Le radici forti dell'Informatica

l'intreccio storico tra tecnologia e fondamenti logici della Matematica [1]

[1]Francesco Fabris ed Eugenio Omodeo, Dipartimento di Matematica e Informatica
Università degli Studi di Trieste, via Valerio 12b, 34127 Trieste

David Hilbert

Kurt Godel

Alan Turing

Konrad Zuse

Prefazione

Quando si pensa alla parola *Informatica*, che deriva dalla contrazione francese di *Informa*tion Automa*tique*, l'immagine corre necessariamente al calcolatore e ai suoi accessori periferici (la tastiera, lo schermo, il *mouse* ecc.), al punto che la traduzione inglese viene resa con la locuzione *Computer Science*. Anche se è inevitabile riconoscere l'importanza del calcolatore, inteso come macchina fisica che attua gli schemi concettuali evocati dall'Informatica e che ha decretato il successo e la permeabilità delle tecnologie informatiche, è necessario prendere coscienza del fatto che l'Informatica non è *riducibile* alla macchina. Essa non solo è indipendente dalla tecnologia specifica impiegata per costruire i calcolatori (nella fattispecie la tecnologia elettronica dei semiconduttori), ma è indipendente persino dall'esistenza di una macchina fisica che la renda operativa, tant'è che i fondamenti dell'Informatica, dati dalla *Teoria della Computabilità*, furono sviluppati prima della costruzione materiale del primo calcolatore digitale, lo *Z1*, attuata dall'ingegnere tedesco *Konrad Zuse* tra il 1936 e il 1938.

La tecnologia informatica si sviluppa a partire dalla metà degli anni '30, in un momento felice di congiunzione tra due correnti operative e di pensiero ben distinte: da una parte c'era chi inseguiva il sogno millenario di una macchina per fare i calcoli in modo automatico (meccanica nelle prime versioni, elettromeccanica ed elettronica nelle ultime); dall'altra c'era chi si occupava dei *fondamenti logici e assiomatici della Matematica*, sognando una sorta di "meccanizzazione" della stessa, che consentisse di ricavare tutti i *teoremi* di una certa teoria matematica a partire dai suoi *assiomi* e dalle *regole di inferenza*. L'interazione tra queste due correnti di pensiero costituì il contesto fecondo attraverso il quale si passò dai sogni alla realtà.

Dalle prime macchine numeriche al primo calcolatore

La storia della computazione numerica parte dagli abachi cinesi del 1200 D.C., mentre la prima realizzazione di una macchina automatica per il calcolo aritmetico viene fatta risalire a *Blaise Pascal*, filosofo, matematico e fisico francese, che nel 1643 realizza un dispositivo meccanico per eseguire automaticamente addizioni e sottrazioni, la cosiddetta *Pascalina*. È però acclarato che già 150 anni prima *Leonardo da Vinci* aveva progettato una macchina analoga, anche se non arrivò mai a una sua costruzione. Qualche anno dopo, a partire dal 1674, il famoso filosofo e matematico tedesco *Gottfried Wilhelm Leibniz* presentò il progetto di una macchina calcolatrice a ruote e ingranaggi (le *Ruote di Leibniz*), che era in grado di effettuare moltiplicazioni e divisioni. Leibniz è però famoso soprattutto per il suo contributo fondamentale all'individuazione delle basi della Logica Simbolica ("*L'Arte Combinatoria*"), su cui si regge il funzionamento di moderni calcolatori. I successivi sviluppi in tale settore, ad opera di *George Boole*, *Alfred Whitehead*, *Bertrand Russell* e *Giuseppe Peano*, diedero consistenza al sogno di Leibniz di un ragionamento simbolico universale, con la nascita di una nuova disciplina matematica, la Logica Simbolica. L'idea di fondo dell'*Arte Combinatoria* è quella di trovare una logica capace non soltanto di dimostrare la verità di ogni proposizione vera, ma anche di costruire nuove proposizioni con la certezza dei procedimenti matematici.

