Le origini del calcolo digitale – 4

Epistemologia, Deontologia ed Etica dell'Informatica
Storia dell'Informatica e della Comunicazione Digitale

Federico Gobbo
federico.gobbo@uninsubria.it
CRII – Centro di Ricerca "Informatica Interattiva"
Università dell'Insubria, Varese–Como

A.A. 2010-11

La matematica nel primo Novecento

In questa sezione ci occupiamo dei risultati straordinari e inattesi della ricerca nel campo della matematica, perché ci serve per capire la matrice teorica dei fondamenti dell'informatica a noi già noti:

La matematica nel primo Novecento

In questa sezione ci occupiamo dei risultati straordinari e inattesi della ricerca nel campo della matematica, perché ci serve per capire la matrice teorica dei fondamenti dell'informatica a noi già noti:

(quali sono?)

La matematica nel primo Novecento

In questa sezione ci occupiamo dei risultati straordinari e inattesi della ricerca nel campo della matematica, perché ci serve per capire la matrice teorica dei fondamenti dell'informatica a noi già noti:

(quali sono?)

Almeno:

- le macchine astratte di Alan Turing;
- l'architettura di John von Neumann;

La matematica nel primo Novecento

In questa sezione ci occupiamo dei risultati straordinari e inattesi della ricerca nel campo della matematica, perché ci serve per capire la matrice teorica dei fondamenti dell'informatica a noi già noti:

(quali sono?)

Almeno:

- le macchine astratte di Alan Turing;
- l'architettura di John von Neumann;

Avendo questi due modelli saremo in grado di costruire il primo calcolatore moderno, l'ENIAC (1946). Seguiamo la periodizzazione storica del libro di testo di Paul E. Ceruzzi.

David Hilbert

David Hilbert (1862–1943) nasce a Königsberg (la città di Kant) dove si addottora nel 1885 con Ferdinand von Lindemann con una tesi sulle funzioni circolari, dove poi insegna matematica. Grazie all'interessamento di Felix Klein, nel 1895 si trasferisce all'Università di Gottinga, alla cattedra che fu di Gauss, Riemann e Dirichlet. Hilbert attira studenti e Gottinga torna ad essere un centro d'eccellenza mondiale in matematica.

Nel 1898 tiene un corso dal titolo 'elementi di geometria euclidea', in cui fonda la geometria mediante dimostrazioni puramente logiche, senza usare l'intuizione geometrica delle figure. Hilbert dimostra che la geometria è coerente sugli assiomi se lo è l'aritmetica di Peano (v. sotto), allora problema ancora aperto.

Figura: David Hilbert

Hilbert contro Kronecker

Hilbert si occupa del **problema fondazionale della matematica**, riducendo la geometria euclidea all'aritmetica – e aprendo le porte inconsapevolmente alle geometrie non euclidee.

Leopold Kronecker – la nemesi di Cantor – osteggia l'approccio di Hilbert sostenendo che una dimostrazione è accettabile se e solo se esiste un numero *finito* di passi che permetta di *costruire* gli oggetti matematici di cui si parla (**finitismo**). Per Kronecker, i mattoni sono i numeri naturali:

> *Dio fece i numeri naturali; tutto il resto è opera dell'uomo.*

Il lavoro di Hilbert sfida il finitismo di Kronecker.

Figura: Leopold Kronecker

Parigi, anno 1900

L'alba del nuovo secolo celebra il trionfo della fiducia nel progresso e nella scienza a Parigi, che diventa il centro del mondo: l'Esposizione Universale, le Olimpiadi, numerosi congressi scientifici e di categorie professionali accadono in quell'anno. Per esempio, al Congresso Internazionale di Filosofia il matematico Louis Couturat lancia il progetto di adozione di una lingua ausiliaria internazionale per la scienza e per i commerci.

Al Secondo Congresso Internazionale dei Matematici Hilbert espone 23 problemi aperti in matematica da risolvere nel Novecento noti come **Problemi di Hilbert**: il primo è dimostrare l'ipotesi del continuo di Cantor.

Figura: Parigi, anno 1900

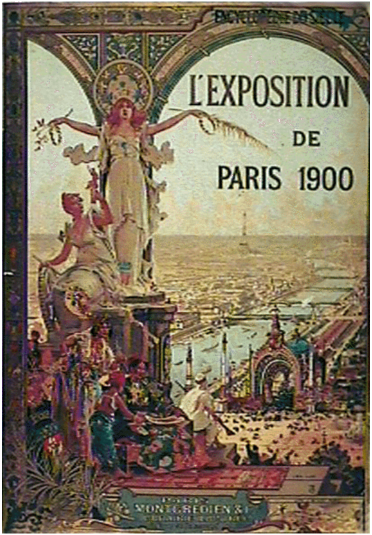

Figura: L'Esposizione Universale di Parigi, anno 1900

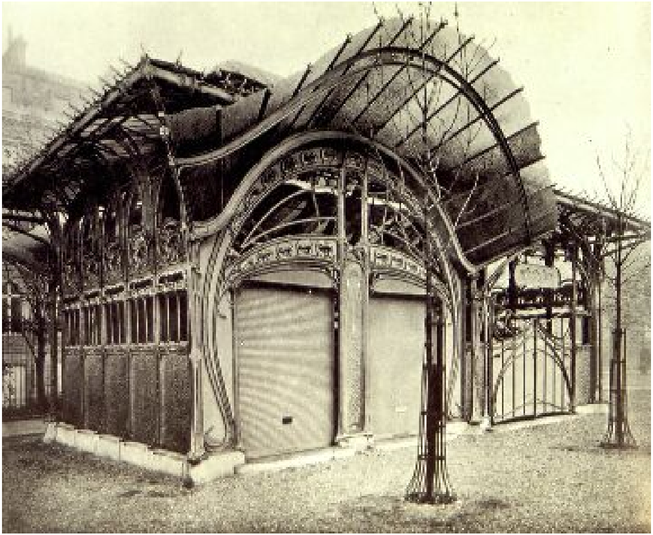

Figura: Entrata del metrò (Parigi, anno 1900)

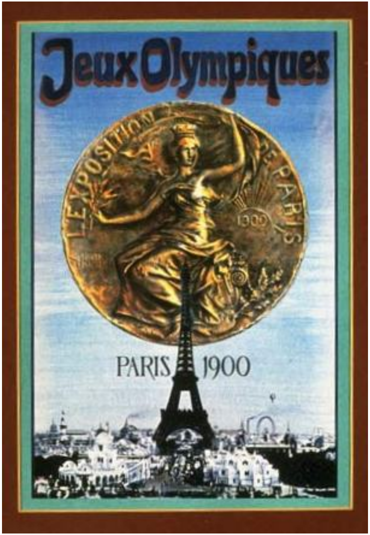

Figura: Olimpiadi di Parigi, anno 1900

Figura: Veduta di Parigi, anno 1900

Figura: La moda di Parigi, anno 1900

Il programma formalista

Nasce il **programma formalista**, che considera la matematica priva di contenuto, puro gioco sintattico, formale. Hilbert intende trovare il fondamento ultimo della matematica attraverso l'assiomatizzazione in formule logiche, analogamente alla riduzione della geometria euclidea all'aritmetica di Peano. Dal suo discorso (David 2000:90)

> *Ogni matematico condivide la convinzione che qualsiasi problema matematico definito deve essere necessariamente suscettibile di formalizzazione esatta [...] Noi sentiamo dentro di noi questo richiamo perpetuo: C'è il problema. Cerca la soluzione. Puoi trovarla per mezzo della pura ragione.*

Giuseppe Peano

Giuseppe Peano (1858–1932) nasce a Cuneo e insegna all'Università di Torino. Inizia come analista, precisando la nozione di limite superiore, scopre la Curva di Peano e fonda il calcolo vettoriale.

