Informática y matemáticas *

Ernesto García Camarero†

11 diciembre 2000

Indice

1 Introducción

Ante todo agradecer al Profesor D. Federico Gaeta su invitación a participar en los actos que ha venido promoviendo en el Ateneo de Madrid con motivo del año mundial de las matemáticas, de las que como muestra permanente se expone una vitrina en el vestíbulo de esta casa.

El tema que me propuso para esta charla fue el de "informática y matemáticas".

Al aceptar, la primera cuestión que nos planteamos fue ¿cómo presentar las implicaciones y relaciones que existen entre matemáticas e informática? o ¿qué aspectos de esas relaciones exponer aquí?

Como respuesta vamos a destacar al concepto de "cálculo" o "cómputo" como la relación fundamental entre matemática e informática. Rescatar esta relación no es tarea facil en un momento como el actual, en el que todo el mundo usa la informática apoyándose en una máquina misteriosa (mágica caja negra), pero en la que, en su empleo, no se percibe directamente la presencia de las matemáticas, y en la que su nombre "ordenador" (ejecuta ordenes) oculta su origen, de forma diferente a como lo dejaba patente en las épocas en las que se llamaba "computadora" (realiza cómputos o cálculos).

En efecto, considerada como máquina de utilidad general, está muy extendido el uso directo, por gran número de personas, de los procesadores de texto, que se comportan como máquinas de escribir sofisticadas y que ayudan al almacenamiento y archivo de los documentos así generados. Tambien es cada vez más común el uso del correo electrónico (como un híbrido entre la máquina de escribir y el teléfono), y de otras aplicaciones de Internet que, aunque potentes y misteriosas, tampoco se vinculan directamente con las matemáticas.

También en las distintas profesiones se utilizan, cada vez más y más, los ordenadores y las aplicaciones informáticas; pero estas aplicaciones solo en profesiones muy especificas utilizan explícitamente el cálculo numérico, la estadística y otras funcionalidades matemáticas. En la mayor parte de las profesiones se

*Conferencia dada en el Atenéo de Madrid en el ciclo dedicado al Año Mundial de las Matemáticas, dirigido por el Prof. Federico Gaeta

†Ha sido Director del Centro de Cálculo y Profesor de Teoría de Autómatas y Lenguajes Formales de la Universidad Complutense de Madrid, y Presidente de la Sociedad Española de Historia de la Ciencia

utilizan aplicaciones orientadas a las bases de datos, al tratamiento de imagen, a la gestión administrativa, y aunque en todas ellas se utilizan algoritmos matematicos muy complejos, estos no se perciben y por tanto no aparecen explicitamente las matemáticas empleadas en ellos, o lo hace solamente en sus aspectos mas elementales, como puede ser la aritmética contable.

Todo el mundo sabe que hay aplicaciones informáticas a la ingeniería, y a otras disciplinas en las que las matemáticas juegan un papel importante, pero precisamente por eso se estima que esas aplicaciones más tienen que ver con la matemática que con la informática propiamente dicha.

Pero ¿en que consiste la informática propiamente dicha?

Por un lado, forman parte de la informática las propias máquinas: los *ordenadores*; esas cajas negras provistas de propiedades portentosas, que se han llegado a llamar, incluso, "cerebros electrónicos", y que aparecieron rodeadas de una aureola (que en alguna medida aún conservan) que otras máquinas no tienen.

Por otro lado, forma tambien parte de la informática algo que se sabe es esencial para que los ordenadores funcionen, como son los *programas*. Los programas son textos escritos en determinados lenguajes comprensibles por la máquina, llamados *lenguajes de programación*, para que una vez interpretados por el ordenador realicen posteriormente su ejecución. Para escribir esos programas se requiere de unos especialistas informáticos que conozcan los lenguajes propios de las máquinas.

Nos estamos refiriendo a los dos aspectos generales de la informatica; es decir a la parte material (*hardware*, o ferretería) y a la parte inmaterial (*software*, o parte blanda o impalpable). Nos estamos refiriendo a los dos pilares que fundamentan la informática, y en los que se apoya su tercer elemento formado por las *aplicaciones*.

Pero, ¿de que forma, tanto el hardware como el software, son resultado, consecuencia, y aplicación de la matemática? Vamos a intentar en esta conferencia, dar respuesta a esta pregunta, o al menos a delinear, según mi apreciación, cómo el vínculo fundamental que relaciona a la informática con la matemática es la noción de cálculo.

2 La matemática como cálculo.

No vamos a entrar a caracterizar a la matemática, ni a intentar dar una definición parcial que sirva siquiera para los fines de esta conferencia, diremos simplemente que uno de los resultados y finalidades de la matemática es el cálculo. Es decir, la matemática busca formas razonadas de procedimientos seguros mediante los que podamos contar, medir, y obtener los resultados de ciertas serie de operaciones que nos permitan predecir algunos acontecimientos que puedan ocurrir en la naturaleza.

Al aludir a formas razonadas nos estamos refiriendo a la reflexión, al pensamiento, a la *lógica*; al aludir a procedimientos seguros nos estamos refiriendo al *cálculo*.

Como entendemos que esta última caracteristica de la matemática es el fundamento de la informática, dedicaremos nuestra conferencia a precisar lo que se entiende por *cálculo*. Y al ir avanzando en la precisión de esta idea, iremos percibiendo lo que, a mi juicio, es el vínculo esencial entre matemáticas e informática.

Un *cálculo* es un procedimiento que nos dice como debemos aplicar unas reglas, construidas a partir de operaciones sencillas sobre unos datos conocidos, para obtener el resultado buscado.

En un cálculo los datos no siempre son numéricos, como suele creerse, pueden ser de otro tipo, por ejemplo, geométricos (puntos, rectas, figuras, ...), letras o palabras, oraciones o proposiciones lingüísticas o lógicas. Estos datos corresponden a magnitudes, u otros conceptos, a cuya definición dedica la matemática gran esfuerzo.

Las reglas y operaciones deben ser conocidas y sencillas, en el sentido de que cualquiera persona con un pequeño entrenamiento pueda realizarlas (de aquí la idea de *automatismo* como opuesta a la de *reflexión* o de pensamiento). También puede considerarse la tarea de definir esas operaciones, y estudiar sus propiedades, como una de las actividades a las que se ha dedicado y dedica la matemática.

La historia del cálculo es tan vieja como la historia de la propia matemática. Como todo el mundo sabe la palabra cálculo significa *piedrecilla*, y con ella se alude al procedimiento matemático mas antiguo que se conoce: *contar*. También se usan piedrecillas (en los conjuntos de piedrecillas ya esta la idea de número) en procedimientos mas complejos, como la suma y la resta. El *ábaco chino*[1], que todavía se usa en algunas colectividades, es un superviviente, que tal vez viene desde épocas prehistóricas, de los primitivos usos de los "cálculos" . Así, el ábaco es el primer instrumento utilizado en el largo camino de la computación.

2.1 El cálculo geométrico

Veamos también, para ilustrar la idea de cálculo, algunos ejemplos geométricos, y cuales fueron los primeros instrumentos utilizados para ayudar a efectuarlos: la *regla* y el *compás*. Construir un triángulo equilátero[2] (la trinidad), construir un exagono regular, trazar una perpendicular por un punto dado a una recta dada, hallar la *bisectríz* de un ángulo, hallar el lado de un cuadrado que tenga una *superficie doble* de un cuadrado dado (ver figura 1),... y una infinidad de otros más, son problemas, llamados elementales, que desde la geometría clásica se vienen planteando y resolviendo mediante el empleo de procedimientos que se basan en el solo uso de la regla y del compás, y de los que Euclides en sus famosos *Seis Libros* da cumplido repertorio.

También se usaron la regla y el compás para realizar algunos cálculos aritmeticos. Un ejemplo curioso es la forma de calcular, por procedimientos geométricos, la raíz cuadrada de la serie de los números naturales $\sqrt{2}$, $\sqrt{3}$, $\sqrt{4}$, $\sqrt{5}$ ...(ver figura 1).

[1]El *quipu* andino es un instrumento con ciertas caracteristicas análogas al ábaco.

[2]La primera proposición del *Libro I* de los *Elementos* de Euclides dice: *Construir un triangulo equilátero sobre una recta finita dada.*

1 1

1

$\sqrt{4}$

$\sqrt{5}$ $\sqrt{3}$

$\sqrt{2}$ 1

$l\sqrt{2}$ l

1

l

Duplo del cuadrado **Raíces de números naturales**

Figura 1

Pero tambien se plantearon otros problemas que se resistieron a que su resolucion se pudiera obtener aplicando *cálculos* con la regla y el compás . Algunos eran simples generalizaciones de otros ya resueltos, como hallar la trisectriz (no hay solución al problema de la *trisección del ángulo*), hallar la arista de un cubo que tenga volumen doble de un cubo dado (no hay solución al problema de la *duplicación del cubo*),. . . y el problema estrella durante muchos siglos fue: hallar el lado de un cuadrado que tenga el mismo área que un circulo dado (no hay solución al problema de la *cuadratura del circulo*). Como veremos mas adelante, decir en estos términos que un problema no tiene solucion, solo quiere decir que no existe un *algoritmo*, es decir un procedimiento, mediante el cual podamos encontrar la solución aplicando un número finito de veces las operaciones que se pueden realizar con la regla y el compás. La demostración de la inexistencia de estos algoritmos para los problemas de la trisección del ángulo, la duplicación del cubo y la cuadratura del círculo solo se logró en la segunda mitad del siglo XIX.