Il primo modello di calcolatore così come noi lo intendiamo oggi, che fosse cioè in

grado di manipolare non solo numeri, ma anche simboli, lo si deve a *Charles Babbage*, matematico, filosofo e ingegnere britannico, il quale descrisse nel 1834 il progetto della cosiddetta *Macchina Analitica*, modello per tutti i successivi calcolatori digitali universali. La macchina non fu mai realizzata per le difficoltà legate alla complessità meccanica delle sue 25 mila parti, anche perchè i concetti sui quali avrebbe basato il suo funzionamento anticipavano di almeno cent'anni il livello tecnologico necessario alla loro attuazione pratica. Per questa macchina egli aveva infatti immaginato la possibilità di introdurre da un lato le "regole" della computazione (che noi oggi chiameremmo *algoritmi*) e dall'altro i valori da associare alle variabili e alle costanti, e tutto ciò impiegando schede o nastri perforati del tutto simili a quelli usati nei telai tessili di Jacquard fin dai primissimi anni dell'ottocento. I concetti che stanno alla base della *Macchina Analitica* sono gli stessi usati oggi per i moderni calcolatori elettronici. La macchina era costituita da due parti: la memoria (*Store*) che immagazzinava variabili e costanti e nella quale erano conservati anche tutti i risultati intermedi dei calcoli; l'unità di calcolo (*Mill*) che conteneva il programma vero e proprio. Lo schema generale del suo calcolatore è talmente simile a quello dei computer moderni che la tardiva riscoperta dei suoi scritti invalidò alcuni brevetti della IBM. L'opera di Babbage venne poi esaltata da una singolare nobildonna inglese, *Ada Byron*, contessa di *Lovelace* (figlia del poeta Lord Byron), che per prima intuì l'universalità delle idee espresse da Babbage. Tra i due iniziò un fitto scambio di lettere, piene di numeri, idee, fatti e fantasie e nel 1843, in uno scritto ormai famoso, Ada Byron descrisse le possibili applicazioni della macchina nel calcolo matematico, ipotizzando persino il concetto di *Intelligenza Artificiale* e affermando che la macchina, quando realizzata, sarebbe stata cruciale per il futuro della scienza. A titolo di esempio spiegò il modo in cui la macchina avrebbe potuto effettuare un certo calcolo, e così facendo scrisse quello che viene unanimemente riconosciuto come il primo *software* della storia. In onore di Ada Byron, nel 1979 il Dipartimento della Difesa degli Stati Uniti battezzò *Ada* un linguaggio di programmazione che era stato appena realizzato.

Nel frattempo *George Boole*, logico e matematico britannico, cominciò a gettare le basi dello strumento concettuale che sta alla base del funzionamento dei moderni calcolatori, cioè la logica binaria, o *Logica Booleana*, scrivendo l'opera "*An investigation of the Laws of Thought*". Si tratta di un calcolo logico a due valori di verità , *Vero* e *Falso*, che consente di operare su proposizioni allo stesso modo in cui si opera su entità matematiche. Nel suo lavoro Boole mostrò che la logica Aristotelica può essere rappresentata tramite equazioni algebriche. Boole sviluppò i concetti precedentemente espressi da Leibniz sul sistema binario e descrisse gli operatori logici che da lui presero il nome di *Operatori Booleani* (AND, OR, NOT), oggi attuati circuitalmente mediante le cosiddette *porte logiche*. Il lavoro di Boole fu considerato però d'interesse solo matematico-speculativo, almeno fino al 1938, quando *Claude Elwood Shannon*, matematico e ingegnere americano, pubblicò la sua tesi al MIT. Shannon stava lavorando sotto la direzione di *Vannevar Bush*, inventore dell'*Analizzatore Differenziale*, il primo calcolatore analogico per risolvere equazioni differenziali (1930); in particolare egli era interessato alla teoria e alla progettazione dei complessi circuiti di relay che controllavano le operazioni della macchina di Bush. Fu in questo contesto che si rese conto che la logica simbolica Booleana, così come si applicava alla rappresentazione di *Vero*

e *Falso*, poteva essere usata per rappresentare le funzioni degli interruttori nei circuiti elettronici. Ciò divenne la base della progettazione dell'elettronica digitale, con applicazioni pratiche nella commutazione telefonica e nell'ingegneria dei computer. I meriti di Shannon vanno però ben oltre, poiché il suo nome è indissolubilmente legato ai due celeberrimi articoli "*A Mathematical Theory of Communications*" del 1948, e "*Communication Theory of Secrecy Sysytems*" del 1949, che gettarono le fondamenta della *Teoria dell'Informazione* e della *Crittografia* moderna.

