Storia dell'Informatica

L'intervallo temporale analizzato va dalla comparsa del primo sistema naturale capace di gestire l'informazione fino al computer, il prototipo artificiale costruito dall'uomo. Può essere suddiviso in tre periodi:

Primo periodo: va dal *big bang* all'*homo sapiens*: ci sono regole che determinano comportamenti (vedi la fisica, la chimica e la biologia). L'universo può essere visto come elaboratore dell'informazione che, col meccanismo dell'evoluzione naturale, produce sistemi via via sempre più complessi fino all'homo sapiens.

Secondo periodo: la *preistoria dell'informatica*, indagine delle esigenze e dei problemi che dai sistemi di scrittura e di numerazione portano, nel tentativo di rendere sempre più efficiente ed efficace il problem solving, alla comparsa di geometria, algebra e logica e dei primi strumenti per gestire l'informazione. Tappe importanti di questo periodo sono: la rivoluzione scientifica, la rivoluzione industriale, lo studio dell'astronomia, le scoperte geografiche, i conflitti, l'emergere delle macchine che hanno cambiato il mondo.

Terzo periodo: la cronologia dell'informatica varia molto, si passa dall'informatica come disciplina scientifica, all'informatica come supporto alla globalizzazione, l'informatizzazione delle professioni (problem solving informatico), le professioni dell'informatica e infine l'intelligenza artificiale: computer come protesi cognitiva.

Il primo periodo
Anche l'universo è in grado di gestire l'informazione. Ogni particella, ogni essere, dall'atomo all'uomo, sembra contenere al suo interno un livello di informazione, di intelligenza (concetto if-then: se succede qualcosa, allora reagisci in un certo modo). Ogni rivoluzione ha posto le basi per quella successiva (origine della vita, riproduzione sessuata, sistema nervoso dell'homo sapiens), e tutte sono avvenute grazie alla capacità intrinseca dell'universo di elaborare informazioni. Con il cervello anche l'homo sapiens ha acquisito la capacità consapevole di elaborare l'informazione e sono comparsi il linguaggio, poi la scrittura, la cultura e infine la civiltà e le scienze.

L'Informatica è la disciplina che si occupa dei problemi connessi al trattamento effettivo ed automatico dell'informazione digitale, a prescindere dal suo significato (per questo ha forti legami con la logica). L'informatica è (quindi) nata con:
- La definizione di un linguaggio per descrivere in modo effettivo procedimenti di elaborazione dell'informazione digitale (definizione di algoritmo),
- La costruzione di una macchina per eseguire algoritmi come manipolazione di simboli in modo automatico.

Le dimensioni dell'informatica possono essere rappresentate dai seguenti aggettivi:

Digitale: a partire dalle tacche su ossa di animali (da 40 a 10 mila anni fa), questo percorso, attraverso le lettere degli alfabeti e le cifre dei sistemi di numerazione, giunge fino ai nostri giorni con l'utilizzo dei più recenti *sistemi* digitali *di memorizzazione e trasmissione dell'informazione*.
Automatico (o tecnologico): questo percorso descrive l'ideazione, la costruzione e lo sfruttamento di proprietà naturali (gravità, elettromagnetismo e struttura della materia) che hanno consentito di realizzare *macchine* (predisponibili e programmabili) *capaci di svolgere compiti specifici in modo autonomo* (orologi, automi, telai, calcolatrici, computer).
Effettivo: con la nascita della scrittura si ha la possibilità di conservare e tramandare informazioni e norme di comportamento e si pone quindi il problema di meditare su ciò che si

scrive e di conseguenza inventare *metodi di ragionamento che siano cogenti* come quelli usati per il calcolo aritmetico; questo percorso è iniziato con la scrittura di codici legislativi (Hammurabi) e si è concretizzato con la nascita della filosofia (dialettica, retorica e logica) e della logica matematica.
Scientifico: col passaggio della logica da disciplina filosofica a disciplina matematica si è posto il *problema della calcolabilità e trattabilità*.
Cognitivo: questo percorso è il più recente e nasce all'inizio degli anni 50 del secolo scorso con le *provocazioni* dei due padri fondatori della disciplina informatica: Alan Turing (*Il computer può pensare?)* e John von Neumann (*Il calcolatore e il cervello*).

Tavola riassuntiva

Metodi e strumenti	Esigenze e problemi	Linguaggi
***Big Bang*, evoluzione naturale e *homo sapiens* : ci sono regole che determinano comportamenti.**		
Gravità Forze nucleari Elettromagnetismo Vita DNA Sistema nervoso	Mettere ordine nel caos Sopravvivenza	Fisica Chimica Biologia (Darwin)
***Protostoria. Homo sapiens* genera problemi e soluzioni: filosofia, logica, aritmetica e geometria**		
Scrittura e numerazione Abaco, orologi, automi Codici legislativi Tavole numeriche Filosofia Cultura indiana e araba Fibonacci, Lullo	Documentare e calcolare (Gilgamesh) Amministrare lo stato (Hammurabi) Descrivere l'astronomia Gestione delle assemblee Esplorazioni e commerci	Aritmetica Problem solving Pseudo-Algoritmi-Rindt Retorica, dialettica Logica, algebra Calcolo combinatorio
***Storia*: vapore, elettricità, elettronica, logica matematica**		
Logaritmi e regoli Meccanica e vapore (orologi, automi, telai) Babbage Elettromeccanica Hollerith Zuse Elettronica Colossus Eniac EDVAC: manufatto elettronico, digitale, automatico, effettivo, intelligente, il COMPUTER.	Rivoluzione copernicana Tavole numeriche Geodesia e navigazione "Errori" Automazione negli uffici Anagrafi e censimenti Calcolabilità Calcoli balistici Crittografia Calcoli di fluidodinamica	Nepero "Calculemus" di Leibniz I *computer* di de Prony Menabrea e Ada Boole Frege Russell Hilbert Goedel Turing e Church "Cespugli" USA Von Neumann
***Cronologia dell'informatica*: disciplina scientifica e supporto alla globalizzazione**		

Professioni e prodotti informatici Programmatore Interpreti Sistemi operativi DBMS Terminali e reti	Problem solving per la globalizzazione Progetti militari Progetti civili Sistemi informativi	Ricerca e sviluppo Corsi di laurea Dipartimenti Discipline

Protostoria

La civiltà comincia con la nascita del linguaggio. Si formano le tribù fino a diventare stati. Emerge l'esigenza di ricordare e di demandare e trasmettere compiti. Compare la scrittura evolve la organizzazione sociale: clan, tribù, stato. L'uomo ha imparato a usare un linguaggio.

Col diffondersi di testi scritti (commerciali, letterari, scientifici, normativi, economici,…) emerge l'esigenza di regole *effettive* per produrre testi corretti e convincenti (retorica e logica), interpretarne i contenuti (dialettica), eseguire calcoli. L'uomo ha imparato a servirsi della scrittura: grammatica, letteratura, astronomia, aritmetica, geometria, logica.

Con l'aumentare della complessità, emerge l'esigenza di disporre di strumenti e metodi che aiutino nella soluzione di problemi. L'uomo ha imparato ad accumulare conoscenza, a fare scienza e a usare la scienza.

<u>Concettualmente</u>

- Al termine di un percorso durato (circa) 13 miliardi di anni, l'universo ha "calcolato/prodotto" la vita e l'homo sapiens.
- Al termine di un percorso scientifico e culturale durato decine di migliaia di anni, l'uomo ha "calcolato/prodotto" la scienza e la tecnologia da cui è emersa l'informatica.
- Da Leibniz a Turing/von Neumann l'uomo ha costruito una "*protesi*" che sa usare un linguaggio articolato.