La trigonometría, empujada por las aplicaciones astronómicas y náuticas requiere cálculos que se realizan de una forma analógica, (modernamente se ha llamado nomografía a cálculos realizados mediante la representación gráfica de curvas, y levas) construyendo astrolabios, ballestillas, esferas armilares, cartas náuticas y globos terráqueos mediante los que se realizan representaciones de la realidad donde medir es otra forma que calcular (o de aprovechar cálculos realizados con anterioridad).

Durante los siglos XVI y XVII se inventan gran número de instrumentos mátematicos [3] para abordar los mismos y otros problemas con otras reglas básicas, pensando que tal vez la insolubilidad dependiera de las reglas utilizadas. La idea de automatismo se inicia en esta época como la aplicación de métodos para resolver problemas “sin saber mátematicas”, [4] es decir, sin reflexionar y solo aplicando unas reglas aprendidas..

2.2 El cálculo aritmético

Aunque las construcciones geométricas pueden ser consideradas como un cálculo, de todas formas ha sido el *cálculo aritmético* el que ha merecido principal

[3] Citemos solo dos libros españoles del siglo XVII: García de Céspedes *Libros de instrumentos nuevos de geometría* Madrid, 1606; José Zaragoza *Fábrica y uso de varios instrumentos matemáticos* Madrid, 1674.

[4] Más radical es lo que el pintoresco autor Francisco Antonio Artiga dice en el titulo de su libro publicado en 1694 *Modo de Medir los Planos Orizontalemente, sin saber matemáticas, ni Arismetica y sin instrumentos matemátematicos*

atención desde que se estableció un sistema de representación numérica mediante el cual la realización de las operaciones aritméticas podía hacerse de forma sencilla (obsérvese la dificultad de hacer las operaciones aritméticas con la representación numérica establecida por los romanos). A partir del *Liber abaci* de Leonardo de Pisa (Fibonacci), datado en 1202, se difunde la representación decimal de los números, utilizando para ello las cifras o los guarismos hindúes (arábigos), entre los que se contiene el cero. Las aplicaciones mercantiles y comerciales se ven ampliamente beneficiadas por esta "nueva tecnología".

A partir de ahí se desarrollan formas practicas de realizar las *cuatro reglas*[5] mediante procedimientos que son auténticos programas (*subrutinas de cálculo* en la terminologia informática) que la gente emplea sin saber bien que es lo que hace (¿alguno de los asistentes sabe que está haciendo cuando realiza una división?¿sabe por qué realiza esa serie de operaciones?. Tambien aparecen reglas para realizar la raíz cuadrada (que siempre ha sido misteriosa y que ustedes no solo habrán ya olvidado su realización sino también su existencia), aunque en ésta epoca era todavía poco utilizada. Pues estas, van a ser las *reglas básicas* mediante las que se construyan los cálculos o algoritmos aritméticos. Cada *procedimiento* nos fija el orden en que debemos emplear las reglas para la realización de los cálculos y obtener los resultados deseados.

Durante los siglos XIV al XVII, el *cálculo aritmético* (como hemos visto) comienza a extenderse, hasta alcanzar un gran desarrollo. Sobre todo en el último de los siglos mencionados se construyen procedimientos para simplificar los cálculos y para realizarlos mediante máquinas. Por una parte tenemos el descubrimiento de los *logaritmos*, [6] que redujeron considerablemente la fatiga de los cálculos al reducir el producto a suma, la división a diferencia, y la raíz cuadrada a división por dos, y faciliaron los cálculos apoyandose en la *búsqueda en tablas* (operación que se puede considerar, tambien, como un cálculo), o se materializaron en un instrumento físico usado hasta épocas recientes como fue la *regla de cálculo*. Por otra parte, se inventaron las *máquinas aritméticas* [7] que usaban ruedas y engranajes como elementos constructivos, y que, perfeccionadas, se han conservado hasta bien entrado el siglo XX.

3 El álgebra y los algoritmos.

Hemos dicho que una de las características de los procedimientos de cálculo es que sus reglas han de ser sencillas y fáciles expresar para permitir su aprendizaje y la utilización de las mismas sin mayor esfuerzo.

Los cálculos aritméticos pronto alcanzaron cierta complejidad, y describirlos en el lenguaje corriente o natural hacia difícil su descripción y por tanto su transmisión y utilización, sobre todo cuando se trataba de exponer métodos de resolución para familias enteras de problemas.

Para superar esta dificultad se vio cada vez como más necesario apoyarse en símbolos y notaciones mediante los cuales definir un leguaje (distinto del natural empleado hasta entonces), que fuese más adecuado para expresar y describir

[5]La suma, resta, multiplicación y división, son las operaciones aritméticas básicas con las que se construirán los algoritmos numéricos, análogas a cómo son básicas las que se pueden hacer con la regla y el compás para construir los algoritmos geométricos

[6]Nepper, *Mirafici logarithmorum canonis descriptio*, 1614

[7]Por Pascal (1623-1662) en 1640 y por Leibniz (1646-1716) posteriormente

las ideas y los procedimientos matemáticos. Así apareció y se fue desarrollando el *álgebra*, como lenguaje formal, y la idea de *algoritmo*, o *cálculo algebraico*, como automatismo para la resolución de problemas. Esta formalización de la aritmética se va depurando, desde los primeros tratados de la "regla de la cosa" [8], hasta alcanzar su madurez mediante las expresiones algebraicas, que permitían describir con sencillez las operaciones del álgebra. Utilizando las *expresiones algebraicas* es mas facil encontrar y dar las fórmulas para la resolución de ecuaciones algebraicas de los grados inferiores. Estas fórmulas sintetizaban algoritmos, es decir procedimientos automáticos mediante los cuales a partir de los datos del problema obtener la solución, o dicho en términos matemáticos, a partir de los coeficientes de la ecuación obtener sus raíces.

En efecto, estas formulas indican el orden en que deben realizarse ciertas *operaciones* con los coeficientes para obtener el resultado. Estas operaciones son, en el álgebra clásica (el álgebra del siglo XVI) , la suma, la resta, el producto, la división y la raíz cuadrada, y se decía "resolver ecuaciones por radicales" [9] cuando se utilizaban estas formulas o los algoritmos por ellas representados, en las que la raíz cuadrada jugaba un papel esencial en las mismas.

Con este tipo de algoritmos con radicales, se obtuvieron, en el siglo XVI, procedimientos "automáticos" para resolver tambien las ecuaciones de tercer y cuarto grado. Pero no pudieron encontrarse algoritmos de este tipo para

[8] De esta manera se denominaba en sus orígenes al álgebra antes de que su lenguaje comenzara a formalizarse; con la palabra "cosa" se indicaba a la incógnita. Así puede verse en el título del libro de Juan Bautista Tolra, publicado en Tarragona en 1619: *Tratado de Arte mayor de Aritmetica, llamada Algebra o regla de la cosa*

[9] Así para la ecuación de segundo grado $ax^2 + bx + c = 0$, la formula de resolución es la bien conocida:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

que corresponde al algoritmo que podría expresarse por la siguiente secuencia de las operaciones básicas :

1 Calcular

$$b^2 =$$
$$4ac =$$

2 Calcular el discriminante

$$d = b^2 - 4ac =$$

3 Según sea el valor de d, positivo o cero (Hasta el siglo XIX, no tiene sentido hablar de la raíz cuadrada de números negativos), realizar los calculos indicados en el punto 4, o en el punto 5.

4 Calcular dos raíces simples

$$\sqrt{d} =$$
$$2a =$$
$$-b + \sqrt{d} =$$
$$-b - \sqrt{d} =$$
$$x_1 = \frac{-b + \sqrt{d}}{2a} =$$
$$x_2 = \frac{-b - \sqrt{d}}{2a} =$$

5 Calcular una raíz doble

$$x_1 = x_2 = \frac{-b}{2a} =$$

ecuaciones algebraicas de grado superior al cuarto [10], lo que significó un acicate para buscar otros procedimientos de cálculo.

Mucho del esfuerzo matemático de los siglos XVII y XVIII, se dedicó a reducir el pensamiento a cálculo, es decir buscar la forma de realizar procedimientos efectivos mediante los que obtener de forma “automática” (no depender de la feliz idea) la resolución de problemas.

Aunque esa pretensión no se consiguió, en esta búsqueda se desarrolló el *cálculo analítico* o *formal* (*cálculo infinitesimal* de Newton (1642-1727) y de Leibniz (1646-1716), la *geometría analítica* de Descartes (1596-1650)) y *cálculo numérico* (como fueron los desarrollos en serie para realizar el cálculo efectivo de funciones matemáticas, uno de cuyos principales artífices fue Euler (1707-1783)).

4 El cálculo de proposiciones.

4.1 Las leyes del pensamiento.

Una vez que hemos visto, con mayor generalidad, lo que se entiende por un cálculo, veremos que esta noción se aplica, no solo a las operaciones geométricas, numéricas y algebraicas, sino también a las operaciones lógicas. Para ello demos unas ideas sobre en que consiste el cálculo de proposiciones, tambien conocido como *álgebra de Boole* [11] , y como puede materializarse este cálculo lógico mediante máquinas. Esta teoría matemática es el fundamento de los actuales ordenadores electrónicos y por tanto uno de los aspectos en que de forma más directa esta vínculada la informática con la matemática. Más adelante veremos como la lógica formal, o lógica matemática, también es el fundamento de los lenguajes de programación: otro de los pilares en los que se apoya la informática.

