_0$ y $v = u_{n-1}$ y este ciclo no pasa por $u_{n-1}u_0$, y es un ciclo Hamiltoniano de G.

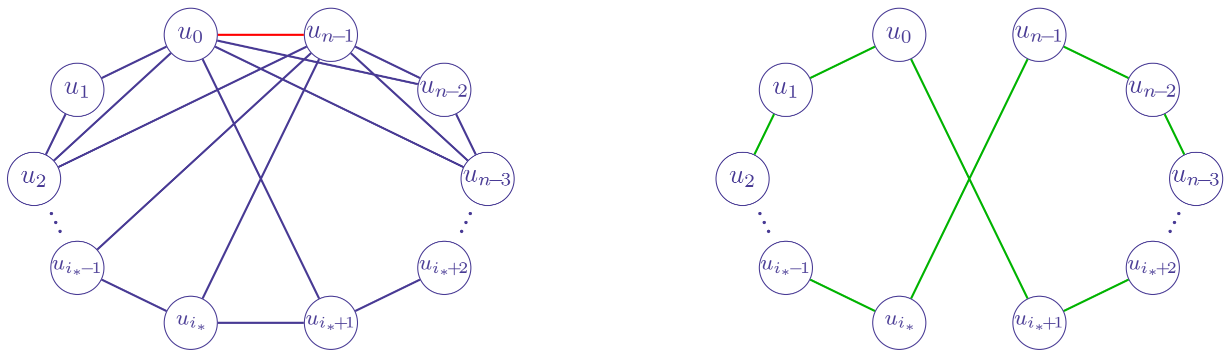


Figura 8.25

■

Teorema 8.26. *Sea $G = (V, E)$ un grafo con $|V| \geq 3$ vértices si $\forall u, v \in V$ no adyacentes $d(u) + d(v) \geq |V|$ entonces G es Hamiltoniano.*

Demostración. Usando el lema anterior llegamos a la conclusión que G es Hamiltoniano si y solo si el grafo completo es Hamiltoniano, lo que por supuesto es verdadero. ■

Corolario 8.27. *Sea $G = (V, E)$ un grafo con $|V| \geq 3$ vértices y $\delta(G) \geq \frac{|V|}{2}$ entonces G es Hamiltoniano.*

Demostración. Usando el teorema anterior, si $\forall u \in V$, $d(u) \geq \frac{|V|}{2}$, entonces $\forall u, v \in V$, $d(u) + d(v) \geq |V|$. Por lo tanto, G es Hamiltoniano. ■

8.14. Ejercicios

P1. Verdadero o falso. Justifique su respuesta en ambos casos.

a) ____ Si G es un grafo tal que $\delta(G) \geq 2$ entonces G es conexo.

b) ____ $K_{4,4}$ es Hamiltoniano y Euleriano.

c) ____ Si G es un grafo tal que tiene todos sus vértices de grado 2 entonces es Euleriano.

d) ____ Existe un grafo bipartito, planar, Euleriano y Hamiltoniano.

e) ____ Existe un grafo planar 6-regular.

f) ____ Existe G conexo con secuencia de grados (1,1,1,1,2,2,2,2)

g) ____ Si un grafo es bipartito y disconexo, entonces es planar.

h) ____ Un grafo conexo con n vértices y n aristas contiene exactamente un ciclo.

i) ____ Existe un grafo conexo de n vértices y $n+1$ aristas que contiene exactamente dos ciclos.

j) ____ Si un árbol tiene un número de hojas par, entonces los otros vértices tienen grado par.

k) ____ Existe un grafo no planar, no bipartito, no Euleriano y no Hamiltoniano.

l) ____ Existe un grafo 4-regular planar y bipartito.

m) ____ Sea G un grafo de 4 aristas y 5 vértices. G es un árbol.

n) ____ Es posible construir carreteras para unir 3 ciudades con 3 aeropuertos sin que haya ningún cruce utilizando solamente 1 paso bajo nivel.

ñ) ____ Existe un grafo 4-regular planar.

o) ____ Todo árbol tiene al menos un vértice de corte.

P2. ¿Es posible que en un grupo de trece personas cada una de ellas salude exactamente a tres?

P3. Muestre que en todo grafo G con $n \geq 2$ vértices existen dos nodos de igual grado.

P4. Pruebe que todo grafo conexo de orden $n \geq 2$ y tamaño $n-1$ tiene al menos dos vértices de grado uno.

P5. Sea $G = (V, E)$ un grafo con exactamente dos vértices de grado impar. Pruebe que existe un camino entre estos vértices.

P6. El objetivo de este problema es demostrar que dada una secuencia $S = \{d_1, d_2, \ldots, d_n\}$ de enteros tales que $d_i \geq 1$ es posible construir un árbol de n vértices cuyos grados son los valores de S si y sólo si:

$$\sum_{i=1}^{n} d_i = 2(n-1). \tag{8.2}$$

Para esto demuestre que:

a) Si $\{d_1, d_2, \ldots, d_n\}$ son grados de los vértices de un árbol, entonces:

$$\sum_{i=1}^{n} d_i = 2(n-1) \tag{8.3}$$

b) Si $\sum_{i=1}^{n} d_i = 2(n-1)$, entonces siempre hay al menos un $d_i = 1$.

c) Si $\sum_{i=1}^{n} d_i = 2(n-1)$, entonces existe un árbol cuyos vértices tienen grados $\{d_1, d_2, \ldots, d_n\}$. Hint: pruebe por inducción sobre n y puede utilizar el resultado de la parte b.

P7. Para todo $n \in \mathbb{N}$ definimos el grafo $G_n = (V_n, E_n)$ como:

- El conjunto de vértices $V_n = \{1, 2, \ldots, n\}$.
- Existe la arista entre los vértices u y v si y sólo si $u \mod v = 0$ o $v \mod u = 0$.

¿Para qué valores de n es G_n planar?

P8. Sea G un grafo con $n \geq 2$ vértices. Pruebe que G es conexo si y solo si $\forall \{U, W\}$ partición de $V(G)$, $\exists u \in U$, $w \in W$ tal que $uw \in E(G)$.

P9. Sea G un grafo conexo. Muestre que todo par de caminos de largo máximo, tienen un vértice en común.

P10. Sea $G = (V, E)$ un grafo con $\delta(G) \geq 2$. Pruebe que $\exists H$ grafo conexo tal que $V(H) = V(G)$ y $\forall v \in V(H)$, $d_H(x) = d_G(x)$.

P11.

1. Pruebe que la secuencia de grados es una invariante en grafos isomorfos.
2. Muestre un ejemplo de grafos no isomorfos con igual secuencia de grados.

P12. Sea $G_n = (V_n, E_n)$ tal que $V_n = \{0,1\}^n$ y $xy \in E_n$ si y solo si existe un único $i \in \{1, \ldots, n\}$ tal que $x_i \neq y_i$.

1. Pruebe que G_n es n regular.
2. ¿Para qué valores de n G_n es Euleriano?
3. Pruebe que para $n \geq 2$, G_n es Hamiltoniano.
4. Pruebe que G_n es bipartito.
5. Determine para que valores de n G_n es planar.

P13. Muestre que las piezas de un domino pueden ser colocadas siguiendo las reglas del juego de manera de formar un único ciclo.

P14. Sea $D = \{d_i\}_i^n$ un conjunto de enteros tal que $0 < d_1 \leq d_2 \leq \cdots \leq d_n$, $n \geq 2$. Pruebe que D es un conjunto de grados de un árbol $\Leftrightarrow \sum_{i=1}^{n} d_i = 2n - 2$

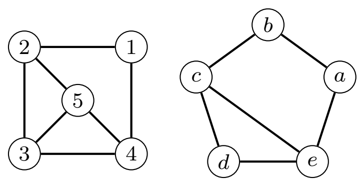
Representar G mediante su matriz de adyacencia y mediante un dibujo.

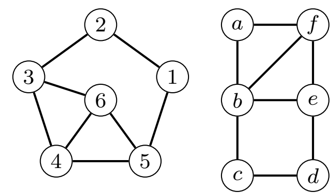
P15. Consideremos los grafos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$. El producto cartesiano de G_1 y G_2, que denotamos $G_1 \times G_2$ se define de la siguiente forma: los vértices son $V_1 \times V_2$, es decir, pares de la forma (u_1, u_2) con $u_1 \in V_1$ y $u_2 \in V_2$. dos vértices $u = (u_1, u_2)$ y $v = (v_1, v_2)$ son adyacentes en los siguientes casos:

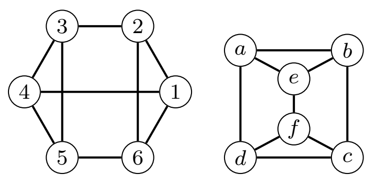
- $u_1 = v_1$ y $\{u_2, v_2\} \in E_2$
- $u_2 = v_2$ y $\{u_1, v_1\} \in E_1$

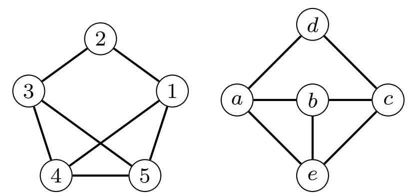
Dar la matriz de adyacencia y un dibujo del grafo $Q_2 \times K_2$ y del grafo $Q_2 \times K_3$. Determinar el número de aristas de $G_1 \times G_2$ en función del número de vértices y aristas de G_1 y de G_2. ($Q_n = (V_n, E_n)$ tal que $V_n = \{0,1\}^n$ y $u, v \in E_n$ si y solo si u y v difieren en una sola coordenada).

P16. Para cada uno de los siguientes pares de grafos, decidir si son o no son isomorfos. Justifique su respuesta.

1. 

3. 

2. 

4. 

P17. Dibujar un grafo conexo con 5 vértices que siga siendo conexo si se eliminan 2 cualesquiera de sus vértices (y las aristas adyacentes). ¿Cuántas aristas debe tener, como mínimo, un grafo que verifique la propiedad anterior?

P18. Sea $G = (V, E)$ un grafo con n vértices tal que $d(v) \geq \frac{n-1}{2}$ para todo $v \in V$. Demostrar que G es conexo. (Indicación: de hecho, se puede demostrar que en ese caso la distancia entre cualquier par de vértices es como mucho 2).

P19. Dado un grafo $G = (V, E)$, se define el grafo complementario, denotado G^c, como el grafo con el mismo conjunto de vértices tal que dos vértices son adyacentes en G^c si, y solo si, no son adyacentes en G. Demostrar que, para cualquier grafo G, G o G^c es conexo.

P20. Sea $G = (V, E)$ un árbol tal que tiene n vértices cuyos grados son los n primeros cuadrados y el resto son hojas. ¿Cuántas hojas tiene el árbol?

(Ind. El árbol tiene secuencia de grados $(1, \ldots, 1, 4, 9, 16, 25, \ldots, n^2)$)

P21. Sea G un grafo Hamiltoniano. Pruebe que:

1. G no tiene vértices de corte.
2. G no tiene puentes.

Capítulo 9

Digrafos

9.1. Conceptos y nociones fundamentales

Definición 9.1. Un *digrafo* es un par ordenado $D = (V, A)$ donde:

- V es un conjunto finito no vacío cuyos elementos llamamos *vértices*.
- $A \subseteq V \times V$ conjunto de pares ordenados de V llamados *arcos*.

Definiciones 9.2. Sea $D = (V, A)$ un digrafo y sea $(u, v) \in A$ un arco, se define lo siguiente:

- u es el *vértice inicial*.
- v es el *vértice final*.
- Si $u = v$ se dice *bucle*.

Definiciones 9.3. Sea $D = (V, A)$ un digrafo, $\forall u \in V$ se define:

- $N^+(u) := \{v \in V : (u, v) \in A\}$ como la *vecindad de salida*.
- $N^-(u) := \{v \in V : (v, u) \in A\}$ como la *vecindad de entrada*.
- $d^+(u) := |N^+(u)|$ como el *grado de salida*.
- $d^-(u) := |N^-(u)|$ como el *grado de entrada*.
- $d(u) := d^-(u) + d^+(u)$ como el *grado total*.

Definiciones 9.4. Sea $D = (V, A)$ un digrafo entonces se define:

- El *grado mínimo de salida* como $\delta^+(D) := \min\limits_{u \in V} d^+(u)$.

- El *grado mínimo de entrada* como $\delta^-(D) := \min_{u\in V} d^-(u)$.
- El *grado máximo de salida* como $\Delta^+(D) := \max_{u\in V} d^+(u)$.
- El *grado máximo de entrada* como $\Delta^-(D) := \max_{u\in V} d^-(u)$.

Proposición 9.1. *En todo digrafo $D = (V, A)$ se tiene que:*

$$\sum_{u\in V(D)} d^+(u) = \sum_{u\in V(D)} d^-(u) = |A|$$

Demostración. Por inducción sobre el número de arcos:

Base. Si D tiene un único arco solo habrá un vértice que tiene grado de salida 1 el resto 0 por lo tanto $\sum_{u\in V(D)} d^+(u) = 1$. Análogo para el grafo de entrada.

Hipótesis de inducción. Si $|A| = m$ entonces $\sum_{u\in V(D)} d^+(u) = \sum_{u\in V(D)} d^-(u) = |A|$.

Paso inductivo. Sea $D = (V, A)$ con $|A| = m + 1$, sea $a \in A$ cualquiera. El digrafo $D' = (V, A \setminus \{a\}$ tiene m arcos, luego:

$$\sum_{u\in V(D')} d^+_{D'}(u) = \sum_{u\in V(D')} d^-_{D'}(u) = m$$

Pero,

$$d^+_{D'}(u) = \begin{cases} d^+_D(u) & \text{Si } \exists v \in V, a \neq (u, v) \\ d^+_D(u) - 1 & \text{Si } \exists v \in V, a = (u, v) \end{cases}$$

$$d^-_{D'}(u) = \begin{cases} d^-_D(u) & \text{Si } \exists v \in V, a \neq (v, u) \\ d^-_D(u) - 1 & \text{Si } \exists v \in V, a = (v, u) \end{cases}$$

Luego,

$$m = \sum_{u\in V(D')} d^+_{D'}(u) = \sum_{u\in V(D)} d^+_D(u) - 1m \qquad = \sum_{u\in V(D')} d^-_{D'}(u) = \sum_{u\in V(D)} d^-_D(u) - 1$$

Por lo tanto,

$$\sum_{u\in V(D)} d^+_D(u) = \sum_{u\in V(D)} d^-_D(u) = m + 1 = |A|$$

■

9.2. Subgrafos

Definición 9.5. Sea $D = (V, A)$ un digrafo, se dice que $D' = (V', A')$ es *subgrafo* de D si D' es un digrafo tal que:

- $V' \subseteq V$.
- $A' \subseteq A$.

y se denota como $D' \subseteq D$

Definiciones 9.6. Sea $D = (V, A)$ y sea $D' \subseteq D$ se define lo siguiente:

- Si $V' = V$ entonces se dice que D' es un *subgrafo generador o recubridor* de D
- Si $A' = \{(u, v) \in A : u, v \in V'\}$ entonces se dice que D' es un *subgrafo inducido* por V' y se denota por $D' = D[V']$

9.3. Caminos y ciclos

Definiciones 9.7. Dado $D = (V, A)$ un digrafo definimos lo siguiente:

- *Recorrido* entre v_0 y v_l como una secuencia ordenada de vértices de D tal que $\forall j \in \{0, \ldots, l-1\}$, $(v_j, v_{j+1}) \in A$.