<u>Parole chiave</u>

L'aggettivo **effettivo**

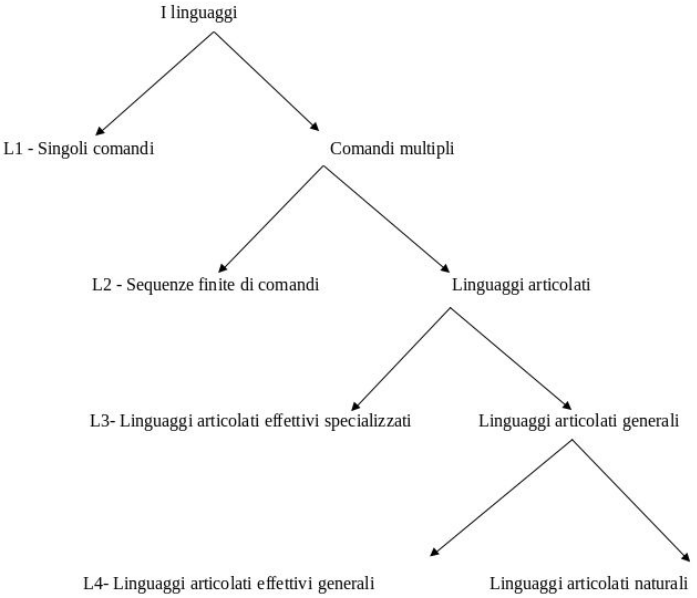
Il linguaggio articolato della "protesi" computer "calcolata/prodotta" dall'uomo è effettivo:

- Usa un numero finito di parole chiave che hanno uno e un solo significato.
- Ogni frase grammaticalmente corretta ha uno e un solo significato e costruzioni sgrammaticate non hanno alcun significato.
- Descrive la gestione dell'informazione come manipolazione di simboli.

Il verbo **calcolare**

Calcolare significa elaborare l'informazione come manipolazione di simboli utilizzando regole *effettive*, senza coinvolgimento di competenze cognitive da parte dell'esecutore. È quindi possibile calcolare il risultato di un'espressione aritmetica, la conclusione di un'argomentazione o un prodotto materiale!

Linguaggio



Il linguaggio è strumento fondamentale per pensare e per comunicare. La qualità della comunicazione dipende dalla qualità del linguaggio usato. Il ruolo del partecipante alla comunicazione dipende dalla qualità del linguaggio che sa gestire. È possibile utilizzare segni per ricordare e comunicare

Un modello di comunicazione può essere lo scambio di dati tra due sistemi attraverso un medium, questi due sistemi hanno informazioni/conoscenza/dati.

Possiamo dire che l'uomo è l'unico animale dotato di linguaggio articolato. e il computer è l'unica macchina dotata di linguaggio articolato. Inoltre l'uomo è «intelligente» perché è consapevole di saper trasformare i dati dell'esperienza in conoscenza. Possono i computer fare lo stesso?

Per simulare di saper trasformare dati in conoscenza è sufficiente un algoritmo. Per simulare l'intelligenza invece si deve essere in grado di interagire in modo autonomo con l'ambiente: avere la possibilità di cambiare il proprio pregiudizio (attitudine) e possedere una funzione di valutazione del proprio comportamento (consapevolezza).

L'informatica è la disciplina scientifica che nel tempo ha portato alla costruzione di un manufatto (computer) con capacità di:
- Interagire con l'ambiente usando un linguaggio articolato
- Simulare di avere un pregiudizio
- E aggiornare il proprio pregiudizio con l'esperienza.

Sistemi di scrittura pre-alfabetica

L'uomo ha imparato ad usare il linguaggio. Il primo passo è stato quello di imparare ad usare dei simboli. Inizialmente si utilizzano segni per ricordare e comunicare. Il vantaggio degli ideogrammi è che si astraggono dalla lingua in sé (Italiano, inglese, ecc.). Gli usi più comuni, esempio con gli egiziani, erano quelli che riguardavano la descrizione di riti, la divinazione e l'onorificenza dei morti. Nel medio oriente, invece, il linguaggio scritto viene usato per le questioni della contabilità. Per quanto riguarda la scrittura cinese, sembra sia un'evoluzione dei sistemi di calcolo numerico. Da noi, invece, è avvenuto il contrario. La scrittura cinese, che ha origine come strumento per disciplinare gli oracoli, è una sorta di combinatoria con numeri binari (i Ching) Tali segni sono stati studiati da Leibniz e, forse, sono stati stimolatori del suo *calculemus*!
Con il diffondersi dei testi scritti emerge l'esigenza di regole effettive per produrre testi corretti e convincenti. Con l'aumentare delle informazioni che sono a disposizione, nasce l'esigenza di avere strumenti che aiutino alla soluzione di problemi. La prima grammatica scritta nasce nel 500 a.C. Successivamente nasce l'alfabeto fenicio che, grazie ai romani, è tuttora utilizzato in quasi tutto il mondo.
I sistemi di scrittura, dunque, non si sono evoluti da un centro e diffusi verso l'esterno. Ognuno ha inventato il proprio sistema.
Un'invenzione proto-informatica si verifica ad Ebla con la *Biblioteca di Ebla.*

Sistemi di numerazione

Il saper contare, come il saper scrivere, è certamente una delle più antiche attività simboliche che l'uomo ha dovuto apprendere per misurare la quantità di cibo da raccogliere o per verificare se mancava qualche animale al ritorno dal pascolo.
Per svolgere questa attività era sufficiente saper incidere tacche su un bastone e saper associare ogni animale a una tacca (**additivo primordiale**).
Successivamente il sistema di numerazione si è evoluto, si è iniziato ad utilizzare dei recipienti (le bulle), contenenti un numero di sassolini corrispondente al numero di oggetti; per facilitare la lettura, sul recipiente veniva riportata una figura evocante l'oggetto cui si riferiva il conteggio. La bulla è poi stata sostituita da una tavoletta con inciso il pittogramma riferito all'oggetto seguito da un numero di tacche corrispondente al conteggio seguito (**additivo evoluto**).
In Egitto, per rappresentare i numeri in forma scritta (tramite sistema additivo), si usavano modalità diverse per rappresentare le unità (con barre verticali), le decine (con cerchi), le centinaia (con corde arrotolate), le migliaia (con fiori di loto), le decine di migliaia (con dita), le centinaia di migliaia (girini) e i milioni (con figure umane a braccia aperte in posizione di sorpresa) (**additivo astratto**).
Un notevole miglioramento tecnico nella numerazione è stato introdotto dai Babilonesi con l'adozione del **sistema posizionale**. In questo sistema il valore è rappresentato non solo dal segno utilizzato (la cifra), ma anche dalla posizione del segno. Il sistema babilonese utilizzava come base della numerazione il numero 60; ancora oggi abbiamo testimonianza del ruolo speciale di questo numero nella suddivisione dell'ora in 60 minuti primi e del minuto primo in 60 secondi. Nasce infine migliaia di anni dopo l'abaco.

La necessità di risolvere problemi ha indotto l'uomo a inventare non solo i sistemi di numerazione e di scrittura, ma anche metodi, strumenti e macchine, quali: la ruota, la leva, l'abaco (non è propriamente una macchina), automi meccanici, orologi ad acqua. Per gli informatici una macchina, invece, è l'insieme delle regole di un procedimento che consente di fare manipolazione di simboli senza il bisogno di capire il significato che ha la manipolazione dell'informazione.

I sistemi di scrittura e di numerazione infatti, non solo permettono l'accumulo di conoscenze, ma incoraggiano la riflessione su contenuti, modi e forme del pensiero e favoriscono la comparsa e la elaborazione di astrazioni. Il fatto che ci sia la scrittura (e che quindi "*verba volant scripta manent"*) induce a dei nuovi modi di pensare per discutere e convincere gli altri. In particolare, come risultato di queste astrazioni si ha la comparsa e lo sviluppo della logica e dell'aritmetica, come discipline che permettono la manipolazione di segni e, quindi, di idee.
Nascono dunque la *logica* e la *retorica* nella comunicazione uno a molti e la *dialettica* nella comunicazione a uno a uno. Una volta i filosofi erano quelli in grado di conversare al massimo livello di tutte le discipline. L'ultimo a farlo è stato Leibnitz. Per questo la storia dell'informatica parte da lui, perché ci lascia in eredità tutto ciò che fa parte del mondo classico.

Eredità del mondo classico

Platone sostiene che la dialettica è lo strumento fondamentale per poter scoprire la verità, ma se non si sa calcolare è inutile intraprendere la strada della dialettica per conoscere il mondo. Ma cosa intendeva con "calcolare"?
Platone individua uno strumento che, per circa 2300 anni, ci seguirà fino a stare alla base dell'idea scientifica che abbiamo oggi. Platone fa riferimento a ciò che aveva formalizzato Euclide, ovvero la geometria. Il sistema formale di Euclide è *la macchina per il calculemus di Platone*. Socrate, tuttavia, non crede al calculemus.
Socrate non lascia nulla di scritto perché riteneva che la scrittura non potesse difendersi da sola. Rispondere che il linguaggio/ la scrittura non fossero effettivi è assolutamente sbagliato, infatti non sono effettivi nemmeno oggi.

