La macchina di Turing

Il cammino intrapreso dall'informatica non era inevitabile.
Ancora oggi i computer mantengono traccia dell'opera del geniale e sventurato scienziato inglese che seppe decifrare i codici segreti della Germania nazista durante la Seconda Guerra Mondiale.

Simson L. Garfinkel

Alla nascita di Alan Turing, il 23 giugno del 1912, il computer non era un oggetto, ma una persona. I "computer", in gran parte donne, venivano impiegati per effettuare calcoli ripetitivi per diverse ore. Si trattava di una prassi normale che risaliva agli anni intorno al 1750, quando Alexis-Claude Clairaut assunse due colleghi astronomi per aiutarlo a tracciare l'orbita della cometa di Halley.

L'idea di Clairaut fu quella di dividere il tempo in segmenti e, utilizzando le leggi di Newton, calcolare i cambiamenti della posizione della cometa mentre transitava davanti a Giove e Saturno. Il gruppo lavorò per cinque mesi, ripetendo il procedimento numerose volte nella loro opera di lenta registrazione del movimento dei corpi celesti.

Oggi questa tecnica viene definita simulazione dinamica. I contemporanei di Clairaut la definivano un obbrobrio perché desideravano una scienza di leggi fondamentali ed equazioni essenziali, non certo di tabulati e tabelle di numeri. Comunque, il gruppo di Clairaut riuscì a prevedere in maniera assai attendibile il perielio della cometa di Halley. Nel successivo secolo e mezzo i metodi computazionali dominarono l'astronomia e l'ingegneria.

Quando Turing entrò al King's College, nel 1931, i computer umani venivano variamente impiegati e spesso erano affiancati da macchine per il calcolo. Le schede perforate erano utilizzate per controllare i telai e tabulare i risultati del censimento americano.

Le telefonate venivano effettuate componendo dei numeri su un disco, interpretati da una serie di ripetitori a dieci fasi. I registratori di cassa erano onnipresenti. Un "milionario" non era solo una persona molto ricca, ma anche un calcolatore meccanico in grado di fare moltiplicazioni e divisioni con sorprendente velocità.

Tutte queste macchine avevano un limite di fondo. Non erano solo più lente, meno affidabili e dotate di una memoria infinitesimale rispetto ai computer attuali. Fondamentalmente, le macchine di calcolo e di commutazione degli anni Trenta – e quelle che sarebbero state introdotte negli anni successivi – erano ideate per uno scopo specifico. Alcune potevano manipolare dati matematici, altre seguivano una sequenza variabile di istruzioni, ma ogni macchina era dotata di un repertorio limitato di operazioni utili. Non venivano destinate a uno scopo generale. In poche parole, non erano programmabili.

Anche la matematica attraversava un momento difficile. Agli inizi degli anni Venti il grande matematico tedesco David Hilbert aveva proposto di formalizzare la matematica in termini di un modesto numero di assiomi e una serie di conseguenti dimostrazioni.

Hilbert immaginò una tecnica da utilizzare per convalidare enunciazioni matematiche arbitrarie, per esempio "x+y=3 e x-y=3", e stabilirne la veridicità o la falsità.

Questa tecnica non si affidava all'intuizione o all'ispirazione di qualche matematico, ma era replicabile, insegnabile e abbastanza semplice da venire eseguita da un computer (nel senso che Hilbert dava a questa parola). Questo sistema di dimostrazione delle enunciazioni rappresentava una novità importante perché molti aspetti del mondo fisico potevano venire facilmente descritti con una serie di equazioni. Se si poteva applicare una procedura replicabile per scoprire la verità o falsità di una enunciazione matematica, allora i principi fondamentali della fisica, della chimica, della biologia – persino della società umana – diventavano comprensibili non attraverso gli esperimenti di laboratorio, ma con dimostrazioni matematiche sulle lavagne.

Nel 1931, tuttavia, un logico austriaco di nome Kurt Gödel pubblicò i suoi teoremi di incompletezza, in cui si evidenziava che è possibile creare enunciati veri per qualsiasi sistema matematico, ma è impossibile offrirne una dimostrazione. Poi arrivò Turing, che assestò il colpo finale al progetto di Hilbert, aprendo la strada al futuro del calcolo informatico.

Come ha spiegato Turing, il problema non è solo l'indimostrabilità di alcuni enunciati matematici; in effetti, non esiste un metodo per determinare in tutti i casi se un dato enunciato è dimostrabile o no. Vale a dire, qualsiasi enunciato potrebbe essere vero, falso o indimostrabile e spesso è impossibile riconoscerli. La matematica aveva dei limiti di base, non a causa della mente umana, ma per sua natura.

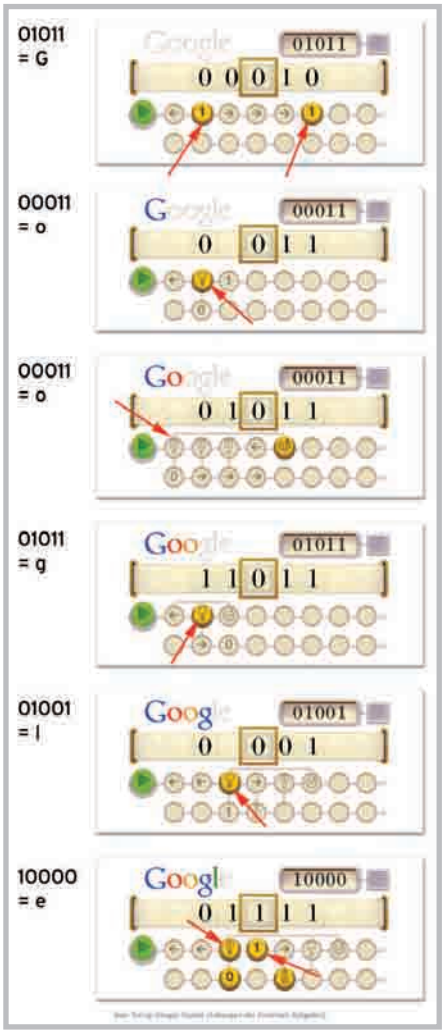
Desta ancora stupore il modo in cui Turing arrivò a formulare il suo test. Il matematico britannico ideò un formalismo logico in cui si descriveva come un computer umano, opportunamente addestrato, avrebbe puntualmente eseguito una serie complessa di operazioni matematiche.