¿En que consiste el cálculo de proposiciones?

Una *proposición* es una frase o expresión a la que se puede asignar el valor lógico de *verdadero* o de *falso*; si toma el valor de verdadero se la llama *proposición verdadera* y si toma el valor de falso se la llama *proposición falsa.* Por ejemplo, la proposicion p

$$p \equiv 3 > 5$$

es una proposición falsa, y la proposicion q

$$q \equiv 4 = 3 + 1$$

es una proposición verdadera.

La proposición $p \equiv$ *la casa de Juan es blanca* será verdadera o falsa según sea el color de la casa de Juan, en este caso a p se llama *variable proposicional.* En la lógica las proposiciones suelen expresarse por letras $p, q, r, \ldots$ y los valores lógicos de *verdadero* y *falso* se representan por las letras V, F, respectivamente.

[10] Esta es una limitación algorítmica, análoga a la que ya se había presentado en la resolución de los problemas geometricos clásicos con la regla y el compás

[11] George Boole (1815-1864) , es un matemático inglés que recogió su teoría en un libro dedicado a las leyes del pensamiento (*An investigation of the laws of thought, on which are founded the mathematical theories of logic and probabilities*), publicado en Londres en 1854. También hizo aportaciones importantes a otros campos de la matemática como las dedicadas a los invariantes algebraicos, a las ecuaciones diferenciales y al cálculo de diferencias finitas.

Al escribir $p = V$, no se quiere decir que "la proposición p *es igual* a V" sino que "la proposición p *toma el valor* verdadero" o que p es verdadera.

Dadas dos proposiciones, p, q, se pueden formar otras proposiciones compuestas de aquellas, aplicando las operaciones lógicas de *negación*, *conjunción*, y *disyunción*:

- *negacion*: **no** p $(\neg\, p)$
- *conjuncion*: p **y** q $(p \wedge q)$
- *disyuncion*: p **o** q $(p \vee q)$

El cálculo de proposiciones nos ayuda a conocer el valor de verdad de una proposición compuesta, en función del valor de verdad de las proposiciones componentes, usando las siguientes tablas mediante las que se asigna el valor a las funciones elementales (que son las que se obtienen simplemente aplicando una vez las operaciones lógicas):

Tabla de verdad de la negación

p	**¬p**
F	V
V	F

Tabla de verdad de la conjunción

p	**p**	**p∧q**
F	F	F
F	V	F
V	F	F
V	V	V

Tabla de verdad de la disyunción

p	**p**	**p∨q**
F	F	F
F	V	V
V	F	V
V	V	V

Estas tablas son conocidas con el nombre de *tablas verdad de las operaciones.*

Una *función proposicional* es una correspondencia entre los valores de verdad de una o varias proposiciones independientes $\{p_1, p_2, ...p_n\}$ llamadas variables, con otra proposición r dependiente de aquellas, llamada función, mediante operaciones lógicas, que excpresamos

$$r \equiv f(p_1, p_2, ...p_n)$$

Como cualquier función se puede obtener por composición de otras funciones más elementales, podemos construir su tabla de verdad descomponiendo la función hasta llegar a las variables proposicionales y a partir de ahí calcular sucesivamente los valores de cada columna aplicando las tablas de verdad de las funciones u operaciones elementales.

El cálculo del valor de verdad de una función proposicional, por ejemplo la siguiente:

$$r \equiv ((p_1 \wedge \neg p_3) \vee \neg(p_1 \wedge \neg p_2)$$

consiste en determinar el valor de verdad de r para unos valores de verdad particulares asignados a p_1, p_2, p_3. Para su cálculo efectivo se procede como indicamos a continuación.

Primero realizamos la asignación de valor a las variables p_1, p_2, p_3 poniendo, por ejemplo, en nuestro caso hacemos $p_1 = V$, $p_2 = V$, $p_3 = F$, es decir, tendriamos :

$$r \equiv ((V \wedge \neg F) \vee \neg(V \wedge \neg V))$$

Después con el auxilio de las tablas de verdad, calculando sucesivamente los valores correspondiente a cada operación, como se indica en la siguiente sucesión:

$$\begin{array}{ll}
r = ((V \wedge \neg \mathbf{F}) \vee \neg(V \wedge \neg V)) & \neg \mathbf{F} = V \\
r = ((V \wedge V) \vee \neg(V \wedge \neg \mathbf{V})) & \neg \mathbf{V} = F \\
r = ((\mathbf{V} \wedge \mathbf{V}) \vee \neg(V \wedge F)) & \mathbf{V} \wedge \mathbf{V} = V \\
r = (V \wedge \neg(\mathbf{V} \wedge \mathbf{F})) & \mathbf{V} \wedge \mathbf{F} = F \\
r = (V \wedge \neg \mathbf{F}) & \neg \mathbf{F} = \mathbf{V} \\
r = (\mathbf{V} \wedge \mathbf{V}) & \mathbf{V} \wedge \mathbf{V} = V \\
r = V &
\end{array}$$

Así que podemos decir que para

$$p_1 = V, \; p_2 = V, \; p_3 = F$$

el valor de r es verdadero ($r = V$).

Si repetimos este cálculo para toda posible terna de valores de p_1, p_2, p_3 tendríamos que la tabla de verdad correspondiente a $r \equiv (p_1 \vee \neg p_3 \vee \neg(p_1 \vee \neg q_2)$ es la siguiente:

$\mathbf{p_1}$	$\mathbf{p_2}$	$\mathbf{p_3}$	$\neg\mathbf{p_3}$	$\neg\mathbf{p_2}$	$\mathbf{p_1} \wedge \neg\mathbf{p_3}$	$\mathbf{p_1} \wedge \neg\mathbf{p_2}$	$\neg(\mathbf{p_1} \wedge \neg\mathbf{p_2})$	$\mathbf{r}$
V	F	F	V	V	V	V	F	V
V	F	V	F	V	F	V	F	F
V	V	F	V	F	V	F	V	V
V	V	V	F	F	F	F	V	V
F	F	F	V	V	F	F	V	V
F	F	V	F	V	F	F	V	V
F	V	F	V	F	F	F	V	V
F	V	V	F	F	F	F	V	V

Para el desarrollo de la informática y para la construcción de los ordenadores ha sido fundamental el estudio del cálculo de proposiciones, y especialmente el hecho de que las proposiciones tienen una *lógica binaria*, ya que solo toman uno entre dos valores posibles, el verdadero o el falso. Este propiedad hace que la lógica de Boole pueda materializarse facilmente mediante circuitos eléctricos que usen algún tipo de elemento biestable (básicamente que en ciertas condiciones permita o no el paso de corriente por un cable dado), como son los relais, los transistores, u otros, que usen propiedades adecuadas de la física.

4.2 Los circuitos lógicos

Vamos a ejemplificar la materialización del cálculo proposicional, empleando el más antiguo de los dispositivos que ya fue utilizado para fines lógicos por nuestro sabio ingeniero Leonardo Torres Quevedo[12], a finales del siglo XIX, al construir sus máquinas aritméticas y su jugador de ajedréz.

Un circuito es un sistema físico compuesto por varios *cables* conductores conectados entre si por *conectores* (o circuito lógico elemental o atómico) de diferente tipo.

Conector: identidad **Conector: negación**

Figura 2

El conector más elemental, es el que corresponde con la *identidad* (vease figura 2), compuesto por una fuente de energía , y por un elemento biestable, (en nuestro caso un relais), de forma que cuando pasa corriente por el cable a actúa el electroimán haciendo bajar la lengueta, que hace contacto en el borne, dejando pasar la corriente por el cable c, y no pasará corriente por el cable c en el caso contrario. Si la proposición p es "pasa corriente por el cable a" y la proposición r es "pasa corriente por el cable c", vemos que r será verdadera cuando p sea verdadera y falsa cuando lo sea p. El circuito anterior se comporta como indica la siguiente tabla de verdad:

Tabla de verdad de la identidad[13]

p	**¬p**
0	0
1	1

De forma análoga se pueden construir conectores que respondan a los operadores de *negación* (vease figura 2), *disyunción* (vease figura 3) y *conjunción* (vease figura 3), cuyas tablas de verdad se indican a continuación:

[12] Leonardo Torres Quevedo (1852-1936) insigne ingeniero español conocido por ser uno de los grandes creadores de automatismos que aplicó a la construccion de máquinas algebraicas, del famoso jugador de ajedrez, y del *telekino* (primer mando a distancia). También construyó dirigibles y un transbordador sobre las cataratas del Niágara

[13] Cuando se trata de la lógica de circuitos, para aproximarse a la aritmética binaria, se suele utilizar el símbolo 0 para indicar *falso* en lugar de la F, y el 1 para indicar *verdadero* en lugar de la V.

Tabla de verdad de la negación

p	**¬p**
0	1
1	0

Tabla de verdad de la conjunción

p	**p**	**p∧q**
0	0	0
0	1	0
1	0	0
1	1	1

Tabla de verdad de la disyunción

p	**p**	**p∨q**
0	0	0
0	1	1
1	0	1
1	1	1

Estas tablas se materializan mediante los circuitos que representamos en las figuras 2 y 3.