I primi anni del '900 furono determinanti per il trapasso tra la tecnologia elettromeccanica e quella elettronica, che nasce con l'invenzione nel 1904 del *diodo a vuoto*, ad opera dell'ingegnere inglese *Sir John A. Fleming*, anche se l'impatto della nuova tecnologia nell'ambito delle macchine da calcolo non sarà immediato, a causa dei problemi di affidabilità ancora presenti. Due anni più tardi l'americano *Lee de Forest*, aggiungendo un terzo elettrodo al diodo di Fleming, la *griglia*, crea il primo *triodo* a vuoto, che consente di amplificare un segnale analogico, ma anche di fungere da interruttore comandato in tensione (senza dispendio di potenza), sostituendo così i lenti e pesanti *relay* elettromeccanici, che necessitano per altro di una rilevante potenza per il controllo. Nello stesso anno viene anche presentata la *Brunsviga*, prototipo di tutte le calcolatrici da tavolo. Alla fine degli anni '20 viene infine brevettato il *nastro magnetico*, ad opera del tedesco *Fritz Pleumer*, mentre le schede perforate passano da 45 a 80 fori, assumendo lo standard adottato da IBM e che rimarrà in uso molti anni.

Il 1936 è l'anno in cui l'ingegnere tedesco *Konrad Zuse* inizia la costruzione del primo calcolatore moderno, la macchina logica "*V1*", successivamente ribattezzata "*Z1*" per evitare qualsiasi riferimento ai tristemente noti razzi V1 tedeschi. Si tratta di un calcolatore meccanico realizzato artigianalmente e con mezzi rudimentali dallo stesso Zuse, nella propria abitazione. Il prototipo rappresenta la prima macchina al mondo, basata su codice binario, completamente programmabile. Zuse, convinto che i programmi composti da combinazioni di bit potessero essere memorizzati, chiese anche un brevetto in Germania per l'esecuzione automatica di calcoli.

Lo *Z1* era un apparecchio programmabile, in grado di processare numeri in formato binario e le cui caratteristiche più apprezzabili, viste con il senno di poi, furono la netta distinzione fra memoria e processore. Questa architettura, che non venne adottata dall'*ENIAC* o dal *Mark I*, (i primi computer realizzati negli Stati Uniti quasi dieci anni più tardi), rispecchia l'architettura del calcolatore ipotizzata solo nel 1945 da *John von Neumann*. Lo *Z1* conteneva tutti i componenti di un moderno computer, anche se era completamente meccanico, come ad esempio le unità di controllo, la memoria, la rappresentazione a virgola mobile, ecc. Aveva una frequenza di lavoro di 1 *Hertz*, era in grado di effettuare una moltiplicazione in 5 secondi, disponeva di 64 celle di memoria a 22 bit e usava al posto dei *relay* circa 20.000 piastre in metallo. Il calcolatore venne poi distrutto assieme ai progetti dai bombardamenti di Berlino durante la seconda guerra mondiale, ma nel 1941 venne costruita la sua terza versione, denominata *Z3*, che diventerà realmente operativa. Lo *Z3* può dunque essere considerato il primo computer automatico digitale perfettamente funzionante con discreta affidabilità.

Negli Stati Uniti inizia nel 1939 il progetto dell'*Automatic Sequence Controlled Calculator* (*ASCC*) della IBM, che in seguito verrà ceduto all'università di Harvard e prenderà il nome di *Mark I*. Quasi contemporaneamente parte anche il progetto del cal-

colatore "*ABC*" di *J.V. Atanasov* e *C. Berry*. Su di esso si sarebbe basato successivamente *J.W. Mauchly* per l'*ENIAC*. È il primo computer che utilizza la nuova tecnologia dei tubi sotto vuoto. Il prototipo, che realizza somme a 16-bit, non arriverà mai in produzione, ma i concetti contenuti nell'*ABC*, come l'*Unità Aritmetico Logica* (ALU) e la memoria riscrivibile, compariranno nei moderni computer. Negli ultimi anni ci sono state molte controversie su chi avesse veramente inventato il primo computer elettronico digitale, anche se una corte di giustizia americana decise in favore di Atanasov.