  La notación al respecto es:

  - Recorrido $R = v_0, v_1, \ldots, v_l$.
  - Vértices de un recorrido $V(R) = \{v_0, v_1, \ldots, v_l\}$.
  - Arcos de un recorrido $A(R) = \{(v_j, v_{j+1}) : j \in \{0, \ldots, l-1\}\}$.
- A los vértices v_0 y v_l se les denomina *vértices externos*.
- A los vértices $v_1, \ldots, v_{l-1}$ se les denomina *vértices internos*.
- Si el recorrido es tal $v_0 = v_l$ entonces lo denominamos *circuito*.
- Si el recorrido no contiene vértices repetidos entonces lo denominamos *camino*.
- Si el circuito no contiene vértices repetidos (excepto por los extremos) entonces lo denominamos *ciclo*.
- El *largo de un recorrido* es $l(R) = l$

Observación 9.1. El largo, vértices y arcos de un recorrido es extensible a circuito, camino y ciclo.

Proposición 9.2. *Dado un D un digrafo cualquiera, si existe un recorrido entre los vértices u y v de D entonces existe un camino entre u y v en D.*

Algoritmo 9.1: CaminoDirigido(recorrido dirigido R)

if *R no tiene vértices repetidos* **then**
    return R;
else
    $i_* \longleftarrow \min \{i \in \{0, \ldots, l-1\} : \exists j > i, v_j = v_i\}$;
    $j_* \longleftarrow \max \{j > i_* : v_j = v_{i_*}\}$;
    return *CaminoDirigido*($v_0 \ldots v_{i_*} v_{j_*+1} \ldots v_l$);

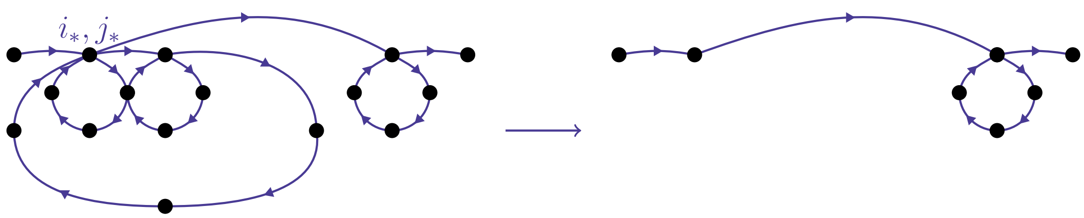


Figura 9.1: Idea de funcionamiento de Algoritmo 8.1

Demostración. Esta demostración es una copia del caso no orientado..

Sea $R = v_0 v_1 v_2 \ldots v_l$ un recorrido de u a v, es decir, $v_0 = u$, $v_l = v$ y para todo $i \in \{0, \ldots, l-1\}$, $v_i v_{i+1} \in A(D)$. A partir de esto construimos un algoritmo que nos permita encontrar un camino entre u y v.

También podemos plantear una demostración puramente matemática. Por reducción al absurdo, supongamos que existe un recorrido de u a v, pero no existe un camino. Sea $R = v_0 v_1 v_2 \ldots v_l$ el recorrido más corto entre u y v, que no es un camino, por lo tanto este recorrido tiene vértices repetidos, así podemos definir:

$$i_* = \min \{i \in \{0, \ldots, l-1\} : \exists j > i, v_j = v_i\}$$
$$j_* = \max \{j > i_* : v_j = v_{i_*}\}$$

Con estas definiciones obtenemos que $R' = v_0 \ldots v_{i_*} v_{j_*+1} \ldots v_l$ también es un recorrido entre u y v y es más corto que R, por lo que tenemos una contradicción. ∎

9.4. Conexidad en digrafos

Definición 9.8. Un digrafo $D = (V, A)$ se dice *fuertemente conexo* si $\forall u, v \in V$, $\exists P$ camino dirigido de u a v en D o D es el digrafo trivial, es decir, $|V| = 1$ y $A = \varnothing$.

Definición 9.9. Dado un digrafo $D = (V, A)$ se define el *grafo fundamental* de D por $G_D = (V_D, E_D)$ donde $V_D = V$ y $ab \in E_D \Leftrightarrow (a, b) \in A \vee (b, a) \in A$.

Definición 9.10. Un digrafo $D = (V, A)$ se dice *conexo* si el grafo fundamental de D, G_D, es conexo.

Definiciones 9.11. Sea $D = (V, A)$ un digrafo se define:

- Las *componentes conexas* de D son los subgrafos correspondientes a las componentes conexas del grafo fundamental de D.

- Las *componentes fuertemente conexas* de D son los subgrafos dirigidos que son fuertemente conexos y maximales de la propiedad.

Observación 9.2. Si $D = (V, A)$ es un digrafo fuertemente conexo no trivial, entonces $\forall u \in V$, $d^+(u) > 0 \wedge d^-(u) > 0$.

Definición 9.12. Una *orientación* de un grafo $G = (V, E)$ es un digrafo $D = (V_D, A_D)$ donde $V_D = V$ y $ab \in E(D) \Longleftrightarrow (a, b) \in A_D \veebar (b, a) \in A_D$.

Definición 9.13. Una orientación de un grafo completo se denomina *torneo*.

Observación 9.3. La conexidad es una invariante en digrafos isomorfos.

9.5. Distancia en digrafos

Tal como en el caso de grafos no orientados también es posible definir una distancia en digrafos. La forma de definir esta distancia es análoga a la de grafos no orientados.

Definición 9.14. Dado D un digrafo y $u, v \in V(D)$ se define la distancia entre u y v como:

$$d(u,v) = \begin{cases} 0 & \text{Si } u = v \\ \text{mín}\,\{l(P) : P \text{ es camino entre } u \text{ y } v\} & \text{Si existe un camino entre } u \text{ y } v \\ +\infty & \text{si no existe camino entre } u \text{ y } v \end{cases}$$

Para calcular esta distancia existe más de un algoritmo disponible, sin embargo el más conocido es el Algoritmo de Dijkstra. Este Algoritmo considera que cada arco tiene un cierto peso positivo y calcula el camino de costo mínimo entre un nodo fuente y el resto de los vértices del grafo. Si queremos calcular la distancia en un grafo sin pesos, basta utilizar este algoritmo considerando que todos los arcos tienen peso 1. Sin embargo, este algoritmo es mucho más útil en problemas aplicados si consideramos los pesos de los arcos.

9.5.1. Algoritmo

El algoritmo de Dijkstra, también llamado algoritmo de caminos mínimos, es un algoritmo para la determinación del camino más corto dado un vértice origen al resto de vértices en un grafo con pesos en cada arista. Su nombre se refiere a Edsger Dijkstra, quien lo describió por primera vez en 1959.

La idea subyacente en este algoritmo consiste en ir explorando todos los caminos más cortos que parten del vértice origen y que llevan a todos los demás vértices; cuando se obtiene el camino más corto desde el vértice origen, al resto de vértices que componen el grafo, el algoritmo se detiene.

Teniendo un grafo dirigido ponderado de n nodos no aislados, sea s el nodo inicial, un vector `distancia` de tamaño n guardará al final del algoritmo las distancias desde s al resto de los nodos.

Inicializar todas las distancias en `distancia` con un valor infinito relativo ya que son desconocidas al principio, exceptuando la de s que se debe colocar en 0 debido a que la distancia de s a s sería 0.

Sea $u = s$ (tomamos u como nodo actual).

Recorremos todos los nodos adyacentes de u, excepto los nodos marcados, llamaremos a estos nodos no marcados v_i.

Si la distancia desde s hasta v_i guardada en `distancia` es mayor que la distancia desde s hasta u, sumada a la distancia desde u hasta v_i; esta se sustituye con la segunda nombrada, esto es:

si (`distancia`$[i]$ > `distancia`$[u] + d(u, v_i)$) entonces `distancia`$[i]$ = `distancia`$[u] + d(u, v_i)$

Marcamos como completo el nodo u.

Tomamos como próximo nodo actual el de menor valor en `distancia` (puede hacerse almacenando los valores en una cola de prioridad) y volvemos al paso 3 mientras existan nodos no marcados.

Una vez terminado al algoritmo, `distancia` estará completamente lleno.

Algoritmo 9.2: DIJKSTRA (Grafo D, nodo fuente s)

```
forall v ∈ V(D) do
    if (v ∈ N^+(s)) then
        distancia[v] ⟵ peso(s, v);
    else
        distancia[v] ⟵ ∞;
    end
    visto[v] ⟵ False;
    padre[v] ⟵ null;
end
distancia[s] ⟵ 0;
visto[s] ⟵ True;
while (∃v ∈ V(D), visto[v] = False) do
    u ⟵ coger el mínimo del vector distancia y que no esté visto;
    visto[u] ⟵ True;
    forall v ∈ N^+(u) do
        if (distancia[v] > distancia[u] + peso(u, v)) then
            distancia[v] ⟵ distancia[u] + peso(u, v);
            padre[v] ⟵ u;
        end
    end
end
```

9.6. Digrafos Eulerianos

Definiciones 9.15. Dado un digrafo D no trivial se define lo siguiente:

- Un recorrido dirigido en D se dice *recorrido dirigido Euleriano* si contiene una y solo una vez cada arco de D.
- Un *circuito dirigido Euleriano* es un recorrido dirigido Euleriano cerrado.
- Un digrafo se dice *Euleriano* si tiene un circuito dirigido Euleriano.

Lema 9.3. *Sea D un digrafo tal que $\delta^+(D) > 0$ (análogo si $\delta^-(D) > 0$) entonces D tiene al menos un ciclo.*

Demostración. Sea $v_0 \in V$ un vértice cualquiera, como $\delta^+(D) > 0$ existe v_1 tal que $(v_0, v_1) \in A(D)$, siguiendo este procedimiento encontramos un recorrido $v_0 v_1 \dots v_n$ $(n = |V|)$, como en ese recorrido hay $n+1$ vértices y el digrafo tiene solo n vértices necesariamente hay al menos uno que se repite, por lo tanto tenemos un ciclo. El caso $\delta^-(D) > 0$ es análogo. ∎

Teorema 9.4. *Sea $D = (V, A)$ un digrafo sin vértices aislados entonces las siguientes proposiciones son equivalentes:*

1. *D es Euleriano*
2. *D es fuertemente conexo y $\forall u \in V(D), d^+(u) = d^-(u)$.*
3. *D es fuertemente conexo y $A(D)$ puede ser particionado en ciclos.*

Demostración.

(1) $\Longrightarrow$ (2) Sea D un digrafo Euleriano sin vértices aislados luego $\exists C : u_0, u_1, \dots, u_m, u_0$ un circuito Euleriano en D se sigue que $V(C) = V$ además $\forall i \in \{0, 1, \dots, m-1\}$ $\quad m \equiv 0$ se tiene que (u_{i-1}, u_i) es un arco que llega a u_i y (u_i, u_{i+1}) es un arco que sale de u_i y como C no repite arcos y si u_i aparece k veces en C entonces $d^-(u_i) = d^+(u_i) = k$. Además, para probar la conexidad basta tomar un recorrido al interior del circuito y a partir de eso se tiene un camino entre cualquier par de vértices.

(2) $\Longrightarrow$ (3) Para esto haremos una algoritmo que encuentra la partición de ciclos, ya que la conexidad está dada. Pero antes debemos justificar la existencia de ciclos. Observemos que en un grafo G sin vértices aislados y con todos sus vértices con igual grado de entrada y salida cumple la condición $\delta^+(D) > 0$ y por Lema 9.3 el digrafo tiene al menos un ciclo.

Cuando se define el digrafo D'' en esta función es claro que este grafo cumple la condición de igualdad de grado en los vértices y la ausencia de vértices aislados, por lo tanto se puede ingresar a la función recursivamente

(3) $\Longrightarrow$ (1) Para probar esto construyamos el circuito Euleriano a partir de la partición en ciclos. Sean $C_1, C_2, \dots, C_k$ una partición en ciclos de D. Como D es fuertemente conexo, sin pérdida de generalidad podemos suponer que:

$$\forall i \in \{2, \dots, k\}, C_i = u_0^i \dots u_{l_i-1}^i u_0^i, \qquad u_0^i \in \bigcup_{j=1}^{i-1} C_j$$

Algoritmo 9.3: ParticionCiclosDir(digrafo D con igual de grado de entrada y salida en todos sus vértices)

```
if D es un ciclo then
    return {A(D)};
else
    C ⟵ Ciclo de D;
    D' ⟵ D − A(C);
    V' ⟵ vértices aislados de D';
    D'' ⟵ D' − V';
    return A(C) ∪ ParticionCiclosDir(D'');
```

Algoritmo 9.4: CircuitoEulerianoDir($C_1, C_2, \ldots, C_k$ partición en ciclos ordenada)

```
if k = 1 then
    return C_1;
else
    R ⟵ CircuitoEuleriano(C_1, ..., C_{k−1}) = v_0 v_1 ... v_l v_0;
    Sea i_* tal que v_{i_*} = u_0^k;
    return v_0 v_1 ... v_{i_*−1} u_0^k ... u_{l_i−1}^i u_0^k v_{i_*+1} ... v_l v_0;
```

■

Corolario 9.5. *Un digrafo D tiene un recorrido Euleriano desde u a v, con $u, v \in V(D)$ no adyacentes, si y solo si D es conexo y (salvo vértices aislados) $\forall w \in V(D) \setminus \{u, v\}$, $d^+(w) = d^-(w)$, $d^+(u) = d^-(u) + 1$ y $d^-(v) = d^+(v) + 1$.*

Demostración. Sean $w \notin V(D)$ y $D' = D + (w, u) + (v, w)$, claramente D' es Euleriano, así quitando los arcos (w, u), (v, w) y el vértice w obtenemos un recorrido Euleriano que comienza en u y termina en v. ■

9.7. Digrafos Hamiltoniano

Definiciones 9.16. Sea D un digrafo no trivial se define lo siguiente:

- Un camino simple dirigido que contiene todos los vértices de D se dice *camino dirigido Hamiltoniano.*
- Un ciclo que contiene todos los vértices de D se dice *ciclo dirigido Hamiltoniano.*
- Un digrafo con ciclo dirigido Hamiltoniano se dice *Hamiltoniano.*

Observación 9.4. De la definición de digrafo Hamiltoniano se tiene que digrafo Hamiltoniano implica digrafo fuertemente conexo. Sin embargo, digrafo fuertemente conexo NO implica digrafo Hamiltoniano.