Si interessa di logica, che insegna surretiziamente nel corso di analisi, specie dopo l'assiomatizzazione dell'aritmetica (1889). Amico di Couturat, dopo la pubblicazione degli opuscoli inediti di Leibniz (1901), riprende il progetto di *lingua generalis*, scrivendo le proprie opere in *Latino sine Flexione (LsF)*.

Fu maestro tra gli altri di Vacca e Vailati, che si occupò anche di didattica della matematica – si vedano gli atti del Congresso tenuto in suo onore a Torino nel 2008.

Figura: Giuseppe Peano

Gli assiomi di Peano (Peano Axioms, PA)

Nel 1889 il matematico piemontese pubblica gli assiomi dell'aritmetica nel suo libro *Arithmetices principia, nova methodo exposita*, i principi dell'aritmetica, esposti in modo nuovo.

1. 0 è un numero.
2. Il successore di un qualsiasi numero è un numero.
3. Se a e b sono numeri, e se i loro successori sono uguali, allora a e b sono uguali.
4. 0 non è il successore di alcun numero.
5. Se S è un insieme di numeri contenente 0, e se il successore di un qualsiasi numero n in S è anch'esso contenuto in S, allora S contiene tutti i numeri.

L'importanza di Peano in matematica

Peano, come Frege, distingue bene i simboli matematici da quelli logici, ma usa una notazione piú semplice di quella dell'ideografia, che non conosceva (si basa su Boole), da cui deriva quella odierna.

Per esempio, i simboli oggi in uso $\{\in\}$ e $\{\subset\}$ derivano dalla notazione del *Formulario Mathematico* (ultima edizione: 1908), contenente circa 4000 teoremi e formule, per la maggior parte dimostrate.

Le sue idee influenzano il programma logicista di Alfred North Whitehead, e Bertrand Russell.

Peano strega il giovane Bertrand Russell

Russell scrive, nella sua *Autobiografia* (in Odifreddi 2000):

> *Il Congresso [dell'anno 1900] fu il punto di svolta della mia vita intellettuale, perché vi incontrai Peano. Lo conoscevo già di nome e avevo visto qualche suo lavoro, ma non mi ero preso la briga di imparare il suo formalismo. Al Congresso notai che era sempre il piú preciso di tutti, e che sistematicamente aveva la meglio in ogni discussione in cui si imbarcava. Col passare dei giorni, decisi che questo era l'effetto della sua logica matematica. Capii che il suo formalismo era lo strumento di analisi logica che avevo cercato per anni.*

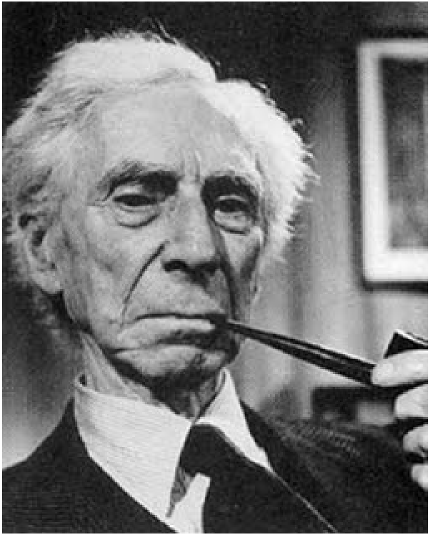

Figura: Bertrand Russell con l'immancabile pipa

Bertrand Russell

Bertrand Arthur William Russell (1872–1970), aristocratico gallese, è stato logico e matematico, filosofo del linguaggio, storico della filosofia (scrive una godibilissima *Storia della filosofia occidentale*) e ancora pacifista (sostiene il disarmo nucleare con Einstein), filosofo morale (non cristiano e ateo, propone una morale genuinamente laica), letterato (Nobel nel 1950 con la seguente motivazione: ≪quale riconoscimento ai suoi vari e significativi scritti nei quali egli si erge a campione degli ideali umanitari e della libertà di pensiero ≫).

Bertrand Russell

Bertrand Arthur William Russell (1872–1970), aristocratico gallese, è stato logico e matematico, filosofo del linguaggio, storico della filosofia (scrive una godibilissima *Storia della filosofia occidentale*) e ancora pacifista (sostiene il disarmo nucleare con Einstein), filosofo morale (non cristiano e ateo, propone una morale genuinamente laica), letterato (Nobel nel 1950 con la seguente motivazione: ≪quale riconoscimento ai suoi vari e significativi scritti nei quali egli si erge a campione degli ideali umanitari e della libertà di pensiero ≫).

In questa sede vediamo solo gli aspetti pertinenti al corso.

La lettera di Russell a Frege

Il 16 giugno 1902, mentre la seconda edizione delle *Grundgesetze der Arithmetik* di Frege era alle stampe, arriva una lettera (Davis 2000:41):

> *I find myself in agreement with you in all essentials [...] I find in your work discussions, distinctions, and definitions that one seeks in vain in other work of other logicians [...] There is just one point where I have encountered a difficulty [...] The exact treatement of logic in fundamental questions has remained very much behind; in your works I find the best I know of our time, and therefore I have permitted myself to express my deep respect to you.*

La reazione di Frege

Frege aggiunge rapidamente un'appendice al volume in corso di stampa (Davis 2000:41–42):

> *Non c'è nulla di peggio che possa accadere a uno scienziato che vedere le fondamenta del proprio lavoro di una vita crollare proprio quando il lavoro è finito. Io sono stato messo in questa posizione da una lettera di Mr. Bertrand Russell.*

Frege rimane cosí sconvolto che di fatto smette di occuparsi di logica! L'ideografia intendeva presentare una teoria di riduzione dell'aritmetica, del calcolo differenziale e integrale alla pura logica: è il **programma logicista**, condiviso da Russell. Russell mostra a Frege che l'intera impalcatura si fonda su una contraddizione nota come antinomia o **paradosso di Russell**.

Il paradosso di Russell 1/2

La regola V dell'ideografia dice che due insiemi sono uguali se e solo se le loro funzioni corrispondenti $f(x)$ coincidono nei loro valori per tutti i possibili argomenti.

Il paradosso di Russell 1/2

La regola V dell'ideografia dice che due insiemi sono uguali se e solo se le loro funzioni corrispondenti $f(x)$ coincidono nei loro valori per tutti i possibili argomenti.

Ciò richiede che l'espressione $f(x)$ sia considerata sia una funzione dell'argomento x che una funzione dell'argomento f, il che è un paradosso.

Il paradosso di Russell 1/2

La regola V dell'ideografia dice che due insiemi sono uguali se e solo se le loro funzioni corrispondenti $f(x)$ coincidono nei loro valori per tutti i possibili argomenti.

Ciò richiede che l'espressione $f(x)$ sia considerata sia una funzione dell'argomento x che una funzione dell'argomento f, il che è un paradosso.