Conector: disyunción **Conector: conjunción**

Figura 3

De manera análoga a como se forman proposiciones compuestas a partir de otras proposiciones, se pueden construir los *circuitos lógicos compuestos* correspondientes a proposiciones compuestas, a partir de los *circuitos lógicos elementales*.

Por composición sucesiva se han ido construyendo circuitos cada vez mas complejos hasta llegar a los modernos microprocesadores y otros dispositivos electrónicos componentes de los actuales ordenadores materializados en los microchips que contienen o integran millones de componentes biestables (conectores).

Hemos empleado en nuestra exposición para describir los circuitos elementales un dispositivo electromecánico que fue el precursor de los modernos circuitos electrónicos utilizados en los ordenadores [14]. El ingeniero español Torres Quevedo fue el primero en utilizar relais para construir máquinas algebraicas automáticas y otros dispositivos automáticos, como su jugador de ajedrez, superando con ello al matemático inglés Babagge [15], precursor de los actuales ordenadores, pero quien no pudo terminar de construir su maquina por solo disponer para ello de la tecnología mecánica, cuyas componentes eran ruedas y engranajes.

Desde el origen de las computadoras electrónicas, ha habido una sucesión de distintos dispositivos biestables con los que se han construido los conectores lógicos elementales y, a partir de ellos, los circuitos mas complejos componentes de aquellas. En cada época las caracteristicas de los dispositivos usados para construir las nuevas maquinas automáticas, han sido uno de los rasgos empleados para definir las distintas generaciones de ordenadores; esta sucesión de dispositivos pasó del *relais* a la *válvula de radio*, y de esta al *transistor*, para llegar despues a los actuales *circuitos integrados* cada vez de mayor densidad. Esta sucesión todavia no ha terminado.

Como ya hemos indicado, fue el matemático inglés George Boole el iniciador de la lógica, o cálculo, de proposiciones, pero fue el matemático americano Claude Shannon [16], quien aplicó el álgebra de Boole al diseño de circuitos de conmutacion utilizados en las centrales telefónicas automáticas. Al matemático húngaro John von Neumann [17], se debe la actual estructura de los ordenadores.

5 La formalización como cálculo.

La extensión del calculo aritmético, al álgebra clásica, al álgebra de las proposiciones y a otras lógicas, ha conducido a considerar a alguno de los aspectos formales de la matematica como cálculo, y esto ha tenido gran importancia para la definición de los sistemas formales deductivos; en particular, en la formalización de los lenguajes, no solo matemáticos (Metamatemática), sino de otros tipos de lenguajes: los lenguajes formales (o artificiales); e incluso del

[14] La utilización de los relais en la construcción de circuitos es algo que desde hace tiempo ha dejado de realizarse, y estos dispositivos están ya olvidados, pero por su claridad expositiva y por su interés histórico, los hemos usado en esta descripción de los circuitos lógicos.

[15] Charles Babagge(1792-1871), diseó una maquina *The analytical engine*, que solo construyó parcialmente aunque dedió a ello varios años. En esta maquina se introduce la idea de memoria para retener información. Aparte de ser el reconocido precursor de los actuales ordenadores, es tambien interesante indicar el esfuerzo que dedicó a la introducción las ideas de Leibniz en la Inglaterra de comienzos del siglo XIX, cuando todavia susistía, en el país británico, el monopolio del pensamiento de Newton en lo que se refiere al cálculo infinitesimal.

[16] Claude Shannon nació en Estados Unidos en 1916. Su tesis de master titulada *A symbolic Analysis of Relay and switching circuits*, se considera como fundamental para la aplicacion del algebra de Boole a la teoria de circuitos de conmutacion. Tambien es muy importante su aportacion a la teoría de la comunicación.

[17] Von Neumann (1903-1957), fue un niño prodigio; estudia matematicas en Budapest y en Berlin. Va por primera vez, como profesor visitante, a Estados Unidos en 1931, pero se traslada definitivamente en 1933 (huyendo de la situacion provocada por Alemania en Europa) al *Institute for Advances Studies* de Princeton, en donde coincide con Gödel y con Turing . Dedicó su actividad a múltiples areas de la matemática, pero su aportacion fue esencial para el desarrollo de la actual estructura de los ordenadors, especialemnete en la idea de programa almacenado, como ya lo describe en su *First Draft of a Report on de EDVAC* escrito en 1945. Tambien es uno de los creadores de la teoría de automatas y de la teoría de la programación. Es autor prolífero, entre su producción se encuentra un libro, editado en 1966 titulado *Theory of Self-Reproducing Automata*

lenguaje natural como lo está intentando la moderna lingüística y la lingüística computacional.

La contribución de Chomsky [18] al desarrollo de la lingüística, desde que apareció, en 1957, su *Syntactic Structures* , ha sido muy importante en los lenguajes naturales y también, de forma muy patente, en los lenguajes de programación. Las gramáticas formales, las gramáticas generativas y transformacionales, han dado nuevas herramientas para estos estudios.

Expongamos brevemente lo que se entiende por *lenguaje formal* y por *sistema formal*.

5.1 Lenguajes formales

La idea básica es considerar a un lenguaje como un conjunto compuesto por cadenas de longitud finita formadas por símbolos tomados de un alfabeto. Es decir, dado un alfabeto $\Sigma = \{\sigma_1, \sigma_2, ...\sigma_n\}$, decimos que $x = \sigma_{i_1}\sigma_{i_2}...\sigma_{i_m}$, (para un m dado, que llamamos longitud de x) es una cadena construida con símbolos de Σ. Si $m = 0$ tenemos la cadena llamada *vacia*, y denotada por Λ. Al conjunto formado por de todas las cadenas que se pueden construir con las letras de dicho alfabeto se le llama lenguaje universal y se le denota por Σ^* . Es evidente que el número de elementos de Σ^* es infinito numerable. Entre las cadenas, como elementos de Σ^* , se define una operación, llamada *concatenación*, mediante la cual a dos cadenas dadas $x, y \in \Sigma^*$ se le asocia otra cadena z obtenida por yuxtaposición de x, y; es decir, si $x = x_1x_2...x_p$ con $x_i \in \Sigma^*$, e $y = y_1y_2...y_q$ con $y_j \in \Sigma^*$, entonces la cadena $z = xy$, sería : $z = x_1x_2...x_py_1y_2 \ldots y_q$.

Llamamos *lenguaje* construido con el alfabeto Σ, a cualquier subconjunto L de Σ^*. Diremos que un lenguaje es finito, si es finito el número de cadenas de que consta; en otro caso diremos que es infinito. El *lenguaje vacio* no tiene ninguna cadena (que no debe confundirse con el lenguaje que solo tiene la cadena vacia).

Una vez dada esta definición tan general de lenguaje, el problema inicial que se nos presenta es como distinguir con precisión las cadenas que pertenecen a un lenguaje L de aquellas que no pertenecen. Hay dos formas de hacerlo: una consiste en dar las reglas mediante las cuales construir las cadenas que forman el lenguaje, y otra es dar un procedimiento para determinar si una cadena dada pertenece o no al lenguaje considerado. En el primer caso se trata de definir las *gramáticas formales*, o generadores, y en el otro los *autómatas* o reconocedores.

Para fijar un poco las ideas de lo que se entiende por lenguaje definido por una gramática formal, demos ligeramente algunos detalles técnicos. Una gramática es un procedimiento finito para formar o generar cualquiera de todas las posibles cadenas de un lenguaje. Formalmente diremos que una gramática es un sistema :

$$G = (V_N, V_T, P, S)$$

Donde V_N es un alfabeto llamado *vocabulario no terminal*; V_T es un alfabeto, llamado *vocabulario terminal*. Las reglas de P son de la forma $\alpha_i \to \alpha_j$, donde

$$\alpha_i \in (V_N \cup V_T)^+, \qquad \alpha_j \in (V_N \cup V_T)^*$$

[18]Noam Chomsky, nacido en Estados Unidos en 1928, es uno de los creadores de la lingüística matemática. Tambien es conocido por ser uno de los más eminentes pensadores disidentes americanos

y S, un símbolo de V_N, llamado símbolo inicial. Para generar una palabra mediante la gramática G, nos apoyamos en secuencias de cadenas de símbolos, $v_1, v_2, ...v_m$. Estas secuencias (cada una de las cuales es llamada *derivación*), se construyen del siguiente modo:

1: El primer elemento de la derivación es siempre el símbolo inicial S (es decir, siempre $v_1 = S$).

2: A partir de un elemento v_i se pasa al siguiente v_{i+1}, (donde v_i y v_{i+1} pertenecen a $(V_N \cup V_T)^+$) , mediante una regla de P, es decir, si $v_i = \delta\alpha_i\delta'$, y la regla $\alpha_i \to \alpha_j \in P$, entonces será $v_{i+1} = \delta\alpha_j\delta'$, (escribiremos $v_i \Rightarrow v_{i+1}$)

3: Si v_m, obtenida aplicando m veces el procedimiento anterior, pertenece a V_T^*, entonces decimos que v_m es una palabra generada por G.