Verso la fine del primo millennio a.C. l'uomo ha a disposizione tutti gli strumenti che permettono l'esplosione della cultura. I sistemi di scrittura e di numerazione infatti, non solo permettono l'accumulo di conoscenze, ma incoraggiano la riflessione su contenuti, modi e forme del pensiero e favoriscono la comparsa e l'elaborazione di astrazioni. In particolare, come risultato di queste astrazioni si ha la comparsa e lo sviluppo della logica e dell'aritmetica, come discipline che permettono la manipolazione di segni e, quindi, di idee.

Nel 1200 **Lullo** afferma che tutti i concetti possono essere scomposti in sotto concetti primitivi ancora più semplici. La stessa cosa avviene per i problemi. Si scompongono in problemi più semplici e poi si ricompongono le varie soluzioni per giungere alla soluzione del problema originario. **Hobbes** interpreta l'idea del calculemus di Platone che radicalizza il concetto ed afferma che "Pensare è calcolare". Noi pensiamo, quindi usiamo un linguaggio.
Siamo in un periodo in cui il mondo cambia da geocentrico ad eliocentrico. La cultura prende un'altra strada, gli scienziati cominciano ad affermare delle verità che sono degne di essere prese in considerazione. La scienza comincia ad avere una posizione autonoma:
- Copernico afferma che il Sole sta al centro ed i pianeti compiono la loro rivoluzione su orbite circolari;
- Tycho Brahe ha osservato tutta la sua vita il moto dei pianeti. Disegna le loro traiettorie e dimostra che l'interpretazione di Copernico è falsa;
- Keplero prende in considerazione questi dati e si accorge che la rivoluzione dei pianeti non è su orbite circolari, ma su orbite ellittiche ed il Sole era uno dei due fuochi. Idea che, per la molteplicità dei dati, si afferma nell'immediato;
- Galileo fa delle osservazioni tramite il telescopio che confermano le teorie di Keplero.
Comincia a venir fuori l'esigenza di saper fare i calcoli. Vengono inventati i logaritmi e delle macchine che facevano somme. Il primo ad inventare una macchina per fare i calcoli di Tycho è Schickard. Pascal successivamente inventa delle macchine per gli esattori delle tasse. Il primo ad inventare una macchina che compiesse anche le moltiplicazioni è Leibnitz. A cavallo tra il '600 ed il '700 Leibniz e Newton lavorano su un altro campo: inventano indipendentemente il calcolo differenziale ed integrale. Il sistema di Leibniz, però, prevale su quello di Newton. Un informatico ha contribuito a cancellare il formalismo inventato da Newton per il calcolo differenziale ed integrale. Leibnitz nota che alcuni simboli descrivono in modo semplice le implicazioni/relazioni transitive e simmetriche e nota che descrivono in modo semplice quello che Aristotele descriveva con il sillogismo. Così in Leibnitz sorge l'idea che sia possibile combinare tutti i concetti con dei simboli in modo tale che un'argomentazione potesse essere dedotta facendo dei calcoli in simboli.

<u>Leibniz</u>
Aveva moltissime competenze: era uno storico (storia dei duchi di Hannover), un diplomatico (Luigi XIV e la campagna d'Egitto), un giurista (dottorato su «Uso esclusivo della ragione nelle questioni giuridiche. Dissertatio de arte combinatoria») un tecnico (macchina calcolatrice, macchina per estrarre acqua dalle miniere di carbone), matematico (calcolo differenziale e integrale) e sognatore (definire uno strumento concettuale (un linguaggio) adatto per manipolare i simboli della argomentazioni in modo automatico).

Tutta l'eredità classica e le nuove idee erano tutte presenti e vive nella testa di Leibnitz e consentono lui di scrivere "la macchina di Leibniz per il calculemus":
Sta per arrivare sul mercato la rivoluzione industriale, nascono le macchine a vapore.
Si inizia ad applicare la condensazione del vapore per estrarre acqua dalle miniere.
Un motore a vapore è un'apparecchiatura adatta a produrre energia meccanica utilizzando, in vari modi, vapore d'acqua. In particolare essa trasforma, tramite il vapore, energia termica in energia meccanica. Il calore è in genere prodotto con il carbone, ma può anche provenire da legna, idrocarburi, sole o reazioni nucleari.

I primi esperimenti di macchine a vapore risalgono a l'eolipila di Erone, una sfera cava di metallo riempita d'acqua, con bracci tangenziali dotati di foro di uscita: quando si scaldava l'acqua, questa si vaporizzava e il vapore acqueo usciva dai fori, facendo ruotare la sfera stessa. I tentativi di usare il vapore di Leonardo da Vinci con la sua macchina detta l'Archituono, e nel 1606 gli esperimenti di Giovanni Battista della Porta che riuscirono ad utilizzarlo come forza motrice. Esperimenti analoghi a quelli del Della Porta vennero compiuti anche dall'ingegnere Salomon de Caus, che nel 1615 pubblicò un trattato sul suo sistema contenente una pompa a vapore. In tempi più recenti, le prime applicazioni del vapore si possono far risalire agli esperimenti di Denis Papin ed alla sua pentola a pressione del 1679.

Il primo esempio di applicazione industriale di questo concetto è la macchina di Newcomen, del 1705, che era però grande, poco potente e costosa, quindi anch'essa veniva in genere usata solo per l'estrazione di acqua dalle miniere. Solo più tardi
però, grazie all'invenzione del condensatore esterno, della distribuzione a cassetti e del meccanismo biella-manovella (che consentiva di creare un movimento rotatorio anziché solo alternativo come fino allora), tutte attribuite a James Watt a partire dal 1765, si è potuti passare da applicazioni sporadiche ad un utilizzo generalizzato nei trasporti e nelle industrie. La macchina di Watt riduceva costi, dimensioni e consumi, e aumentava la potenza disponibile. Dal primo modello con 4,4 kW si è passati in meno di 20 anni a locomotive da 0.4 MW.

Lo sviluppo del motore a vapore ha facilitato l'estrazione ed il trasporto del carbone, che a sua volta ha aumentato le potenzialità del motore a vapore. La seconda applicazione del motore a vapore fu muovere il mantice nelle fonderie nel 1776, mentre dal 1787 esso fu usato anche nelle cotonerie per filare. L'incidenza del motore a vapore è evidente: la produzione mondiale di carbone in 50 anni crebbe di un fattore 10; quella del ferro quasi di 20 volte. Nel 1830 vi erano 15.000 motori a vapore in Inghilterra, tra cui 315 piroscafi. Dal 1860 uno scienziato francese, Augustin Mouchot, iniziò a studiare vari modi, utilizzando l'energia solare, per alimentare i motori a vapore.

L’informatica, dal 1850 al 1940, viaggerà su due percorsi paralleli (uno dell’hardware ed uno del software) che terminano uno con la macchina di Turing e l’altro con la macchina di Von Neumann.

<u>Il percorso del software</u>
Con la traduzione in latino delle opere di Al Kuwarizmi si era diffusa in Europa l’aritmetica indo araba, un meccanismo formale per eseguire il *calcolo aritmetico* come manipolazione formale e meccanica di simboli, regolata da una grammatica. In analogia a quanto avviene nel calcolo aritmetico, Leibnitz ipotizza l’esistenza di un meccanismo formale per eseguire il *calcolo filosofico* come una manipolazione meccanica di simboli regolata da una appropriata grammatica.
Il verbo **calcolare** finisce per avere diversi significati. Il principale è la manipolazione effettiva di simboli digitali.
Perciò, gli oggetti che riescono a fare questo tipo di calcolo sono definite macchine:
- Come grammatiche di lingue che disciplinano la manipolazione dei simboli;
- Macchine automatiche: che interagiscono con menu tipo gli elettrodomestici;
- Macchina automatiche programmabili con linguaggi articolati.

Con le macchine, sorge l’esigenza di fare i conti (es. per le navi che iniziano a girare il mondo). Nascono le tavole numeriche, il compasso di Galileo, le macchine calcolatrici. Nepero inventa i “bastoncini” che permettevano di fare conti anche a chi non conosceva la tavola pitagorica, ed i logaritmi.