Il paradosso di Russell fa crollare la teoria ingenua degli insiemi. Vediamo come.

Il paradosso di Russell 2/2

Russell chiama *straordinario* un insieme che sia membro di se stesso e *ordinario* un insieme che **non** sia membro di se stesso.

Il paradosso di Russell 2/2

Russell chiama *straordinario* un insieme che sia membro di se stesso e *ordinario* un insieme che **non** sia membro di se stesso.

L'esempio originale di Russell è il seguente:

- *the set of all those things that can be defined in fewer than 19 English words*

è una frase di 16 parole, perciò appartiene a un insieme straordinario.

Il paradosso di Russell 2/2

Russell chiama *straordinario* un insieme che sia membro di se stesso e *ordinario* un insieme che **non** sia membro di se stesso.

L'esempio originale di Russell è il seguente:

- *the set of all those things that can be defined in fewer than 19 English words*

è una frase di 16 parole, perciò appartiene a un insieme straordinario.

Sia ε l'insieme di tutti gli insiemi *ordinari*. Se ε è ordinario, allora per definizione appartiene a se stesso e allora è straordinario.

Il paradosso di Russell 2/2

Russell chiama *straordinario* un insieme che sia membro di se stesso e *ordinario* un insieme che **non** sia membro di se stesso.

L'esempio originale di Russell è il seguente:

- *the set of all those things that can be defined in fewer than 19 English words*

è una frase di 16 parole, perciò appartiene a un insieme straordinario.

Sia ε l'insieme di tutti gli insiemi *ordinari*. Se ε è ordinario, allora per definizione appartiene a se stesso e allora è straordinario.

Ma allora ε è straordinario, e allora non può appartenere a se stesso, e ciò lo rende ordinario! Da qualsiasi punto lo si guardi, il ragionamento porta a una contraddizione.

Dentro e fuori dal sistema...

Figura: M.C. Escher, *Reptiles* (1943)

I *Principia Mathematica* di Russell e Whitehead

Russell non si dà per vinto come Frege e, basandosi sulla notazione piú agevole di Peano, impiega dieci anni per scrivere con Alfred North Whitehead i *Principia Mathematica*, 3 volumi di circa 1000 pagine, usciti tra il 1910 e il 1913.

Come Frege, definiscono le entità matematiche con formule logiche, evitando programmaticamente gli aspetti filosofici. A differenza di Frege, le formule logiche sono stratificate in un sistema di **tipi**, per evitare il paradosso di Russell.

Il programma logicista di Russell e Whitehead

Il quarto volume, dedicato alla geometria, non verrà mai pubblicato: l'intero programma logicista viene infatti bruscamente fermato dai risultati limitativi di Gödel, come vedremo.

Russell scrive i *Principia* con Alfred North Whitehead (1861–1947), logico, matematico e filosofo britannico, che propugna una visione organicista della scienza, basata su Leibniz e Bergson, in alternativa al meccanicismo.

I *Principia* sono il sistema di assiomatizzazione piú espressivo mai scritto: contengono tra l'altro una discussione del teorema del buon ordinamento di Zermelo e l'assioma della scelta, nonché gli ordinamenti di Dedekind.

Cantor divide i matematici

Nel 1904 ha luogo il Congresso Internazionale dei Matematici: Hilbert, che sostiene i risultati di Cantor, rilancia il programma logicista, sostenuto da Russell.

Jules Henri Poincaré (1854–1912), è matematico, fisico teorico e filosofo naturale francese, della stessa generazione e calibro di Hilbert, noto per la congettura che porta il suo nome, e per aver gettato le basi della topologia. Poincaré ritiene che la matematica sia *sintetica a priori* (come Kant) anziché analitica, e che quindi le assiomatizzazioni come quella di Peano siano sempre circolari: il lavoro di Cantor non è legittimo.

L'intuizionismo di L. E. J. Brouwer

Luitzen Egbertus Jan Brouwer (1881–1966) si addottora nel 1907 ad Amsterdam in cui mostra un'ostilità al transfinito di Cantor degna di Kronecker. Considera il mondo una mera illusione come Schopenhauer, dove nulla può veramente essere conosciuto, e decide di ricostruire la pratica matematica dalle fondamenta per soddisfare le sue convinzioni.

Per Brouwer, la matematica esiste solo nella mente del matematico e viene dalla Intuizione Primordiale Matematica, non da un'espressione linguistica (Davis 2000:95):

> *esistere in matematica significa: essere costruito per intuizione; e la questione se un certo linguaggio è consistente, non solo è irrilevante in sé, ma anche non è un valido test per l'esistenza matematica.*

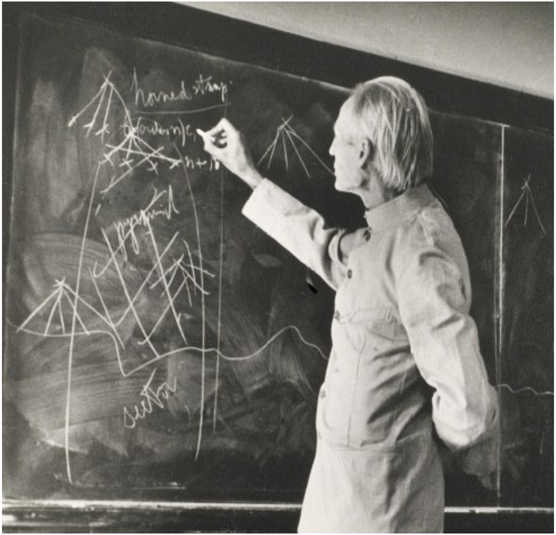

Figura: L. E. J. Brouwer

La metamatematica di Hilbert

Brouwer va oltre Kronecker: egli sostiene che ci sono proposizioni che non sono né vere né false quando applicate a insiemi infiniti, negando la validità delle dimostrazioni che fanno uso della legge aristotelica del terzo escluso (*tertium non datur*).

Applicatosi nell'area emergente della topologia, Brouwer nel 1910 dimostra il **teorema del punto fisso**, che verrà usato tra l'altro per costruire il lambda calcolo da Alonzo Church e nella dissertazione dottorale sulla teoria dei giochi di John Nash.

La risposta di Hilbert

> *Nessuno può cacciarci dal paradiso che Cantor ha creato per noi.*

Nonostante gli sia ostile, Hilbert ammira Brouwer e si adopera per fargli ottenere un posto all'Università di Amsterdam nel 1912. Hermann Weyl, il suo studente prediletto, deluso dai suoi tentativi falliti di dimostrare la CH, aderisce al programma intuizionista.

Hilbert risponde agli intuizionisti con la **metamatematica**, in cui il linguaggio della matematica viene descritto dalla matematica come metalinguaggio: questo uso di metodi finitari per studiare l'assiomatizzazione dei teoremi viene detto anche **proof theory (teoria della dimostrazione)**. Collaborano studenti quali Wilhelm Ackermann, Paul Bernays e John von Neumann.

Kurt Gödel

Kurt Gödel (1906–1978) nasce a Brno, nell'attuale Repubblica Ceca, allora impero austro-ungarico, da una famiglia protestante di lingua tedesca. A otto anni sopravvive a una febbre reumatica, che lo lascia ipocondriaco per tutta la vita. Fin da piccolo, mostra segni di instabilità psichica. Nel 1924 va a studiare matematica in una Vienna tumultuosa, tra pulsioni socialdemocratiche e conservatorismi. Frequenta il Circolo di Vienna, dove viene a contatto con le idee di Russell e di Ludwig Wittgenstein.