A la derivación $S = v_1, v_2, ...v_m$, se la puede expresar:

$$S \Rightarrow v_1 \Rightarrow v_2 \Rightarrow .... \Rightarrow v_m,$$

o simplemente

$$S = * \Rightarrow v_m$$

que podría leerse: v_m se obtiene por derivación de S aplicando reglas de G, o simplemente: v_m *en una derivada de* S.

Podemos sintetizar lo anterior diciendo que el lenguaje generado por la gramática G, es:

$$L(G) = \{x | x \in V_T^*, S = * \Rightarrow x\}$$

Decimos que dos gramáticas son equivalentes, si y solo si generan el mismo lenguaje, es decir

$$G_1 \equiv G_2 \Leftrightarrow L(G_1) = L(G_2)$$

5.2 Sistemas formales

La pretensión de formalización del pensamiento, que se inició con la osadía de Boole al pretender haber encontrado "las leyes del pensamiento", dió origen a un interés renovado por la lógica y a la aparición de la lógica matemática [19]

[19] La aparición (y su consolidación a principios del siglo XIX) de la geometría proyectiva y de las geometrías no euclideas hacen concebir nuevas geometrías que no están en armonía con nuestra intuición del espacio que obligan a una revisión del sistema lógico de Euclides (especialmente su sistema de axiomas), revisión que tiene gran trascendencia en el posterior desarrollo de la matemática y en la aparición de una nueva forma de entender la lógica que viene a confluir con el desarrollo de la lógica inglesa en la que se busca la expresión del pensamiento mediante símbolos para llegar a constituirse lo que actualmente se llama *lógica matemática*.

(Morgan [20] , Frege [21], Russell [22], Hilbert[23]), que se inicia en la segunda mitad del siglo XIX, y que incide de forma determinante en la moderna fundamentación de la matemática, y en el desarrollo de la teoría de conjuntos (Peano, Cantor).

La idea de formalización de una teoría es la que brevemente exponemos a continuación.

Definimos a un *sistema formal*, como una cuádrupla:

$$S = (\Sigma, F, A, R)$$

donde sus elementos los interpretamos como sigue:

Σ : es un *alfabeto.*

F : es un subconjunto recursivo de Σ^*, llamado conjunto de *fórmulas* ($F \subseteq \Sigma^*$).

A: es un subconjunto recursivo de F, cuyos elementos reciben el nombre de *axiomas.* ($A \subseteq F$).

R: es un conjunto finito de *reglas de inferencia*, de la forma $R_i(x_1, x_2, ...x_m; y)$, cuyas variables tomarán valores en F. En estas reglas se dice que la fórmula y se obtiene a partir de las $x_1, x_2, ...x_m$ mediante R_i , o que y es *consecuencia* de $x_1, x_2, ...x_m$.

Dado un sistema formal S, decimos que d es una *demostración* en S, si d es una secuencia finita de fórmulas

$$x_1, x_2, x_3, ...x_n$$

que comienza con un axioma ($x_1 \in A$), y en la que cualquier elemento posterior o es un axioma o se puede deducir a partir de otros elementos que ya están en la demostración.

Decimos que una formula x_n es un teorema de S , si y sólo si existe una demostración

[20] Augustus De Morgan(1806-1871) matemático inglés que se educó en la Universidad de Cambridge pero de la que no pudo obtener los grados por negarse a firmar la declaración teológica a que estaban obligados los candidatos antes de recibirlos. Aunque publicó varios trabajos sobre los fundamentos del álgebra y sobre probabilidades, han tenido gran repercusión sus trabajos sobre lógica. En 1847 apareció su *Formal Logic or the Calculus of Inference necessary and probable.*

[21] Friedrich Frege (1848-1925) matemático alemán que dedicó su principal actividad a intentar probar que la matemática se puede reducir a la lógica (*logicismo*). En 1884 publica un libro sobre los fundamentos de la Aritmética (*Die Grundlagen der Aritmetik*) y en 1893 otro sobre las Leyes básicas de la aritmética (*Grundgesetze der Aritmetik*); la *paradoja de Russell* mostró inconsistencia en el sistema axiomático de Frege, quien se vió obligado a modificarlo.

[22] Bertrand Russell (1872-1970) lógico inglés, autor, en colaboración con Whitehead, de uno de los libros más importantes de lógica mátematica titulado *Principia Mathematica*(1910). Es muy importante el papel que ha jugado en el desarrollo de la lógica la llamada *paradoja de Russell* que tiene que ver con el conjunto de todos los conjuntos que no pertenecen a ellos mismos. Su logicismo le hace llegar a considerar que el conjunto de todos los teoremas de la matemática constituyen un subconjunto de los teoremas de la lógica. Tambien es muy conocido como filósofo y por su activismo pacifista creador del llamado *tribunal Russell.*

[23] David Hilbert (1862-1943) matemático alemán. Su trabajo constituye una de las mayores aportaciones al desarrollo de las matemáticas en el siglo XX. Su axiomatización de la geometría le condujeron al estudio de problemas lógicos. Publicó en colaboracion de Ackermann unos elementos de lógica teórica (*Grundzüge der Theoretischen Logik*) en los que busca probar la consistencia de las matemáticas.

$$d \equiv x_1, x_2, ...x_n$$

.

Un ejemplo de sistema formal para la lógica proposicional, es el que damos en la nota [24], en donde tambien se da un ejemplo de demostracion formal.

Con el desarrollo de los sistemas formales se abrió la espectativa de poder reducir la demostración a cálculo, y con ello se produjo una gran esperanza que llevó a la búsqueda de la pretendida demostración automática, es decir de procedimientos para la definición de algoritmos capaces de construir la secuencias de fórmulas que formen una demostración. Pero pese a que esta búsqueda hizo avanzar la lógica matemática con algunos éxitos [25] estos no lograron el intento de alcanzar la demostración automática, imposibilidad que dejaron patentes los limitadores teoremas de Godel [26] que básicamente dicen que, en general, los

[24] Una formalización de la lógica proposicional podria darse mediante el siguiente sistema:

$$S = (\Sigma, F, A, R)$$

donde el alfabeto viene dado por

$$\Sigma = \{p, q, r, p_1, q_1, r_1, ... \Rightarrow, \neg, (,)\}$$

El conjunto de fórmulas F le definimos inductivamente como sigue:

1 : Toda letra (llamada variable) del alfabeto : $\Sigma - \{\Rightarrow, \neg, (,)\}$ es una fórmula.

2 : Si x es una fórmula, entonces $\neg x$ es una fórmula.

3 : Si x, y, son fórmulas, entonces $(x \Rightarrow y)$, es una formula.

4 : Una palabra x es una fórmula, si y solo si se obtiene a partir de 1,2,3.

El conjunto A de axiomas es el siguiente:

$$\begin{array}{l} A = \{(p \Rightarrow (q \Rightarrow p)), \\ ((p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)), \\ ((\neg p \Rightarrow q) \Rightarrow (q \Rightarrow p)) \end{array}$$

Las reglas de inferencia R, son las siguientes, en donde x , $y \in F$,

$$R = \{R_1(x, (x \Rightarrow y), y), \quad R_2(y, x, x(y|q)\}$$

en donde con $x(y|q)$ queremos indicar la fórmula que se obtiene a partir de la fórmula x, cuando se sustituye toda aparición de la variable q en x por la fórmula y (poner y donde aparezca q).

Con este sistema, probar que la formula $(p \Rightarrow p)$ es un teorema, es construir una demostración como la siguiente:

$$\begin{array}{ll} x_1 \equiv ((p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))) & \text{axioma} \\ x_2 \equiv ((p \Rightarrow (q \Rightarrow p)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow p)) & R_2(p, x, x_1(p/r)) \\ x_3 \equiv (p(q \Rightarrow p)) & \text{axioma} \\ x_4 \equiv ((p \Rightarrow q) \Rightarrow (p \Rightarrow p)) & R_1(x_3, x_2, x_4) \\ x_5 \equiv ((p \Rightarrow)(q \Rightarrow p)) \Rightarrow (p \Rightarrow p)) & R_2(q \Rightarrow p, x_4, x_4(q \Rightarrow p/q)) \\ x_6 \equiv (p \Rightarrow p) & R_1(x_3, x_5, x_6) \end{array}$$

[25] Veanse las notas 4, 5 y 6.

[26] Kurt Gödel (1906-1978), matemático austriaco, profesor de la Universidad de Viena; emigró a Estados Unidos en 1940; allí ejerció como profesor del *Institute for Advanced Study*, donde coincidió con von Neumann y con Einstein. Son muy importantes sus trabajos sobre la teoría de la demostración matemática, que dió a conocer en 1931, en los que de forma rigurosa establece las limitaciones de la teoría axiomática de conjuntos y termina con los intentos que, desde mediados del siglo anterior, se hicieron para probar la consistencia de la formalización de las matemáticas.

sistemas formales o son *incompletos*, o son *inconsistentes*; es decir, en el primer caso se trataría de sistemas que contienen fórmulas para las que no existe una demostración (en el sentido formal), y en el segundo, que contienen fórmulas para las que existe una demostración y también para su negación. Con este planteo renacen y vuelven a aparecer los fantasmas que llevan consigo los dilemas y las aporías lógicas. (Desde las antiguas del mentiroso, del barbero, la del puente y la horca, y las mas recientes como las vinculadas con la teoría de conjuntos como la de Russell, de la que ya hemos subrayado su importancia mas arriba.)