Dal programma di Hilbert ai teoremi di incompletezza di Gödel

L'ideazione e la realizzazione delle prime macchine calcolatrici, secondo il processo storico delineato brevemente nel paragrafo precedente, ebbe come spinta propulsiva la necessità di effettuare in modo automatico le quattro operazioni elementari con i numeri (somme, moltiplicazioni, differenze e divisioni). Tuttavia la complessità strutturale via via crescente di tali macchine, che ebbero come capostipite la *Macchina Analitica* di Babbage, trasformò completamente la loro natura: infatti il "programma" di calcolo, inizialmente incarnato negli ingranaggi meccanici o nei circuiti elettromeccanici delle macchine più avanzate, e deputato alla soluzione di un problema specifico, lascia a un certo punto il posto a un "programma" non cablato, che può essere modificato dall'esterno con lo scopo di poter risolvere un problema nuovo, e ciò senza dover riassemblare la macchina. La macchina acquista dunque una flessibilità che le consente di essere usata più volte per risolvere problemi di natura diversa, e ciò senza dover cambiare la sua topologia. All'inizio questi erano soprattutto problemi legati al calcolo di fattori numerici, ma il potere della "codifica simbolica", ossia la libertà di attribuire un qualunque significato a un simbolo, coniugato con la possibilità di manipolare i simboli in modo logicamente strutturato, portò a disvelare potenzialità inizialmente insospettabili per le macchine sia pur rudimentali dell'epoca.

È a questo punto che il destino di coloro che inseguivano il sogno di una macchina automatica per fare i calcoli s'intreccia con quello di coloro che miravano a una ricostruzione logica e unitaria di tutta quanta la Matematica, che avrebbe dovuto consentire di ricavarne i teoremi in qualsiasi ambito (analisi, geometria, algebra, ecc.) a partire dagli assiomi e dalle regole di inferenza, secondo un approccio che si inquadra perfettamente col pensiero razionalista, determinista, meccanicista e riduzionista di inizio secolo.

Ricordiamo a tal proposito che ogni *Teoria Matematica*, quale ad esempio l'*Aritmetica*, la *Teoria degli Insiemi*, la *Teoria dei Gruppi* ecc., scaturisce da alcune affermazioni iniziali denominate *assiomi*, che sono considerate vere, a partire dalle quali si sviluppa grazie a specifiche *regole di inferenza*, le quali esprimono le modalità lecite per costruire altre affermazioni vere della Teoria, cioè i *teoremi*. In quest'ottica la Teoria è l'insieme di tutti gli assiomi (o *postulati*), che giocano il ruolo di verità primitive, e di tutti i teoremi che si possono provare usando le regole di inferenza. Ecco ad esempio i celebri *postulati di Peano*, sui quali si fonda l'Aritmetica dei numeri naturali:

Postulati di Peano

1. "0" è un numero;
2. se n è un numero, il suo successore è un numero;
3. "0" non è successore di alcun numero;
4. numeri diversi non possono avere lo stesso successore;
5. se un insieme S di numeri comprende lo 0, come anche il successore di qualunque numero in S, allora S comprende tutti i numeri.

Per quanto riguarda le regole di inferenza, possiamo citare come esempi la *Modus Ponens*, *Modus Tollens* e *Reductio ad Absurdum*, illustrate sinteticamente dalla tabella sotto riportata. La barra indica che a partire dalle premesse che stanno sopra, si trae la conseguenza che sta sotto:

Modus Ponens	$\frac{A \to B,\ A}{B}$
Modus Tollens	$\frac{A \to B,\ nonB}{nonA}$
Reductio ad Absurdum	$\frac{A \to B,\ A \to nonB}{nonA}$

Il rappresentante sommo dell'impostazione riduzionista prima citata fu il grande matematico tedesco *David Hilbert* (1862–1943). Al *Secondo Congresso Internazionale di Matematica* di Parigi del 1900, Hilbert tenne un intervento di portata storica - probabilmente la più influente conferenza matematica di ogni tempo - proponendo un elenco di 23 problemi aperti, che a suo giudizio costituivano la sfida per i matematici del secolo a venire. La tabella di figura 1 riporta l'elenco completo.

La natura di questi problemi era varia e disomogenea: se alcuni erano molto specifici e tecnicamente ben delineati (p.es. il Problema 3, che venne risolto immediatamente), altri (p.es. il Problema 6, sull'assiomatizzazione della Fisica, o il Problema 4) erano troppo generali o troppo vaghi per ammettere una risposta incontrovertibile. Altri ancora, i Problemi 1, 2 e 10, portarono a una soluzione inaspettata per Hilbert: essi ci riguardano qui da vicino, per la loro stretta connessione con i fondamenti della *Teoria della Computabilità*, e quindi con un inquadramento formale dei fondamenti dell'Informatica. Data la loro importanza li esaminiamo a parte.