Nel 1928 esce il libro di testo di logica di Hilbert e Wilhelm Ackermann, dove viene posta la questione se nei sistemi di inferenza deduttiva come i *Principia* le regole sono non solo corrette ma anche complete. Hilbert riteneva di sí, ma mancava una dimostrazione. Gödel sceglie questo argomento per la sua dissertazione di dottorato.

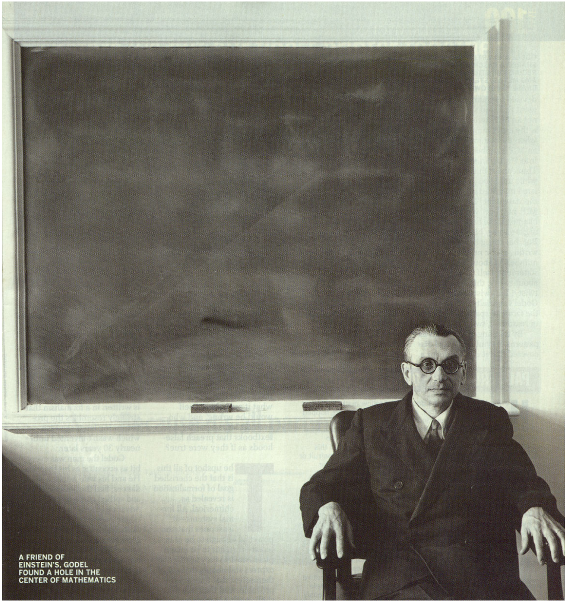

Figura: Kurt Gödel

Kurt Gödel e la consistenza dei numeri reali

Gödel mostra che con le regole di Frege–Russell–Hilbert, per ogni interpretazione delle lettere nelle formule le cui premesse sono asserzioni vere, le conclusioni sono sempre vere, esattamente quanto richiesto da Hilbert: il calcolo dei predicati è completo. [In realtà, questa prova era già stata data nel 1923 da un logico norvegese, Thoralf Skolem, ma né Gödel né i suoi advisor ne erano a conoscenza (Davis 2000:114).]

Il secondo Problema di Hilbert (1900) è la dimostrazione della consistenza dell'aritmetica dei numeri reali: Gödel lo affronta con i metodi finitari consentiti da Brouwer. Nel contempo, Ackermann e John von Neumann fanno lo stesso con l'aritmetica di Peano.

La conferenza a Könisberg del 1930

Nell'Agosto del 1930 a Könisberg (la città di Kant), viene indetta la Conferenza sull'Epistemologia delle Scienze Esatte. Il primo giorno si parla dei fondamenti della matematica: apre i lavori Rudolf Carnap, del Circolo di Vienna, che introduce il positivismo logico, poi parla Arend Heyting, allievo di Brouwer, che introduce l'intuizionismo, e infine John von Neumann, che tratta del programma hilbertiano.

Il secondo giorno Gödel spiega i risultati della sua dissertazione dottorale, ma è il terzo giorno che Gödel sostiene che, anche dimostrando che un sistema come i *Principia* è consistente, è sempre possibile provare che *dall'esterno* del sistema la dimostrazione non è valida.

Il paper di Gödel del 1931

John von Neumann è l'unico che coglie la portata di questo rilievo, e incoraggia Gödel a tenerlo informato. Dopo aver letto il preprint dell' articolo del 1931, von Neumann capisce che il programma hilbertiano è finito e decide di non occuparsi piú di logica.

Nel 1931 pubblica un paper di 25 pagine dal titolo *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, su alcune proposizioni formalmente indecidibili dei Principia Mathematica e di sistemi affini, dove presenta una serie di teoremi che mostrano come, qualsiasi sistema assiomatico si prenda, è *sempre* possibile trovare formule vere che *non* appartengono al sistema.

Il risultato limitativo di Gödel

Nel paper Gödel propone una variante del paradosso del mentitore:

- questa formula non è dimostrabile.

Se tale asserzione è indimostrabile, allora è vera, e la formalizzazione della teoria in questione è **incompleta**. Se tale asserzione è dimostrabile, allora è falsa, e la formalizzazione della teoria in questione è **inconsistente**.

Gödel ha dimostrato che *all'interno* di un sistema logico coerente e sufficientemente ricco si possono formulare proposizioni né dimostrabili né refutabili, dette **indecidibili**.

Il procedimento di Gödel

La dimostrazione originale, di 45 formule numerate, è molto intricata, e assomiglia a un programma scritto in linguaggio macchina (Davis 2000:120). Il primo teorema di incompletezza fa uso del **metodo diagonale** usato da Cantor, e dimostra la non numerabilità del corpo dei numeri reali.

Gödel associa ad ogni formula un numero, espresso univocamente come prodotto di numeri primi: questa procedura di aritmetizzazione delle formule logiche viene chiamata **gödelizzazione**, ed era stata tentata già da Leibniz, che Gödel ammirava molto. Inoltre, in queste dimostrazioni Gödel trova una nuova classe di funzioni, che si rivela fondamentale per l'informatica: le **funzioni ricorsive primitive**.

La fortuna matematica dei risultati di Gödel

Nel 1936 John Barkeley Rosser senior, allievo di Alonzo Church, dimostra una versione rafforzata del teorema di incompletezza: se un sistema matematico sufficientemente espressivo è non contradditorio e coerente, allora *deve* essere incompleto. Completezza e coerenza sono proprietà inconciliabili.

Nel 1965 Emil Post dà una versione del teorema di incompletezza usando gli insiemi ricorsivamente enumerabili, Hofstadter nel 1979 usa i numeri ordinali transfiniti costruttivi, fino alla dimostrazione in termini di teoria dell'informazione algoritmica di Gregory J. Chaitin (1982).

Una valutazione dell'impatto di Gödel

Al momento della pubblicazione, lo shock nella comunità dei matematici fu grande: certezza, obiettività e rigore sembravano non aver piú un posto nella matematica. Dopo i risultati di Alan Turing e Alonzo Church, la situazione si è rovesciata: vedremo come il problema dell'arresto affrontato di Alan Turing sia analogo a quello affrontato da Gödel.

Il teorema di incompletezza di Gödel si applica a sistemi formali e basta, ma viene citato a sproposito – magari con una spruzzata di fisica quantistica – da filosofi postmodernisti, teologi, esperti di new age…

Una valutazione dell'impatto di Gödel

Al momento della pubblicazione, lo shock nella comunità dei matematici fu grande: certezza, obiettività e rigore sembravano non aver piú un posto nella matematica. Dopo i risultati di Alan Turing e Alonzo Church, la situazione si è rovesciata: vedremo come il problema dell'arresto affrontato di Alan Turing sia analogo a quello affrontato da Gödel.

Il teorema di incompletezza di Gödel si applica a sistemi formali e basta, ma viene citato a sproposito – magari con una spruzzata di fisica quantistica – da filosofi postmodernisti, teologi, esperti di new age... Questo per cercare di sminuire la validità della matematica e del metodo scientifico: tutto ciò non ha nulla a che fare con il povero Gödel!