Estos avances pusieron cota a la ilusión de que todo sea calculable. Y si no todo es calculable surgen las preguntas, ¿qué se puede calcular? ¿dónde están los límites de la calculabilidad?.

6 Calculabilidad

Para dar respuesta a estas preguntas lo primero que hay que estudiar, y definir con precisión, es que se entiende por cálculo, y por algoritmo, conceptos estos que se han venido utilizando desde el Renacimiento, sin ser sometidos a la necesaria crítica, (como hemos expuesto en las paginas anteriores), pero que a partir de los descubrimientos de Gödel, era imprescindible que se aclararan, pues ya se había perdido definitivamente la esperanza, acariciada por Raimundo Lulio [27], y también pretendida por Leibniz, de que ante cualquier situación conflictiva, en la que se presentase una discrepancia entre personas, esta se resolviese, en vez de utilizar discusiones acaloradas, mediante el cálculo (calcular en lugar de discutir).

En los años 30 del siglo XX, varios lógicos matemáticos [28], inician la tarea de definir con precisión lo que se entiende por *calculabilidad*, profundizando en las ideas de algoritmo y de función calculable, dando como resultado los conceptos de *funciones recursivas*, y de *máquinas de Turing*. En el primer caso se trata de encontrar las funciones calculables más simples posibles a partir de las cuales por composición y por recursión se van obteniendo las demás funciones que pueden ser efectivamente calculables o computables. En el segundo caso se trata de definir máquinas compuestas por conjuntos de instrucciones de la mayor sencillez posible con la finalidad de obtener de forma efectiva el resultado de una función calculable.

6.1 Funciones recursivas

Vamos a ver como se construye una clase de funciones, llamadas *recursivas primitivas*, definidas entre n-uplas de números naturales sobre los números na-

[27] Ramon Llull (1235-1315) mallorquín, es uno de los sabios y místicos mas notables de la Edad Media, cuando comenzaba vislumbrarse el Renacimiento. Se le atribuyen el conocimiento temprano de la brújula y la invención de los protulanos. Su aportación a los inicios de una lógica simbólica es universalmente reconocida. Es autor del *Ars Magna combinatoria* y del *Arbre de sciencia* y de un trabajo sobre el arte de encontrar la verdad (*Arte abreujada de trobar la veritat).*

[28] Son varios los enfoques que se han dado para obordar los problemas surgidos en torno a la computabilidad, planteados tras los teoremas limitadores de Gödel. Los matemáticos que se han dedicado principalmente a este tema son, entre otros, Church, Turing, Kleene, Post, Davis.

turales [29], (es decir $f : N^n \rightarrow N$), con la idea de caracterizar las funciones que son efectivamente calculables, es decir, aquellas funciones para las que dada la n-upla de sus argumentos podemos definir un procedimiento para encontrar en un numero finito de pasos el valor de la función.

Usaremos para ello una definición recursiva, es decir, nos apoyaremos en un conjunto de funciones que por definición son recursivas (conjunto inicial que se denomina *base de la recursión*), y en un conjunto de reglas que aplicándolas a funciones recursivas primitivas ya definidas obtenemos nuevas funciones recursivas. En nuestro caso la base esta formada por las funciones *nula*, *sucesor* y *proyección*, y las reglas que llamamos de *composición* y de *recursión primitiva*. Estos elementos quedan definidos de la siguiente forma:

Base de recursión:

Función nula $N(x) = 0$ **:** mediante la que se hace corresponder a cualquier numero natural el numero 0 (borrar el numero).

Función sucesor $S(x) = x'$ **:** mediante la cual a cada numero natural x se le hace corresponder su sucesor, que denotamos por x' (encontrar el siguiente).

Función proyección $I_i^n(x_1, x_2, \ldots x_i, \ldots x_n) = x_i$ **:** mediante la cual a cada n-upla se le hace corresponder su i-esima componente (elegir uno de una sucesión finita)

Reglas:

Regla de composición **:** dadas las funciones

$$g_i(x_1, x_2, ..., x_n), \qquad (i = 1, 2, ...m)$$

y la función f que depende de las m funciones anteriores, es decir

$$f = (g_1, g_2, ..., g_m),$$

entonces decimos que

$$h(x_1, x_2, ..., x_n)$$

es la función compuesta de las g_i mediante f si está definida de la siguiente forma:

$$h(x_1, x_2, ..., x_n) = f(g_1(x_1, x_2, ..., x_n), g_2(x_1, x_2, ..., x_n), ...g_m(x_1, x_2, ..., x_n))$$

Regla de recursion primitiva con parametros**:** dadas dos funciones recursivas conocidas

$$f(x_1, x_2, ..., x_n),$$

[29] Aparte del interés intrinseco de las funciones definidas entre numeros naturales, estas toman una gran importancia en la lógica a partir de la llamada *numeración de Gödel* que consiste en un procedimiento mediante el cual a toda expresión lingüistica se le asocia de forma única un número natural

$$g(y, x_1, x_2, ..., x_n, z),$$

que dependen de los parámetros $x_1, x_2, .., x_n$, se define la función

$$h(y, x_1, x_2, .., x_n),$$

mediante el siguiente esquema de recursión:

$$h(0, x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n)$$

$$h(y', x_1, x_2, ..., x_n) = g(y, x_1, x_2, ..., x_n, h(y, x_1, x_2, ..., x_n))$$

***Regla de recursion primitiva sin parametros*:** es un caso particular del anterior en el que no aparecerán los parámetros y el esquema de recursión sería:

$$h(0) = k$$

$$h(y') = g(y, h(y))$$

donde $g(y, z)$ es una función recursiva conocida y k es una constante (un numero natural dado).

La clase de funciones definidas de esta manera, es una clase de funciones que se puede calcular efectivamente, ya que son construidas a partir un conjunto base, cuyo cálculo puede ser considerado trivial, y mediante procedimientos o esquemas de cálculo sencillos y que se realizan por pasos sucesivos [30]. Se prueba que esta clase de funciones es la misma que la que se define utilizando para ello las Maquinas de Turing, que describimos a continucion.

[30] Para ver como se construyen estas funciones, pongamos algunos ejemplos sencillos, que solo utilizan funciones de la base, o de las ya construidas en alguno de estos mismos ejemplos. *Suma* $h(x, y) = x+y$ Esta función la construimos apoyándonos en las funciones f, g definidas de la siguiente manera

$$f(x) = I_1^1(x)$$

$$g(y, x, z) = S(I_3^3(y, x, z))$$

que son recursivas por emplear funciones de la base y la regla de recursion primitiva, tendríamos el siguiente esquema de recursión primitiva con el parámetro x

$$h(x, 0) = I_1^1(x)$$

$$h(x, y') = g(y, x, h(x, y)) = S(I_3^3(y, x, z))$$

en otras palabras

$x + 0 = x$	x más 0 es igual a x
$x + y' = (x + y)'$	x más el siguiente de y es igual al siguiente de $x + y$

Producto $h(x, y) = xy$ En este caso hacemos

$x0 = 0$	x por 0 es igual a 0
$xy' = xy + x$	x por el siguiente de y es igual a x por y más x

Factorial $h(y) = y!$ En este caso, por recursión primitiva sin parámetros, haciendo $k = 1$, y que la función $g(y, h(y))$ sea el producto, tenemos que $g(y, h(y)) = yh(y)$, luego

$$h(0) = 1$$

$$h(y') = yh(y)$$

o sea:

$0! = 1$	factorial de 0 es igual a 1
$(y')! = y!y'$	factorial del siguiente de y es igual a factorial de y por el siguiente de y

6.2 Maquinas de Turing.

Otra forma de caracterizar la clase de las funciones computables se hace mediante las llamadas *máquinas de Turing* [31] . Estas son máquinas formales, es decir sin cables ni componentes físicos. Su finalidad es definir los cálculos a partir de las operaciones más sencillas posibles, y utilizando las cuales calcular efectivamente funciones dadas. Las funciones que así pueden realizarse se llaman *funciones calculables* o *computables*.

Este tipo de máquina consta hipoteticamente de una unidad de control capáz de interpretar las instrucciones que reciba, y de una cabeza lectora que permite leer el contenido de una de las casillas en que esta dividida una memoria lineal, ilimitada en ambas direcciones de sus extremos.

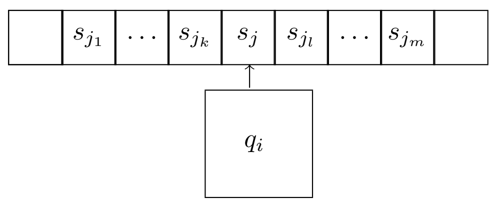

Figura 4

La máquina en su funcionamiento pasa por diferentes estados q_i en instantes t sucesivos. El argumento de la función que queremos calcular estará almacenado previamente en la memoria, y en el instante inicial, antes de que la máquina comience a funcionar, la cabeza lectora apuntará al símbolo más a la izquierda del argumento. A partir de ese momento la máquina realizará operaciones, que dependerán del estado en que ella se encuentre, y del símbolo que en ese momento lea la cabeza lectora. Con estas operaciones se podrán realizar las siguientes atreas: sustituir el símbolo leído por otro, pasar a leer el símbolo que esta en memoria a la derecha del símbolo leído, pasar a leer el símbolo que esta en memoria a la izquierda, o saltar directamente a ejecutar otra instrucción si se cumple una condición especificada [32]; en todos los casos, y una vez ejecutada la tarea indicada, se pasaría al estado que tambien se indica en la propia instrucción.