De Prony e Babbage

Le tavole numeriche sono la risoluzione ad un problema, ma esse stesse lo diventano!
L'organizzazione di De Prony consisteva nella scomposizione elementare del lavoro: assegna a dei matematici il compito di sviluppare le funzioni in serie di Taylor delle funzioni necessarie e, individuata la precisione che si voleva ottenere, occorreva individuare il grado del polinomio. Occorreva quindi trovare altre persone specializzate che calcolavano n+1 valori del polinomio in n+1 distinti di quell'intervallo.
Ovviamente questo metodo è molto dispendioso. Questa è la premessa per l'origine della macchina di Babbage. In Francia c'era una scuola diffusa di automi meccanici, in particolare giocattoli, detti carillon. Importante perché bastava cambiare una scheda e cambiava la musica che veniva riprodotta.
Da qua la nascita della **macchina analitica di Babbage**. Un po' di storia:
Il progetto di de Prony prefigura una gerarchia "informatica" definita da:
- Agente 1: per la definizione formale del problema;
- Agente 2: per la descrizione effettiva del procedimento di soluzione.
- Agente 3: per l'esecuzione dei calcoli, il computer umano.

Questa organizzazione è effettiva per la presenza di linguaggi (formali) condivisi dagli agenti coinvolti:
L'agente 1 e l'agente 2 condividono il linguaggio della matematica; l'agente 2 e agente 3 condividono il linguaggio di pseudo programmazione. Il progetto di de Prony non è stato portato a compimento a causa della mancanza di finanziamenti adeguati alla complessità del progetto, ma resta comunque significativa l'intuizione di de Prony di poter eseguire calcoli complessi utilizzando persone (computer) capaci solo di eseguire somme e sottrazioni.
Nel 1840 presso L'Accademia delle Scienze di Torino si svolse il II Congresso degli Scienziati Italiani al quale partecipò Charles Babbage, invitato a presentare il suo progetto di 'macchina analitica'. La presentazione dettagliata interessò particolarmente il fisico Ottaviano Mossotti e Luigi Menabrea. Menabrea pubblicò in francese nel 1842 una descrizione del progetto di Babbage, "Notions sur la Machine Analytique de M Charles Babbage", che può considerarsi il primo lavoro scientifico di informatica.
Menabrea, illustra il funzionamento della macchina, non la struttura della macchina; il suo lavoro si può classificare come il primo lavoro scientifico sul software; esso è infatti la descrizione di uno pseudo linguaggio di programmazione che consente di fare riferimento all'operazione da eseguire e alle variabili coinvolte per ogni passo del calcolo eseguibile dalla macchina analitica
La grande idea del tedesco Mueller è stata quella di aver ipotizzato di sostituire i calcolatori umani del terzo livello dello schema di de Prony con un calcolatore meccanico ipotizzato ad imitazione del telaio di Jacquard. Questo progetto non è stato immediatamente realizzato perchè Mueller non ha trovato finanziatori! Successivamente, Babbage, venuto a conoscenza del lavoro di Mueller, ha proposto la realizzazione del progetto all'Ammiragliato britannico, ottenendo i finanziamenti necessari per la realizzazione della macchina. Dopo aver lavorato al progetto per una macchina alle differenze per tabulare polinomi, Babbage intraprende un progetto più ambizioso per realizzare una **macchina analitica** che fosse in grado di eseguire una qualunque sequenza di calcoli aritmetici. La collocazione della macchina analitica nella storia dell'informatica è avvenuta con la descrizione delle potenzialità operative di questa macchina da parte dell'italiano Luigi Menabrea diffusa nel mondo anglosassone dalla traduzione fattane da Ada Lovelace. Con la macchina analitica è possibile eseguire sequenze delle quattro operazioni dell'aritmetica.
I risultati finali vengono trasferiti direttamente su carta senza interventi umani. Il vantaggio della macchina non sta nel fare i calcoli in fretta, ma nel farli e riprodurli su carta senza errori.
Si prospettano due specializzazioni:
- Quella dei costruttori di macchine;
- Quella dei costruttori di programmi per le macchine.

Prospettiva intravista da Menabrea, compresa e valorizzata da Ada Lovelace nella traduzione in inglese da lei eseguita con aggiunta di osservazioni e note.

La sequenza di calcolo richiede quindi la predisposizione di schede che specifichino:
- L'operazione da eseguire;
- Le pile contenenti i dati di input e il dato di output.

In sintesi, un programma per la macchina analitica di Babbage è costituito da una tabella contenente le seguenti informazioni:

Codice operativo	Primo operando	Secondo operando	Risultato	Note e commenti

Un calcolo completo viene descritto da un pacco di schede.
Menabrea, dunque fa nascere un vero e proprio linguaggio di programmazione. Ne consegue che nasce il mondo della scrittura dei programmi.

L'algebra di Boole

Seguendo il progetto del calculemus di Leibniz, Boole propone un linguaggio artificiale, un'algebra con due operazioni.
Babbage dimostra di non conoscere Boole. Conosce il quo facto e porta in Inghilterra il sistema di Leibniz che poi sostituisce quello di Newton. Per Babbage non esistono i linguaggi di programmazione. Menabrea e Ada li intravedono, ma finisce lì.
Diventa interessante lo sviluppo dei linguaggi basati sul quo facto di Leibnitz. Il primo passo viene compiuto nel suo lavoro *Le leggi del pensiero* in cui si percepisce la possibilità di realizzare (almeno in parte) il sogno di Leibniz di esprimere il calcolo filosofico (*quo facto, calculemus*) con un linguaggio formale. Boole, nella prospettiva del "sogno" di Leibniz, studia le leggi fondamentali delle operazioni della mente per mezzo delle quali si attua il ragionamento e le formula con un linguaggio simbolico di un calcolo per fondare la logica matematica. È un principio generale del linguaggio (non solo di quello matematico) che sia consentito di usare simboli (come nomi) per rappresentare qualunque cosa si scelga di voler rappresentare. *Boole, con questa proposta, ha dimostrato che la deduzione logica poteva essere trattata come un calcolo.*
In logica matematica, l'algebra di Boole è un linguaggio con due operazioni nel quale i valori delle variabili sono due (spesso denotati con 1 e 0). A proposito dell'algebra di Boole, Frege osservava che una delle due operazioni di questo linguaggio poteva essere interpretata come simbolo della moltiplicazione tra numeri, dell'intersezione tra classi, della congiunzione tra proposizioni in algebra di Boole, cioè un insieme di operazioni indicate con + e con – fatte con i simboli 0 ed 1.
Tutte le deduzioni logiche prodotte con sillogismi possono essere descritte con il linguaggio di Boole ed essere ottenute con calcoli della sua algebra. Il sillogismo di Aristotele non diventa più un ragionamento logico, ma vero e proprio calcolo.

L'algebra di Boole è un principio generale del linguaggio (non solo di quello matematico) che sia consentito di usare simboli (come nomi) per rappresentare qualunque cosa si scelga di voler rappresentare. Uso di simboli per rappresentare proposizioni, 0 è falso, 1 è vero; + OR e * è AND. La macchina di Boole fa il calcolo delle proposizioni. Uso di simboli per rappresentare insiemi: 0 è vuoto, 1 è universo; + è l'unione, * è intersezione. La macchina di Boole fa unione e intersezione di insiemi.

Frege

Tutte le deduzioni logiche prodotte con sillogismi possono essere descritte con il linguaggio di Boole e essere ottenute con calcoli della sua algebra: questo è il primo risultato parziale positivo

nella prospettiva ipotizzata da Leibniz, positivo, ma parziale. Infatti, la proposizione tutti gli studenti bocciati sono pigri o stupidi non è del tipo tutti gli X sono Y e non può quindi essere descritta col linguaggio di Boole.