La fuga dalla Germania...

La crisi economica mondiale del 1929 in Germania dà forza alle istanze nazionaliste, e in ultima analisi facilitano la presa del potere da parte di Hitler, che avviene nel 1934, per completarsi nel 1938 con l'annessione dell'Austria.

La situazione diventa intollerabile per molti matematici dell'epoca, alcuni di origine ebraica, altri di simpatie socialiste o anarchiche, altri ancora pacifisti o semplicemente liberali. Alcune cattedre già assegnate vengono ritirare per mancanza di "fede ariana" o per "sospette simpatie giudaiche".

La fuga dalla Germania. . .

Il nazismo segna la fine della scuola di Gottinga promossa da Hilbert: nomi come Albert Einstein, J. Robert Oppenheimer, Hermann Weyl, Kurt Gödel, John von Neumann, Erwin Panofsky, George Kennan, fuggono al neonato **Institute for Advanced Study a Princeton**, NJ: nel dopoguerra il ruolo guida della ricerca nella fisica e nella scienza dell'informazione – ma non solo – verrà preso dagli Stati Uniti d'America.

Alcuni personaggi preferiscono invece andare a Cambridge, UK: vedremo con Turing tra poco che anche questo fatto è rilevante per la storia dell' informtica.

Figura: Albert Einstein e Kurt Gödel a Princeton

Figura: Alan Turing

Alan Turing

Alan Mathison Turing (1912–1954) è figlio dell'impero britannico, da una famiglia di mercanti, soldati e uomini di chiesa, attiva soprattutto nelle indie (come la famiglia di George Orwell: Hodges 2006:14). Cresciuto da tutori scelti dal padre, ha enormi difficoltà nei primi anni di scuola, specie con la grammatica latina, e diventa schivo e assente. Nel 1922 riceve in dono un libro che spiega ai bambini le meraviglie della natura, che lo inizia ai misteri della scienza. Ben presto il suo interesse si rivolge alla fisica e alla matematica del suo tempo, ben al di là dei programmi scolastici. Leggendo un libro di Einstein, scrive nel 1928 (a 16 anni!):

> *Qui Einstein mette in dubbio che gli assiomi di Euclide siano validi quando siano applicati a corpi rigidi [. . .] Si accinge quindi a mettere alla prova [. . .] le leggi o assiomi di Galileo e Newton (Hodges 2006:49).*

Alan Turing e lo sport

Alan non permetteva che la passione quasi religiosa per il gioco intellettuale portasse con sé un disprezzo per il corpo. Ciò che avrebbe voluto era un pari successo del corpo e della mente, e con entrambi incontrava le stesse difficoltà: un difetto di coordinazione e un'incapacità di espressione. Ma in quel periodo scoprí di saper correre piuttosto bene [...] La corsa di fondo gli si confaceva perfettamente, essendo una forma di esercizio autosufficiente, senza bisogno di alcun equipaggiamento speciale e senza nessuna connotazione sociale [...] Alan non era il primo intellettuale a imporsi in questo genere di disciplina fisica, e a trarre soddisfazioni non passaggere dalla dimostrazione del proprio vigore nella corsa, nella marcia, nel ciclismo, nell'alpinismo, e nella capacità di affrontare gli elementi (Hodges 2006:79–80).

Figura: Alan Turing maratoneta (1946)

Gli anni di Cambridge

La noncuranza degli studi classici gli costa l'ammissione al Trinity, mentre viene ammesso al King's College di Cambridge nel 1931. Nel 1932 conosce la meccanica quantistica attraverso il testo di John von Neumann *Mathematische Grundlagen der Quantenmechanik*, che affronta il tema con gli strumenti della logica e della matematica pura, nella fattispecie gli spazi di Hilbert: fare scienza non significa raccogliere fatti, ma dubitare degli assiomi (Hodges 2006:110). Nel 1933 legge l'introduzione alla filosofia matematica di Bertrand Russell, e segue le lezioni di meccanica quantistica di Max Born e Richard Courant, allievi di Hilbert che hanno preferito Cambridge a Princeton (Hodges 2006:119). Con gli strumenti della matematica, dimostra l'equivalenza delle teorie quantistiche di Schrödinger e Heisenberg. Completati brillantemente gli studi *undergraduate*, diventa *fellow* nel 1935

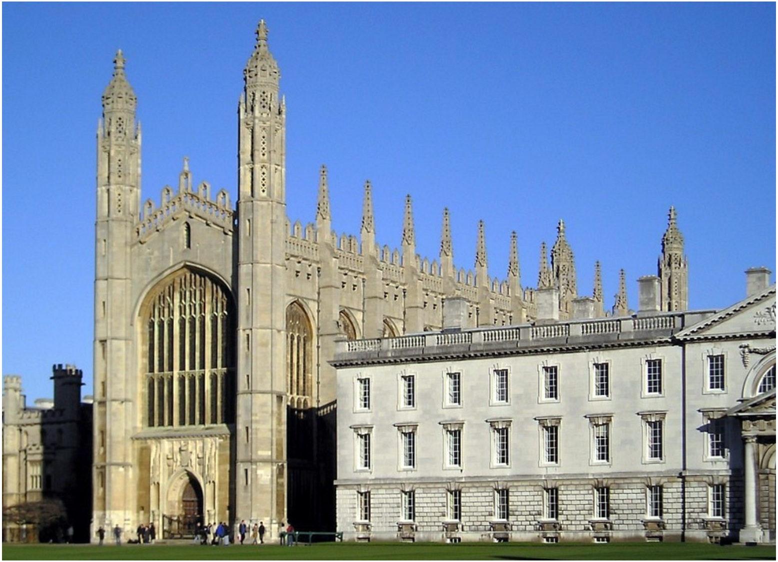

Figura: King's College, Cambridge, UK

Turing, Maggio 1936

Nel maggio 1936 Turing spedisce l'articolo fondamentale *On Computable Numbers, with an Application to the Entscheidungsproblem*, pubblicato nel 1937 (`doi:10.1112/plms/s2-42.1.230`): riformulando i risultati limitativi di Gödel del 1931, Turing formula il suo formalismo, **le macchine di Turing (MdT)**, chiamata **Universal Machine**, macchina universale, echeggiando l'*Analitical Engine* di Babbage.

In quell'articolo definisce il problema della decisione hilbertiano (*Entscheidungsproblem*) nei termini del **problema dell'arresto (halting problem)**, che è indecidibile.

Turing, Maggio 1936

Nel maggio 1936 Turing spedisce l'articolo fondamentale *On Computable Numbers, with an Application to the Entscheidungsproblem*, pubblicato nel 1937 (`doi:10.1112/plms/s2-42.1.230`): riformulando i risultati limitativi di Gödel del 1931, Turing formula il suo formalismo, **le macchine di Turing (MdT)**, chiamata **Universal Machine**, macchina universale, echeggiando l'*Analitical Engine* di Babbage.

In quell'articolo definisce il problema della decisione hilbertiano (*Entscheidungsproblem*) nei termini del **problema dell'arresto (halting problem)**, che è indecidibile.

La forma normale delle funzioni ricorsive, definite in vari modi da Gödel, Turing, e Alonzo Church, verrà definita da Stephen Kleene, allievo di Church (v. piú avanti).