1^o Problema - Ipotesi del continuo (IC)

Non esiste una cardinalità intermedia tra quella dei naturali e quella dei reali.

Si tratta di accertare se esista un insieme S (infinito) dotato di cardinalità inferiore a quella dei reali e superiore a quella dei naturali. Nel 1938 Kurt Gödel stabilì che IC non è refutabile nell'ambito assiomatico della teoria (di Zermelo-Fraenkel)

Problema	1	risolto (1963)	*L'Ipotesi del Continuo*
Problema	2	risolto (1930)	*Consistenza degli assiomi dell'aritmetica*
Problema	3	risolto	Uguaglianza di volumi tra tetraedri
Problema	4	troppo vago	Costruzione di tutte le metriche con linee geodetiche
Problema	5	risolto	Differenziabilità dei gruppi continui di trasformazioni
Problema	6	aperto	Assiomatizzazione della Fisica
Problema	7	risolto	Trascendenza di a^b, con $a \neq 0, 1$ e b irrazionale
Problema	8	aperto	Ipotesi di Riemann e congettura di Goldbach
Problema	9	parzialm. risolto	Trovare la legge più generale di reciprocità in un qualunque campo algebrico numerico
Problema	10	risolto (1970)	*Risolubilità delle equazioni Diofantee*
Problema	11	parzialm. risolto	Forme quadratiche con coefficienti numerici algebrici
Problema	12	aperto	Estensioni di campi numerici algebrici
Problema	13	risolto	Risoluzione di equazioni di 7-imo grado usando funzioni di due argomenti
Problema	14	risolto	Dimostrazione di finitezza di certi sistemi completi di funzioni
Problema	15	parzialm. risolto	Fondamenti del calcolo enumerativo di Schubert
Problema	16	aperto	Topologia di curve e superfici algebriche
Problema	17	risolto	Espressione di funzioni razionali definite come quozienti di somme di quadrati
Problema	18	risolto	Riempimento spaziale tramite poliedri non regolari
Problema	19	risolto	Analiticità delle soluzioni di Lagrangiani
Problema	20	risolto	Risolvibilità di ogni problema variazionale fissate certe condizioni al contorno
Problema	21	risolto	Esistenza di equazioni differenziali lineari aventi un gruppo monodromico assegnato
Problema	22	risolto	Uniformizzazione di relazioni analitiche per mezzo di funzioni automorfiche
Problema	23	risolto	Sviluppi ulteriori del calcolo variazionale

Figura 1: I 23 Problemi di Hilbert

degli insiemi; nel 1963, Paul Cohen stabilì che in tale ambito non è neppure dimostrabile. Siamo, dunque, di fronte a un problema *indecidibile*.

2^o Problema - Assiomi dell'aritmetica

Accertare che gli assiomi dell'aritmetica sono consistenti.

Gödel dimostrò (1931, *1^o Teorema di Incompletezza*) che in qualunque sistema assiomatico sufficientemente espressivo da contenere almeno l'aritmetica si può individuare un enunciato circa i numeri naturali che

o è indecidibile, cioè indimostrabile e irrefutabile all'interno del sistema (che è dunque *incompleto*);
o può venire sia provato che refutato all'interno del sistema (che è dunque *inconsistente*).

In altre parole *ogni sistema assiomatico sufficientemente espressivo è o inconsistente o incompleto*. Se escludiamo la prima (più catastrofica) eventualità , possiamo esprimere il teorema più semplicemente: non è detto che un enunciato vero sia un teorema (cioè che discenda dagli assiomi tramite le regole di inferenza del sistema).
Da qui Gödel dedusse (*2^o Teorema di Incompletezza*) che quando un sistema assiomatico è consistente e sufficientemente espressivo da contenere almeno l'aritmetica, *non può* provare la propria consistenza. Ciò fornisce una risposta, per quanto negativa, al 2^o problema di Hilbert.

10^o Problema - Risolubilità delle equazioni Diofantee.

