Introducción y antecedentes históricos

Primeros algoritmos

Si consideramos que una serie de actos encaminados a realizar un cálculo es un algoritmo, entonces las acciones de correspondencia biuniquivoca utilizadas para establecer el número de cosas de un grupo desconocido utilizando otro grupo conocido, se podrían decir que fueron los primeros Algoritmos de la antigüedad. Avanzando en el tiempo hasta los primeros algoritmos documentados, podemos encontrar constancia de sistemas de numeración posicional **sexagesimal** (base 60) sin el cero perteneciente a los **Babilonios de Mesopotamia**. Conocían ya, al menos, las cuatro operaciones básicas. Se conserva una tablilla de arcilla en escritura cuneiforme una división que se considera la prueba más antigua conservada de la aplicación de un algoritmo. También conocían el algoritmo para el cálculo para aproximaciones sucesivas de **raíces cuadradas y ecuaciones cuadráticas e incluso cúbicas**.

Hacia el oeste encontramos en **Egipto** un sistema de numeración no posicional sin el cero con una **escala numérica decimal**. Usaban **fracciones unitarias** y la fracción 2/3 para descomponer otras fracciones en ellas. Otras civilizaciones como China llegaron a calcular el valor de π, en **India** estaba asentado un sistema de numeración en **base diez, posicional y tenía cero** asi como la elaboración de las **tablas de la función trigonométrica seno**. Este sistema de numeración sería heredado por los Árabes y posteriormente por Occidente, facilitando el cálculo con lápiz y papel.

Origen de la palabra Algoritmo

En el siglo 8, el califa de Bagdad Hârûn fundó **"La casa de la Sabiduría"**, impulsado por su hijo como un lugar para el desarrollo y protección del saber y de los sabios. Durante muchos años fue el foco intelectual del mundo, entre ellos algunos con gran importancia desde el punto de vista algorítmico. El origen de la palabra algoritmo viene de **Mohamed ibn Musa**, cuya forma original era **algorismo**. Mohamed tiene contribuciones en astronomía, geografía, historia y álgebra.

Procedimientos generales

Sabemos que la matemática Mesopotamica influyó a los Árabes y estos a su vez transmitieron sus conocimientos a España y el resto de Europa. En concreto, **Raimundo Luio** fue de peregrinación a Tierra santa, donde se cruzó con la matemática Árabe y sus obras. Los métodos algorítmicos de esas obras le inspiraron a crear su obra **"Ars Magna"**, donde describe un procedimiento combinatorio para hallar todas las "verdades" (motivación religiosa). Este perseguía construir un lenguaje formal lo más amplio posible para expresar cualquier procedimiento, de tal forma que fuera inequívoco referirse a él sin duda alguna.

El trabajo de Lulio tuvo gran influencia en la matemática posterior. Autores como **Cardano**, quien escribe su libro sobre algoritmos algebráicos denominado **"Artis magnae seu de regulis algebraicis liber unus"**, y Leibniz. Pretendían desarrollar un "calculus ratiocinator" para decidir las verdades lógicas. Perseguían un lenguaje formal con lo que expresar cualquier enunciado y de forma inequívoca. El **Ars iudicandi** y el **Ars inveniendi**

La lógica

Para poder determinar qué se puede resolver de forma algorítmica y que se puede resolver eficientemente se necesitaba de una expresión más precisa que vino de mano de la **lógica**. **Aristoteles** fue un primer intento en esta dirección, pero es en el siglo 19 donde se produce el desarrollo de la lógica moderna. Los métodos de cálculo de **George Boole** se constituyeron en gran medida de acuerdo con los métodos del álgebra. Tras diversos desarrollos, **Frege** crea un sistema suficientemente amplio como para proceder a una formalización. Define en su obra **Begriffschrift** la **completitud** (todos los enunciados son demostrables) o **decidibilidad** (existen algoritmos para demostrar los enunciados). La importancia de su obra fue reconocida por **B. Russell** quien reconoció su importancia y la divulgó en su libro **Principia Mathematica** En paralelo, se desarrolla toda la teoría de números naturales por **Guiseppe Peano** quien escribio **Arithmeticae Principia**. Este fue el modelo que eligió **Kleene** para la formalización de la **teoría de la recursividad**.