Turing a Princeton

Turing era stato preceduto nel suo risultato di un solo mese (!) da Alonzo Church, il quale venne a sapere della formalizzazione di Turing, piú elegante della sua, grazie al collega cantabrigese Max H.A. Newman, topologo.

Church invita il giovane matematico inglese a Princeton, dove Turing lavora ad alcune implicazioni dei risultati di Gödel con Church, conseguendo il dottorato. Poco socievole, soggetto a depressione, non riesce a legare con Einstein, Gödel o Weyl: solo John von Neumann riesce a capirlo, e gli propone di diventare suo assistente.

Da Wittgenstein alla crittoanalisi

Turing rifiuta, e nel 1938 si imbarca per l'Inghilterra. Con sé ha una macchinetta montata nella sua stanza a Princeton, tra una lezione e l'altra, che era in grado di moltiplicare tra loro due lunghi numeri binari, uno un testo in chiaro, l'altro la chiave di crittazione.

Tornato a Cambridge, senza prospettive chiare, Turing partecipa alle discussioni guidate da Wittgenstein sui fondamenti della matematica. Ma ormai il suo interesse principale ora è la crittografia.

Turing in guerra 1/3

Con l'inizio della guerra l'intelligence britannica ha un problema: decifrare il cifrario tedesco Enigma, e Turing si mette al lavoro al Bletcheley Park, decifrandone la versione navale nel 1939.

Turing dà il contributo fondamentale alla costruzione di una macchina decrittatrice, *the Bombe*, e crea la teoria dell'informazione e la statistica che danno il fondamento scientifico alla crittoanalisi, sempre in contatto con gli americani.

Turing in guerra 2/3

Jack Good, crittoanalista che lavorava con Turing ad Enigma, ricorda:

> *Turing's most important contribution, I think, was of part of the design of the bombe, the cryptanalytic machine. He had the idea that you could use, in effect, a theorem in logic which sounds to the untrained ear rather absurd; namely that from a contradiction, you can deduce everything (English Wikipedia 2009).*

Mentre lavorava a Bletchley, Turing a volte correva per 40 miglia (64 km) fino a Londra per partecipare alle riunioni di alto livello.

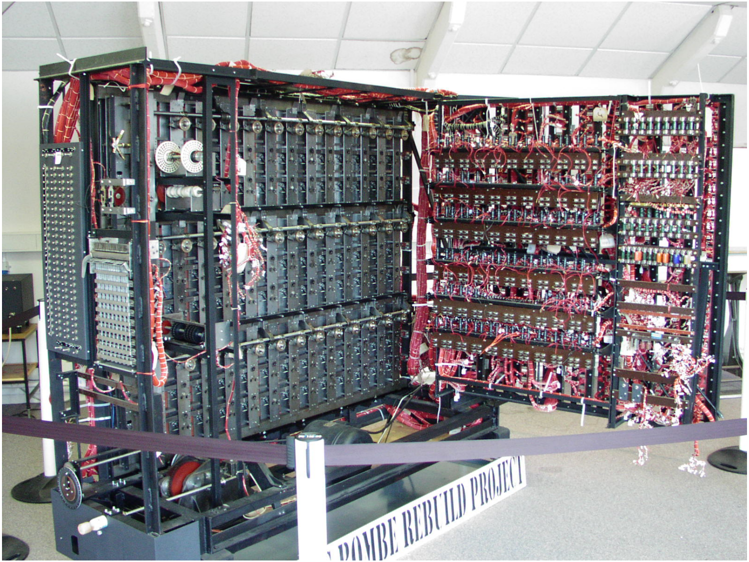

Figura: Ricostruzione della macchina *Bombe*

Turing in guerra 3/3

Nel 1942 torna negli Stati Uniti e lavora ai Bell Labs per costruire un'altra macchina decrittatrice. Tornato al Betchley Park nel 1943, capitanato da Sir Alexander C. Hugh, che cosí ricorda (nome in codice del progetto: Hut 8):

> *It is always difficult to say that anyone is absolutely indispensable but if anyone was indispensable to Hut 8 it was Turing. The pioneer's work always tends to be forgotten when experience and routine later make everything seem easy and many of us in Hut 8 felt that the magnitude of Turing's contribution was never fully realized by the outside world (English Wikipedia 2009).*

Durante gli ultimi anni di guerra Turing stabilisce un protocollo per la comunicazione verbale cifrata, nome in codice *Delilah*, che non viene però usato.

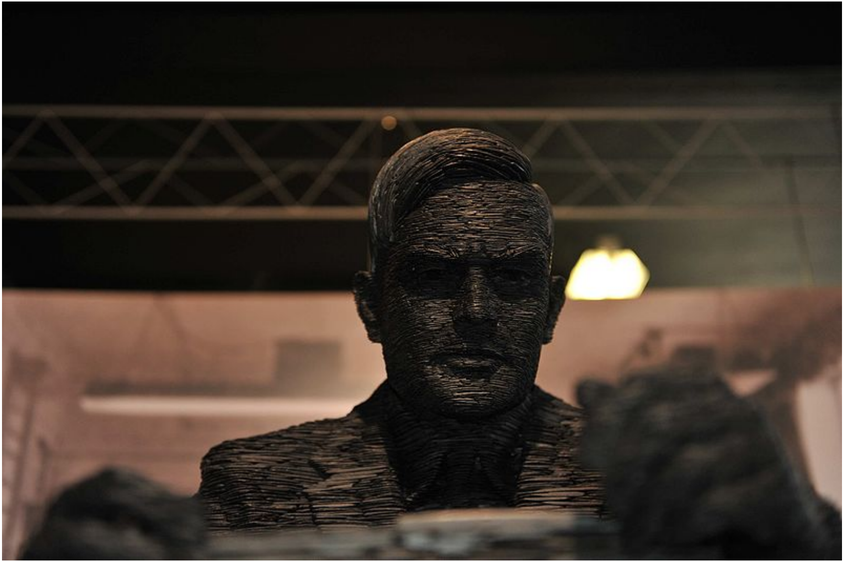

Figura: Statua in onore di Turing al Bletchley Park

Turing e i calcolatori elettronici

Tra il 1945 e il 1947 Turing lavora al design del **ACE (Automatic Computing Engine)**, un elaboratore elettronico dotato di memoria, la cui costruzione va a rilento per colpa del segreto militare.

Presosi un anno sabbatico, nel 1948 ottiene un posto al *computing laboratory* dell'Università di Manchester, dove lavora al software di uno dei primi elaboratori dotati di memoria, il **Mark I**. Ma mentre le sue idee venivano realizzate principalmente negli Stati Uniti da John von Neumann e collaboratori (come vedremo), Turing comincia a occuparsi delle potenzialità della sua macchina universale: nel 1948 scrive un programma per giocare automaticamente a scacchi, in cui l'elaborazione viene simulata.

Figura: Alan Turing Building, Manchester

Turing fonda l'Intelligenza Artificiale

Nel 1950 Turing pubblica sulla rivista *Mind* l'articolo fondamentale *Computing machinery and intelligence*, in cui propone il "gioco dell' imitazione", noto come **test di Turing**. L'analisi di questo articolo è una parte importante del corso di Epistemologia, e dunque non viene trattato qui.

Nel 1952 pubblica un paper dal titolo *The Chemical Basis of Morphogenesis*, che testimonia dei suoi interessi in biologia matematica.