Le macchine sono solo quelle che possono essere programmate. Per ottenere un sistema logico capace di descrivere tutte le inferenze deduttive della matematica, Frege introduce simboli speciali usabili per analizzare la struttura di una singola proposizione. Da questi esempi si vede che Frege non sta solo elaborando un trattamento matematico della logica. Frege con questo sistema non solo elabora un trattamento matematico della logica, ma sta creando un nuovo linguaggio, concretizzando l'idea di Leibniz di una lingua universale la cui potenza espressiva derivasse da una scelta oculata dei simboli.
Di fatto Frege sta creando un nuovo linguaggio artificiale (Begriffsschrift), col quale scrivere inferenze logiche come operazioni eseguibili sui simboli in modo meccanico (cioè senza la necessità di capirne il significato), ovvero eseguire il calcolo dei predicati. Si può dire che Frege abbia inventato una macchina.
La Begriffsschrift di Frege è il primo esempio di linguaggio formale artificiale dotato di sintassi e per questo si può considerare l'*antesignano dei linguaggi di programmazione*. Partendo da opportune premesse per raggiungere un risultato, era possibile applicare le regole del linguaggio per tentare di raggiungere la conclusione, ma se il tentativo falliva non c'era modo di sapere la causa, cioè se era applicato male il metodo o se era incompleta la premessa.
Frege introdusse (1879) nella logica il concetto di variabile:
per ogni x*, Se x è vero allora y è vero;*
esiste un x tale che*: Se x è vero, allora z è vero.*
Cioè non ragioniamo più su predicati fissi, ma su predicati variabili che si possono affermare:
1) su tutte le entità di un certo insieme – quantificatore universale;
2) per almeno un elemento dell'insieme – quantificatore esistenziale.

Il linguaggio di Frege è un ulteriore passo avanti (rispetto all'algebra di Boole) per il progetto di Leibniz: consente, in linea di principio, di descrivere tutti i ragionamenti (matematici), ma come calcolo filosofico non garantisce di raggiungere un risultato concreto in un tempo finito.

Russel
Dopo Boole e Frege, Russell ha contribuito a formulare un insieme di assiomi e di regole di inferenza che permettano di derivare tutte le verità logiche. L'obiettivo di Frege e di Russell era quello di assiomatizzare la logica (il pensiero) così come Euclide aveva assiomatizzato la geometria.
Nei *Principia Mathematica*, tre volumi scritti con Whitehead, viene presentato un sistema di logica simbolica (un linguaggio per descrivere deduzioni) capace di realizzare il programma di Frege di riduzione dell'aritmetica alla logica pura senza incorrere nei paradossi.
Russel, con i *Principia Mathematica*, definisce un sistema formale, il calcolo dei predicati del primo ordine, la logica del primo ordine e dimostra che la formalizzazione completa della matematica entro un sistema di logica simbolica fosse possibile.

Hilbert
I Principia non risolvono però la questione di contraddizioni che possono essere derivate dagli assiomi adottati da Russell e Whitehead, né tantomeno se esistano verità matematiche che non possano essere provate o confutate nel sistema stesso. Da qui nascono le esigenze di chiarezza proposte da Hilbert. Hilbert vuole dimostrare che alla correttezza sintattica corrisponde la correttezza semantica. Hilbert propone due problemi per venire a capo della questione:
- Dimostrare che la logica del primo ordine era completa, cioè che ogni formula che, vista dall'esterno, apparisse valida, poteva essere derivata *dentro* il sistema;

- Trovare un metodo che, data una formula della logica del primo ordine, sia in grado di determinare, in un numero finito di passi effettivi e ben definiti, se la formula è o non è valida; cioè verificare se l'*Enscheidungsproblem* è risolubile con un algoritmo.

Hilbert immagina un linguaggio simbolico puramente formale (un linguaggio di programmazione?); quindi vuole dimostrare che per ogni inferenza valida esiste una derivazione della conclusione dalle premesse scrivibile, passo dopo passo, utilizzando questo linguaggio. (per Frege/Russell/Hilbert, questo linguaggio sarà il Prolog)

Gödel

I due problemi di Hilbert sono una riproposizione formale del sogno di Leibniz (limitato alla matematica): risolti questi due problemi la matematica si riduce a un calcolo (quo facto ... calculemus). La dimostrazione viene data da Gödel. Il linguaggio della logica è completo, ma non lo è il linguaggio utilizzato da Hilbert. Gödel, inoltre, risponde anche al secondo quesito affermando che il quesito posto da Hilbert non può avere una soluzione positiva se si aggiunge un assioma che non è logico, il sistema che viene fuori non è completo.

Turing

Turing Introduce una grammatica formale per manipolare simboli digitali interpretabile come linguaggio di programmazione di basso livello (la Macchina Universale di Turing) esempio concreto formalmente definito di linguaggio alla Frege/Russell/Hilbert; con questo linguaggio è possibile scrivere algoritmi (macchine di Turing) eseguibili in modo meccanico. Con questi strumenti Turing definisce la classe dei problemi Turing-calcolabili, cioè dei problemi risolubili con un programma, un algoritmo o macchina di Turing e mostra che esistono problemi non Turing-calcolabili; con questo viene mostrato costruttivamente che l'*Enscheidungsproblem* di Hilbert non è risolubile.

Egli scompone il processo di elaborazione dell'informazione riducendolo al trattamento di simboli ed introduce un linguaggio col quale definisce la classe dei problemi calcolabili e dimostra che il problema della decisione di Hilbert non è risolubile con un algoritmo, dunque esistono problemi non calcolabili. Lo stesso problema viene affrontato da un matematico americano, Church, il quale giunge alle stesse conclusioni di Turing.

Turing ha formalizzato un linguaggio per il problema della decisione. Questo linguaggio, «interpretabile» dalla macchina di von Neumann, diventa il prototipo dei linguaggi di programmazione e definisce (con le funzioni ricorsive di Church) la calcolabilità. Tesi di Church-Turing (sperimentalmente verificata): la nozione matematica di funzione ricorsiva e la nozione di funzione calcolabile con una macchina di Turing sono effettive e coincidenti.

Questa tesi stabilisce la formale coincidenza fra algoritmo e macchina di Turing.

Ma perché il metodo di Turing smentisce le affermazioni di Hilbert? Apparentemente, i metodi di Church e Turing erano diversi, ma nella sostanza giungono alle stesse conclusioni, quindi si dimostrano entrambi veri.

La proposta di Turing è la più semplice poiché riconduce tutto il calcolo a dei simboli digitali. Le macchine di Turing sono programmi scritti nel linguaggio di Turing e la macchina universale di Turing è un interprete per eseguire qualsiasi macchina di Turing, cioè qualsiasi programma scritto nel linguaggio di Turing.

Una **macchina di Turing** (MdT) è definita da un *insieme di regole* che definiscono il comportamento della macchina su simboli scritti su un *nastro* di input-output. Il nastro, potenzialmente di lunghezza infinita, è diviso in *celle* e ogni cella contiene un simbolo oppure è vuota. Una MdT ha una *testina* che si sposta lungo il nastro leggendo, scrivendo oppure cancellando simboli nelle celle del nastro. La macchina analizza il nastro, una cella alla volta, iniziando dalla cella che contiene il simbolo più a sinistra nel nastro. Ad ogni passo, la MdT legge un simbolo sul nastro ed in accordo al suo *stato interno*:

1. cambia il suo stato interno, e scrive un simbolo sul nastro *oppure*
2. sposta la testina a sinistra o a destra di una posizione.

Bisogna interpretare il significato dei termini:
- La macchina di Turing è un programma.
- Turing fa vedere che, per poter eseguire calcoli sempre più complessi, non fosse necessario costruire macchine ancora più complesse, perché se ho una macchina capace di interpretare quello che è scritto nelle macchine, è sufficiente quella macchina per poter eseguire qualsiasi calcolo di qualsiasi macchina. Questa è la macchina universale di Turing.

«È possibile inventare un'unica macchina che può essere usata per computare qualsiasi sequenza computabile» (Turing, 1936).

Alan Turing non solo ha intuito che questa impresa era possibile: ha anche esattamente mostrato come realizzare questa macchina in modo effettivo. Con la sua dimostrazione nasceva l'era dei computer. È importante ricordare che esistevano entità chiamate computer anche prima che a Turing venisse questa idea, ma allora erano persone, impiegati con sufficiente conoscenza della matematica, pazienza e passione per il proprio lavoro da generare risultati affidabili in ore e ore quotidiane di computazione. *La macchina di Zuse è Turing compatibile.

Questa macchina risolve parzialmente il sogno di Leibniz!

Il percorso dell'hardware: Hollerith

Hollerith introduce macchine tabulatrici automatiche con la gestione dei dati registrati su schede perforate: un primo brevetto è del 1884, quello attuale è del 1889.