Al final de esta época está bien establecido que gran parte de la matemática puede ser deducida con la ayuda de un calculo lógico. Todos estos desarrollos perseguían reducir los procesos de demostración a meros procedimientos mecánicos. Además, también aparecen tres grandes escuelas de pensamiento sobre la fundamentación de la matemática:

- **Logicista**: *La matemática es una rama de la lógica*. Las nociones matemáticas han de ser definidas en términos lógicos y demostrados con lógica
- **Intucionista**: Defiende la no aceptación de la ley del tercero excluido para conjuntos infinitos. No se pueden usar contradicciones basadas en suposiciones
- **Formalista** (Hilbert): Formula la matemática clásica con una teoría axiomática formal y deberá demostrarse que esta teoría es *consistente* (libre de contradicción)

En este momento, aparece el **problema de la decisión** (Entscheidungsproblem). Consiste en determinar si existen métodos que en tiempo y espacio finito puedan ser validos o no. Años más tarde **Hilbert** y **Ackerman** trabajaran en un cálculo deductivo para la lógica de primer orden. **Gödel** demostrará posteriormente que mediante axiomas y reglas de inferencia de la lógica toda fórmula válida es deducible. Todo esto será marcado de contradictorio por Gödel, afirmando que todos los sistemas formales de la matemática clásica son incompletos. En este trabajo, Gödel define y utiliza las funciones recursivas primitivas que tienen la importante propiedad de que para cada conjunto dado de argumentos el valor de la función puede computarse mediante un procedimiento finito.

Formalización del concepto de Algoritmo

En 1935, **Alonzo Church** presentó una formalización de las funciones recusivas en términos del lambda cálculo y enunció una equivalencia entre su clase de funciones y las calculables por procedimientos efectivos. Tras un primer rechazo por parte de Kleene, este terminó aceptando el trabajo de Church y presentó una tesis doctoral donde usó los resultados de Gödel en la demostración del teorema de incompletitud. Definió las funciones recusivas primitivas y generales. Demostraba la existencia de conjuntos indecibles, definía recursivamente los enumerables y demostraba el teorema de la Forma Normal que lleva su nombre. Ambos trabajos se publicaron en forma de artículos donde demostraron la existencia de problemas indecidibles y definieron las propiedades de funciones calculables

En 1936 **Alan Turing** da una nueva formalización definiendo lo que hoy se conoce como **máquina de Turing**. **Demostró la indecidibilidad del problema de la parada y del problema de la decisión** por métodos constructivos usando lo que conocemos como máquina de Turing Universal que posteriormente demostraría su equivalencia con los modelos de calculabilidad vía lambda cálculo. Entre sus otros trabajos se encuentra la **Máquina con oráculo** y la **reducibilidad entre problemas para comparar dificultades**

de resolución.

Ese mismo año, **Emil Post** define la máquina que lleva su nombre. Muy parecido al modelo de Turing que publicó en un artículo con pocos meses de diferencia. Todos estos trabajos presentan evidencias a favor del modelo de idea intuitiva de Church sobre los algoritmos: Equivalencia entre varios modelos, concepto de la máquina de Turing que reproduce las operaciones que un calculador humano es capaz de realizar, así como evidencia heurística (todas las operaciones han sido reproducidas en máquinas de Turing y todas las funciones que quedarían fuera de la clase o bien quedan fuera de la clase o buen no puede ser considerada computable)

Otros modelos formales

Posterior a los modelos de Church, Turing y Post han aparecido distintas orientaciones del mismo concepto. Destacamos la aparición de los ordenadores y lenguajes de programación de la mano del modelo **URM** (Unlimited Registers Machine) donde se sustituyen los recorridos por cinta de la máquina de Turing por registros que almacenan datos sin importar su tamaño, se introducen operaciones básicas, saltos y el modelo **RAM**. El siguiente paso fue pasar de registros a variables, de forma que una máquina pasa aspecto de programa. Inicialmente se usaron lenguajes no estructurado con variables de entrada, interna y salida. Posteriormente apareció la informática teórica con modelos de cómputo más avanzados. Entre ellos el bucle FOR y WHILE.