Teorema 9.6. *Todo torneo con $|V| \geq 2$ tiene un camino Hamiltoniano.*

Teorema 9.7 (Teorema de Meyniel)**.** *Sea $D = (V, A)$ un digrafo fuertemente conexo no trivial si $\forall u, v \in V$, $u \neq v$ no adyacente, es decir, $(u, v) \notin A \wedge (v, u) \notin A$, $d(u) + d(v) \geq 2n - 1$ entonces D es Hamiltoniano.*

9.8. Matriz de adyacencia

Dado un digrafo $D = (V, A)$ con $V = \{v_1, \ldots, v_n\}$ se define la matriz de adyacencia del grafo como $B \in \mathcal{M}_{n\times n}(\{0, 1\})$, tal que:

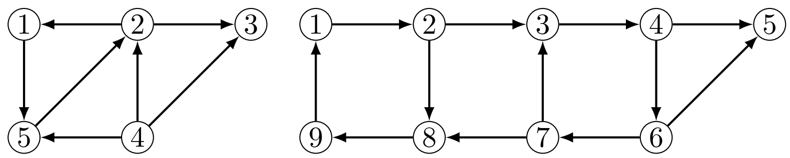
$$b_{i,j} = 1 \iff (v_i, v_j) \in A$$

Algunas propiedades de la matriz de adyacencia son:

1. Para un grafo no dirigido la matriz de adyacencia es simétrica.
2. Si existe k tal que $[B^k]_{i,j} = 1$ entonces existe un camino entre el vértice v_i y el vértice v_j.
3. Si D es fuertemente conexo entonces $\sum_{i=1}^{n} B^i$ estará llena de unos.

9.9. Ejercicios

P1. Determinar las componentes fuertemente conexas de los grafos de la figura.



P2. Dado D un digrafo. Pruebe que si $\delta^-(D) \geq 1$ entonces D tiene al menos un ciclo.

P3. Pruebe que un torneo tiene un camino Hamiltoniano.

P4. Un grafo se dice orientable si tiene una orientación fuertemente conexa. Pruebe que:

1. Un árbol no es orientable.
2. Un grafo Hamiltoniano es orientable.
3. Si un grafo es orientable, tiene al menos dos orientaciones fuertemente conexas.
4. Un grafo conexo es orientable si y solo si no tiene puentes.

P5. Pruebe que un digrafo $D = (V, A)$ es fuertemente conexo si y solo existe $v^* \in V$ tal que para todo $u \in V$ existe un camino de u a v^* y de v^* a u.

P6. Dado un digrafo $D = (V, A)$ se define el grafo potencia $k \in \mathbb{N}$, denotado por $D^k = (V^k, A^k)$, como:

- $V^k = V$
- $(u, v) \in A^k \Longleftrightarrow 1 \leq d_D(u, v) \leq k$,

donde $d_D(u, v)$ es la distancia en D entre los nodos u y v.

1. Encuentre un ejemplo de grafo D con 5 nodos tal que D^2 sea isomorfo a D. Justifique.
2. Si $|V| = n$, pruebe que D es fuertemente conexo si y solo si D^n es isomorfo al digrafo completo de n nodos sin bucles.

Parte II

Máquinas

Capítulo 10

Lenguajes

En primer lugar daremos las definiciones y notaciones de lenguajes.

Definición 10.1. Un *alfabeto* es un conjunto finito de símbolos que denotaremos por Σ.

Por ejemplo,

$$\begin{aligned}
&\Sigma = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\} \\
&\Sigma = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, \tilde{n}, o, p, q, r, s, t, u, v, w, x, y, z\} \\
&\Sigma = \{0, 1\} \qquad \text{alfabeto binario}
\end{aligned}$$

Definición 10.2. Una *palabra o string* en Σ es una secuencia finita $w = (\sigma_1, \sigma_2, \ldots, \sigma_n) \in \Sigma^n$. Para simplificar notación escribiremos $w = \sigma_1\sigma_2 \ldots \sigma_n$. El largo de una palabra $w \in \Sigma^n$ es igual a n y es denotado por $|w| = n$.

Definición 10.3. Definimos la *palabra vacía* como la palabra que no tiene símbolos y la denotamos por ε. En este caso $|\varepsilon| = 0$.

Σ^n es el conjunto de todas las palabras de largo $n \in \mathbb{N}$. Definimos

$$\Sigma^* = \{\varepsilon\} \cup \bigcup_{n\in\mathbb{N}} \Sigma^n \equiv \bigcup_{n\in\mathbb{N}\cup\{0\}} \Sigma^n$$

es decir, Σ^* es el conjunto de todas las palabras en Σ. También denotamos $\Sigma^+ = \bigcup_{n\in\mathbb{N}} \Sigma^n$ las palabras de largo mayor o igual a 1 en Σ.

La concatenación es una función definida por:

$$\begin{aligned}
\circ : \Sigma^* \times \Sigma^* &\to \Sigma^* \\
(u, v) \quad &\to \circ(u, v) = u \circ v = u_1u_2 \ldots u_nv_1v_2 \ldots v_m
\end{aligned}$$

donde,

$$\begin{aligned}
u &= u_1u_2 \ldots u_n \\
v &= v_1v_2 \ldots v_m
\end{aligned}$$

Si $u = \varepsilon$ o $v = \varepsilon$ entonces $u \circ \varepsilon = u$ y $\varepsilon \circ v = v$.

Claramente la concatenación es asociativa, por lo tanto tiene una estructura de monoide, es decir, $(\Sigma^*, \circ)$ es:

1. cerrada
2. tiene neutro
3. es asociativa

Dado un alfabeto Σ, $\forall w \in \Sigma^*$ se define

$$w^0 = \varepsilon$$
$$w^{i+1} = w^i \circ w$$

por ejemplo, su $w = ab \Rightarrow w^2 = (ab)^2 = abab$.

Dadas $v, u \in \Sigma^*$ se dice que u es una subpalabra de v si $\exists x, y \in \Sigma^*$, tal que $v = xuy$. En este caso x es un prefijo de v e y es un sufijo de v.

Dada $w = \sigma_1\sigma_2 \dots \sigma_n \in \Sigma^*$ se define la palabra inversa $w^r = \sigma_n \dots \sigma_2\sigma_1$ y $\varepsilon^r = \varepsilon$. Si $w = w^r$ w es un palíndromo.

Definición 10.4. Un *Lenguaje* es un conjunto (finito o infinito) de palabras en un alfabeto. Si $L \subseteq \Sigma^*$, diremos que L es un lenguaje en el alfabeto Σ.

Por ejemplo: $\Sigma^*, \varnothing, \{\varepsilon\}, \Sigma$.

10.1. Operaciones en lenguajes

Definición 10.5. Dados $L, L_1, L_2 \subseteq \Sigma^*$ dos lenguajes se define:

1. Complemento: $\bar{L} = \Sigma^* \setminus L$
2. Concatenación: $L = L_1 L_2 = \{xy : x \in L_1 \wedge y \in L_2\}$
3. Potencias de $L \subseteq \Sigma^*$: $L^0 = \{\varepsilon\}, \quad L^{i+1} = L^i L$
4. Estrella de Kleene: $L^* = \bigcup_{n \in \mathbb{N} \cup \{0\}} L^n$

   Observe que, $\varnothing^* = \{\varepsilon\}$

10.2. Propiedades

Dado un alfabeto Σ y $L_1, L_2, L_3 \subseteq \Sigma^*$. Entonces:

1. $L_1 \{\varepsilon\} = \{\varepsilon\} L_1 = L_1$

Demostración.

$$
\begin{array}{l}
\text{Sea } w \text{ cualquiera} \\
w \in L_1 \{\varepsilon\} \iff w = w'w'' \wedge w' \in L_1 \wedge w'' \in \{\varepsilon\} \\
w \in L_1 \{\varepsilon\} \iff w = w'w'' \wedge w' \in L_1 \wedge w'' = \varepsilon \\
w \in L_1 \{\varepsilon\} \iff w = w'\varepsilon \wedge w' \in L_1 \\
w \in L_1 \{\varepsilon\} \iff w = w' \wedge w' \in L_1 \\
w \in L_1 \{\varepsilon\} \iff w \in L_1 \\
(\forall w \; w \in L_1 \{\varepsilon\} \iff w \in L_1) \\
L_1 \{\varepsilon\} = L_1
\end{array}
$$

■

2. $L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3$

Demostración.

$$
\begin{array}{l}
\text{Sea } w \text{ cualquiera} \\
w \in L_1(L_2 \cup L_3) \iff (\exists w_1 \exists w' \; w_1 \in L_1 \wedge w' \in (L_2 \cup L_3) \wedge w = w_1w') \\
w \in L_1(L_2 \cup L_3) \iff (\exists w_1 \exists w' \; w_1 \in L_1 \wedge (w' \in L_2 \vee w' \in L_3) \wedge w = w_1w') \\
w \in L_1(L_2 \cup L_3) \iff (\exists w_1 \exists w' \; (w_1 \in L_1 \wedge w' \in L_2 \wedge w = w_1w') \vee (w_1 \in L_1 \wedge w' \in L_3 \wedge w = w_1w')) \\
w \in L_1(L_2 \cup L_3) \iff (\exists w_1 \exists w' \; (w_1 \in L_1 \wedge w' \in L_2 \wedge w = w_1w')) \vee (\exists w_1 \exists w' \; (w_1 \in L_1 \wedge w' \in L_3 \wedge w = w_1w')) \\
w \in L_1(L_2 \cup L_3) \iff w \in L_1L_2 \vee w \in L_1L_3 \\
w \in L_1(L_2 \cup L_3) \iff w \in (L_1L_2 \cup L_1L_3) \\
(\forall w \; w \in L_1(L_2 \cup L_3) \iff w \in (L_1L_2 \cup L_1L_3)) \\
L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3
\end{array}
$$

■

3. $(L_1 \cup L_2)L_3 = L_1L_3 \cup L_2L_3$

Demostración. Análoga a la anterior. ■

4. $L_1(L_2 \cap L_3) \subseteq L_1L_2 \cap L_1L_3$

Demostración.

$$
\begin{array}{l}
\text{Sea } w \text{ cualquiera} \\
w \in L_1(L_2 \cap L_3) \iff (\exists w_1 \exists w' \; w_1 \in L_1 \wedge w' \in (L_2 \cap L_3) \\
w \in L_1(L_2 \cap L_3) \iff (\exists w_1 \exists w' \; w_1 \in L_1 \wedge (w' \in L_2 \wedge w' \\
w \in L_1(L_2 \cap L_3) \iff (\exists w_1 \exists w' \; (w_1 \in L_1 \wedge w' \in L_2 \wedge w = \\
w \in L_1(L_2 \cap L_3) \implies (\exists w_1 \exists w' \; (w_1 \in L_1 \wedge w' \in L_2 \wedge w = \\
w \in L_1(L_2 \cap L_3) \implies w \in L_1L_2 \wedge w \in L_1L_3 \\
w \in L_1(L_2 \cap L_3) \implies w \in (L_1L_2 \cap L_1L_3) \\
(\forall w \; w \in L_1(L_2 \cap L_3) \implies w \in (L_1L_2 \cap L_1L_3)) \\
L_1(L_2 \cap L_3) \subseteq L_1L_2 \cap L_1L_3
\end{array}
$$

■

5. $(L_1 \cap L_2)L_3 \subseteq L_1L_3 \cap L_2L_3$

Demostración. Análoga a la anterior. ■

6. $L_1(L_2L_3) = (L_1L_2)L_3$

Demostración.

$$
\begin{array}{l}
\text{Sea } w \text{ cualquiera} \\
w \in L_1(L_2L_3) \iff (\exists w_1 \exists w' \; w_1 \in L_1 \wedge w' \in (L_2L_3) \wedge w \\
w \in L_1(L_2L_3) \iff (\exists w_1 \exists w_2 \exists w_3 \; w_1 \in L_1 \wedge w_2 \in L_2 \wedge w_3 \\
w \in L_1(L_2L_3) \iff (\exists w'' \exists w_3 \; w'' \in (L_1L_2) \wedge w_3 \in L_3 \wedge w \\
w \in L_1(L_2L_3) \iff w \in (L_1L_2)L_3 \\
(\forall w \; w \in L_1(L_2L_3) \iff w \in (L_1L_2)L_3) \\
L_1(L_2L_3) = (L_1L_2)L_3
\end{array}
$$

■

Teorema 10.1. *Sean $L_1, L_2 \subseteq \Sigma^*$. Entonces:*

1. $L_1 \subseteq L_1L_2^*$

Demostración. *Sea $w \in \Sigma^*$ cualquiera*

$$w \in L_1 \implies w = w\varepsilon \implies \exists w' \exists w'' \; w' \in L_1 \wedge w'' \in L_2^* \wedge w = w'w'' \implies w \in L_1L_2^*$$

■

2. $L_1 \subseteq L_2^*L_1$

Demostración. *Análoga a la anterior.* ■

3. $L_1 \subseteq L_2 \implies L_1^+ \subseteq L_2^+$

Demostración.

$$
\begin{array}{l}
\text{Supongamos } L_1 \subseteq L_2. \\
(\forall w \; w \in L_1 \implies w \in L_2) \\
\text{Sea } w \in \Sigma^* \text{ cualquiera} \\
\text{Supongamos } w \in L_1^+ \\
(\exists n \in \mathbb{N}, w \in L_1^n) \\
(\exists n \in \mathbb{N} \exists w_1, \ldots, w_n \in L_1, w = w_1 \ldots w_n) \\
(\exists n \in \mathbb{N} \exists w_1, \ldots, w_n \in L_2, w = w_1 \ldots w_n) \\
(\exists n \in \mathbb{N}, w \in L_2^n) \\
w \in L_2^+ \\
w \in L_1^+ \implies w \in L_2^+ \\
(\forall w \in \Sigma^* \; w \in L_1^+ \implies w \in L_2^+ 9 \\
L_1^+ \subseteq L_2^+ \\
L_1 \subseteq L_2 \implies L_1^+ \subseteq L_2^+
\end{array}
$$

■

4. $L_1 \subseteq L_2 \implies L_1^* \subseteq L_2^*$

Demostración. *Análoga a la anterior.* ■

5. $L_1L_1^* = L_1^*L_1 = L_1^+$

Demostración. *Probemos que: $L_1L_1^* = L_1^+$, la otra igualdad se prueba de manera análoga.*

Sea w cualquiera
$w \in L_1L_1^* \iff \exists w_1 \exists w_2 \; w_1 \in L_1 \wedge w_2 \in L_1^* \wedge w = w_1w_2$
$w \in L_1L_1^* \iff \exists w_1 \exists w_2 \exists n \in \mathbb{N}_0 \; w_1 \in L_1 \wedge w_2 \in L_1^n \wedge w = w_1w_2$
$w \in L_1L_1^* \iff \exists n \in \mathbb{N}_0 \; w \in L_1^{n+1}$
$w \in L_1L_1^* \iff \exists n \in \mathbb{N} \; w \in L_1^n$
$w \in L_1L_1^* \iff w \in L_1^+$
$(\forall w \; w \in L_1L_1^* \iff w \in L_1^+)$
$L_1L_1^* = L_1^+$

■

6. $L_1^*L_1^* = L_1^* = (L_1^*)^* = (L_1^*)^+ = (L_1^+)^*$

Demostración.