La prima macchina tabulatrice usava nastri perforati; la successiva introduzione delle schede perforate ha consentito di effettuare anche operazioni di selezione.

La prima tabulatrice fu costruita in collaborazione con il comitato per il censimento USA del 1890; ne è seguito un immediato successo commerciale di questa macchina dovuto alla decisiva riduzione dei tempi richiesti per le elaborazioni dei dati raccolti col censimento: meno di un anno invece degli otto anni impiegati per il censimento del 1880; questo censimento ha coinvolto 63 milioni di persone e 150 mila comunità. La macchina poteva esaminare fino a 800 schede al minuto. Finalmente il computer meccanico è diventato più efficiente del computer umano!

Successivamente la macchina venne usata anche in moltissimi altri paesi (Russia, Austria, Canada, Francia, Norvegia, Porto Rico, Cuba, Filippine).

Nel 1896 Hollerith fonda la *Tabulating Machine Company* e la macchina viene quindi utilizzata anche per la gestione dei dati aziendali. Alcune invenzioni connesse con la Tabulatrice sono:
- Scheda perforata per contenere i dati da elaborare (Babbage usava le schede per le istruzioni del programma da eseguire);
- Una codifica binaria dei caratteri (codice Hollerith usato per oltre 80 anni); la scheda del censimento era suddivisa in 288 zone perforabili;
- Una macchina perforatrice di schede dotata di tastiera.

Per decodificare le informazioni si usava una scheda hardware contenente 288 aghi retrattili che incontrando una perforazione chiudevano un circuito che faceva avanzare di una unità uno dei 40 contatori che alla fine producevano il risultato del conteggio. La macchina era costruita ad hoc per eseguire un particolare conteggio.

Dato il successo sul mercato aziendale, si pone presto il problema non solo di fare dei conteggi (quante schede hanno particolari perforazioni), ma anche di eseguire calcoli usando i dati perforati su scheda come operandi.

Hollerith ottenne questo ulteriore miglioramento realizzando una versione elettromeccanica della macchina di Leibniz-Poleni (1895). Un miglioramento decisivo (1906) fu introdotto con l'adozione di un pannello mobile per realizzare diversi tipi di collegamento fra gli aghi e i relè dei contatori; si potevano realizzare diversi tipi di conteggi con la medesima macchina, "*programmando*" i calcoli da eseguire mediante i collegamenti sui pannelli. La macchina sarà anche usata per scopi militari per calcolare le traiettorie dei proiettili.

Nel 1910 erano in uso un centinaio di macchine di Hollerith, ma l'Istituto per il Censimento ha usato una macchine fornita da James Power che ha superato il brevetto di Hollerith modificando la macchine perforatrice delle schede.

Zuse

Konrad Zuse iniziò a progettare un calcolatore automatico nel 1934. Nel 1936 descrive un calcolatore automatico con le seguenti caratteristiche:
- Rappresentazione binaria dei numeri con virgola mobile;
- Programma memorizzato su nastro come sequenza di operazioni ciascuna rappresentata da codice operativo, due indirizzi degli operandi e un indirizzo per il risultato;
- Una memoria meccanica per i dati costituita da registri con indirizzo numerico;
- Un dispositivo meccanico con tastiera per l'input collegato via cavo alla memoria: ogni dato registrato sulla tastiera viene trasmesso e memorizzato in uno dei registri della memoria. Zuse ha quindi progettato per primo, in apparenza senza conoscenza del lavoro di Babbage, un calcolatore generale controllato da programma senza istruzioni di scelta, denominato Z1.

Zuse ha il merito di aver costruito il primo calcolatore automatico funzionante avente insieme tutte le seguenti caratteristiche (già ipotizzate singolarmente):
- Aritmetica binaria (Leibniz);
- Controllo da programma (Babbage);
- Formato delle istruzioni con indirizzo di memoria numerico (Ludgate);
- Rappresentazione dei numeri in virgola mobile (Torres y Quevedo).

Atanassov

Il primo progetto per costruire una macchina calcolatrice elettronica è di John Atanassoff nel 1935 (circa) il quale era interessato a risolvere (anche in modo approssimato) complessi problemi di analisi statistica. La parte elettronica è diventata operativa, mentre l'input-output delle schede è rimasto incompiuto. Con la guerra Atanassoff e Berry si sono divisi lasciando il progetto incompiuto. Questa esperienza è stata successivamente recuperata da Mauchly per progettare la ENIAC.

Aiken

"*Babbage's Dream Comes True!"*

Un matematico interessato al problema di risolvere numericamente equazioni differenziali. Viene a conoscenza del calcolatore a schede perforate installato ad Harvard e convince la IBM a progettare e costruire un calcolatore utile per i suoi problemi. Nasce il calcolatore ASCC Automatic Sequence Controlled Calculator noto come Harvard Mark 1 terminato in laboratorio a gennaio 1943 e reso operativo ad Harvard in maggio 1944 dove rimase funzionante fino al 1959. Aiken riconosce di essere debitore a Babbage e si rende conto dell'importanza di prevedere anche l'introduzione di istruzioni di salto condizionato che saranno introdotte in una versione successiva della macchina.

Successivamente Aiken e IBM si sono separati. Aiken ha continuato a migliorare la struttura del Mark 1 costruendo Mark 2, Mark 3 e Mark 4, una versione elettronica completata nel 1952.

IBM

IBM, in collaborazione con la Columbia University ha iniziato a costruire macchine più orientate dalla precedente esperienza di sistemi basati su relais e a schede perforate più che continuare sulla linea del Mark 1. In particolare, il programma era specificato su un pannello invece che essere perforato su nastro e questo rendeva la macchina molto più veloce. Il risultato più significativo di questa collaborazione è la macchina SSEC, Selective Sequence Electronic Calculator, con l'utilizzo anche di tubi a vuoto. Terminata nel 1948 con grande clamore, è stata dismessa nel 1952. Contemporaneamente allo sviluppo della SSEC, l'IBM ha prodotto una serie di macchine CPC, Card Programmed Calculator, sulla scia delle macchine della serie 600. Con

queste macchine (SSEC e CPC), la IBM ha accumulato esperienze decisive che le hanno consentito di avviare la produzione industriale dei computer serie 650 e 701.

Stibitz
Nel 1937 presso i Bell Telephone Laboratories G. Stibitz ha iniziato a costruire una macchina calcolatrice capace moltiplicare e dividere numeri complessi, operazioni utili per il progetto di filtri. Modificato con l'aggiunta della addizione e sottrazione e collegato fino a tre telescriventi, questo "Complex Number Computer" è rimasto in uso fino al 1949.

Mauchly, Eckert e la macchina ENIAC
Nella corsa verso la realizzazione del primo computer i progetti importanti sono quelli svolti presso la Moore School of Electrical Engineerig della University of Pennsylvania. In questa attività era coinvolto John Mauchly già interessato all'utilizzo dell'elettronica; conosceva i lavori di Atanassoff e Berry alla Iowa University e di Stibitz alla Bell, ma pare non fosse a conoscenza dei progetti di Babbage e di Aiken. Mauchly scrisse un rapporto sul lavoro di Atanassoff in cui si dichiara a favore dei calcolatori "a impulsi" (cioè digitali) rispetto a quelli analogici e descrive la possibilità di costruire un calcolatore elettronico digitale.
Erano i problemi di affidabilità a rendere difficile la costruzione di calcolatori completamente elettronici. Questa difficoltà fu superata con la collaborazione di Presper Eckert e, con la partecipazione di Goldstine e Gillon, nel 1943 è stato preparato dalla Moore School e approvato dal Governo degli Stati Uniti il progetto per la costruzione del calcolatore ENIAC (Electronic Numerical Integrator and Computer). Il reale punto di partenza del progetto ENIAC è la nota preparata da Mauchly in agosto 1942 intitolata "L'uso di dispositivi con tubi a vuoto ad alta velocità per eseguire calcoli": questo lavoro è uno dei più importanti documenti della storia dell'informatica.
La costruzione di ENIAC termina in autunno 1945, entra in funzione nel gennaio 1946 presso la Moore School; trasferita presso il Ballistic Research Laboratory è rimasta in funzione fino al 1955.
La difficoltà di costruire i programmi scoraggiava l'uso di ENIAC che di fatto veniva utilizzata solo per problemi che comportavano l'esecuzione di enormi quantità di calcoli. Questa lacuna ha dato il via al progetto di EDVAC prima ancora di terminare ENIAC.