Estas instrucciones, o cuaternas, las podemos representar e interpretar así:

[31] Alan Turing (1912-1954), es un matemático inglés, que se graduó en Cambrige (UK), e hizo su doctorado (1931) en Princeton , donde coincidió con von Neumann y Gödel durante su estancia como profesor entre 1936 y 1938. Son esenciales sus trabajos sobre computación que se expresan mediante su máquina como un formalismo teórico. Tambien es conocido por sus trabajos de criptofrafía que desarrolló en el mítico laboratorio de Bletchley Park (1939-45) donde se construyó la máquina *Colossus* para desencriptar los mensajes cifrados por los alemanes mediante la maquina germana *Enigma*.

[32] Las máquinas de Turing que contienen cuaternas de este tipo se llaman *no simples*, o máquinas con "oráculo", elemento externo a la propia máquina que hay que consultar para tomar la decisión antes de ejecuatar este tipo de cuaternas.

$q_i\ s_j\ s_k\ q_l$:	si estando en el estado q_i se lee el simbolo s_j, entonces s_j se cambia por s_k y se pasa al estado q_l
$q_i\ s_j$ R q_l :	si desde q_i se lee s_j, entonces se pasa a leer la casilla situada a su derecha y se cambia al estado q_l
$q_i\ s_j$ L q_l :	si desde q_i se lee s_j, entonces se pasa a leer la casilla a su izquierda y se cambia al estado q_l
$q_i\ s_j\ q_k\ q_l$:	si desde q_i se lee s_j, entonces se cambia al estado q_k o al q_l según una cierta condición

donde: q_i indica un estado de la máquina tomado del conjunto de estados Q; s_j indica uno de los símbolos que pueden aparecer en la memoria tomado del alfabeto S; R es un símbolo que indica pasar a leer la casilla de memoria situada a la derecha; L es un símbolo que indica pasar a leer la casilla de memoria situada a la izquierda.

Se define una *máquina de Turing* (M) como un conjunto finito, no vacío, de cuaternas, de forma que no contenga dos cuaternas con los dos primeros símbolos correspondientes iguales.

Indicaremos por $Q = \{q_i\}$ al conjunto de estados de la máquina, por $S = \{s_j\}$ al alfabeto de símbolos de la memoria.

En Q siempre existe un estado particular, que se suele indicar por q_0 y llamarse *estado inicial*, en el que se supone está la máquina al comenzar a operar. En el alfabeto S siempre figurarán, entre otros posibles, dos símbolos: el blanco (B), y el uno (expresado por un palote |) . A las cadenas formadas por símbolos de este alfabeto se las llama *expresiones de memoria*. Si en una expresión de memoria incluimos un único símbolo q_i (que indique un estado de Q) siempre que no le situemos a la derecha de cualquier otro, obtendremos una expresión que llamaremos *descripción instantánea* de la maquina M.

Los números naturales se representan en estas máquinas, de la forma más simple, es decir usando un solo símbolo (|). Se emplean dos clases de representación numérica; una llamada *de entrada* mediante la cual con un solo palote representaremos el cero, y cualquier otro número n se representará por $n + 1$ palotes; y la otra, llamada *de salida*, consiste en contar el número de palotes que hay en la expresión de memoria (ningún palote se interpretaría, en este caso, como el 0).

La descripción instantánea de la maquina M en el instante inicial podría representarse por

$$q_0\, s_{i1}\, s_{i2}\, s_{i3} \ldots s_{in}$$

En cualquier otro instante una descripción instantánea sería de la forma

$$\alpha = s_{j1}\ \ldots s_{jk}\, q_i\, s_j s_{jl}\ \ldots s_{jm}$$

Para ver como funciona una máquina de Turing, veamos como se realizan las transiciones de unas descripciones instantaneas a otras. Dada una descripción instantanea α , en la que aparezcan el par de símbolos $q_i\ s_j$, buscaríamos la cuaterna de la máquina que comience con estos dos símbolos y operaríamos en consecuencia, es decir, para cada uno de los tipos de cuaternas, construiríamos la descripción instantánea siguiente, β, como indicamos a continuación:

para	$q_i s_j s_k q_l$	sería	$\beta = s_{j_1} \ldots s_{j_k} q_i s_k s_{j_l} \ldots s_{j_m}$
para	$q_i s_j R q_l$	sería	$\beta = s_{j_1} \ldots s_{j_k} s_j q_i s_{j_l} \ldots s_{j_m}$
para	$q_i s_j L q_l$	sería	$\beta = s_{j_1} \ldots q_i s_{j_k} s_j s_{j_l} \ldots s_{j_m}$
para	$q_i s_j q_k q_l$	sería	$\beta = s_{j_1} \ldots s_{j_k} q_k s_j s_{j_l} \ldots s_{j_m}$ si el número representado por cinta en ese instante *pertenece* a un conjunto dado A , o bien $\beta = s_{j1} \ldots s_{jk} q_l s_j s_{jl} \ldots s_{jm}$ si el número representado por la cinta en ese instante *no pertenece* a un conjunto dado A

En el último caso aparece el conjunto A, que es un conjunto de números naturales, que no forma parte de la máquina, y al que hay que consultar antes de tomar la decisión sobre una de las alternativas propuestas (es el "oráculo" a que nos referiamos en una nota de la pagina anterior).

Si no existiese en M ninguna cuaterna que comenzase por $q_i s_j$ diríamos que la descripción instantánea α es *terminal*.

En cualquiera de los casos anteriores decimos que de la descripción instantanea α se pasa a la β mediante la maquina de Turing M, lo que se denota $\alpha \rightarrow \beta(M)$.

Llamamos computación o cálculo de una máquina de Turing M, a una sucesión finita de descripciones instantáneas $\alpha_1, \alpha_2, \ldots \alpha_n$, de forma que para $1 \leq i < n$, sea $\alpha_i \rightarrow \alpha_{i+1}(M)$, y sea α_n , una descripción instantánea terminal.

Para calcular una función $f : N^n \rightarrow N$, mediante una maquina de Turing, se comenzará representando la n-upla de los argumentos mediante una expresión de memoria de la forma $||..|B||..|B||..|B...B||..|$, a partir de la cual se formará la descripción instantánea inicial

$$\alpha_1 = q_0||..|B||..|B||..|B...B||..|,$$

a la que se aplicaran sucesivamente las cuaternas que correspondan de la maquina de Turing hasta llegar a una descripción instantánea terminal. En esta contamos el numero de palotes que contiene, y este será el valor de la función. [33]

[33] Veamos como ejemplo, el funcionamiento de una máquina para sumar dos enteros. Dada la función $f(x, y) = x + y$, existe una maquina de Turing que la calcula, compuesta por las siguientes cuaternas:

$$\{q_0 \mid B\ q_0, \quad q_0\ B\ R\ q_1, \quad q_1 \mid R\ q_1, \quad q_1\ B\ R\ q_2, \quad q_2 \mid B\ q_2\}$$

Esta maquina tiene como conjunto de estados

$$Q = \{q_0, q_1, q_2\},$$

como estado inicial a q_0 , y como alfabeto a

$$S = \{|, B\}$$

Para sumar 3 + 5 , procederíamos así:

1) La descripción instantánea inicial es $q_0 \,|\,|\,|\,|\, B \,|\,|\,|\,|\,|\,|$, que contiene la representacion del par de números 3 y 5 , usando la *representación de entrada*.

2) Los pasos sucesivos del cálculo, usando la máquina anterior son:

Dada una función $f : N^n \to N$, no siempre existe una Máquina de Turing, mediante la cual, a partir de cualquier argumento, podamos llegar desde el estado inicial a una descripción instantánea terminal; cuando existe una tal máquina decimos que la función es *computable*.

7 Conclusión: Las máquinas automáticas

Hasta aquí hemos dado un sucinto panorama de la evolución del papel jugado por la matemática en los fundamentos y orígenes de la informática. Como hemos visto, este papel ha consistido en la búsqueda de automatismos de cálculo, desarrollando para ello aparatos teóricos cada vez mas potentes.

Aunque entre matemática e informática existen muchos otros vínculos, en el marco de una conferencia solo se puede aludir a alguno de los aspectos que relacionan a ambas disciplinas. Por ejemplo, también debería haberse tenido en cuenta el aspecto reciproco, es decir, considerar que si la matemática ha sido el fundamento teórico que ha permitido la aparición y desarrollo de la informática, también la informática brinda ahora un potente instrumento de cálculo que facilita el estudio de ciertos problemas matemáticos que hasta ahora no habian podido abordarse con éxito, como ocurre, entre otros muchos, con varios problemas de topología y de teoría de números. Este tema de la informática como auxiliar en la investigación de algunos problemas matemáticos, es un tema importante que requiere una atención específica.

Pero no queremos terminar sin subrayar el hecho, que resulta realmente sorprendente, de cómo estos estudios teóricos encaminados a encontrar procedimientos de cálculo se hayan materializado en máquinas, con cierta autonomía para actuar, que pueden permitir al hombre liberarse de los trabajos repetitivos y mecanicos, (características estas que son las que mejor definenen a los cálculos), para poder dedicarse a tareas creativas mas propias de la complejidad de la naturaleza humana, alcanzada tras millones de años de una evolución natural todavía inconclusa.