Trovare una procedura in grado di stabilire, di qualunque data equazione Diofantea, se ammetta soluzioni intere

Un'equazione Diofantea è un'equazione polinomiale $p(x_1, x_2, ..., x_n) = 0$ a coefficienti interi, che s'intende risolvere assegnando valori interi alle incognite x_i. Yuri Matiyasevich dimostrò , nel 1970, che una procedura risolutiva generale non può esistere: a meno che non si pongano fortissime limitazioni al numero di incognite o al grado del polinomio, siamo di fronte a un ulteriore importante problema indecidibile della matematica.

È evidente che l'impostazione riduzionista di Hilbert, implicita per altro già negli enunciati dei problemi (nei quali si chiede di trovare *la* soluzione, e non *se* una certa soluzione esiste), subì un duro e inaspettato contraccolpo dall'enunciazione dei *Teoremi di Incompletezza* di Gödel, che rimangono sicuramente una delle più importanti scoperte matematiche del '900. Essi gettarono lo scompiglio tra le fila dei matematici dell'epoca, poiché l'idea che qualcosa di matematicamente vero potesse non esser dimostrabile implicava un ridimensionamento essenziale, anche se circoscritto a singoli problemi, nella capacità argomentativa del metodo matematico. D'altra parte il programma riduzionista (chiaramente perseguito, in lieve anticipo rispetto ad Hilbert, dai matematici Gottlob Frege e Giuseppe Peano) aveva implicitamente subito qualche incrinatura, proprio al volgere del secolo e dunque in singolare contemporaneità con l'elencazione dei

23 problemi di Hilbert, ad opera di *Bertrand Russell*, il cui famoso paradosso aveva destabilizzato l'opera di Frege, aprendo un periodo di *crisi dei fondamenti* per la matematica. Tale paradosso riguarda *gli insiemi che non sono membri di sé stessi*. A prima vista la loro stessa definizione potrebbe sembrare mal posta; e in effetti, se prendiamo come riferimento un insieme di numeri, esso non è un numero, per cui sembra privo di senso chiedersi se appartenga o meno a sé stesso. Tuttavia l'insieme degli argomenti trattati in questo paragrafo è esso stesso un argomento (ne stiamo parlando ora!), e dunque è un insieme che appartiene a sé stesso.

L'antinomia di Russell

Se chiamiamo T l'insieme di tutti gli insiemi che non appartengono a sé stessi si ha:

> se $T \in T$ allora $T \notin T$, poiché T contiene per definizione solo insiemi che *non appartengono a sé stessi*
>
> se $T \notin T$ allora $T \in T$, poiché T contiene per definizione tutti gli insiemi che *non appartengono a sé stessi*

Il paradosso aveva famosi precedenti storici, quali il *Paradosso del mentitore*, attribuito ad *Eubulide di Mileto* (filosofo greco del IV secolo A.C.): *Un uomo dice che sta mentendo. Sta dicendo il vero o il falso?* Di questo paradosso è nota anche la variante *Questa frase è falsa*, e una sua versione precedente, attribuita ad *Epimenide*, cretese: *I cretesi son tutti bugiardi*, che non sembra però essere stata scritta con l'intento di illustrare un paradosso. Tuttavia il *Paradosso del mentitore* è una contraddizione logica che gioca sull'autoreferenzialità in un contesto, come quello linguistico, che non è formalizzato matematicamente; infatti la spiegazione più semplice consiste nell'assumere che ogni frase pronunciata (o scritta) esprima implicitamente un'affermazione di verità sull'oggetto della frase stessa, per cui la frase *Questa frase è falsa* andrebbe letta in realtà come *Questa frase è vera e questa frase è falsa*, il che corrisponde all'enunciazione di una semplice contraddizione del tipo *A e non A*, che è falsa. Nel caso del paradosso di Russell le cose erano invece molto più compromesse: il suo argomento evidenziava come una teoria matematica proposta come fondamentale, la *Teoria Elementare degli Insiemi*, nell'assetto formale raggiunto a fine '800, fosse minata da contraddizioni.

Nel 1908 *Ernst Zermelo* riuscirà a sanare l'antinomia di Russell, impostando un nuovo sistema noto oggi come *Teoria assiomatica degli Insiemi di Zermelo-Fraenkel*; ma con la nuova destabilizzazione causata dai teoremi di Gödel, il programma Hilbertiano, teso alla riorganizzazione di tutta la matematica in un edificio formale che avrebbe dovuto autocertificare la propria consistenza, dovrà venire definitivamente archiviato.