Conceptos intuitivos de la computabilidad

Empezaremos con la definición de Algoritmo: **Un algoritmo es una secuencia finita de instrucciones precisas que, para cierto tipo de entrada o bien devuelve una salida o bien no termina nunca**. Diremos que una función **es computable sí existe un algoritmo que para cualquier argumento de la función como entrada nos devuelve el valor de la función como salida**. Si la función para cierto argumento no toma valor, entonces el algoritmo para ese argumento como entrada no termina nunca. De aquí se deduce que **si una función computable es total entonces el algoritmo que computa es un algoritmo conclusivo**. Definimos un conjunto **decidible** B como aquel donde dado un elemento a un algoritmo conclusivo determina en tiempo finito si a pertenece a B. Definimos un conjunto **enumerable** C como aquel donde donde existe un algoritmo para determinar si un elemento a pertenece a B.

> Todo conjunto decidible es enumerable, pero no a la inversa (cardinal finito, cardinal infinito)

Todo lenguaje regular es decidible, ya que existe un autómata finito determinista (algoritmo conclusivo) que es capaz de decidir si un elemento pertenece o no. Sin embargo, **solo podemos asegurar que todo lenguaje con estructura de frase es enumerable, puesto que para dicho lenguaje no existe ningún dispositivo reconocedor**.

Tabla de autores y obras

Autor	Contribución	Descripción
Idea de sistema de numeración		Aplicación biyectiva de conjuntos para contar cosas
Escritura		Primera aparición de la escritura

Mesopotamia	Sistema de numeración. Operaciones básicas (tablilla de arcilla con división del 2650 ac). Algoritmo para calcular raíces cuadradas. Resolución de ecuaciones cuadráticas y cúbicas	Posicional, sexagesimal y sin cero
China	Valor aproximado de π. (500 ac)	
India	Sistema de numeración (900 dc)	Sistema de numeración base 10, posicional y con cero
Harûn al-Rasîd	La casa de la sabiduría (s VIII)	Lugar de conocimiento de la antigüedad
Raimundo Lulio	*Ars Magna* (1300 bc)	Describe un procedimiento general de base combinatoria para hallar todas las “verdades”. Describe la idea de "procedimiento"
Cardano	*Artis magnae seu de regulis liber unus* (1545 bc)	Libro sobre algoritmos algebraicos
Leibnitz		Desarrollar un calculus ratiocinator para decidir las verdades lógicas. Construir un lenguaje formal riguroso con el que definir enunciados
Frege	*Begriffschrift* (1879)	Presenta el primer lenguaje formal, en el que se pueden expresar enunciados tales como completitud o decidibilidad
Russell	*Principia Mathematica* (1910-1913)	Basado en *Begriffschrift*
Peano	*Arithmaticae principia* (1910-1913)	Axiomatiza la aritmética de primer orden y deduce la teoría de números naturales
Hilbert y Ackerman	*Elementos de la lógica teórica* (1928)	Mostraba su preocupación sobre si el cálculo deductivo era semánticamente suficiente (permitir deducir todas las fórmulas válidas). Posibilidad de desarrollar sistemas formales y demostrar su consistencia
Gödel	*La suficiencia de los axiomas del cálculo lógico de primer orden* Teorema de incompletitud (1930)	Demuestra mediante axiomas y reglas de inferencia de la lógica que toda formula válida es deducible, es decir, es un conjunto recursivamente enumerable

Gödel	*Sobre las sentencias formalmente indecidibles de los Principia Mathematica y sistemas afines*	Desmiente lo publicado por Hilbert. Define las funciones recusivas primitivas que tienen la importante propiedad de que para cada conjunto dado de argumentos el valor de la función puede computarse mediante un procedimiento finito. Posteriormente Ackerman demostrará que las funciones recusivas para formalizar el concepto de "procedimiento efectivo"
Alonzo Church	--- (1935)	Formalización de las funciones recusivas en términos del Lambda calculo. Equivalencia de lamba calculo y procedimientos efectivos
Kleene	--- (1935)	Intentó demostrar la falsedad de Church usando diagonalización, y al no poder, le puso nombre a su tesis. Definió las funciones recusivas primitivas y las u-recursivas. Demostraba la existencia de conjuntos indecibles, definia los enumerables y demostraba el teorema de la Forma Normal que lleva su nombre (cada programa admite uno equivalente usando bucles FOR y WHILE)
Alan Turing	Máquina de turing Universal (1936), Máquina con Oráculo, problema de la parada	Demostración de la indecidibilidad del problema de la parada y del problema de la decisión, la reducibilidad entre problemas. Paso de cómputo (complejidad)
	URM (Unlimited Registers Machine) 1963	
	RAM (Random Access Memory)	