$q_0 \mid\mid\mid\mid B \mid\mid\mid\mid\mid\mid$	descripción instantanea inicial
$q_0\, B \mid\mid\mid B \mid\mid\mid\mid\mid\mid$	obtenida al aplicar la cuaterna $q_0 \mid B\ q_0$
$B\, q_1 \mid\mid\mid B \mid\mid\mid\mid\mid\mid$	obtenida al aplicar la cuaterna $q_0\ B\ R\ q_1$
$B \mid q_1 \mid\mid B \mid\mid\mid\mid\mid\mid$	obtenida al aplicar la cuaterna $q_1 \mid R\ q_1$
$B \mid\mid q_1 \mid B \mid\mid\mid\mid\mid\mid$	obtenida al aplicar la cuaterna $q_1 \mid R\ q_1$
$B \mid\mid\mid q_1\, B \mid\mid\mid\mid\mid\mid$	obtenida al aplicar la cuaterna $q_1 \mid R\ q_1$
$B \mid\mid\mid B\, q_2 \mid\mid\mid\mid\mid\mid$	obtenida al aplicar la cuaterna $q_1\ B\ R\ q_2$
$B \mid\mid\mid B\, q_2\, B \mid\mid\mid\mid\mid$	obtenida al aplicar la cuaterna $q_2 \mid B\ q_2$, que es *terminal* por no existir en M ninguna cuaterna que comience por $q_2\ B$

3) Como en la máquina dada no hay ninguna cuaterna que comience por q_2 B, la máquina se detiene y por tanto la expresión $B \mid\mid\mid B\, q_2\, B \mid\mid\mid\mid\mid$, es una descripción instantánea terminal, y el resultado, utilizando la *representación de salida*, es el número de $\mid$ que existen en ella , es decir 8.

Los automatismos, que eran realizados al principio directamente por el hombre, han ido materializandose paulatinamente hasta convertirse en herramientas cada vez mas participativas, que han ido aportando, con eficacia creciente, su colaboracion en la realización de esos cálculos. En esta evolución de la materialización de los procedimientos se ha llegado, a mediados del siglo XX, a la construcción de máquinas en las que cada vez intervienen menos, de forma directa, las personas.

En efecto, aunque a lo largo de nuestra conferencia hemos aludido varias veces a algunos dispositivos físicos utilizados por el hombre como herramienta de cálculo (ábaco, regla y compás, máqinas aritméticas, regla de cálculo, ...), no podemos considerar todavía a estos dispositivos como máquinas automáticas, ya que ninguno de ellos funciona sin que el hombre opere directamente sobre los mismos.

Los primeros ejemplos que suelen citarse como dispositivos físicos automáticos (entendiendo aquí automatismo como la ausencia de intervención humana en la ejecución de un proceso) son el telar de Jaquard (1752-1834), y el regulador de Watt (1736-1819). Aquél, por que es la primera máquina capaz de leer información previamente grabada en una tarjeta perforada (dispositivo digital) y realizar por sí misma las operaciones indicadas en esa información; y el segundo porque es capáz de medir directamente una magnitud física (la presión del vapór de la caldera) mediante un dispositivo analógico, y cambiar su comportamiento de acuerdo con esa medida.

Este es un nuevo enfoque del concepto de automatismo, en el que lo característico es la existencia de máquinas con capacidad para recibir información y de ajustar su comportamiento de acuerdo con la información recibida . La importancia de este nuevo concepto consiste en el decubrimiento de sistemas, tanto digitales como analógicos, en los que que la información puede depositarse, circular y ser interpretada por y en dispositivos materiales fuera del sistema nervioso humano. Han aparecido en torno a este concepto dos nuevas disciplinas: la *Teoría de la Información*[34] y la *Cibernética* [35] . La *cibernética* es una de las disciplinas que estudia el comportamiento de estos sistemas de información, en los que la realimentación y homeostasis son dos de los factores siempre presentes en los mismos. La *teoría de la información* estudia los aspectos matematicos de la informacion. Estas nuevas disciplinas que han abierto nuevos campos de estudio a la matemática, y la relacionan con la informática, considerada esta última en su sentido más amplio.

Asi se llega a percibir que la *información* se comporta como un elemento físico, material, externo al hombre, análogo a la *materia* o a la *energía* [36] , y

[34]Claude Shannon,el matemático norteamericano que uso el algebra de Boole en el diseño de circuitos fue tambien el creador de la teoría matemática de la información. Fue profesor en el MIT y colaboró con los *Bell Laboratories.* En 1948 publicó en el *Bell Sydtem Technological Journal* un artículo titulado *A mathematical theory of Communication*, que al año siguiente amplió en colaboración con Weaver y publicó en forma de libro con el mismo titulo.

[35]El matemático norteamericano Norbert Wiener es considerado el padre de la Cibernética, teoría que difunde en un libro titulado *Cybernetics, or control and communication in the animal and the machine*, publicado en 1948. Fue profesor de matemáticas en el MIT (1932-1960).

[36]Es un hecho trasdendental considerar a la informacion en su naturaleza fisica, analoga a la materia y a la energia. En la comparación y relación de la información con la energía recordemos la fabula del diablillo de Maxwell que contradice al Segundo principio de la Termodinámica, y cómo la negantropía es un concepto equivalente al de información. También es un hecho evidente que la información ahorra energía.

este hecho, de aparición tan reciente (apenas 200 años), es de una transcendencia tal, que está modificando de forma radical la estructura de las sociedades humanas. En estas modificaciones están incidiendo de forma muy notable los sistemas cibernéticos , de complejidad creciente, que podríamos agrupar en dos grandes categorías y denominar simbólicamente a cada una de ellas como *maquina sapiens* y *maquina faber*, así como las redes de comunicación que los interconectan.

La actividad inteligente del hombre le ha conducido al descubrimiento de cálculos y algoritmos para no tener que pensar en como actuar cada vez en que se presentan las mismas condiciones, de manera que una vez pensado el procedimiento este se reduce a una sucesión de reglas que aplicadas correctamente nos llevan con certeza a obtener el resultado deseado. Ya hemos visto como la materialización de estos procedimientos nos han conducido a la aparición del ordenador y de otros dispositivos automáticos. Durante siglos el hombre era el único capáz de operar estos instrumentos. Solo desde hace unas decadas puede decirse que esos instrumentos y dispositivos han alcanzado un nivel de desarrollo suficiente para poder interpretar directamente la informacion y los algoritmos y, de acuerdo con ellos, actuar sin la atención humana directa. El ordenador es el máximo exponente de este tipo de dispositivos, aunque no el único ni será el último. Pero estos dispositivos solo actuan sobre información, solo es información lo que transforman y transportan. Esta característica de este tipo de máquinas y dispositivos es la nos permite denominarla, abusando evidentemente de la expresión, como *máquina sapiens*. Estas maquinas facilita el acceso a la informacion [37] y a la cultura y permite la cooperacion intelectual de las personas.

Pero el hombre no solo actua sobre la *información*, actua tambien sobre la *materia*, la transforma y la transporta, y para ello necesita *energía*. En la transformación de la materia el hombre ha usado de forma directa su energía corporal, su fuerza física, así como de la información que como individuo poseía sobre los procesos de transformación. También desde épocas remotas recurrió a pensar procedimientos para incrementar el resultado de su fuerza, pensamiento que fue materializandose en herramientas, instrumentos y otros dispositivos que se convirtieron en máquinas productivas cada vez mas elaboradas. A la clase de esta gran familia de dispositivos productivos es a la que podemos llamar *maquina faber*.

La conjunción entre estas dos clases de máquinas ha hecho aparecer otras de nuevo tipo (nos referimos al *robót*, que puede considerarse como un ordenador dotado de fuerza y movilidad) que ya desde los años 50 [38] se preconizaba como el elemento básico para el desarrollo de la *automación*, es decir de la producción automática total. Este vaticinio no se ha producido, pero no por dificultades

[37] La posesión de información está dejando de ser un hecho singular, reservado a pocos, y dejando de constituir un privilegio, para pasar a ser accesible a todos y para poder circular sin la necesidad de la presencia del hombre. El efecto multiplicador de esta circunstancia es todavía inconcebible.

[38] En la primavera de 1956 asistí en Milán a un *Convegno internazionale sui problemi dell'automatismo* organizado por el CNR italiano. Fue un magno cogreso internacional (en el que participaron 15 paises entre ellos también la URSS) y cuyos trabajos se recogen en tres volúmenes; el primero dedicado a los aspectos científicos y técnicos, pero es curioso que los otros dos extensos volumenes ya se dedicaran a las implicaciones sociales de esta nueva disciplina; el volumen segundo se titula *Posibilitá Tecnico-economiche*, y el tercero *Riflessi Economico-sociali*.

tecnicas insuperables, sino para evitar los cambios sociales que esos cambios tecnológicos acarrearían.

Vemos, pues, como el hombre en su desarrollo intelectual, y a lo largo de su producción técnica y cientifica, especialmenete matemática, ha ido creando dispositivos para liberarse de los trabajos repetitivos y mecánicos, simbolizados por la informática, para alcanzar así la posibilidad de dedicarse a tareas más propiamente humanas.