Sea w cualquiera
$w \in L_1^*L_1^* \iff \exists w_1 \exists w_2 \; w_1 \in L_1^* \wedge w_2 \in L_1^* \wedge w = w_1w_2$
$w \in L_1^*L_1^* \iff \exists w_1 \exists w_2 \exists n_1 \in \mathbb{N}_0 \exists n_2 \in \mathbb{N}_0 \; w_1 \in L_1^{n_1} \wedge w_2 \in L_1^{n_2} \wedge w = w_1w_2$
$w \in L_1^*L_1^* \iff \exists w' \exists n_1 \in \mathbb{N}_0 \exists n_2 \in \mathbb{N}_0 \; w' \in L_1^{n_1+n_2}$
$w \in L_1^*L_1^* \iff \exists w' \exists n \in \mathbb{N}_0 \; w' \in L_1^n$
$w \in L_1^*L_1^* \iff w' \in L_1^*$
$(\forall w \; w \in L_1^*L_1^* \iff w' \in L_1^*)$
$L_1^*L_1^* = L_1^*$

Sea w cualquiera
$w \in (L_1^*)^* \iff \exists n \in \mathbb{N}_0, w \in (L_1^*)^n$
$w \in (L_1^*)^* \iff \exists n \in \mathbb{N}_0 \exists w_1, \ldots, w_n \bigwedge_{i=1}^{n} (w_i \in L_1^*) \wedge w = w_1 \ldots w_n$
$w \in (L_1^*)^* \iff \exists n \in \mathbb{N}_0 \exists w_1, \ldots, w_n \exists n_1, \ldots, n_n \in \mathbb{N}_0 \bigwedge_{i=1}^{n} (w_i \in L_1^{n_i}) \wedge w = w_1 \ldots w_n$
$w \in (L_1^*)^* \iff \exists n \in \mathbb{N}_0 \exists n_1, \ldots, n_n \in \mathbb{N}_0 \; w \in L_1^{n_1+\cdots+n_n}$
$w \in (L_1^*)^* \iff \exists n \in \mathbb{N}_0 \; w \in L_1^n$
$w \in (L_1^*)^* \iff w' \in L_1^*$
$(\forall w \; w \in (L_1^*)^* \iff w' \in L_1^*)$
$(L_1^*)^* = L_1^*$

■

7. $(L_1 \cup L_2)^* = (L_1^* \cup L_2^*)^*$

Demostración. *Basta con demostrar* $(L_1^* \cup L_2^*)^* \subseteq (L_1 \cup L_2)^*$, *ya que la otra inclusión es evidente por propiedad (4).*

Sea w cualquiera
Supongamos $w \in (L_1^* \cup L_2^*)^*$
$(\exists n \in \mathbb{N}_0, w \in (L_1^* \cup L_2^*)^n)$
$(\exists n \in \mathbb{N}_0, \exists w_1, \ldots, w_n \forall i \in \{i, \ldots, n\}, w_i \in (L_1^* \cup L_2^*) \wedge w =$
$(\exists n \in \mathbb{N}_0, \exists w_1, \ldots, w_n \forall i \in \{i, \ldots, n\}, (w_i \in L_1^* \vee w_i \in L_2^*)$
$(\exists n \in \mathbb{N}_0, \exists w_1, \ldots, w_n \forall i \in \{i, \ldots, n\} \exists n_i \in \mathbb{N}_0, (w_i \in L_1^{n_i} \vee$
$(\exists n \in \mathbb{N}_0, \exists w_1, \ldots, w_n \forall i \in \{i, \ldots, n\} \exists n_i \in \mathbb{N}_0, \exists w_{i_j}, (w_{i_j} \in$
$(\exists n \in \mathbb{N}_0, \exists w_1, \ldots, w_n \forall i \in \{i, \ldots, n\}, (w_i \in L_1 \vee w_i \in L_2)$
$(\exists n \in \mathbb{N}_0, \exists w_1, \ldots, w_n \forall i \in \{i, \ldots, n\}, (w_i \in L_1 \cup L_2) \wedge w =$
$(\exists n \in \mathbb{N}_0, w \in (L_1 \cup L_2)^n)$
$w \in (L_1 \cup L_2)^*$
$w \in (L_1^* \cup L_2^*)^* \implies w \in (L_1 \cup L_2)^*$
$(\forall w \; w \in (L_1^* \cup L_2^*)^* \implies w \in (L_1 \cup L_2)^*)$
$(L_1^* \cup L_2^*)^* \subseteq (L_1 \cup L_2)^*$

■

Capítulo 11

Autómatas Finitos

Definición 11.1. Un Autómata Finito Determinista (AFD) es una 5-tupla $(Q, \Sigma, \delta, q_0, F)$ donde:

1. Q es un conjunto finito de estados,
2. Σ es un alfabeto,
3. $\delta : Q \times \Sigma \to Q$ es la función de transición,
4. $q_0 \in Q$ estado inicial, y
5. $F \subseteq Q$ conjunto de estados de aceptación.

11.1. Funcionamiento de un AFD

Dado $A = (Q, \Sigma, \delta, q_0, F)$ un AFD y $w \in \Sigma$. El AFD A va leyendo los símbolos de la palabra w y va pasando de un estado a otro según la regla de transición δ, de este modo los estados del sistema en la i–ésima iteración son:

$$\begin{aligned} e_0 &= q_0 \\ e_i &= \delta(e_{i-1}, \sigma_i) \end{aligned}$$

Diremos que A acepta la palabra $w = \sigma_1 \ldots \sigma_n$ si $e_n \in F$

Definición 11.2. Dado $A = (Q, \Sigma, \delta, q_0, F)$ un AFD, se define:

$$L(A) = \{w \in \Sigma^* : A \text{ acepta } w\}$$

Definición 11.3. Se dice que un lenguaje es regular si es reconocido por un autómata finito determinista.

11.2. Autómata finito no determinista

Definición 11.4. Un Autómata Finito No Determinista (AFND) es una 5-tupla $(Q, \Sigma, \delta, q_0, F)$ donde:

1. Q es un conjunto finito de estados,
2. Σ es un alfabeto,
3. $\delta : Q \times \Sigma_\varepsilon \to \mathcal{P}(Q)$ es la función de transición,
4. $q_0 \in Q$ estado inicial, y
5. $F \subseteq Q$ conjunto de estados de aceptación.

Teorema 11.1. *Cada Autómata finito no determinista tiene un autómata finito determinista equivalente.*

Demostración. Sea $A = (Q, \Sigma, \delta, q_0, F)$ un AFND, supongamos que A no tiene transiciones con ε. A partir de A se define $A' = (Q', \Sigma, \delta', q'_0, F')$ un AFD equivalente como:

1. $Q' = \mathcal{P}(Q)$
2. $\delta'(R, \sigma) = \bigcup_{r \in R} \delta(r, \sigma)$
3. $q'_0 = \{q_0\}$
4. $F' = \{R \in Q' : R \cap F \neq \varnothing\}$

En el caso que existan transiciones con ε, se define $E : Q' \to Q'$ como:

$$E(R) = \{q \in Q : q \text{ es alcanzado por algún elemento de } R \text{ siguiendo arcos con } \varepsilon\}$$

En este caso:

1. $Q' = \mathcal{P}(Q)$
2. $\delta'(R, \sigma) = \bigcup_{r \in R} E(\delta(r, \sigma))$
3. $q'_0 = E(\{q_0\})$
4. $F' = E(\{R \in Q' : R \cap F \neq \varnothing\})$

■

11.3. Operaciones Regulares

Teorema 11.2. *Los lenguajes regulares son cerrados para complemento,unión, intersección, concatenación y estrella de Kleene.*

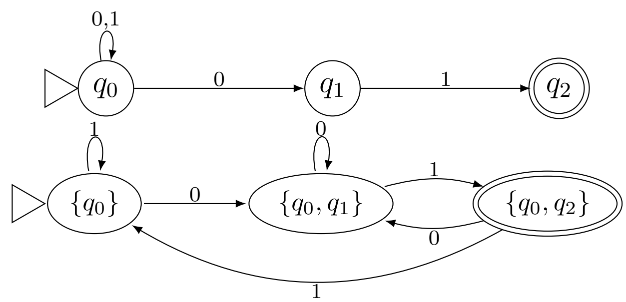


Figura 11.1: Ejemplo del algoritmo para pasar de un AFND a un AFD

11.4. Expresiones Regulares

Definición 11.5. Diremos que R es una expresión regular si R es:

1. σ para algún $\sigma \in \Sigma$
2. ε
3. $\varnothing$
4. $(R_1 \cup R_2)$, donde R_1 y R_2 son expresiones regulares.
5. $(R_1 \circ R_2)$, donde R_1 y R_2 son expresiones regulares.
6. (R_1^*), donde R_1 es una expresión regular.

Teorema 11.3. *Un lenguaje es regular si y solo si puede describirse por una expresión regular.*

11.5. Lema del bombeo

Teorema 11.4 (Lema del Bombeo)**.** *Si A es un lenguaje regular, entonces existe un número p (largo de bombeo) tal que si w es una palabra en A de largo al menos p, entonces w puede dividirse en tres partes, $w = xyz$, satisfaciendo las siguientes condiciones:*

1. *para cada $i \geq 0$, $xy^iz \in A$,*
2. *$|y| \geq 0$, y*
3. *$|xy| \leq p$.*

11.6. Reducción de Autómata Finito

Definición 11.6. Decimos que los estados p y q son equivalentes si para toda palabra de entrada w, $\delta(p, w)$ es un estado de aceptación si y solo si $\delta(q, w)$ es un estado de aceptación.

Dicho de manera más informal, es imposible distinguir dos estados equivalentes p y q simplemente partiendo de uno de los estados y preguntando si una determinada cadena de entrada lleva o no a un estado de aceptación cuando el autómata parte de ese estado (desconocido). Observe que no requerimos que $\delta(p, w)$ y $\delta(q, w)$ sean el mismo estado, solo que ambos sean estados de aceptación o de no aceptación.

Si los dos estados no son equivalentes, entonces decimos que son distinguibles. Es decir, el estado p es distinguible del estado q si existe al menos una palabra w tal que $\delta(p, w)$ es un estado de aceptación y $\delta(q, w)$ no, o viceversa.

Para hallar estados equivalentes, es preciso determinar pares de estados que sean distinguibles. Quizá parezca sorprendente, pero es cierto que si se aplica el algoritmo que se describe a continuación, entonces cualquier par de estados que no sean distinguibles serán equivalentes. El algoritmo al que nos referimos es el algoritmo de llenado de tabla, que consiste en un descubrimiento recursivo de pares distinguibles en un AFD $A = (Q, \Sigma, \delta, q_0, F)$.

Base. Si p es un estado de aceptación y q es de no aceptación, entonces el par $\{p, q\}$ es distinguible.

Paso Inductivo. Sean p y q dos estados tales que para un símbolo de entrada a, $r = \delta(p, a)$ y $s = \delta(q, a)$ son un par de estados que se sabe que son distinguibles. Entonces $\{p, q\}$ es un par de estados distinguibles.

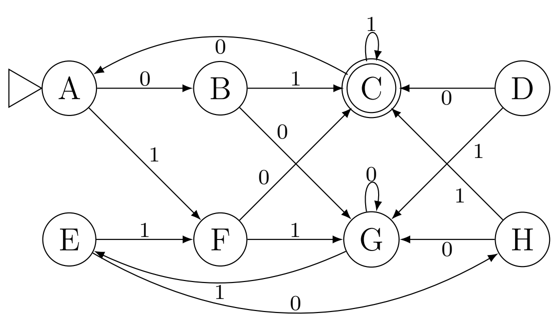


Figura 11.2: Ejemplo de AFD para reducir

La razón por la que esta regla tiene sentido es que tiene que existir alguna cadena w que distinga r de s; es decir, en concreto o $\delta(r, w)$ o $\delta(s, w)$ es un estado de aceptación. Luego la cadena aw tiene que distinguir p de q, ya que $\delta(p, aw)$ y $\delta(q, aw)$ es el mismo par de estados que $\delta(r, w)$ y $\delta(s, w)$.

Teorema 11.5. *Si dos estados no pueden distinguirse mediante el algoritmo de llenado de tabla, entonces los estados son equivalentes.*

Teorema 11.6. *Dado un AFD M, existe un AFD M' con $L(M) = L(M')$ y tal que M' tiene el mínimo número de estados de entre todos los AFD que reconocen $L(M)$.*

B								
C	x	x						
D			x					
E			x					
F			x					
G			x					
H			x					
	A	B	C	D	E	F	G	H

B	x							
C	x	x						
D	x	x	x					
E		x	x	x				
F	x	x	x		x			
G	x	x	x	x	x	x		
H	x		x	x	x	x	x	
	A	B	C	D	E	F	G	H

Figura 11.3: Tablas del algoritmo de reducción

Teorema 11.7. *Dados dos autómatas M' y M' tales que $L(M) = L(M')$ y tales que M y M' tienen el mínimo número de estados de entre todos los AFD que reconocen $L(M)$, entonces $M = M'$ (salvo cambio de nombre de los estados).*

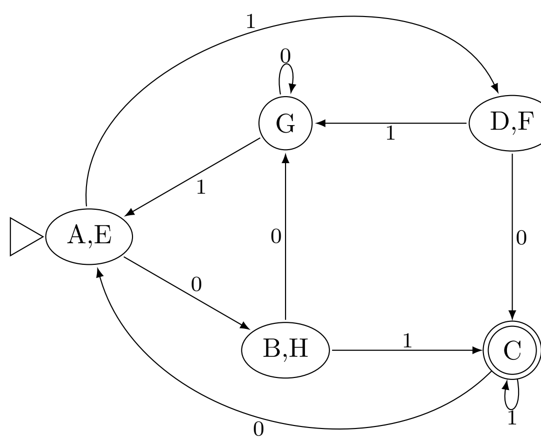


Figura 11.4: Ejemplo autómata reducido

Parte III

Apéndices

Apéndice A

Estructuras algebraicas

Definición A.1. Dado X un conjunto no vacío se define una *ley de composición interna* como una función:

$$\begin{aligned} * : X \times X &\to X \\ (x, y) &\to *(x, y) = x * y \end{aligned}$$

Algunos ejemplos de leyes de composición interna son:

- $(\mathbb{N}, +)$
- $(\mathbb{N}, \cdot)$
- $(\mathbb{Z}, +)$
- $(\mathbb{Z}, \cdot)$
- $(\mathbb{Z}, -)$
- $(\mathbb{R}, +)$
- $(\mathbb{R}, \cdot)$
- $(\mathbb{R}, -)$
- $(\mathbb{R}^+, +)$
- $(\mathbb{R}^+, \cdot)$
- $(\mathbb{R}^+, \div)$
- $(\mathcal{M}_{n\times n}(\mathbb{R}), +)$
- $(\mathcal{M}_{n\times n}(\mathbb{R}), \cdot)$
- $(\mathcal{F}_A = \{ f : A \to A \}, \circ)$
- $(\mathbb{R}[x], +)$
- $(\mathbb{R}[x], \cdot)$
- $(\{V, F\}, \wedge)$
- $(\{V, F\}, \vee)$
- $(\mathcal{P}(A), \cup)$
- $(\mathcal{P}(A), \cap)$
- $(\mathcal{P}(A), \Delta)$

No son leyes de composición interna:

- $(\mathbb{N}, -)$
- $(\mathbb{N}, \div)$
- $(\mathbb{R}, \div)$

Definición A.2. Una *estructura algebraica* es un conjunto X no vacío dotado de una o varias leyes de composición interna.