La nascita della Computabilità

Sul solco delle riflessioni inerenti gli aspetti logico-fondazionali della Matematica sopra evocati, si sviluppò quella corrente di pensiero che riuscì in seguito a delineare il nucleo fondante dell'Informatica, cioè la *Teoria della Computabilità*, intesa come studio, modellizzazione e individuazione dei limiti relativi all'approccio computazionale

basato sulle *procedure effettive*. Di nuovo lo spunto iniziale partì da Hilbert, che nel 1928 scrisse con W. Ackermann il libro "*Grundzüge der theoretischen Logik*"; in quest'opera compare per la prima volta l'enunciazione del famoso *Entscheidungsproblem* (Problema della decisione) per la *Logica dei predicati (del Primo Ordine)*, cioè per il sistema formale che incorpora la logica classica basata sugli operatori *and* ($\wedge$), *or* ($\vee$), *not* ($\neg$), *implica* ($\implies$), *per ogni* ($\forall$), *esiste* ($\exists$). Per capire il significato del *Entscheidungsproblem*, ricordiamo che in tale sistema formale si possono formare delle formule, le cosiddette *formule ben formate*, come per esempio

$$(\exists F)\{(F(a) = b) \wedge (\forall x)[p(x) \implies (F(x) = g(x, F(f(x))))]\}$$

che si legge come "esiste una funzione F tale che $F(a) = b$ e tale che $\forall x$, se è vero il predicato $p(x)$, allora $F(x) = g(x, F(f(x)))$". Ciascuna formula è suscettibile di una *interpretazione*, che consiste nell'assegnazione delle funzioni, delle variabili e delle costanti. Per esempio, assegnando $f(x) = x - 1$ e $g(x) = xy$ sui numeri naturali, l'interpretazione diventa:

Interpretazione 1: $f(x) = x - 1$ e $g(x, y) = xy$

$$(\exists F)\{(F(0) = 1) \wedge (\forall x)[x > 0 \implies (F(x) = xF(x - 1)]\}$$

che si legge come "esiste una funzione F tale che $F(0) = 1$ e tale che $\forall x$, se $x > 0$ allora $F(x) = xF(x - 1)$; tale interpretazione è vera, poiché corrisponde alla funzione fattoriale. Viceversa, l'interpretazione seguente

Interpretazione 2: $f(x) = x$ e $g(x, y) = y + 1$

$$(\exists F)\{(F(0) = 1) \wedge (\forall x)[x > 0 \implies (F(x) = F(x) + 1]\}$$

risulta evidentemente falsa. Una formula si dice allora *valida* se è vera in tutte le interpretazioni. L'oggetto del *Entscheidungsproblem* riguarda proprio la validità delle formule nella logica dei predicati.

Entscheidungsproblem

> *Trovare una procedura algoritmica per decidere se una qualunque formula nella logica dei predicati è valida (p.es. se una qualunque formula dell'aritmetica è un teorema, cioè derivabile dagli assiomi mediante le regole di inferenza).*

Il problema fu risolto indipendentemente da *Alonzo Church*, che pubblicò nel 1936 un articolo intitolato "*An Unsolvable Problem in Elementary Number Theory*", e da *Alan Turing*, che nello stesso anno pubblicò l'articolo "*On Computable Numbers, with an Application to the Entscheidungsproblem*". Essi dimostrarono, con argomentazioni molto diverse, *la non esistenza di un siffatto algoritmo*. Pertanto, in particolare, è impossibile decidere algoritmicamente se un qualunque enunciato sui numeri naturali è vero o meno. Il lavoro di Church fu l'atto di nascita di un formalismo matematico, denominato λ-*calcolo*, che costituisce un vero e proprio modello di computazione. Tuttavia l'approc-

