Sapere

bimestrale, agosto 2012

ISSN 0036-4681 edizioni Dedalo
anno 78°, numero 4 (1081) 978-88-220-9396-7 / € 7,50

Calcolabilità, crittoanalisi, intelligenza artificiale, morfogenesi. Che cosa ci ha svelato Alan Turing prima di essere costretto al suicidio.
Interventi di: Bernasconi, Codenotti, Gadducci, Cignoni, Cordeschi, Tamburrini, Pisanti, Longo

I nuovi padroni della terra

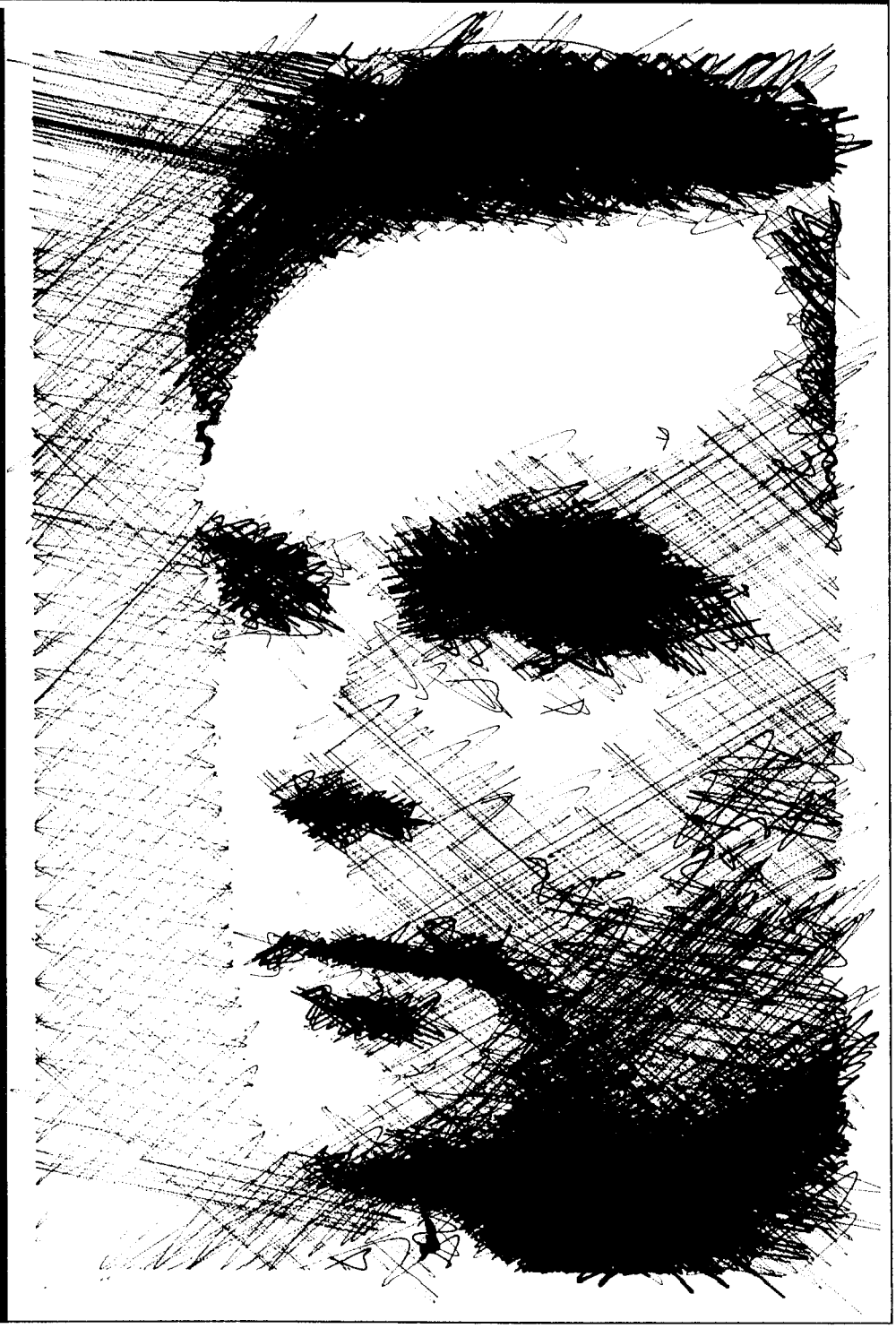
Eduardo Baccari, un gentiluomo in missione nel cuore di tenebra