A.1. Propiedades básicas

Sea X conjunto no vacío, $* : X \times X \to X$ y $\diamond : X \times X \to X$, leyes de composición interna.

Asociatividad. Diremos que $*$ es asociativa si y solo si:

$$\forall x, y, z \in X, \quad x * (y * z) = (x * y) * z$$

La asociatividad es la propiedad más básica que se le puede pedir a una estructura algebraica con ley de composición interna, es por eso que cuando pensamos en leyes de composición interna son estas las que primero asoman por nuestra cabeza, ya que son las que hemos estudiado desde que eramos pequeños. Las operaciones que no tienen esta propiedad no cumplen buenas propiedades y por ello ya no las consideraremos un ejemplo de aquí en adelante.

Son asociativas:

- $(\mathbb{N}, +)$
- $(\mathbb{N}, \cdot)$
- $(\mathbb{Z}, +)$
- $(\mathbb{Z}, \cdot)$
- $(\mathbb{R}, +)$
- $(\mathbb{R}, \cdot)$
- $(\mathbb{R}^+, +)$
- $(\mathbb{R}^+, \cdot)$
- $(\mathcal{M}_{n\times n}(\mathbb{R}), +)$
- $(\mathcal{M}_{n\times n}(\mathbb{R}), \cdot)$
- $(\mathcal{F}_A, \circ)$
- $(\mathbb{R}[x], +)$
- $(\mathbb{R}[x], \cdot)$
- $(\{V, F\}, \wedge)$
- $(\{V, F\}, \vee)$
- $(\mathcal{P}(A), \cup)$
- $(\mathcal{P}(A), \cap)$
- $(\mathcal{P}(A), \Delta)$

Vale la pena probar el caso de la composición de funciones: Sean $h, g, h \in \mathcal{F}_A$, sabemos que dos funciones son iguales, si la imagen de ambas es igual para cada elemento del dominio, de modo que para probar la asociatividad de $(\mathcal{F}_A, \circ)$ debemos probar que $\forall x \in A ((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$. Sea $x \in A$ cualquiera:

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$$

No son asociativas:

- $(\mathbb{Z}, -)$
- $(\mathbb{R}, -)$
- $(\mathbb{R}^+, \div)$

Conmutatividad. Diremos que $*$ es conmutativa si y solo si:

$$\forall x, y \in X, \quad x * y = y * x$$

Si bien, la conmutatividad es una propiedad que usamos regularmente y le atribuimos a muchas operaciones, sin ella aún podemos tener muy buenas propiedades en una estructura algebraica por dar dos ejemplos relevantes podemos considerar: $(\mathcal{M}_{n\times n}(\mathbb{R}), \cdot)$ y $(\mathcal{F}_A, \circ)$. Es muy frecuente que la demos por hecho, sin ir más lejos existe el dicho popular "el orden de los factores no altera el producto" y, aunque esto es cierto en números reales, naturales, enteros, etc. no es así en la matrices.

Son Conmutativas

- $(\mathbb{N}, +)$
- $(\mathbb{N}, \cdot)$
- $(\mathbb{Z}, +)$
- $(\mathbb{Z}, \cdot)$
- $(\mathbb{R}, +)$
- $(\mathbb{R}, \cdot)$
- $(\mathbb{R}^+, +)$
- $(\mathbb{R}^+, \cdot)$
- $(\mathcal{M}_{n\times n}(\mathbb{R}), +)$
- $(\mathbb{R}[x], +)$
- $(\mathbb{R}[x], \cdot)$
- $(\{V, F\}, \wedge)$
- $(\{V, F\}, \vee)$
- $(\mathcal{P}(A), \cup)$
- $(\mathcal{P}(A), \cap)$
- $(\mathcal{P}(A), \Delta)$

Existencia de neutro. Diremos que $*$ tiene elemento neutro si y solo si:

$$\exists e \in X, \forall x \in X, \quad x * e = e * x = x$$

Esta también es una propiedad muy básica, cabe notar que aunque la operación sea o no conmutativa la operación con el neutro, sea por la derecha o la izquierda debe dar el mismo resultado. En el caso de las estructuras algebraicas conmutativas basta con probar el resultado solo por un lado, pero en las que no lo son se hace indispensable hacer la verificación por izquierda y derecha.

Tienen elemento neutro:

- $(\mathbb{N}, \cdot), e = 1$
- $(\mathbb{Z}, +), e = 0$
- $(\mathbb{Z}, \cdot), e = 1$
- $(\mathbb{R}, +), e = 0$
- $(\mathbb{R}, \cdot), e = 1$
- $(\mathbb{R}^+, \cdot), e = 1$
- $(\mathcal{M}_{n\times n}(\mathbb{R}), +), e = \theta$ (matriz nula)
- $(\mathcal{M}_{n\times n}(\mathbb{R}), \cdot), e = I$ (matriz identidad)
- $(\mathcal{F}_A, \circ), e = f_{id}, (\forall x \in A, f_{id}(x) = x)$
- $(\mathbb{R}[x], +), e = 0$
- $(\mathbb{R}[x], \cdot), e = 1$
- $(\{V, F\}, \wedge), e = V$
- $(\{V, F\}, \vee), e = F$
- $(\mathcal{P}(A), \cup), e = \varnothing$
- $(\mathcal{P}(A), \cap), e = A$
- $(\mathcal{P}(A), \Delta), e = \varnothing$

No tienen elemento neutro:

- $(\mathbb{N}, +)$
- $(\mathbb{R}^+, +)$

Teorema A.1. *Si el neutro existe es único.*

Demostración. Por reducción al absurdo, supongamos que existen $e_1, e_2 \in X$ tales que para todo $x \in X$:

$$x * e_1 = e_1 * x = x \tag{A.1}$$
$$x * e_2 = e_2 * x = x \tag{A.2}$$

Luego por (A.2):

$$e_1 = e_1 * e_2$$

pero también por (A.1)

$$e_2 = e_1 * e_2$$

Por lo tanto, $e_1 = e_2$. $\rightarrow\leftarrow$ ■

Existencia de inverso. Dada $(X, *)$ una estructura algebraica con elemento neutro, diremos que $x \in X$ tiene elemento inverso si y solo si:

$$\exists y \in X, \quad x * y = y * x = e$$

(Notación: el inverso de x se denota por x^{-1}).

Observación A.1. Cabe notar que esta es una propiedad de los elementos de X y no de la operación. Además, el neutro siempre tiene inverso que es sí mismo.

Algunas estructuras algebraicas con elemento inverso en todos su elementos son:

- $(\mathbb{Z},+), e=0$
- $(\mathbb{R},+), e=0$
- $(\mathbb{R}^+,\cdot), e=1$
- $(\mathcal{M}_{n\times n}(\mathbb{R}),+), e=\theta$
- $(\mathbb{R}[x],+), e=0$
- $(\mathcal{P}(A),\Delta), e=\varnothing$

Algunas estructuras algebraicas con elemento inverso en algunos de sus elementos aparte del neutro son:

- $(\mathbb{R},\cdot), e=1$. Tienen inverso todos excepto 0.
- $(\mathcal{M}_{n\times n}(\mathbb{R}),\cdot), e=I$. Tienen inverso solo las matrices invertibles ($|A|\neq 0$)
- $(\mathcal{F}_A,\circ), e=f_{id}$. Tienen inverso solo las funciones biyectivas.

Algunas estructuras algebraicas con elemento inverso solo para el neutro son:

- $(\mathbb{N},\cdot), e=1$
- $(\mathbb{Z},\cdot), e=1$
- $(\mathbb{R}[x],\cdot), e=1$
- $(\{V,F\},\wedge), e=V$
- $(\{V,F\},\vee), e=F$
- $(\mathcal{P}(A),\cup), e=\varnothing$
- $(\mathcal{P}(A),\cap), e=A$

Elemento cancelable. Diremos que $a\in X$ es cancelable si y solo si:

$$\begin{aligned}\forall x,y\in X,\ \ & a*x=a*y\Longrightarrow x=y,\\ & x*a=y*a\Longrightarrow x=y\end{aligned}$$

Algunas estructuras donde todos sus elementos son cancelables son:

- $(\mathbb{N},+)$
- $(\mathbb{N},\cdot)$
- $(\mathbb{Z},+)$
- $(\mathbb{R},+)$
- $(\mathbb{R}^+,+)$
- $(\mathbb{R}^+,\cdot)$
- $(\mathcal{M}_{n\times n}(\mathbb{R}),+)$
- $(\mathbb{R}[x],+)$
- $(\{V,F\},\wedge)$
- $(\{V,F\},\vee)$

- $(\mathbb{Z},\cdot)$ excepto el cero
- $(\mathbb{R},\cdot)$ excepto el cero
- $(\mathcal{M}_{n\times n}(\mathbb{R}),\cdot)$ solo las matrices invertibles
- $(\mathcal{F}_A,\circ)$ solo las funciones biyectivas y las inyectivas son cancelables por la izquierda
- $(\mathbb{R}[x],\cdot)$ excepto 0.

Elemento absorbente. Diremos que $*$ tiene elemento absorbente si y solo si:

$$\exists a\in X,\forall x\in X,\quad x*a=a*x=a$$

Existen varios ejemplos de elementos absorbentes, 0 con la operación "$\cdot$" en $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, la matriz nula en el producto de matrices, F con la operación $\wedge$ en $\{V,F\}$, etc.

Elemento idempotente. Diremos que $x\in X$ es idempotente si y solo si:

$$x*x=x$$

Claramente si existe el neutro, este siempre es idempotente, pero no es necesarimente el único caso. El caso más simple es en $\{V,F\}$ donde ambos elementos son idempotentes con las operaciones "$\wedge$" y "$\vee$".

Distributividad. Diremos que $\diamond$ es distributiva con respecto a $*$ si y solo si:

$$\forall x, y, z \in X, \quad x \diamond (y * z) = (x \diamond y) * (x \diamond z)$$
$$\forall x, y, z \in X, \quad (y * z) \diamond x = (y \diamond x) * (z \diamond x)$$

Hasta aquí habíamos estudiado propiedades con solo una ley de composición interna. La distributividad requiere de dos leyes de composición interna. Es importante notar el orden en que van las dos operaciones ya que, por ejemplo, en $\mathbb{Z}$ "$\cdot$" es distributiva con respecto a "$+$", pero "$+$" no es distributiva con respecto a "$\cdot$". Por otro lado, sabemos que en $\{V, F\}$ "$\wedge$" es distributiva con respecto a "$\vee$" y "$\vee$" es es distributiva con respecto a "$\wedge$".

A.2. Clasificación de estructuras algebraicas

Dependiendo de las propiedades que cumplen las leyes de composición interna asociadas a una estructura algebraica podemos clasificar estas estructuras. Una clasificación básica es:

A.2.1. Monoide

$(M, *)$ es un monoide si y solo si:

1. $*$ es asociativa
2. $*$ tiene elemento neutro.

Propiedades. Si $(M, *)$ es monoide:

1. El neutro es único.

   Ya fue demostrado.

2. Si el inverso existe es único.

   Demostración. Por reducción al absurdo, sea $x \in X$ con inverso para la operación $*$, supongamos que existen $y, y' \in X$ tal que $y \neq y'$ y:

   $$x * y = y * x = e$$
   $$x * y' = y' * x = e$$

   Consideramos que:

   $$\begin{aligned} y * x &= e && / * y' \\ (y * x) * y' &= e * y' \\ y * (x * y') &= y' && \text{(Por asociatividad y definición de neutro)} \\ y * e &= y' \\ y &= y' \rightarrow\leftarrow \end{aligned}$$

   ■

3. Si $a \in M$ tiene inverso, entonces a es cancelable.

Demostración. Sea $a \in M$ con inverso a^{-1}. Supongamos que:

$$\begin{aligned} a * x &= a * y && /a^{-1}* \\ a^{-1} * (a * x) &= a^{-1} * (a * y) && \\ (a^{-1} * a) * x &= (a^{-1} * a) * y && \text{(Por asociatividad de } *) \\ e * x &= e * y && \text{(Por definición de inverso)} \\ x &= y && \text{(Por definición de neutro)} \end{aligned}$$

Luego, $a * x = a * y \Longrightarrow x = y$. Para probar que $x * a = y * a \Longrightarrow x = y$ se hace de manera análoga.

■

A.2.2. Grupos

Definición A.3. Un grupo es una estructura algebraica $(G, *)$ tal que:

1. $*$ es asociativa
2. $*$ tiene elemento neutro
3. todos los elementos tienen elemento inverso.

Definición A.4. $(G, *)$ es grupo Abeliano si y solo si:

1. $(G, *)$ es grupo
2. $*$ es conmutativa.

Definición A.5. $(G, *)$ es un grupo finito si y solo si:

1. $(G, *)$ es grupo
2. $|G| < \infty$.

Definición A.6. $(G, *)$ es grupo cíclico si y solo si:

1. $(G, *)$ es grupo
2. $\exists a \in G, \forall x \in G, \exists n \in \mathbb{Z}, x = a^n$.

Propiedades. Si $(G,*)$ es grupo:

1. $\forall a,b \in G, \exists! x \in G, a*x = b$

   Demostración. Para ver que x existe basta con verificar que $x = a^{-1}*b$ cumple con la ecuación:

   $$a*(a^{-1}*b) = (a*a^{-1})*b = e*b = b$$

   Para ver que x es único, supongamos que existe x e y solución de la ecuación:

   $$\left.\begin{array}{r} a*x=b \\ a*y=b \end{array}\right\} \Longrightarrow a*x = a*y$$

   Luego,

   $$\begin{aligned}
   a*x &= a*y && /a^{-1}* \\
   a^{-1}*(a*x) &= a^{-1}*(a*x) && \\
   (a^{-1}*a)*x &= (a^{-1}*a)*x && \text{(Por asociatividad de } *) \\
   e*x &= e*y && \text{(Por definición de elemento inverso)} \\
   x &= y && \text{(Por definición de neutro)}
   \end{aligned}$$

   ■

2. $\forall a \in G, a$ es cancelable.

3. Si G es finito, cada línea o columna de la tabla pitagórica de G es una permutación de los elementos de G.

4. Si G es finito, es isomorfo a un grupo de permutaciones.

Subgrupos

Dado $(G,*)$ un grupo se dice H es un subgrupo de G si $H \subseteq G$ y $(H,*)$ es grupo.

Teorema A.2 (Caracterización de subgrupos)**.** *Dado $(G,*)$ un grupo y $H \subseteq G$, $H \neq \varnothing$. H es un subgrupo de G si y solo si:*

$$\forall h_1, h_2 \in H, h_1 * h_2^{-1} \in H$$

Demostración. En primer lugar, notemos que el teorema plantea una equivalencia, de este modo comenzaremos por probar la implicancia más simple que es: si H es un subgrupo, entonces $\forall h_1, h_2 \in H, h_1 * h_2^{-1} \in H$.