Una fine tragica

Turing era omossessuale. Nel 1952 aveva iniziato una relazione con un giovane, tale Arnold Murray, il quale aveva aiutato un complice a fare irruzione in casa di Turing. Denunciato Murray, durante le indagini Turing ammette la relazione omosessuale con Murray, che era illegale per le leggi del Regno Unito del tempo.

Turing viene condannato alla castrazione chimica, e muore avvelenato da una mela al cianuro, apparentemente suicida, nel 1954. Secondo Hodges (2006), la sua incontrollabilità minava la sicurezza nazionale inglese, e dunque sarebbe stato suicidato. Nel 2009, il governo inglese fa ufficialmente ammenda del trattamento riservato al grande matematico, fondatore dell' informatica.

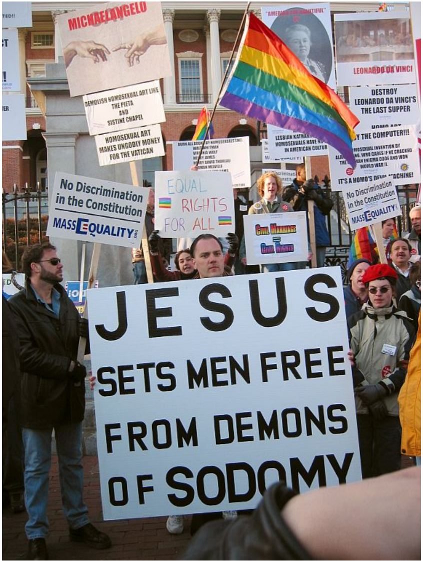

Figura: Manifestazione inglese omofoba

Figura: Turing capro espiatorio dei nuovi luddisti

Turing, il padre dell'informatica

Dal 1966, il **Turing Award**, una specie di Nobel dell'informatica, viene dato annualmente dall'**Association for Computing Machinery (ACM)**.

Turing, il padre dell'informatica

Dal 1966, il **Turing Award**, una specie di Nobel dell'informatica, viene dato annualmente dall'**Association for Computing Machinery (ACM)**.

Sitografia essenziale su Turing

- http://www.turing.org.uk/;
- http://www.turingarchive.org/;
- http://turing.cs.washington.edu/;
- http://turing100.blogspot.com/.

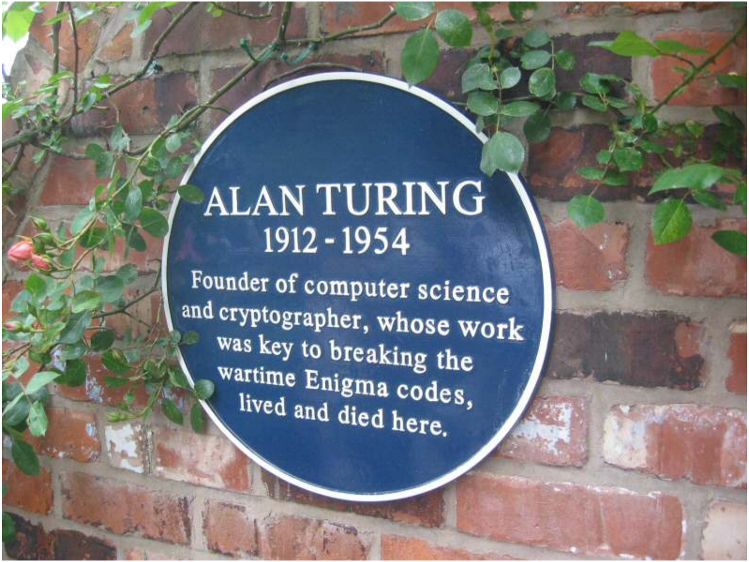

Figura: Placca commemorativa della casa a Wilslow, Cheshire

Andrej Markov

Andrej Andreevič Markov sr. (1856–1922), matematico russo, si laurea nel 1880 a San Pietroburgo e diviene ordinario nel 1894.

Dopo i tumulti studenteschi del 1908, si rifiuta di diventare ≪un agente del governo ≫e nel 1910 abbandona l'insegnamento, che riprende dopo la rivoluzione del Febbraio del 1917.

L'importanza di Markov

Markov propone un modello di calcolo basato sull'elaborazione di stringhe con un algoritmo privo di stato – a differenza delle MdT – basato su **regole di riscrittura** di stringhe (**catena di Markov)**.

Le idee di Markov influenzano profondamente tra gli altri Claude Shannon e Noam Chomsky. I modelli nascosti di Markov (**Hidden Markov Models, HMM**) si sono rivelati fondamentali in campi quali il riconoscimento acustico e ottico, l'apprendimento automatico e la bioinformatica.

Figura: Andrej Markov

Emil Post

Emil Leon Post (1897–1954) nato in Polonia ma naturalizzato statunitense, è logico e matematico. Nella sua dissertazione dottorale del 1921 alla Columbia University dà la prima dimostrazione della completezza sintattica del calcolo proposizionale e dell'indecidibilità del calcolo dei predicati, e introduce le tavole di verità a n valori – indipendentemente da Ludwig Wittengstein e Charles Peirce.

L'importanza di Post

Nel 1936 fornisce una definizione del concetto di computabilità indipendentemente da Turing ma equivalente alla MdT – talvolta detta macchina di Post-Turing. Nel 1943 fornisce una precisazione della nozione di algoritmo (**algoritmo di Post**) e si occupa del problema della riducibilità e di problemi di decisione, sviluppando la nozione di gradi di insolubilità (gradi di Turing), risolta da lui stesso e da Stephen Kleene nel **1954**, mediante la nozione di **Turing-equivalenza**.

L'importanza di Post

Nel 1936 fornisce una definizione del concetto di computabilità indipendentemente da Turing ma equivalente alla MdT – talvolta detta macchina di Post-Turing. Nel 1943 fornisce una precisazione della nozione di algoritmo (**algoritmo di Post**) e si occupa del problema della riducibilità e di problemi di decisione, sviluppando la nozione di gradi di insolubilità (gradi di Turing), risolta da lui stesso e da Stephen Kleene nel **1954**, mediante la nozione di **Turing-equivalenza**.

Dalle sue ricerche deriva la teoria della ricorsione classica (Odifreddi 1989).

Figura: Emil Post

Alonzo Church

Alonzo Church (1903–1995), logico e matematico statunitense, consegue il dottorato nel 1927 all'Università di Princeton, dove diventa professore di matematica nel 1929. Ossessivo e maniacale, pulisce accuratamente la lavagna con il sapone anche per un'ora prima di iniziare la lezione, e le sue lezioni sono una lettura parola per parola dei suoi appunti. Nel 1967 si trasferisce in California alla UCLA.

Il sui risultato scientifico principale è la definizione del **lambda calcolo (λ-calcolo)**, pubblicato nel 1936, e la **tesi di Church-Turing**, che dà il fondamento matematico alla scienza dell'informazione.

All'interno del λ-calcolo, Church definisce il concetto di **booleano di Church**, la cui aritmetica viene implementata nel linguaggio di programmazione Smalltalk (vediamo piú avanti).

Figura: Alonzo Church a Princeton

L'importanza del problema dell'arresto

La *characteristica universalis* di Leibniz aveva due scopi ideali:

1. essere in grado di scrivere qualsiasi problema logico-matematico;
2. trovare un metodo di decisione per risolvere tutti i problemi espressi in tale linguaggio formale.

