ALAN TURING: Computabilidad, Criptoanálisis, Primeros Ordenadores y Test de Turing

David de Frutos Escrig

Departamento de Sistemas Informáticos y Computación, UCM.

Matemáticas en Acción 2012, Universidad de Cantabria
28 de noviembre de 2012

Agr: Luca Aceto (Reykjavik Univ), Carlos Gregorio, Ignacio Fábregas (UCM)

Índice

Biografía

- Alan Turing (Londres 1912 - Wilmslow, Cheshire 1954)
- Grado en Matemáticas - King's College, Cambridge 1934

  On Computable Numbers and the Decision Problem (Entscheidungsproblem) 1936
- Doctorado en Matemáticas - Princeton, USA 1936-38

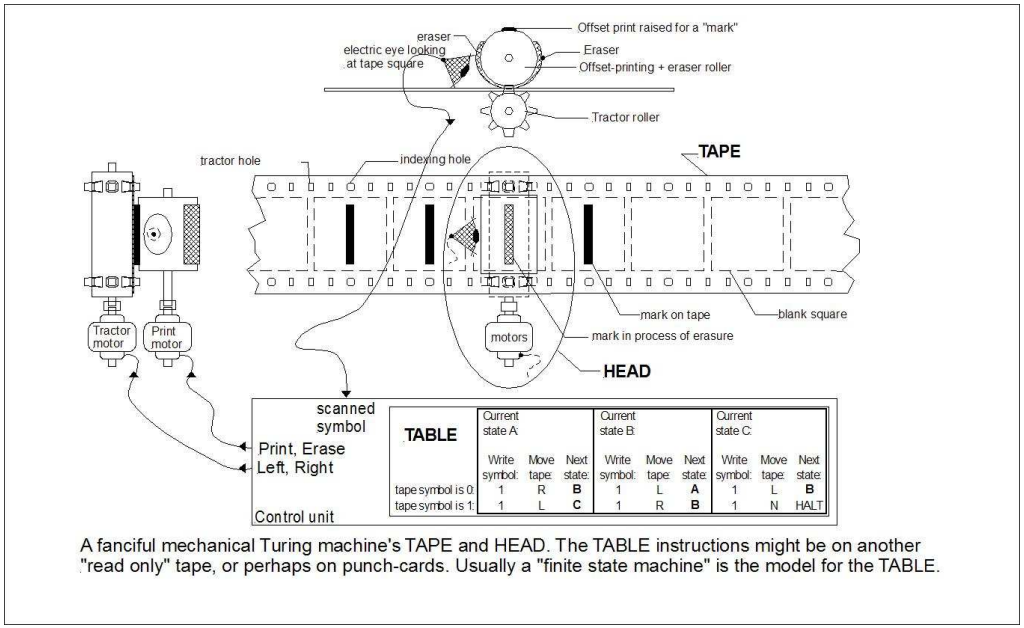
  Systems of logic based on ordinals 1939

Biografía

- Government Code and Cypher School - Bletchley Park 1939-43
  - The *bombe*
- ACE (Automatic Computing Engine) - National Physical Laboratory 1945-48
  - Intelligent Machinery 1948
- Mathematics Department - University of Manchester 1948-54
  - Computing Machinery and Intelligence - Turing Test 1950
  - Artificial Life y Morphogenesis 1952

Máquinas de Turing

- Cinta *infinita dividida en casillas; Alfabeto finito:* $\{0, 1\}$.
- *Scanner para leer la casilla actual; Movimiento (right,left) de la cabeza lectora.*
- *Estado del controlador (memoria reciente finita).*
- *Instrucciones:* print, erase, move, cambio de estado.



A fanciful mechanical Turing machine's TAPE and HEAD. The TABLE instructions might be on another "read only" tape, or perhaps on punch-cards. Usually a "finite state machine" is the model for the TABLE.

La máquina universal

Standard descriptions

Codificación de los programas: palabra finita –> número natural.

Subroutines

Renombramiento de los estados de un programa generando bloques disjuntos.

The Universal Computing Machine

- ¡Los programas devienen datos!; ¡un único programa los interpreta todos!
- De la Máquina Universal al Computador (Von Neumann - ENIAC y Turing - ACE).

Números computables - Problema de parada

- Secuencias infinitas computables ¡por una máquina que no para nunca, ni deja de escribir símbolos!
  - Números (reales) computables
- Conjunto numerable de secuencias computables
- Satisfactoriness problem - Problema de parada

The Church-Turing Thesis

- Turing Machines = Cualquier método de cómputo digital.
- Funciones recursivas y Lambda definibles.