Supongamos que H es subgrupo, entonces se tiene que:

1. $e \in H$
2. $\forall h \in H, h^{-1} \in H$
3. $\forall h, h' \in H, h*h' \in H$

Sean $h_1, h_2 \in H$ cualesquiera. De (2) se tiene que $h_2^{-1} \in H$, como $h_1, h_2^{-1} \in H$ de (3) se deduce que $h_1 * h_2^{-1} \in H$. De este modo como esto se cumple para $h_1, h_2 \in H$ cualesquiera, podemos hacer una generalización universal y tenemos $\forall h_1, h_2 \in H, h_1 * h_2^{-1} \in H$.

Ahora debemos demostrar que si:

$$\forall h_1, h_2 \in H, h_1 * h_2^{-1} \in H \tag{A.3}$$

se cumplen las tres condiciones que ya hemos enumerado. Veamos el caso de (1). De este modo supongamos que se cumple (A.3).

Sea $h \in H$, este existe ya que sabemos que $H \neq \varnothing$, luego instanciamos (A.3) con $h_1 = h_2 = h$, así obtenemos $h * h^{-1} \in H$, pero $h * h^{-1} = e$, luego $e \in H$.

Ahora que ya hemos demostrado que $e \in H$, podemos usar este hecho para demostrar (2). Sea $h \in H$ cualquiera, instanciemos (A.3) con $h_1 = e$ y $h_2 = h$, y obtenemos: $e * h^{-1} \in H$, por definición de e tenemos que $h^{-1} \in H$ y como esto se cumple para h cualquiera, tenemos que $\forall h \in H, h^{-1} \in H$.

Por último demostraremos (3). Como de costumbre, sean $h, h' \in H$ cualesquiera. Nuevamente, basta instanciar (A.3) y obtendremos la propiedad; en este caso; las instancias serán $h_1 = h$ y $h_2 = h'^{-1}$ (recordemos que acabamos de probar que, bajo el supuesto de (A.3) el inverso de un elemento en H también está en H). Así obtenemos: $h * (h'^{-1})^{-1} \in H$, pero como el inverso del inverso es el mismo elemento, tenemos que $h * h' \in H$. Como esto se cumple para $h, h' \in H$ cualesquiera, entonces $\forall h, h' \in H, h * h' \in H$.

■

A.2.3. Anillo

Definición A.7. $(A, *, \diamond)$ es un anillo si y solo si:

1. $(A, *)$ es grupo Abeliano
2. $(A, \diamond)$ es asociativa
3. $\diamond$ es distributiva con respecto a $*$.

Definición A.8. $(A, *, \diamond)$ es un anillo con unidad si y solo si:

1. $(A, *, \diamond)$ es un anillo
2. $\diamond$ tiene neutro.

Definición A.9. $(A, *, \diamond)$ es un anillo conmutativo si y solo si:

1. $(A, *, \diamond)$ es un anillo
2. $\diamond$ es conmutativa.

Propiedades. Sea $(A, +, \cdot)$ un anillo. Se define la ley de composición interna "$-$" como:

$$\forall a, b \in A, \quad a - b = a + (-b)$$

donde $-b$ es el inverso de b para $+$. Entonces, se cumple que:

1. $\forall a \in A, \quad a \cdot 0 = 0 \cdot a = 0$, donde 0 es el neutro para $+$.

   Demostración. Sea $a \in A$ cualquiera,

   $$a \cdot 0 = a \cdot (0 + 0)$$

   Por distributividad de $\cdot$ con respecto a $+$

   $$\begin{aligned} a \cdot 0 &= (a \cdot 0) + (a \cdot 0) && / + -(a \cdot 0) \\ (a \cdot 0) + -(a \cdot 0) &= [(a \cdot 0) + (a \cdot 0)] + -(a \cdot 0) \end{aligned}$$

   Por asociatividad de $+$

   $$(a \cdot 0) + -(a \cdot 0) = (a \cdot 0) + [(a \cdot 0) + -(a \cdot 0)]$$

   Como la suma de un número y su opuesto es cero, obtenemos

   $$\begin{aligned} 0 &= (a \cdot 0) + 0 \\ 0 &= a \cdot 0 \end{aligned}$$

   De este modo $\forall a \in A, a \cdot 0 = 0$. El caso $0 \cdot a = 0$ es análogo. ■

2. $\forall a, b \in A, \quad -(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

   Demostración. Sean $a, b \in A$ cualesquiera, probemos que $(a \cdot b) + ((-a) \cdot b) = 0$. Por distributividad

   $$(a \cdot b) + ((-a) \cdot b) = (a + (-a)) \cdot b = 0 \cdot b = b$$

   El caso $(a \cdot b) + (a \cdot (-b)) = 0$ es análogo. ■

3. $\forall a, b, c \in A, \quad \begin{aligned} a \cdot (b - c) &= (a \cdot b) - (a \cdot c) \quad \text{y} \\ (b - c) \cdot a &= (b \cdot a) - (c \cdot a) \end{aligned}$

   Demostración. Sean $a, b, c \in A$ cualesquiera.

   $$a \cdot (b - c) = a \cdot (b + (-c)) = (a \cdot b) + (a \cdot (-c)) = (a \cdot b) + -(a \cdot c) = (a \cdot b) - (a \cdot c)$$

   Nuevamente el caso $(b - c) \cdot a = (b \cdot a) - (c \cdot a)$ es análogo. ■

Teorema A.3. *Sea $(A, +, \cdot)$ un anillo y $\varnothing \neq A' \subseteq A$. A' es subanillo de A si y solo si se cumplen:*

$$\forall a, a' \in A', a - a' \in A' \tag{A.4}$$

$$\forall a, a' \in A', a \cdot a' \in A' \tag{A.5}$$

Demostración. Claramente la condición (A.4) garantiza que A' es un subgrupo de A y la condición (A.5) garantiza que $\cdot$ es ley de composición interna en A', las propiedades de asociatividad y distributividad no es necesario verificarlas ya que se heredan por el hecho que $A' \subseteq A$. ■

Definición A.10. Un anillo $(A, +, \cdot)$ tiene divisores de cero si y solo si:

$$\exists a, b \in A \setminus \{0\}, \quad a \cdot b = 0$$

A.2.4. Cuerpo

Definición A.11. $(K, +, \cdot)$ es cuerpo un si y solo si:

1. $(K, +, \cdot)$ es anillo con unidad.
2. todo elemento distinto de 0 tiene inverso para $\cdot$.

Definición A.12. $(K, +, \cdot)$ es cuerpo conmutativo un si y solo si:

1. $(K, +, \cdot)$ es cuerpo
2. $\cdot$ es conmutativa.

Propiedades. Si $(K, +, \cdot)$ es un cuerpo, no tiene divisores de cero.

Demostración. Por reducción al absurdo, supongamos que $a \cdot b = 0$ $a \neq 0$ y $b \neq 0$. Como $a \neq 0$ y K es cuerpo, a tiene inverso a^{-1}, luego:

$$\begin{aligned}
a \cdot b &= 0 && /a^{-1} \cdot \\
a^{-1} \cdot (a \cdot b) &= a^{-1} \cdot 0 && \\
(a^{-1} \cdot a) \cdot b &= 0 && \text{(Por asociatividad y propiedad (1) de anillos)} \\
1 \cdot b &= 0 && \text{(Por definición de inverso)} \\
b &= 0 \rightarrow\leftarrow &&
\end{aligned}$$

■

Teorema A.4. *Dado $(K, +, \cdot)$ un cuerpo. Sea $(\mathcal{M}_{n\times n}(K), +, \cdot)$ las matrices de $n \times n$ con coeficientes en K, dotadas de la suma componente a componente y el producto:*

$$\forall A, B \in \mathcal{M}_{n\times n}(K), [A \cdot B]_{i,j} = A_{i1}B_{1j} + A_{i2}B_{2j} + \cdots + A_{in}B_{nj}$$

Entonces, $(\mathcal{M}_{n\times n}(K), +, \cdot)$ es un anillo con unidad.

Demostración. En primer lugar, notemos que como $(K, +, \cdot)$ es un anillo podemos trabajar con $A_{i1}B_{1j} + A_{i2}B_{2j} + \cdots + A_{in}B_{nj}$ como $\sum\limits_{k=1}^{n} A_{ik}B_{kj}$. Ya que las propiedades de las sumatorias solo utilizan las propiedades de un anillo.

En primer lugar debemos probar que $(\mathcal{M}_{n\times n}(K), +,)$ es un grupo Abeliano, pero al ser esta una operación componente a componente en un grupo Abeliano, podemos heredar todas las propiedades que necesitamos.

En segundo lugar debemos probar que:

1. $(\mathcal{M}_{n\times n}(K), \cdot)$ es asociativo.

$$[(A\cdot B)\cdot C]_{ij} = \sum_{k=1}^{n}[A\cdot B]_{ik}C_{kj} = \sum_{k=1}^{n}\sum_{l=1}^{n}(A_{il}\cdot B_{lk})\cdot C_{kj}$$
$$[(A\cdot B)\cdot C]_{ij} = \sum_{k=1}^{n}\sum_{l=1}^{n}(A_{il}\cdot B_{lk}\cdot C_{kj})$$
$$[(A\cdot B)\cdot C]_{ij} = \sum_{l=1}^{n}\sum_{k=1}^{n}(A_{il}\cdot B_{lk}\cdot C_{kj})$$
$$[(A\cdot B)\cdot C]_{ij} = \sum_{l=1}^{n}A_{il}\cdot\sum_{k=1}^{n}(B_{lk}\cdot C_{kj})$$
$$[(A\cdot B)\cdot C]_{ij} = \sum_{l=1}^{n}A_{il}\cdot[B\cdot C]_{lj}$$
$$[(A\cdot B)\cdot C]_{ij} = [A\cdot(B\cdot C)]_{ij}$$

2. $\cdot$ es distributivo con respecto a $+$

$$[A\cdot(B+C)]_{ij} = \sum_{k=1}^{n}A_{ik}\cdot[B+C]_{kj} = \sum_{k=1}^{n}A_{ik}\cdot(B_{kj}+C_{kj})$$
$$[A\cdot(B+C)]_{ij} = \sum_{k=1}^{n}((A_{ik}\cdot B_{kj})+(A_{ik}\cdot C_{kj}))$$
$$[A\cdot(B+C)]_{ij} = \sum_{k=1}^{n}(A_{ik}\cdot B_{kj})+\sum_{k=1}^{n}(A_{ik}\cdot C_{kj})$$
$$[A\cdot(B+C)]_{ij} = [A\cdot B]_{ij}+[A\cdot C]_{ij}$$
$$[A\cdot(B+C)]_{ij} = [(A\cdot B)+(A\cdot C)]_{ij}$$

Para probar que $[(A+B)\cdot C]_{ij} = [(A\cdot C)+(B\cdot C)]_{ij}$ se procede de manera análoga.

3. Existe neutro para $\cdot$.

Sea I la matriz identidad definida como:

$$I_{ij} = \begin{cases} 1 & \text{Si } i=j \\ 0 & \text{Si } i\neq j \end{cases}$$

$$[A\cdot I]_{ij} = \sum_{k=1}^{n}(A_{ik}\cdot I_{kj}) = A_{ij}\cdot I_{jj} = A_{ij}$$
$$[I\cdot A]_{ij} = \sum_{k=1}^{n}(I_{ik}\cdot A_{kj}) = I_{ii}\cdot A_{ij} = A_{ij}$$

■

A.3. Homomorfismos

Dadas $(X, *)$, $(Y, \diamond)$ estructuras algebraicas y una función $f : X \to Y$. Se dice que f es un homomorfismo si y solo si:

$$\forall x_1, x_2 \in X, f(x_1 * x_2) = f(x_1) \diamond f(x_2)$$

Además si f es biyectiva, diremos que es un isomorfismo; y si $X = Y$ y f es biyectiva, entonces es un automorfismo.

Teorema A.5. *Sean $(X, *)$ e $(Y, \diamond)$ estructuras algebraicas y $f : X \to Y$ un epimorfismo. Entonces:*

1. *Si $*$ es asociativa en X, $\diamond$ es asociativa en Y.*
2. *Si $*$ es conmutativa en X, $\diamond$ es conmutativa en Y.*
3. *Si $*$ tiene un neutro e_* en X, $\diamond$ tiene un neutro $e_\diamond = f(e_*)$ en Y*
4. *Si $(X, *)$ e $(Y, \diamond)$ tienen elemento neutro, entonces si $x \in X$ tiene elemento inverso x^{-1}, $f(x) \in Y$ tiene elemento inverso y $f(x)^{-1} = f(x^{-1})$*

Demostración.

1. Supongamos que f es un homomorfismo sobreyectivo y $(X, *)$ es asociativa. Sean $y, y', y'' \in Y$ cualesquiera, como f es sobreyectiva $\exists x, x', x'' \in X, y = f(x) \quad \wedge \quad y' = f(x') \quad \wedge \quad y'' = f(x'')$. Luego:

$$\begin{aligned}
y \diamond (y' \diamond y'') &= f(x) \diamond (f(x') \diamond f(x'')) \\
&= f(x) \diamond f(x' * x'') && \text{(Por definición de homomorfismo)} \\
&= f(x * (x' * x'')) && \text{(Por definición de homomorfismo)} \\
&= f((x * x') * x'') && \text{(Por asociatividad de } *) \\
&= f(x * x') \diamond f(x'') && \text{(Por definición de homomorfismo)} \\
&= (f(x) \diamond f(x')) \diamond f(x'') && \text{(Por definición de homomorfismo)} \\
&= (y \diamond y') \diamond y''
\end{aligned}$$

   Luego, $\forall y, y', y'' \in Y, y \diamond (y' \diamond y'') = (y \diamond y') \diamond y''$

2. Supongamos que f es un homomorfismo sobreyectivo y $(X, *)$ es conmutativa. Sean $y, y' \in Y$ cualesquiera, como f es sobreyectiva $\exists x, x' \in X, y = f(x) \quad \wedge \quad y' = f(x')$. Luego:

$$\begin{aligned}
y \diamond y &= f(x) \diamond f(x') \\
&= f(x * x') && \text{(Por definición de homomorfismo)} \\
&= f(x' * x) && \text{(Por conmutatividad de } *) \\
&= f(x) \diamond f(x') && \text{(Por definición de homomorfismo)} \\
&= y' \diamond y
\end{aligned}$$

   Luego, $\forall y, y' \in Y, y \diamond y' = y' \diamond y$

3. Supongamos que f es un homomorfismo sobreyectivo y $(X,*)$ tiene neutro e_*. Sea $y \in Y$ cualquiera, como f es sobreyectiva $\exists x \in X, y = f(x)$. Probemos que $f(e_*)$ cumple la función del neutro en Y. Luego:
$$y \diamond f(e_*) = f(x) \diamond f(e_*) = f(x * e_*) = f(x) = y$$
$$f(e_*) \diamond y = f(e_*) \diamond f(x) = f(e_* * x) = f(x) = y$$
Luego, $\forall y \in Y, y \diamond f(e_*) = f(e_*) \diamond y = y$, por lo tanto $(Y,\diamond)$ tiene neutro $e_\diamond = f(e_*)$.
4. Supongamos que f es un homomorfismo sobreyectivo, $(X,*)$ tiene neutro e_* y $x \in X$ tiene inverso x^{-1}. Sea $f(x) \in Y$, probemos que $f(x^{-1})$ cumple la función del inverso de $f(x)$ en Y. Luego:
$$f(x) \diamond f(x^{-1}) = f(x * x^{-1}) = f(e_*) = e_\diamond$$
$$f(x^{-1}) \diamond f(x) = f(x^{-1} * x) = f(e_*) = e_\diamond$$
Luego, $f(x)^{-1}$ existe y es: $f(x^{-1})$.