cio di Turing, basato su un semplice dispositivo chiamato *macchina di Turing* (MdT), e che oggi riconosciamo come la descrizione del primo modello formale di calcolatore, risultò subito molto più convincente e credibile, al punto che Gödel stesso rimase inizialmente dubbioso sulla correttezza del λ-*calcolo*, ma immediatamente convinto dal modello di Turing. La *Macchina di Turing* incarna implicitamente la prima definizione del concetto di *algoritmo*, al punto che oggi la stretta corrispondenza tra ciò che si considera intuitivamente calcolabile mediante una procedura effettiva di tipo algoritmico e la *Macchina di Turing* costituisce il nucleo forte della cosidetta *Tesi di Church-Turing*. Turing risolse (negativamente, come accennato sopra) l'*Entscheidungsproblem* facendo riferimento al problema della *fermata della macchina di Turing*, e dimostrando che, assegnata una qualunque MdT, non è possibile decidere algoritmicamente se essa si fermerà o meno a partire da certe condizioni iniziali. Il successivo concetto di *macchina di Turing Universale*, cioè di una macchina che sia in grado di simulare la computazione di qualunque altra macchina, getta poi le basi teoriche del calcolatore programmabile.

Conclusioni

L'impetuoso sviluppo dell'informatica e il suo rapido affermarsi come disciplina a sé non si può però ricondurre solamente alla storia millenaria dell'algoritmica o all'incontro fra questa componente del pensiero matematico e la tecnologia elettronica: la nuova disciplina si è sviluppata anche a partire da nuove idee fondanti. Assolutamente basilare, fra tali idee, è quella di una macchina a "versatilità completa", cioè programmabile per l'espletamento dei piú diversi compiti (senza modifiche della sua architettura fisica). Il sogno di Leibniz di una logica universale, il fervore progettuale di Babbage e i lavori fondamentali di Turing e Church, hanno instradato il pensiero scientifico verso la conquista di un concetto esplicito di "computabilità", che ha preceduto di circa dieci anni la realizzazione dei primi calcolatori. Altra idea-chiave, ben manifesta nei progetti di Turing e Zuse, è che l'autoreferenzialità - tradizionale fonte di intriganti paradossi - può essere sfruttata anche in senso positivo. Non c'è una ragione per cui i programmi debbano risiedere all'esterno del calcolatore (come avveniva per i nastri perforati rispetto ai telai Jacquard); un programma caricato in memoria, viceversa, potendo non solo indirizzare le azioni del computer, ma anche subire modifiche per effetto delle sue elaborazioni, avrebbe la duplicità di ruolo necessaria all'apprendimento automatico e alla gestione delle altre tematiche proprie dell'Intelligenza Artificiale. Mentre questa seconda idea tarda a dispiegare tutte le potenzialità presenti nella visione di Turing, l'obiettivo di "universalità" del calcolatore può dirsi largamente raggiunto: in effetti, un modesto *laptop* del giorno d'oggi surclassa di molto i colossali calcolatori realizzati da pionieri dell'informatica quali Zuse e von Neumann, che peraltro suscitavano grandi entusiasmi in chi aveva la consapevolezza delle ambizioni che tali prototipi incarnavano. Sarebbe un vero peccato se proprio oggi, mentre si fa un gran parlare di "informatica pervasiva" (o "*ubiquitous computing*") in quanto aspetti tecnologici particolari dell'informatica sono migrati all'interno di palmari, di dispositivi legati alla casa, all'auto, ecc., l'idea originaria venisse persa di vista a favore di logiche proprietarie e di mercato tendenti a riportare in auge soluzioni *ad hoc* o linguaggi programmativi di nicchia, riducendo

di fatto il calcolatore alle funzionalità di una mera calcolatrice cablata, sia pure di tipo sofisticato.

Riferimenti bibliografici

[1] J.L. Casti, W. De Pauli, “Gödel, A Life of Logic”, Perseus Publishing

[2] M. Davis, “Il Calcolatore Universale”, Adelphi, Biblioteca Scientifica 35

[3] M. Davis, “Is Mathematical Insight Algorithmic?”, http://cs.nyu.edu/cs/faculty/davism/penrose.ps

[4] M. Davis, “How Subtle is Gödel’s Theorem”, http://cs.nyu.edu/cs/faculty/davism/penrose2.ps

[5] J.J. Gray, “The Hilbert Challenge”, Oxford Univ. Press.

[6] G.O. Longo, “Il nuovo Golem - Come il computer cambia la nostra cultura”, Edizioni Laterza.

[7] Z. Manna, “Teoria Matematica della Computazione”, Boringhieri.

[8] J. Roulston, “A Rough History of Computing”, www.gadae.com/news/Papers/A Rough History of Computing.pdf

[9] R. Spelta, www.storiainformatica.it

[10] www.wikipedia.org