The Entscheidungsproblem (Hilbert)

Incompletitud e indecidibilidad.

De Hilbert a Turing

La lógica matemática aparece para confrontar la crisis en la fundamentación de la matemática al comenzar el siglo XX.

Hilbert's Program (1900–1928)

Busca formalizar las matemáticas llegando a que son

- consistentes,
- completas y
- decidibles.

Hilbert estaba convencido de que así era y así se probaría.
Con ello las mátematicas quedarían reducidas a un mero cálculo mecánico

El derrumbe de las ilusiones de Hilbert

K. Gödel (1931–1933):
— Incompletitud de la aritmética.
— Imposibilidad de probar la consistencia dentro del propio formalismo.
A. Church and A. Turing (1936–1937): Indecidibilidad de la lógica de primer orden
— El conjunto de fórmulas válidas no es decidible,
— ni por tanto tampoco recursivamente enumerable.

Los (demás) matemáticos respiran hondo!

El derrumbe de las ilusiones de Hilbert

K. Gödel (1931–1933):
— Incompletitud de la aritmética.
— Imposibilidad de probar la consistencia dentro del propio formalismo.
A. Church and A. Turing (1936–1937): Indecidibilidad de la lógica de primer orden
— El conjunto de fórmulas válidas no es decidible,
— ni por tanto tampoco recursivamente enumerable.

Los (demás) matemáticos respiran hondo!

Alonzo Church vs. Alan Turing

- A. Church introduce el λ-calculus y prueba que hay problemas elementales irresolubles con él.

  Gödel no está convencido de que esa sea una formalización razonable de función computable.

- A. Turing introduce sus Máquinas de Turing, prueba la indecidibilidad del Problema de Parada y demuestra la equivalencia entre λ-calculus y la computabilidad con sus máquinas.

  Gödel queda convencido de su propuesta ...
  ¡y por ende de la de Church!

Alonzo Church vs. Alan Turing

- A. Church introduce el λ-calculus y prueba que hay problemas elementales irresolubles con él.

  Gödel no está convencido de que esa sea una formalización razonable de función computable.

- A. Turing introduce sus Máquinas de Turing, prueba la indecidibilidad del Problema de Parada y demuestra la equivalencia entre λ-calculus y la computabilidad con sus máquinas.

  Gödel queda convencido de su propuesta ...
  ¡y por ende de la de Church!

- De como se ganó la Guerra en una plácida mansión.
- 9000 personas trabajando en el proyecto.

La máquina Enigma

- Un teclado y otro gemelo iluminable: codificación carácter a carácter.
- Tres ruedas dentadas conectadas entre sí; Colocación inicial de las ruedas; Visores para generar una combinación de letras.
- Un tablero de conexiones para complicar los resultados.

La máquina Enigma

- Cuadernos de claves para fijar las configuraciones iniciales diarias.
- Varias redes con cuadernos diferentes para complicar la decodificación.
- Indicador de comienzo y consecuente control al recibirlo.

La máquina Enigma

La contribución polaca

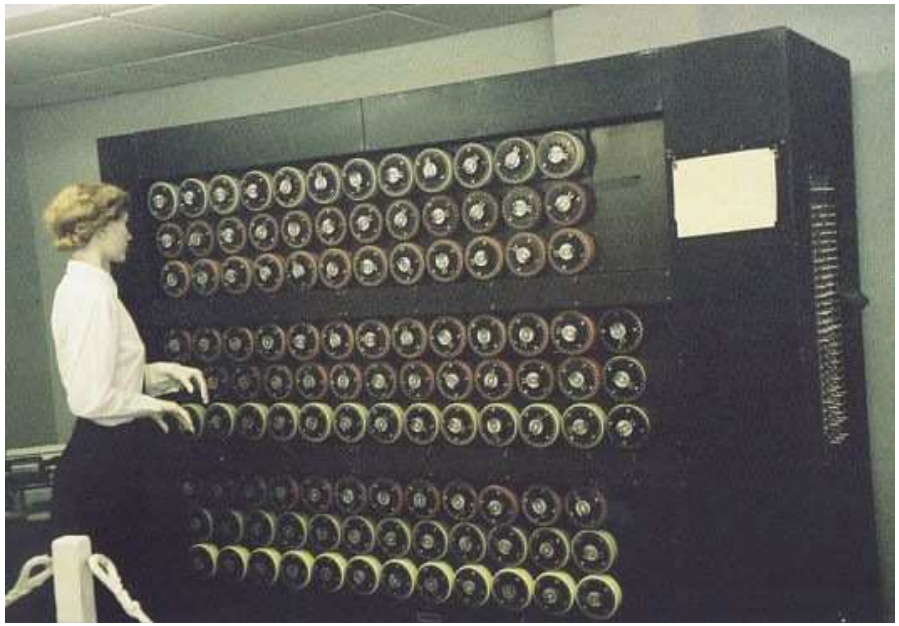
- De los indicadores se dedujo la colocación de los anillos.
- Colección de réplicas de Enigma para buscar las configuraciones iniciales diarias.