■

Corolario A.6. *Sean $(X,*)$ e $(Y,\diamond)$ estructuras algebraicas y $f: X \to Y$ un isomorfismo. Entonces:*

1. *$*$ es asociativa en X si y solo si $\diamond$ es asociativa en Y.*
2. *$*$ es conmutativa en X si y solo si $\diamond$ es conmutativa en Y.*
3. *$*$ tiene un neutro e_* en X si y solo si $\diamond$ tiene un neutro $e_\diamond = f(e_*)$ en Y*
4. *Si $(X,*)$ e $(Y,\diamond)$ tienen elemento neutro, entonces $x \in X$ tiene elemento inverso x^{-1} si y solo si $f(x) \in Y$ tiene elemento inverso y $f(x)^{-1} = f(x^{-1})$*

Demostración. Basta aplicar el teorema anterior considerando los homomorfismos f y f^{-1}. ■

Definición A.13. Dados $(G,*)$ y $(H,\circ)$ dos grupos y $f: G \to H$ un homomorfismo, diremos que f es un homomorfismo de grupos.

Teorema A.7. *Dados $(G,*)$ y $(H,\circ)$ dos grupos y $f: G \to H$ un homomorfismo de grupos. Entonces:*

- $e_\circ = f(e_*)$
- $f(g)^{-1} = f(g^{-1})$

Demostración.

1. Sea $g \in G$, luego $f(g) \in H$, como H es grupo existe una única solución para la ecuación $f(g) \circ x = f(g)$, esta solución claramente corresponde a $e_\circ$, pero:
$$f(g) \circ f(e_*) = f(g * e_*) = f(g)$$
Luego $f(e_*)$ cumple la ecuación y como la solución es única $e_\circ = f(e_*)$
2. Sea $g \in G$, luego $f(g) \in H$, como H es grupo existe una única solución para la ecuación $f(g) \circ x = e_\circ$, esta solución claramente corresponde a $f(g)^{-1}$, pero:
$$f(g) \circ f(g^{-1}) = f(g * g^{-1}) = f(e_*) = e_\circ$$
Luego $f(g^{-1})$ cumple la ecuación, y como la solución es única $f(g)^{-1} = f(g^{-1})$

■

A.4. Ejercicios

P1. Estudie las estructuras:

1. $(\mathbb{R}^2, *), (a,b)*(c,d) = (a+c, b+d+2bd)$
2. Sea $S = \left\{a + b\sqrt{2} : a, b \in \mathbb{R}\right\}$, se definen $*, \diamond$ tales que:

$$x * y = (a + b\sqrt{2})(c + d\sqrt{2})$$
$$x \diamond y = (a + b\sqrt{2}) + (c + d\sqrt{2})$$

3. $(\mathbb{N}, *), a * b = \text{máx}\{a, b\}$
4. $(\mathbb{N}, *), a * b = \text{máx}\{a, b\} - \text{mín}\{a, b\}$
5. $S = \{1, 2, 3, 6\}$ estudie $(S, *)$ donde $a * b = \text{MCD}(a, b)$. (MCD = máximo Común Divisor).
6. $S = \{1, 2, 5, 10\}, (S, \wedge, \vee)$ donde: $a \vee b = \text{MCD}(a, b), a \wedge b = \text{mcm}(a, b)$ (mcm: mínimo común múltiplo).
7. $X \neq \varnothing, (\mathcal{P}(X), \cup, \cap)$
8. $X \neq \varnothing, (\mathcal{P}(X), \Delta, \cap)$ donde Δ es la diferencia simétrica.

P2. Sea $G = \{a \in \mathbb{R} : -1 < a < 1\}$ y sea $a * b = \dfrac{a+b}{1+ab}$ Demuestre que $(G, *)$ es grupo Abeliano.

P3. Sea $(G, *)$ un grupo tal que: $\forall a, b \in G, (a*b)^2 = a^2 * b^2$ (Notación: $a^n = \underbrace{a * \cdots * a}_{n \text{ veces}}$).

1. Demuestre que $(G, *)$ es Abeliano.
2. Pruebe que: $\forall n \geq 2, \forall a, b \in G, (a*b)^n = a^n * b^n$

P4. Demuestre que si G es un grupo finito de orden impar, necesariamente algún elemento es su propio inverso.

P5. Sea $(G, *)$ un grupo, y estudie del punto de vista de morfismo, las aplicaciones:

1. $\phi : G \to G$, $\phi(x) = a * x$
2. $\phi : G \to G$, $\phi(x) = a^{-1} * x * a$ ¿Qué sucede si G es Abeliano?

P6. Dado un polígono regular convexo de 6 lados. Estudie el grupo de rotaciones asociado. Generalice para polígono regular de n lados.

P7. Sea la permutación $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$. Sea $G = \{p^n : n \in \mathbb{N}\}$ Demuestre que $(G, \circ)$ es un grupo cíclico de orden 6. Estudie los subgrupos.

P8. Sea $G = \left\{ \phi_{a,b} : x \to ax + \dfrac{b}{a} : b \in \mathbb{R}, a \neq 0 \right\}$

1. Demuestre que $(G, \circ)$ es un grupo.
2. Demuestre que $G^1 = \left\{ \phi_b : x \to x + b : b \in \mathbb{R} \right\}$ es un subgrupo

P9. Demuestre que $T=\left\{\begin{pmatrix} a & b\\ 0 & c\end{pmatrix} : a,c,d\in\mathbb{Z}\right\}$ es un subanillo de $M_{22}(\mathbb{Z})$ con la suma y el producto de matrices usuales.

P10. Sea $M(\mathbb{Z}_3)=\left\{\begin{pmatrix} a & b\\ -b & a\end{pmatrix} : a,b\in\mathbb{Z}_3\right\}$. Pruebe que $(M,+,\cdot)$ ($+,\cdot$ suma y producto de matrices inducidas por $\mathbb{Z}_3$) es un cuerpo de 9 elementos y $\left(M\setminus\left\{\begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix}\right\},\cdot\right)$ es un grupo cíclico de orden 8.

P11. Sea $(A,+,\cdot)$ un anillo, definimos: $\mathrm{CE}(A)=\{c\in A : c\cdot x=x\cdot c,\forall x\in A\}$ Demuestre que $\mathrm{CE}(A)$ es un subanillo de A.

P12. Sea $X\neq\varnothing$

1. Demuestre $(\mathcal{P}(X),\Delta,\cap)$ es un anillo.
2. Dado $S\subseteq X$ se define la función $\begin{array}{rl} f:\mathcal{P}(X) & \to\mathcal{P}(X)\\ A & \to f(A)=A\cap S\end{array}$. Pruebe que f es un homomorfismo.

P13. Sea $(A,+,\cdot)$ un anillo, dado $a\in A$, definimos $\begin{array}{rl} f_a: A & \to A\\ x & \to f(x)=a\cdot x\end{array}$. Sea $F_a=\{f_a : a\in A\}$, pruebe que:

1. $(F_a,+,\circ)$ es un anillo con la suma y composición de funciones.
2. $(F_a,+,\circ)$ es isomorfo a $(A,+,\cdot)$ (considere $\begin{array}{rl} \varphi: A & \to F_A\\ a & \to\varphi(a)=f_a\end{array}$)

P14. Estudie las propiedades de $F_{\sqrt{3}}=\left\{a+b\sqrt{3} : a,b\in\mathbb{Q}\right\}$ y de $F_{\sqrt{3}}(\mathbb{R})=\left\{a+b\sqrt{3} : a,b\in\mathbb{R}\right\}$ clasifique las estructuras $(F_{\sqrt{3}},+,\cdot)$ y $(F_{\sqrt{3}}(\mathbb{R}),+,\cdot)$

P15. Estudie las propiedades de $*$ definida por: $* : (\mathbb{Z}_2\times Z_3)^2\to\mathbb{Z}_2\times Z_3 :$

$$([a]_2,[b]_3)*([c]_2,[d]_3)=([a]_2\odot_2[c]_2,[b]_3\oplus_3[d]_3)$$

P16. Sea $E\neq\varnothing$, sobre E se definen dos leyes de composición interna $*$ y $\diamond$, son elementos neutros e y f respectivamente, y que cumplen:

$$\forall x,y,u,v\in E,(x*y)\diamond(u*v)=(x\diamond u)*(y\diamond v)$$

1. $e=f$
2. $\forall x,v\in E, x*v=x\diamond v$
3. $*$ es asociativa y conmutativa.

P17. Sea $\mathcal{F}=\left\{f :\ f:\mathbb{N}\to\mathbb{R}\right\}$. Se define en $\mathcal{F}$ la ley de composición interna $*$ por:

$$(f*g)(n)=\sum_{j=0}^{n} f(j)g(n-j),\qquad\forall n\in\mathbb{N}$$

1. Dadas $f(n) = n$ y $g(n) = 1$ pruebe que:

   1.1) $(g * g)(n) = n + 1$

   1.2) $(f * g)(n) = \dfrac{n(n+1)}{2}$

   1.3) $(f * f)(n) = \dfrac{n(n+1)(n-1)}{6}$

2. Pruebe que $*$ es asociativa, conmutativa, posee elemento neutro, distribuye con respecto a $+$ (suma de funciones $(f + g)(n) = f(n) + g(n)$). (Indicación: para demostrar que es asociativa puede usar que $\sum_{i=0}^{n} \sum_{j=0}^{i} S_{i,j} = \sum_{j=0}^{n} \sum_{i=j}^{n} S_{i,j}$)

Apéndice B

Espacios Vectoriales

Un espacio vectorial es una estructura algebraica creada a partir de un conjunto no vacío, una operación interna (llamada suma, definida para los elementos del conjunto) y una operación externa (llamada producto por un escalar, definida entre dicho conjunto y otro conjunto, con estructura de cuerpo), con 8 propiedades fundamentales.

A los elementos de un espacio vectorial se les llama vectores y a los elementos del cuerpo, escalares. Más formalmente:

Definición B.1. Un espacio vectorial sobre un cuerpo $\mathbb{K}$; (como el cuerpo de los números reales o los números complejos) es un conjunto V no vacío, dotado de dos operaciones para las cuales será cerrado:

$$\begin{aligned} \text{Suma} \quad + : V \times V &\to V \\ (u, v) &\to w = u + v \end{aligned}$$

operación interna tal que:

1. $+$ es conmutativa
2. $+$ es asociativa,
3. $+$ tiene elemento neutro $\vec{0}$
4. $\forall v \in V$ existe elemento opuesto para v

y la operación producto por un escalar:

$$\begin{aligned} \text{Producto} \quad \cdot : \mathbb{K} \times V &\to V \\ (\lambda, u) &\to \lambda \cdot u \end{aligned}$$

operación externa tal que:

1. $\cdot$ es asociativa:

2. $\cdot$ tiene elemento neutro multiplicativo (1 si $\mathbb{K} = \mathbb{R}$)

3. $\cdot$ es distributiva con respecto a la suma de vectores.

4. $\cdot$ es distributiva con respecto a la suma de escalares.

Ejemplo B.1. Un ejemplo clásico de espacio vectorial es $\mathbb{R}^n$, usando como cuerpo $\mathbb{R}$. Este conjunto corresponde a las n-tuplas de números reales. Así $\vec{x} \in \mathbb{R}$ corresponde a $\vec{x} = (x_1, \ldots, x_n)$ denominaremos a x_i la i-ésima componente del vector $\vec{x}$.

Teniendo este conjunto se define la suma de dos vectores $\vec{x}$ e $\vec{y}$ como la suma componente a componente, es decir:

$$(\forall \vec{x}, \vec{y} \in \mathbb{R}^n, \vec{x} + \vec{y} = (x_1 + y_1, \ldots, x_n + y_n))$$

Y el producto por escalar como:

$$(\forall \lambda \in \mathbb{R}, \forall \vec{x} \in \mathbb{R}^n, \lambda \vec{x} = (\lambda x_1, \ldots, \lambda x_n)).$$

Con estas operaciones es fácil verificar que se cumplen las propiedades anteriores, teniendo como $\vec{0} = (0, \ldots, 0)$.

Ejemplo B.2. Otro ejemplo de espacio vectorial son las matrices de $m \times n$ con coeficientes reales que se denotan por: $\mathcal{M}_{n \times m}(\mathbb{R})$, también usando el cuerpo $\mathbb{R}$ para los escalares. Recordemos que la suma de matrices también se realiza componente a componente y el producto por escalar corresponde a multiplicar el escalar por cada componente de la matriz.

Ejemplo B.3. Otro ejemplo es el de las sucesiones $\mathcal{F} = \left\{ f : \mathbb{N} \to \mathbb{R} \right\}$ con el cuerpo $\mathbb{R}$. En el caso particular de las funciones la imagen de n por la función f se denota como f_n. Dadas $f, g \in \mathcal{F}$ se define:

1. $\begin{aligned}(f+g) : \mathbb{N} &\to \mathbb{R} \\ n &\to f_n + g_n\end{aligned}$, es decir $(\forall n \in \mathbb{N}, (f+g)_n = f_n + g_n)$.

2. $\left(\forall \lambda \in \mathbb{R},\ \begin{aligned}(\lambda f) : \mathbb{N} &\to \mathbb{R} \\ n &\to \lambda f_n\end{aligned}\right)$, es decir $(\forall n \in \mathbb{N}, (\lambda f)_n = \lambda f_n)$.

Estas sucesiones pueden verse como tuplas de largo infinito, de modo que se cumplen las propiedades de espacio vectorial, al igual que en el caso de las n-tuplas.

Cuando trabajamos con espacios vectoriales a veces nos interesa trabajar con conjuntos más pequeños, pero que cumplen todas las propiedades de un espacio vectorial, este tipo de conjuntos los llamamos subespacios vectoriales.

Definición B.2. Dado V un espacio vectorial, se dice que E es un subespacio vectorial de V, si $E \subseteq V$ y E es un espacio vectorial.

Teorema B.1. *Dado V un espacio vectorial, $E \subseteq V$ es un subespacio vectorial de V si:*

1. $\vec{0} \in E$

2. $(\forall u, v \in E, u + v \in E)$

3. $(\forall u \in E, \forall \lambda \in \mathbb{K}, \lambda u \in E)$

Demostración. Para verificar las propiedades de la suma lo primero de debemos notar es que la asociatividad y conmutatividad se heredan para cualquier subconjunto, por lo tanto lo que hace falta verificar es que sea ley de composición interna, que se verifica en el punto 2, que el $\vec{0} \in E$, lo que se verifica en 1, y que para todo $v \in E$ el opuesto está en E. Para lograr esto tomamos $-1 \in \mathbb{K}$ (-1 es el opuesto de 1 en $\mathbb{K}$), como $(\forall u \in E, \forall \lambda \in \mathbb{K}, \lambda u \in E)$, esto se cumple en particular para $\lambda = -1$, y de ahí tenemos que se cumple la cuarta propiedad de la suma.

