

Università degli Studi di Trieste
Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Computabilità e Linguaggi

Breve introduzione storica alla Computabilità ¹

¹Francesco Fabris, 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 *Information Automatique*, 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, 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, elettromeccaniche ed elettronica nelle ultime); dall'altra c'era chi si occupava dei *Fondamenti 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 abaci 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*. E' 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 vere, 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 inglese, 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 inglese 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 ha onorato battezzò *Ada* un linguaggio di programmazione che era stato appena realizzato.

Nel frattempo *George Boole*, logico e matematico inglese, 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 on the Law 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), ora 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 Systems" 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 *triode* 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 "VI", successivamente ribattezzata "ZI" 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 ZI 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 ZI 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 operativo. 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*. E’ 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”, di poter cioè attribuire un qualunque significato a un simbolo o a un numero, coniugato con la possibilità di manipolare tali simboli in modo logicamente strutturato, portò a disvelare potenzialità inizialmente insospettabili per le macchine sia pur rudimentali dell’epoca.

E’ 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 ipotizzavano una ricostruzione logica di tutta la Matematica, che consentisse cioè di ricavare tutti i teoremi 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 per esempio l’*Aritmetica*, la *Teoria degli Insiemi*, la *Teoria dei Gruppi* ecc. è basata su alcune affermazioni iniziali denominati *assiomi*, che sono considerate vere, e su alcune *regole di inferenza* che esprimono le modalità lecite per costruire altre affermazioni vere della Teoria, cioè i *teoremi*. In questo modo 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. Un esempio noto di assiomi è dato dai *postulati di Peano* per i numeri naturali, sui quali si basa l’*Aritmetica*:

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. due numeri con lo stesso successore sono uguali;
5. se un insieme S di numeri contiene 0 e anche il successore di ogni numero di S , allora ogni numero è in S .

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

<i>Modus Ponens</i>	$\frac{A \rightarrow B, A}{B}$
<i>Modus Tollens</i>	$\frac{A \rightarrow B, non B}{non A}$
<i>Reductio ad Absurdum</i>	$\frac{A \rightarrow B, A \rightarrow non B}{non A}$

Il rappresentante sommo dell'impostazione riduzionista prima citata fu il grande matematico tedesco *David Hilbert*, che al *Secondo Congresso Internazionale di Matematica* di Parigi del 1900 fece un intervento di portata storica, che viene oramai riconosciuto come la più influente conferenza matematica che sia mai stata tenuta. Hilbert enumerò 23 problemi aperti, che secondo lui 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, poiché alcuni erano molto specifici e tecnicamente ben delineati (p.es. il Problema 3, che venne risolto immediatamente), altri erano troppo generali o troppo vaghi (p.es. il Problema 6, sull'assiomatizzazione della Fisica, o il Problema 4). I più interessanti furono però quelli che portarono a una soluzione inaspettata per Hilbert; essi sono essenzialmente i Problemi 1, 2 e 10, che come vedremo sono molto importanti dal nostro punto di vista, poiché strettamente connessi 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° Problema - Ipotesi del continuo (IC)

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

Si tratta di stabilire la non esistenza di un insieme S la cui cardinalità sia strettamente minore di quella dei reali, e strettamente maggiore di quella dei naturali.

Problema	1	risolto	<i>L'Ipotesi del Continuo</i>
Problema	2	risolto	<i>Consistenza degli assiomi dell'aritmetica</i>
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	parzialm. 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	risolto	Trovare la legge più generale di reciprocità in un qualunque campo algebrico numerico
Problema	10	risolto	<i>Risolubilità delle equazioni Diofantee</i>
Problema	11	risolto	Forme quadratiche con coefficienti numerici algebrici
Problema	12	risolto	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	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	Risolubilità 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

Gödel dimostrò (1938) che IC non può essere refutata con il sistema assiomatico della teoria degli insiemi (di Zermelo-Fraenkel). Nel 1963 P. Cohen dimostrò che non può neanche essere provata (nello stesso sistema assiomatico). Di conseguenza il problema è indecidibile.

2° Problema - Assiomatizzazione dell'aritmetica

Verificare se gli assiomi dell'aritmetica sono consistenti.

K. Gödel dimostrò (1931, *I Teorema di Incompletezza*) che in ogni sistema assiomatico (sufficientemente espressivo, cioè da contenere almeno l'aritmetica) si può costruire una sentenza sui numeri naturali la quale:

o non può essere né provata né refutata all'interno del sistema (sistema *incompleto*);

o può essere provata e refutata all'interno del sistema (sistema *inconsistente*).

In altre parole *ogni sistema assiomatico sufficientemente espressivo o è inconsistente o è incompleto*. Un'altra formulazione informale è che non tutte le sentenze vere sono teoremi (cioè derivabili dagli assiomi usando le regole di inferenza del sistema). Gödel dimostrò inoltre (*II Teorema di Incompletezza*) che ogni sistema assiomatico (sufficientemente espressivo, cioè da contenere almeno l'aritmetica) non può provare la propria consistenza, risolvendo così in negativo il 2° problema di Hilbert.

10° Problema - Risolubilità delle equazioni Diofantee.

Trovare una procedura per stabilire se una qualunque equazione Diofantea ammette soluzioni intere

Un'equazione Diofantea è un'equazione polinomiale del tipo $p(x_1, x_2, \dots, x_n) = 0$, nella quale i coefficienti delle variabili x_1, x_2, \dots, x_n sono interi. Matijasevič dimostrò, nel 1970, che una tale procedura non può esistere, individuando un altro importante problema indecidibile della matematica.

E' 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 di Hilbert aveva implicitamente subito qualche incrinatura già subito dopo l'elencazione dei 23 problemi, ad opera di *Bertrand Russell*, che propose il famoso paradosso a lui intitolato. Esso riguarda *gli insiemi che non sono membri di sé stessi*. A prima vista potrebbe sembrare che già la loro definizione sia infondata; e infatti, se prendiamo per esempio un insieme di numeri esso non è un numero, e dunque non ha senso chiedersi se appartiene 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.

Paradosso 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, poiché si era di fronte a una teoria matematica, la *Teoria Elementare degli Insiemi*, che così come formulata da Cantor aveva evidentemente in sé delle contraddizioni insanabili. In seguito *Ernst Zermelo* riuscì a superare il paradosso, impostando un nuovo sistema assiomatico che portò all'enunciazione della *Teoria assiomatica degli Insiemi di Zermelo-Fraenkel*. Era però chiaro che l'approccio Hilbertiano teso alla ricostruzione sistematica di tutta la matematica doveva essere 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:

$$\text{Interpretazione 1: } f(x) = x - 1 \text{ e } g(x, y) = xy$$

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

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

$$\text{Interpretazione 2: } f(x) = x \text{ e } g(x, y) = y + 1$$

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

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 Unsolvble 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 una qualunque sentenza sui numeri naturali è vera 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’approccio di Turing, basato su un semplice dispositivo, chiamato *macchina di Turing* (MdT), 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 cosiddetta *Tesi di Church-Turing*.

Turing risolse l'*Entscheidungsproblem* facendo riferimento al problema della *fermata della macchina di Turing*, e dimostrando che, assegnata una qualunque MdT, non è possibile decidere alitmicamente 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.

Riferimenti bibliografici

- [1] J.L. Casti, W. De Pauli, "Gödel, A Life of Logic", Perseus Publishing
- [2] M. Davis, "The Universal Computer", Pub. Norton
- [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](http://www.gadae.com/news/Papers/A%20Rough%20History%20of%20Computing.pdf)
- [9] R. Spelta, www.storiainformatica.it
- [10] www.wikipedia.org