Las *bomba polacas*

- Búsqueda de coincidencias mediante cribas o usando la repetición del indicador.
- Efecto limitado del cableado sobre el tablero.

The bombe

- 36 réplicas trabajando juntas.
- Cribas obtenidas a partir de (torpes) estereotipos.
- Búsqueda automática de posibles soluciones y chequeo manual de cada una de ellas.



The bombe

- Método de los bucles para determinar el cableado del tablero.
- Método de las repeticiones para aislar una respuesta.

Enigma de la Marina (Dolphin)

- Se encuentran máquinas y tablas en navíos abandonados.
- Banburismus: detección de ruedas en uso.

Inteligencia Artifical

IA en Bletchley Park

- Mecanización de la resolución de problemas.
- Aprendizaje basado en la experiencia.
- Búsqueda (inteligente) en el espacio de soluciones posibles basado en heurísticas.

  Generate and test.
- Inteligencia = Reglas de búsqueda. . . que una máquina puede seguir.

IA en la posguerra

Intelligent Machinery: connectionist style neural simulation.

Inteligencia Artifical

Computing Machinery and Intelligence - Turing Test

¿Cuánto tiempo se puede hacer pasar una máquina por un humano?

Los primeros programas de la IA

- Programa para jugar a las *damas - Christopher Strachey* (1951-52).
- *Introducción del aprendizaje: Samuel* 1955.
- *Aprendizaje: reconociendo relaciones, casos particulares, generalización, comprobación.*

¡No hay necesidad de entender (meta-aprendizaje)!

Artificial Life

Vida artificial

- Simulando la vida en un computador.

Morphogenesis

- Crecimiento guiado por patrones (o viceversa) - Series de Fibonacci.
- Reaction-diffusion model: generación de manchas, pecas,. . .
- Ecuaciones no-lineales: su estudio con computadoras.

Artificial Life

Reaction-diffusion model

- Patrones de crecimiento con simetría esférica.
- Pequeñas perturbaciones causan grandes cambios.

Algoritmos genéticos

- Los mecanismos exitosos *sobreviven.*
- *Auto-reproducción y la máquina universal ejecutandose a sí misma.*

¿Y después de todo esto?

- En enero de 1952, Turing, homosexual desde su juventud, fue acusado de gross indecency.
- Aceptó como pena la castración química con estrógenos.
- El 7 de junio de 1954, Turing se suicida mordiendo una manzana envenenada, posiblemente recreando una imagen de los cuentos de la niñez..

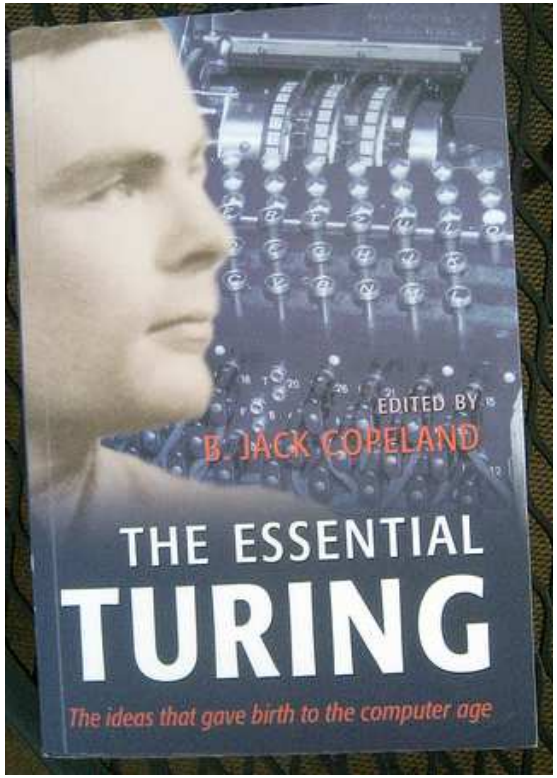
Turing believes machines think
Turing lies with men
Therefore machines do not think

- En 2009 y 2012 la Cámara de los Comunes le ha negado el indulto póstumo: law was law.

Los Premios Turing

Tributo a Turing

Los Premios Turing 1966–



2012 Alan Turing Year

http://www.turingcentenary.eu/