Las propiedades del producto por escalar (asociatividad, distributividad y neutro) todas se heredan por tratarse de un subconjunto del espacio vectorial ∎

Ejemplo B.4. Se define el producto punto entre dos vectores como:

$$\begin{aligned} \cdot : \mathbb{R}^n \times \mathbb{R}^n &\to \mathbb{R} \\ (\vec{x}, \vec{y}) \quad &\to \sum_{i=1}^{n} x_i y_i \end{aligned}$$

Probaremos que $E = \left\{ \vec{x} \in \mathbb{R}^n : \vec{x} \cdot \vec{1} = 0 \right\}$ es un subespacio vectorial de $\mathbb{R}^n$, donde $\vec{1} = (1, \ldots, 1)$.

Notemos que $E = \left\{ \vec{x} \in \mathbb{R}^n : \sum_{i=1}^{n} x_i = 0 \right\}$

1. $\vec{0} \in E$. Claramente $\vec{0} \cdot \vec{1} = \sum_{i=1}^{n} 0 \cdot 1 = \sum_{i=1}^{n} 0 = 0$, luego $\vec{0} \in E$.

2. $\forall \vec{x}, \vec{y} \in E, \vec{x} + \vec{y} \in E$. Sean $\vec{x}, \vec{y} \in E$ cualesquiera:

$$\begin{aligned} \sum_{i=1}^{n} x_i &= 0 \\ \sum_{i=1}^{n} y_i &= 0 \\ \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i &= 0 \\ \sum_{i=1}^{n} (x_i + y_i) &= 0 \\ \sum_{i=1}^{n} (\vec{x} + \vec{y})_i &= 0 \\ \vec{x} + \vec{y} &\in E \end{aligned}$$

3. $\forall \vec{x} \in E, \lambda \vec{x} \in E$

$$\begin{aligned}
\sum_{i=1}^{n} x_i &= 0 \\
\lambda \sum_{i=1}^{n} x_i &= 0 \\
\sum_{i=1}^{n} \lambda x_i &= 0 \\
\sum_{i=1}^{n} (\lambda \vec{x})_i &= 0 \\
(\lambda \vec{x}) &\in E
\end{aligned}$$

Note que esta demostración funciona también usando cualquier otro vector de $\mathbb{R}^n$ en vez de $\vec{1}$

Ejemplo B.5. Matrices triangulares superiores.

Ejemplo B.6. $\mathcal{F}_h = \left\{ h \in \mathcal{F} : h_n = \sum_{i=1}^{k} a_i h_{n-i} \right\}$ es subespacio vectorial de $\mathcal{F}$.

En primer lugar probemos que $\vec{0} \in \mathcal{F}_h$, Esto obviamente es cierto ya que:

$$0 = \vec{0}_n = \sum_{i=1}^{k} a_i \cdot \vec{0}_{n-i} = 0$$

En segundo lugar probemos que $\mathcal{F}_h$ es cerrado para la suma. Sean $f, g \in \mathcal{F}_h$:

$$\begin{aligned}
f_n &= \sum_{i=1}^{k} a_i f_{n-i} \\
g_n &= \sum_{i=1}^{k} a_i g_{n-i}
\end{aligned}$$

sumando ambas ecuaciones obtenemos:

$$\begin{aligned}
f_n + g_n &= \sum_{i=1}^{k} a_i f_{n-i} + \sum_{i=1}^{k} a_i g_{n-i} = \sum_{i=1}^{k} (a_i f_{n-i} + a_i g_{n-i}) \\
f_n + g_n &= \sum_{i=1}^{k} a_i (f_{n-i} + g_{n-i}) \\
(f + g)_n &= \sum_{i=1}^{k} a_i (f + g)_{n-i}
\end{aligned}$$

Por último, probemos que es cerrado con producto por escalar. Sea $f \in \mathcal{F}_h$:

$$\begin{aligned} f_n &= \sum_{i=1}^{k} a_i f_{n-i} && / \cdot \alpha \\ \alpha f_n &= \alpha \sum_{i=1}^{k} a_i f_{n-i} = \sum_{i=1}^{k} a_i \alpha f_{n-i} \\ (\alpha f)_n &= \alpha \sum_{i=1}^{k} a_i f_{n-i} = \sum_{i=1}^{k} a_i (\alpha f)_{n-i} \end{aligned}$$

Definición B.3. Dado un espacio vectorial V, diremos que un vector u es combinación lineal de los vectores de $S = \{v_1, \dots, v_n\} \subseteq V$ si existen escalares $a_1, \dots, a_n$ tales que

$$u = a_1 v_1 + \cdots + a_n v_n$$

Notaremos como $\langle S \rangle_V$ el conjunto resultante de todas las combinaciones lineales de los vectores de $S \subseteq V$. Llamaremos a $\langle S \rangle_V$ el espacio generado por S.

Ejemplo B.7. Consideremos el espacio vectorial $\mathbb{R}^3$. EL vector $(2, 2, 1)$ es una combinación lineal de $(1, 0, -1), (0, 1, 0), (0, 0, 1)$.

$$(2, 2, 1) = 2(1, 0, -1) + 1(0, 1, 0) + 3(0, 0, 1)$$

También, $(4, 0, 0)$ es una combinación lineal de $(1, 0, 1), (0, 1, 0), (0, 0, 1)$.

$$(4, 0, 0) = 4(1, 0, -1) + 0(0, 1, 0) + 4(0, 0, 1)$$

Proposición B.2. *Dado V un espacio vectorial y $S \subseteq V$ un conjunto de vectores, el conjunto $F = \langle S \rangle$ es el subespacio vectorial más pequeño contenido en V y que contiene a S.*

Demostración. Primero veamos que $\langle S \rangle_V$ es un subespacio vectorial de V.

1. $\vec{0} \in \langle S \rangle_V$. Claramente $\vec{0} = \sum_{v \in S} 0 \cdot v$. Por lo tanto, $\vec{0} \in \langle S \rangle_V$.
2. $\langle S \rangle_V$ es cerrado para la suma. Sean $u, w \in \langle S \rangle_V$ cualesquiera. Luego:

   $$u = \sum_{v \in S} \alpha_v \cdot v \qquad \wedge \qquad w = \sum_{v \in S} \beta_v \cdot v$$

   Sumando ambas ecuaciones, tenemos:

   $$\begin{aligned} u + v &= \sum_{v \in S} \alpha_v \cdot v + \sum_{v \in S} \beta_v \cdot v \\ u + v &= \sum_{v \in S} (\alpha_v \cdot v + \beta_v \cdot v) \\ u + v &= \sum_{v \in S} (\alpha_v + \beta_v) \cdot v \end{aligned}$$

   Luego, $u + v \in \langle S \rangle_V$

3. $\langle S\rangle_V$ es cerrado para el producto por escalar. Sea $u \in \langle S\rangle_V$ cualquiera:

$$u = \sum_{v\in S} \alpha_v \cdot v \qquad / : \lambda\cdot$$

$$\lambda u = \lambda \sum_{v\in S} \alpha_v \cdot v$$

$$\lambda u = \sum_{v\in S} \lambda\alpha_v \cdot v$$

$$\lambda u = \sum_{v\in S} (\lambda\alpha_v) \cdot v$$

Luego, $\lambda u \in \langle S\rangle_V$

Veamos ahora, que cualquier subespacio vectorial que contiene S contiene $\langle S\rangle_V$.

Por reducción al absurdo, supongamos que existe $S \subseteq G \subsetneq \langle S\rangle_V$, subespacio vectorial de V. Si existe un elemento que está en $\langle S\rangle_V$, pero no en G quiere decir que hay una combinación lineales de elementos de S que no está en G, y como loes elementos de S están en G, quiere decir que G no es cerrado para combinaciones lineales, y esto es una contradicción con el hecho que G es subespacio vectorial. ■

Definición B.4. Dado V un espacio de vectorial, se dice que $v_1, \ldots, v_k \in V$ son linealmente independientes (l.i.) si:

$$\sum_{i=1}^{k} \alpha_i v_i = \vec{0} \implies (\forall i \in \{1, \ldots, k\}, \alpha_i = 0)$$

Definición B.5. Dado V un espacio vectorial, se dice que $v_1, \ldots, v_k \in V$ es una base de V si $v_1, \ldots, v_k \in V$ son linealmente independientes y $V = \langle v_1, \ldots, v_k\rangle_V$, es decir:

$$(\forall v \in V, \exists \alpha_1, \ldots, \alpha_k \in \mathbb{K}, v = \sum_{i=1}^{k} \alpha_i v_i)$$

Proposición B.3. *Dado un espacio vectorial V, $\{v_1, \ldots, v_n\} \subseteq V$ es una base si y solo si $\forall u \in E, \forall i \in \{1, \ldots, n\}\ \exists! a_i \in \mathbb{K}, u = \sum_{i=1}^{n} a_i v_i$*

Proposición B.4. *Dado un espacio vectorial V, $S = \{v_1, \ldots, v_n\} \subseteq V$, linealmente independiente y $u \notin \langle S\rangle \Rightarrow \{u\} \cup S = \{u, v_1, \ldots, v_n\}$ son linealmente independientes.*

Demostración. Por reducción al absurdo, supongamos que $S = \{u, v_1, \ldots, v_n\}$ no son linealmente independientes, entonces existen $\alpha_0, \alpha_1, \ldots, \alpha_k$ tal que $\bigvee_{i=0}^{n} \alpha_i \neq 0$ y:

$$\alpha_0 u + \sum_{i=1}^{n} \alpha_i v_i = 0$$

Si $\alpha_0 = 0$, entonces $\sum_{i=1}^{n} \alpha_i v_i = 0$, como los elementos de S son linealmente independientes esto no puede ocurrir. De modo que $\alpha_0 \neq 0$. De aquí

$$u + \sum_{i=1}^{n} \frac{\alpha_i}{\alpha_0} v_i = 0$$

Luego:

$$u = \sum_{i=1}^{n} -\frac{\alpha_i}{\alpha_0} v_i$$

Por lo tanto, u es una combinación lineal de los elementos de S lo que nos lleva a una contradicción ■

Teorema B.5 (Teorema de la base de generadores)**.** *Todo sistema de generadores tiene una base.*

Demostración. Sea $S = \{v_1, \dots, v_n\}$ un conjunto generador. Si S es linealmente independiente, tenemos una base. Si no el es probemos que podemos eliminar un vector, tal que el espacio generado es el mismo, pero tiene un vector menos. Siguiendo un procedimiento como ese, podemos encontrar una base que genera el mismo espacio.

Sea $S = \{v_1, \dots, v_n\}$ un conjunto linealmente dependiente, es decir, existen $\alpha_1, \dots, \alpha_n$ no todos distintos de 0, tal que:

$$\sum_{i=1}^{n} \alpha_i v_i = 0$$

Sea $i_* = \min i \in \{1, \dots, n\} : \alpha_i \neq 0$, luego:

$$\sum_{i=1}^{i_*-1} \alpha_i v_i + \alpha_{i_*} v_{i_*} + \sum_{i=i_*+1}^{n} \alpha_i v_i = 0$$

De aquí, despejamos el vector v_{i_*}:

$$v_{i_*} = \sum_{i=1}^{i_*-1} -\frac{\alpha_i}{\alpha_{i_*}} v_i + \sum_{i=i_*+1}^{n} -\frac{\alpha_i}{\alpha_{i_*}} v_i$$

Como v_{i_*} es una combinación lineal del resto de los vectores, puedo eliminar este vector, ya que si aparece en una combinación lineal podemos reemplazar ese vector por una combinación lineal del los otros. ■

Teorema B.6 (Teorema Steinitz)**.** *Toda base de un espacio vectorial puede ser cambiada parcialmente por vectores linealmente independientes.*

Corolario B.7. *Si un espacio vectorial V tiene una base de n vectores entonces cualquier otra base posee n vectores.*

A partir esto se define la dimensión de un espacio vectorial.

Definición B.6. Dado V un espacio vectorial tal que $V = \langle v_1 \dots, v_k \rangle_V$, vectores linealmente independientes, entonces V tiene dimensión k, lo que se denota por: $\dim V = k$

Ejemplo B.8. Veremos cual es la dimensión de algunos espacios vectoriales que hemos visto en los ejemplos anteriores.

1. $\dim \mathbb{R}^n = n$, ya que $\mathbb{R}^n = \langle \vec{e}^1, \dots, \vec{e}^n \rangle$, donde $\vec{e}^j_i = 1$ si y solo si $i = j$.

2. $\dim \left\{ \vec{x} \in \mathbb{R}^n : \vec{x} \cdot \vec{1} = 0 \right\} = n - 1$. en este caso el conjunto generador es:$\langle \vec{e}^1 - \vec{e}^n, \vec{e}^2 - \vec{e}^n, \dots, \vec{e}^{n-1} - \vec{e}^n \rangle$

3. $\dim \mathcal{F}_h = k$ Para probar que su dimensión es k debemos encontrar k sucesiones linealmente independientes que generen todo el espacio. Sean $e_n^1, \ldots, e_n^k$ las sucesiones definidas por:

$$e_j^i = \begin{cases} 1 & j \leq k \wedge i = j \\ 0 & j \leq k \wedge i \neq j \\ \sum\limits_{l=1}^{k} a_l e_{j-l}^i & j > k \end{cases}$$

Como estas sucesiones cumplen la ecuación de recurrencia son elementos de $\mathcal{F}$. Veamos que son linealmente independientes. Supongamos:

$$\sum_{i=1}^{k} a_i e_n^i = \vec{0}$$

Entonces:

$$\forall j \leq k, \sum_{i=1}^{k} a_i e_j^i = 0$$

Pero como $e_j^i \neq 0$ si y solo si $i = j$

$$\forall j \leq k, a_j e_j^j = 0$$

Por lo tanto, $\forall j \leq k, a_j = 0$. Luego estas recurrencias son l.i.

Ahora solo necesitamos probar que cualquier sucesión de $\mathcal{F}$ puede escribirse como una combinación lineal de $e_n^1, \ldots, e_n^k$. Sea $f \in \mathcal{F}$ cualquiera, f debe ser tal que:

$$f_j = \begin{cases} b_j & j \leq k \\ \sum\limits_{i=1}^{k} a_i f_{j-i}^j & j > k \end{cases}$$

Claramente:

$$f_j = \sum_{i=1}^{k} b_i e_j^i$$

Luego, $e_n^1, \ldots, e_n^k$ es una base de $\mathcal{F}$.

Definición B.7. Un subespacio vectorial afín B de un espacio vectorial V es un conjunto $B = \{u + a : u \in E\}$, donde $a \in V$, y E es un subespacio vectorial de V.