Von Neumann
Perché non abbiamo il computer con questi prodotti? Fondamentalmente perché non veniva usata l'elettronica. Fino alla macchina di Von Neumann, esistevano delle macchine programmate tramite dei fori, quindi il programma non era modificabile perché registrato su un supporto non volatile. Von Neumann, che aveva lavorato insieme ad Hilbert nelle sue dimostrazioni, nel 1930 partecipò ad un congresso di logica per presentare dei risultati parziali nel tentativo di dimostrare la correttezza del sistema di Hilbert. Allo stesso congresso, Godel presenta un risultato intermedio, capito solo da Von Neumann. Quindi abbandona la logica e si dedica a problemi di fisica (anche per la bomba atomica).
Nel 1944 venne a conoscenza da un suo collega, Herman Goldstein, impegnato anch'esso nel Progetto Manhattan, dei tentativi effettuati presso il laboratorio balistico di costruire una macchina capace di trecento operazioni al secondo. Von Neumann ne fu profondamente colpito e vide nuovi e affascinanti scenari.
Il primo incontro con un calcolatore fu poco tempo dopo, con la macchina Harvard Mark I (ASCC) di Howard Aiken, costruita in collaborazione con l'IBM; poi conobbe ENIAC (Electronic Numerical Integrator And Computer) presso il Ballistic Research Laboratory, un ammasso enorme di valvole, condensatori e interruttori da trenta tonnellate di peso, costruita da Presper Eckert e John Mauchly.
(1 e 2 dicono la stessa cosa. 1 versione Wikipedia, 2 appunti delle lezioni)

1. Questo primordiale computer era utile nei calcoli balistici, meteorologici o sulle reazioni nucleari, ma era una macchina limitata, quasi priva di memoria e di elasticità, che

eseguiva solo operazioni predeterminate. Per migliorarla bisognava utilizzare l'intuizione avuta da Alan Turing una decina d'anni prima nel suo articolo sui numeri computabili, cioè permettere al computer (l'hardware) di eseguire istruzioni codificate in un programma (software) inseribile e modificabile dall'esterno. Nel 1945 pubblicò come frutto di questi studi First Draft of a Report on the Edvac.

2. Va a vedere questa macchina in esecuzione (ENIAC) e capisce che non è fatta bene e che doveva esser progettata con altri criteri per giungere a quella che era la macchina ipotizzata da Turing. Von Neumann afferma che la macchina andasse modificata affinché potesse diventare programmabile, dunque il programma andava scritto in una memoria interna riscrivibile (che poteva essere modificata). Propone dunque il progetto di una macchina dove anche le istruzioni dovevano poter essere modificate.

Da queste premesse, viene fuori una cosa in più se c'è la macchina che ha un linguaggio macchina Turing completo, ma non ha la possibilità di modificare il programma che sta eseguendo, non è possibile pensare di realizzare sistemi intelligenti.

La macchina EDVAC

La storia delle macchine calcolatrici digitali controllate da programma ha una solida conclusione con il progetto di un calcolatore elettronico digitale a programma memorizzato, descritto nel "First Draft Report on the EDVAC" presentato da John von Neumann il 30 giugno 1945. Questo rapporto che definisce l'architettura fondamentale di un computer, il progetto della macchina analitica di Babbage su calcolatori controllati da programma, il lavoro di Menabrea e Ada sulla nascita del software e la nota di Mauchly sull'impiego dell'elettronica, descrivono i passi fondamentali che hanno portato alla realizzazione del computer.
La macchina EDVAC si può considerare una evoluzione di ENIAC basata sull'architettura di Von Neumann con il programma memorizzato sul dispositivo contenente anche i dati; con questa modifica si ottengono 4 vantaggi decisivi :
1. Un decisivo miglioramento nella velocità di esecuzione;
2. Il programma può auto modificarsi in fase di esecuzione;
3. Il computer diventa "interattivo" e può aiutare il programmatore nella fase di preparazione del programma, anticipando l'idea di interpreti, compilatori e sistemi operativi;
4. La possibilità di scrivere programmi che apprendono dall'esperienza.

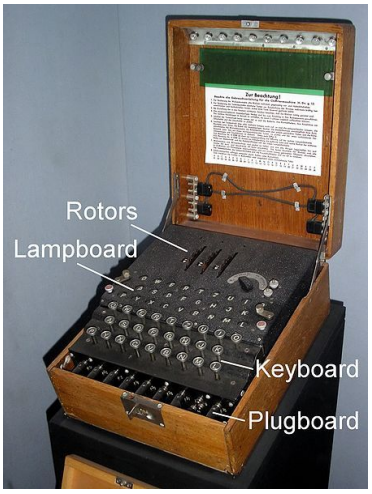
Con EDVAC i calcolatori digitali, elettronici a programma memorizzato sono diventati COMPUTER. Il progetto di EDVAC è stato l'argomento principale delle "Lectures Notes" tenute nell'estate 1946 presso la Moore School della University of Pennsylvania. Dopo questo evento, l'architettura di von Neumann è stata adottata universalmente per la realizzazione di computer. In particolare, in Gran Bretagna è stato avviato nel 1947 il progetto per la EDSAC (Electronic Delay Storage Automatic Calculator) che è il primo computer entrato in attività nel 1949.
Eckert e Mauchly abbandonarono il progetto EDVAC e fondarono la Electronic Control Company e progettarono un computer da installare su missili per controllarne la traiettoria detto BINAC, che non divenne mai completamente operativo; essi ebbero gran successo invece con la realizzazione di UNIVAC, un computer per applicazioni sia scientifiche sia commerciali. La società divenne una divisione della Sperry Rand Corporation e per alcuni anni è stata la maggior produttrice di computer al mondo.
Nel 1946 ha preso il via il progetto guidato da von Neumann a Princeton per la costruzione del computer IAS terminato nel 1952. L'importanza di questo progetto risiede nel grande numero di pubblicazioni che ha generato che sono di fatto state utilizzate come libro di testo per il progetto logico di computer e per la programmazione. In questa prospettiva va segnalata la serie IBM 701 che dominerà la scena per parecchi anni.

ENIGMA

Storia

Viene ideata da Arthur Scherbius intorno al 1915 Enigma, una macchina elettro-meccanica per cifrare e decifrare messaggi. La Polonia comincia ad intercettare (non decifrare) i messaggi nel 1930, anno in cui l'università di Poznań istituisce un corso di matematica discreta: alla fine i tre con migliori voti sono assunti dal controspionaggio; tra essi il più famoso sarà Marian *Rejewski*. Una spia tedesca (Ans-Thilo Smidt), nel 1931 passa ai francesi i "manuali d'uso" per i mesi di settembre e ottobre 1932 (non la struttura o il funzionamento della macchina). Enigma viene ricostruita dai Polacchi con la teoria e metodi di calcolo manuali e i messaggi sono decifrati pure con metodi manuali. A metà del 1933 esisteva una replica polacca di Enigma. Tra il 1938 e il 1939 cambia la modalità d'uso da parte della Wermacht: i metodi manuali non sono più sufficienti per decifrare. Nel 1939 i polacchi condividono le conoscenze con i francesi e gli inglesi. Nel 1941 gli inglesi recuperano un Enigma marino (M4) intatto da un sommergibile.

La macchina



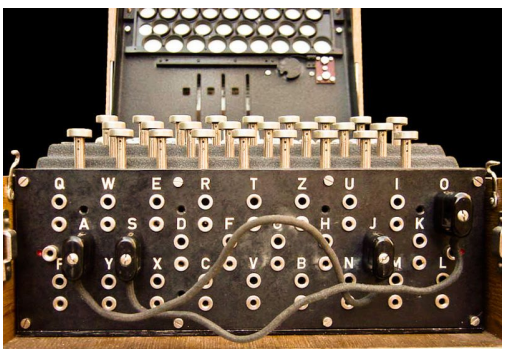
- 3 rotori (scelti prima tra tre, poi tra cinque o più), ciascuno dotato di un anello girevole (con 26 posizioni), opportunamente disposti in 3 alloggiamenti;
- 26 tasti: lettere (maiuscole), quindi senza: "spazio", cifre, segni di interpunzione o speciali;
- 26 lampadine, ciascuna associata a una lettera;
- 1 pannello con 26 coppie di fori (di diverso diametro), ciascuna associato a una lettera, e 6 (o 10) cavetti terminati da due spinotti (asimmetrici).