Turing non sapeva come funzionava la memoria umana, così la immaginò alla stregua di un lungo nastro che poteva andare avanti e indietro, sul quale si potevano scrivere, cancellare e leggere simboli.

Non conosceva neanche i meccanismi dell'apprendimento umano, così formulò un complesso di regole legate ai simboli che la "macchina umana" doveva rispettare, e a un qualche tipo di "stato mentale" interiore.

Turing descrisse l'intero meccanismo in modo talmente accurato che una macchina poteva eseguirlo al posto di un computer umano. Turing definì questa entità teorica una "macchina automatica" o *a-machine*; oggi è conosciuta come la macchina di Turing.

Alan Turing e il Doodle che Google gli ha dedicato nel centenario della nascita (23 giugno 1912).



In un saggio del 1936, Turing dimostrò che una *a-machine* era in grado di risolvere qualsiasi problema di calcolo che potesse venire suddiviso in sequenze di passaggi matematici. Inoltre, verificò che ogni *a-machine* era in grado di replicare il comportamento di un'altra *a-machine*.

Tutto ciò era reso possibile dal nastro che poteva memorizzare dati e istruzioni. Con le parole di George Dyson, uno storico della scienza, il nastro contiene «sia numeri che significano cose, sia numeri che fanno cose».

Il lavoro di Turing cambiò radicalmente la situazione e rese chiaro ai progettisti dei primi computer elettronici che le macchine da calcolo non richiedevano operazioni o istruzioni di particolare complessità, ma alcuni registri sempre disponibili (lo "stato mentale") e una memoria di archiviazione per conservare dati e codici. Gli ideatori delle macchine potevano avere la matematica certezza di risolvere qualsiasi problema la mente umana potesse programmare.

Queste intuizioni hanno spianato la strada ai computer digitali, anche se fu John von Neumann che riprese le idee di Turing e realizzò la prima macchina digitale programmabile. La sua "creazione" era dotata di un nucleo centrale che prelevava istruzioni e dati dalla memoria, eseguiva operazioni matematiche e archiviava i risultati. La macchina era anche in grado di ricercare, su richiesta, i contenuti in memoria.

L'architettura di von Neumann è stata recepita da ogni microprocessore ed elaboratore centrale esistente. Malgrado sia molto più efficiente della *a-machine* di Turing, dal punto di vista matematico si tratta della stessa cosa.

Incidentalmente, questa caratteristica fondamentale dei computer aiuta a spiegare perché la ciber-sicurezza sia uno dei problemi più difficili da risolvere dell'era moderna.

Da una parte, Turing ha dimostrato che tutte le *a-machines* si equivalgono, il che rende possibile a un hacker di attaccare un computer e modificare un programma a sua scelta.

Dall'altra parte, poiché non si può sempre riconoscere cosa si può dimostrare, una macchina di Turing non è nelle condizioni di valutare – al di là di quanta memoria, velocità o tempo abbia a disposizione – l'affidabilità di un'altra macchina di Turing e stabilire in modo attendibile se questa seconda macchina sia in grado di portare a termine con successo una serie di calcoli.

Con questi presupposti diventa impossibile la scoperta di un virus. Un programma non può valutare se un pezzo di software mai visto prima sia maligno senza renderlo operativo. Potrebbe risultare innocuo o potrebbe impiegare anni a danneggiare i file dell'utente. Non c'è modo per saperlo prima, se non attivando il programma.

Nel 1938, Turing cominciò a collaborare con il governo inglese e contribuì alla creazione di una serie di macchine per decifrare i codici utilizzati dai tedeschi durante le prime fasi della Seconda Guerra Mondiale.

La vicenda è narrata con dovizia di particolari nella biografia *Alan Turing: The Enigma* di Andrew Hodges.

Sfortunatamente, alcuni dettagli sul lavoro di Turing nel periodo bellico non sono stati resi di dominio pubblico fino al 2000, vale a dire 17 anni dopo il libro di Hodges (e quasi 50 anni dopo il suicidio di Turing). Dai nuovi dati emerge, in realtà, che il suo contributo non era emerso nel giusto valore.

Molte storie della nascita dell'informatica danno l'impressione che sia stato qualche gruppo di ingegneri a decidere di utilizzare le schede perforate, poi i relè, successivamente le valvole e infine i transistor per costruire le più avanzate macchine da calcolo.

Ma le cose andarono diversamente. I computer universali sono stati possibili grazie all'intuizione di Turing che dati e codici si possono rappresentare facilmente nello stesso modo.

Non si deve dimenticare, inoltre, che tutti i computer moderni sono stati prodotti con l'aiuto di computer più lenti, che a loro volta sono stati realizzati con il contributo dei precedenti computer ancora più lenti.

Se Turing non avesse fatto le sue scoperte in quel periodo storico, la rivoluzione informatica avrebbe subito un ritardo di decenni. TR

Simson L. Garfinkel, collaboratore di "Technology Review", edizione americana, è docente di Informatica alla Naval PostGraduate School.