Il primo ideale ha preso la forma della logica predicativa al prim'ordine di Frege. Il secondo ideale invece ha ricevuto risposta negativa con i risultati di Church e Turing: *Entscheidungsproblem* significa 'problema della decisione' ed è la formulazione di Hilbert. Turing lo riformula come problema dell'arresto (halting problem), mentre Church trova un'altra strada, che Turing dimostra equivalente nel 1937.

Il lambda calcolo di Church

Nell'aprile 1936 (un mese prima di Turing!) Church pubblica nel *Journal of Symbolic Logic* – di cui è co-fondatore e dove rimane editor fino al 1979 – un paper dove estende i risultati di Gödel, al tempo in visita a Princeton mediante il λ-calcolo. Nel suo formalismo la nozione intuitiva di 'decidibile', viene interpretata come **funzione effettivamente computabile**: Church presenta una fondazione della matematica basata sul concetto di **lambda, ovvero l'astrazione di funzione**.

Mentre la maggior parte dei matematici preferiranno una teoria degli insiemi assiomatica come fondamento, il λ-calcolo viene (ri)scoperto negli anni 1960 in informatica e Intelligenza Artificiale (I.A.) da John McCarthy, Christopher Strachey, Peter J. Landin e Dana Scott.

Basi del λ-calcolo alla Church

Church definisce il λ-calcolo estendendo gli assiomi di Peano e l'intuizione di con due regole:

- α**-conversione**: permette di cambiare nome alle variabili legate;
- β**-conversione**: è la regola di calcolo per sostituzione.

La scrittura λx sta per 'astrazione di funzione di x'. Funzioni a piú argomenti possono essere ottenute iterando l'applicazione di β mediante i combinatori, dovuti a Schönfinkel (1924), operazione nota con il nome di **currying**, da Haskell B. Curry, che l'ha introdotta indipendentemente (Barendregt-Barendsen 2000:8).

Il paradigma di programmazione funzionale

Tutti i linguaggi di programmazione imperativi, dall'assembler al Fortran e al Pascal sono basati sulle MdT: le istruzioni sono sequenze di *statement*.

Esiste però una classe di linguaggi di programmazione basati sul concetto di funzione, la cui esecuzione è fatta da una **macchina di riduzione**, che implementa la β-riduzione del λ-calcolo.

Il paradigma di programmazione funzionale

Tutti i linguaggi di programmazione imperativi, dall'assembler al Fortran e al Pascal sono basati sulle MdT: le istruzioni sono sequenze di *statement*.

Esiste però una classe di linguaggi di programmazione basati sul concetto di funzione, la cui esecuzione è fatta da una **macchina di riduzione**, che implementa la β-riduzione del λ-calcolo.

Esempi di linguaggi funzionali: Miranda, ML, Haskell, Scheme sono puri, mentre Lisp, Erlang, o Python sono ibridi (Barendregt-Barendson 2000:5). Il λ-calcolo implementato dentro è una qualche variante tipata (non lo vediamo).

La tesi di Church-Turing ridefinisce l'algoritmo

La tesi sostiene che i *computable numbers* delle MdT includono tutti i numeri che si possono in modo naturale considerare come calcolabili. In altri termini, le funzioni effettivamente calcolabili sono le stesse delle funzioni ricorsive. Si tratta di una definizione *operativa* (non è dimostrabile!) di **algoritmo** come procedura effettiva: sequenze di operazioni su simboli (matematici o logici) in accordo a un insieme finito di regole. In particolare:

La tesi di Church-Turing ridefinisce l'algoritmo

La tesi sostiene che i *computable numbers* delle MdT includono tutti i numeri che si possono in modo naturale considerare come calcolabili. In altri termini, le funzioni effettivamente calcolabili sono le stesse delle funzioni ricorsive. Si tratta di una definizione *operativa* (non è dimostrabile!) di **algoritmo** come procedura effettiva: sequenze di operazioni su simboli (matematici o logici) in accordo a un insieme finito di regole. In particolare:

- le macchine di Turing;
- il sistema formale di Post;
- il lambda-calcolo di Church;
- gli algoritmi di Markov;

La tesi di Church-Turing ridefinisce l'algoritmo

La tesi sostiene che i *computable numbers* delle MdT includono tutti i numeri che si possono in modo naturale considerare come calcolabili. In altri termini, le funzioni effettivamente calcolabili sono le stesse delle funzioni ricorsive. Si tratta di una definizione *operativa* (non è dimostrabile!) di **algoritmo** come procedura effettiva: sequenze di operazioni su simboli (matematici o logici) in accordo a un insieme finito di regole. In particolare:

- le macchine di Turing;
- il sistema formale di Post;
- il lambda-calcolo di Church;
- gli algoritmi di Markov;
- le grammatiche dipendenti dal contesto di Chomsky (1956);

La tesi di Church-Turing ridefinisce l'algoritmo

La tesi sostiene che i *computable numbers* delle MdT includono tutti i numeri che si possono in modo naturale considerare come calcolabili. In altri termini, le funzioni effettivamente calcolabili sono le stesse delle funzioni ricorsive. Si tratta di una definizione *operativa* (non è dimostrabile!) di **algoritmo** come procedura effettiva: sequenze di operazioni su simboli (matematici o logici) in accordo a un insieme finito di regole. In particolare:

- le macchine di Turing;
- il sistema formale di Post;
- il lambda-calcolo di Church;
- gli algoritmi di Markov;
- le grammatiche dipendenti dal contesto di Chomsky (1956);

…sono tutti formalismi equivalenti, ovvero **Turing-completi**.

La tesi di Church-Turing ridefinisce l'algoritmo

La tesi sostiene che i *computable numbers* delle MdT includono tutti i numeri che si possono in modo naturale considerare come calcolabili. In altri termini, le funzioni effettivamente calcolabili sono le stesse delle funzioni ricorsive. Si tratta di una definizione *operativa* (non è dimostrabile!) di **algoritmo** come procedura effettiva: sequenze di operazioni su simboli (matematici o logici) in accordo a un insieme finito di regole. In particolare:

- le macchine di Turing;
- il sistema formale di Post;
- il lambda-calcolo di Church;
- gli algoritmi di Markov;
- le grammatiche dipendenti dal contesto di Chomsky (1956);

...sono tutti formalismi equivalenti, ovvero **Turing-completi**. Con le parole di Gödel: ≪un miracolo epistemologico ≫.

L'informatica è una scienza?

Possiamo ora dare una risposta dal punto di vista **formale** a questa domanda:

L'informatica è una scienza?

Possiamo ora dare una risposta dal punto di vista **formale** a questa domanda:

(proposte?)

L'informatica è una scienza?

Possiamo ora dare una risposta dal punto di vista **formale** a questa domanda:

(proposte?)

> *"il fondamento scientifico dell'informatica risiede nella tesi di Church-Turing, e nell'approccio matematico ad essa collegato, l'approccio di* ***matematica costruttiva****, erede dell'intuizionismo di Brouwer, dove tutti gli enti matematici devono poter essere costruibili mediante un algoritmo."*

Grazie. Domande?

Potete scaricare questa presentazione qui:

`http://www.slideshare.net/goberiko/`