I rotori (da destra)

- 26 contatti in entrata sporgenti (retrattili)
- 1 ruota dentata con 26 denti
- 1 disco sporgente con 26 ondulazioni smussate usato per ruotare manualmente i dischi
- 1 corpo attraversato da collegamenti che realizzano una permutazione tra i 26 contatti in entrata (a destra) e i 26 contatti in uscita (a sinistra)
- 1 anello girevole con 26 posizioni contrassegnate dalle 26 lettere (o numeri)
- 1 corona circolare liscia con una tacca solidale col corpo (di diametro poco più grande della ruota dentata)
- 26 contatti in uscita fissi

Il movimento dei rotori, quindi, è simile a quello di un contachilometri, ma con una eccezione: due scatti successivi per il rotore 2 quando ruota il rotore 1.

Il pannello



Codifica

Si imposta la macchina: chiave del mese + chiave del giorno. Si sceglie la chiave di messaggio (es.: ABC). Si codifica la chiave di messaggio duplicata (es.: ABCABC → KPZDTF). Si posizionano i rotori con la chiave di messaggio visibile e si codifica il testo del messaggio. Infine avviene la trasmissione di {(chiave di messaggio codificata) + (testo codificato)} per telegrafo o telefono.

Decodifica

Avviene la ricezione del messaggio codificato (telegrafo o telefono). Si imposta la macchina: chiave del mese + chiave del giorno. Avviene la (de)codifica dei primi 6 caratteri del messaggio per ottenere la chiave di messaggio decodificata (es.: KPZDTF → ABCABC). Poi si posizionano i rotori con visibili le 3 lettere della chiave di messaggio decodificata, e si (de)codifica il (resto del) messaggio.

Decifratura polacca

Fino al 1937 vi erano due problemi:
1. determinare le permutazioni fisse associate al riflettore e ai tre rotori, cioè determinare la struttura della macchina.
2. decifrare i messaggi (nota la struttura della macchina), quando non è nota la chiave.

Fino al 1937 la ripetizione della chiave di messaggio consentiva di determinare la caratteristica; tre (soli) rotori davano la possibilità di scegliere tra ~100 | 000 configurazioni; l'associazione caratteristica-configurazione poteva essere costruita e invertita manualmente una volta per tutte.
Dal 1937 al 1939 ci furono vari cambiamenti: (cambiamento del riflettore, dotazione di 5 rotori per macchina da cui sceglierne tre, ecc.); i cambiamenti vengono "facilmente" individuati e la ricostruzione delle permutazioni associate al riflettore e ai due nuovi rotori viene fatta "rapidamente" e in maniera manuale, ma:
3 rotori: 6 possibilità di disporli nei 3 alloggiamenti
5 rotori: 60 possibilità di disporli nei 3 alloggiamenti ~1 | 000 | 000 config.

Decifratura inglese

Alan Turing migliora la macchina di decifratura polacca "Bomb". L'unico attacco possibile era il *plaintext attack*, ovvero individuare la chiave del messaggio. Con la Bomba si velocizza notevolmente questo processo, fornendo agli alleati una macchina che potesse decriptare enigma.

Concetti chiave

Informatica: la disciplina che si occupa dei problemi connessi al trattamento effettivo ed automatico dell'informazione digitale, a prescindere dal suo significato.
Macchina: insieme di regole di un procedimento che consente di fare manipolazione di simboli senza il bisogno di capire il significato.
Digitale: dalle tacche su ossa, le lettere degli alfabeti, le cifre, fino ai sistemi di memorizzazione.
Automatico: macchine capaci di svolgere compiti specifici in modo autonomo.
Effettivo: un linguaggio articolato è effettivo se: usa un numero finito di parole chiave che hanno uno e un solo significato. Ogni frase grammaticalmente corretta ha uno e un solo significato (e frasi scorrette non ne hanno alcuno). Descrive la gestione dell'informazione come manipolazione di simboli.
Scientifico: problema della calcolabilità e trattabilità.
Cognitivo: il computer può pensare? Il calcolatore e il cervello.
Intelligenza: consapevolezza di saper trasformare i dati dell'esperienza in conoscenza.
Simulare intelligenza: interagire in modo autonomo con l'ambiente cambiando il proprio pregiudizio.
Sistemi di scrittura: in occidente per culti religiosi, in oriente prima i numeri (Ching) poi la scrittura.
Sistemi di numerazione: additivo primordiale (tacche su ossa), additivo evoluto (bulle con sassi), additivo astratto (Egiziani, disegni) e infine sistema posizionale (babilonesi, base 60).
Platone: la dialettica è lo strumento fondamentale per poter scoprire la verità, ma solo se si sa calcolare.
Socrate: non lascia nulla di scritto perché "la scrittura non può difendersi da sola".
Lullo: tutti i concetti possono essere scomposti in sotto concetti primitivi ancora più semplici.
Hobbes: giudizio *affermativo*: somma di 2 nomi, *negativo*: sottrazione e *ragionamento* somma di 3 nomi.
Rivoluzione scientifica: Copernico (eliocentrico), Keplero (orbite ellittiche) e Galileo (telescopio).
Leibniz: macchina per le 4 operazioni aritmetiche (tamburo di Leibniz), ipotizza la costruzione di un sistema di simboli per rappresentare il pensiero, e come manipolare tali simboli per costruire argomentazioni e ragionamenti corretti [quo facto, calculemus - ciò ch'è stato fatto può essere calcolato]
De Prony: deve costruire per conto di Napoleone tavole logaritmiche e trigonometriche, per far ciò utilizza squadre di calcolatori umani che si suddividono il lavoro in parti più piccole.
Mueller: intuisce che l'ultimo livello del modello di De Prony può essere eseguito da una macchina.
Babbage: macchina analitica di Babbage, 3 agenti: il primo definisce formalmente un problema, il secondo descrive in modo effettivo come raggiungere la soluzione e il terzo esegue i calcoli.
Boole: linguaggio con due operazioni: OR e AND. Dimostra che deduzione logica può essere calcolata.
Frege: aggiunge alla logica "per ogni x" (tutte le entità di un certo insieme) ed "esiste un x tale che" (per almeno un elemento dell'insieme).
Russell: Principia Mathematica, riduzione dell'aritmetica alla logica pura senza ricorrere in paradossi.
Hilbert: vuole dimostrare che alla correttezza sintattica corrisponde la correttezza semantica.
Godel: afferma che il quesito di Hilbert non può avere soluzione se si aggiunge un assioma non logico.
Turing: introduce una grammatica formale per manipolare simboli digitali, con questo linguaggio è possibile scrivere algoritmi di classe Turing-calcolabili (esistono quindi problemi non calcolabili).
Macchina di Turing: una macchina con un nastro e una testina definita da un insieme di regole che definiscono il comportamento della macchina su simboli scritti su un nastro di input-output. "È possibile inventare un'unica macchina che può essere usata per computare qualsiasi sequenza computabile".
Hollerith: macchina tabulatrice automatica con la gestione dei dati registrati su schede perforate.
Zuse: calcolatore con: aritmetica binaria, indirizzo di memoria numerico e numeri in virgola mobile.
ENIAC: 1945 - U.S. - calcolatore elettronico a impulsi (digitale) non più analogico
Von Neumann: ENIAC non lo convince perché utilizzava ancora schede perforate, voleva creare un calcolatore programmabile, in cui il programma andava scritto in una memoria interna riscrivibile. Propone un progetto di macchina in cui anche le istruzioni potessero venire modificate.
EDVAC: evoluzione di ENIAC basata sull'architettura di Von Neumann.
Enigma: macchina per criptare/decriptare testi. 3 rotori, 26 tasti, 26 lampadine, 26 coppie di fori. La codifica e decodifica avveniva solo dopo aver impostato la macchina (con chiave del mese e chiave del giorno). La codifica prevedeva all'inizio del messaggio la doppia chiave cifrata e poi il testo. La

decodifica prevedeva il mettere in chiaro la chiave e decriptare il plaintext. Turing modifica la macchina Bomb per attacchi plaintext, ovvero trovare la chiave utilizzata e decifrare il messaggio.