Prove tecniche di medicina partecipata

Un puzzle lasciato a metà

Anche le formiche si vaccinano

Teheran non si ferma con le bombe



Il genio con due anime in petto

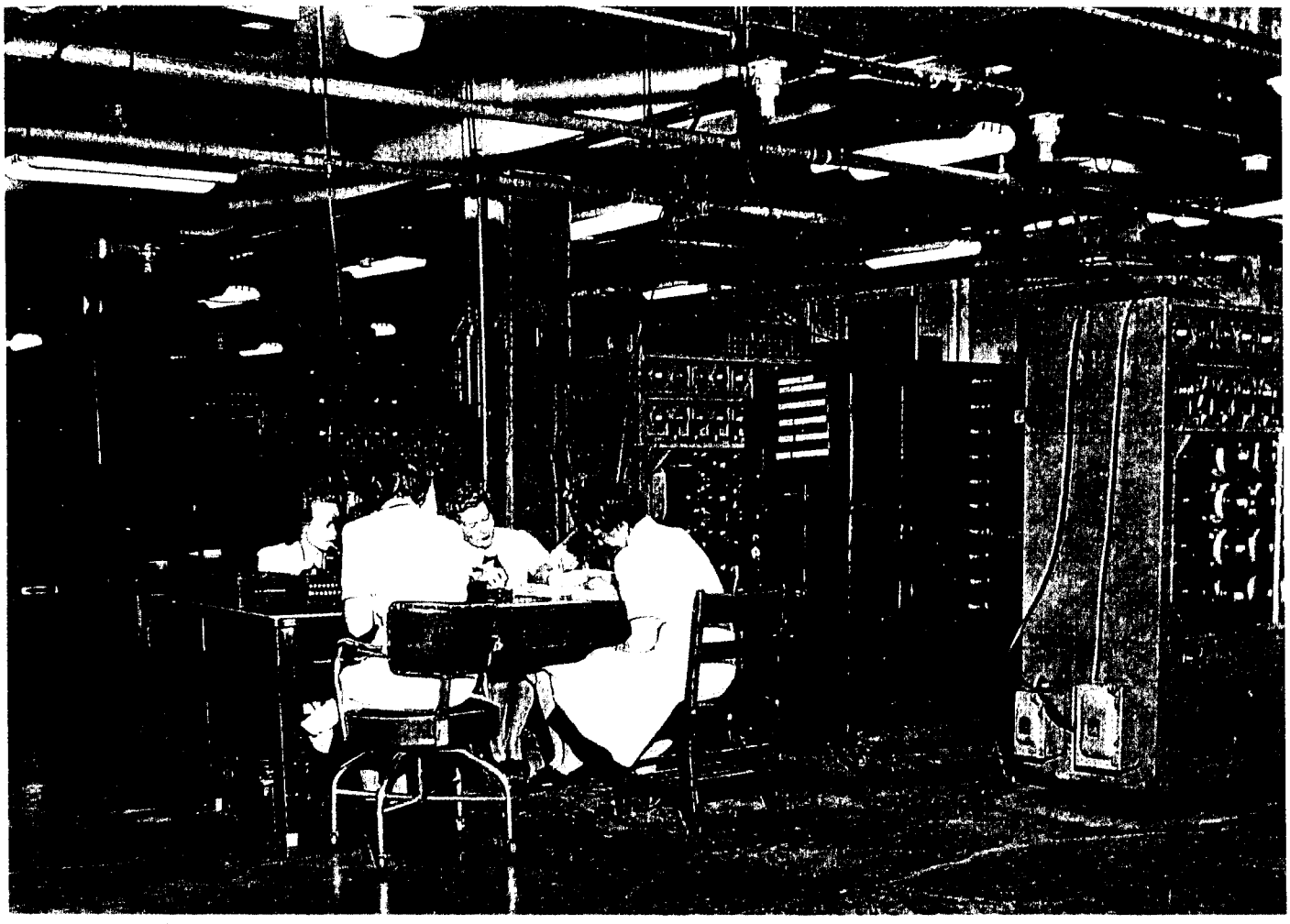
Giovanni Antonio Cignoni

Dalla battaglia dei cifrari durante la seconda guerra mondiale alla realizzazione di primi computer moderni nell'immediato dopoguerra. Il contributo originale, e spesso determinante, di Turing tecnologo

Quando si pensa ad Alan Turing e al suo contributo all'informatica moderna, con ogni probabilità, le prime cose che vengono in mente sono la macchina universale e la prova per decidere se un calcolatore è capace di riprodurre un comportamento umano. Ed è giusto così: le basi formali del calcolo e la speculazione sul confronto fra la macchina e l'uomo danno un'affascinante raffigurazione dell'opera dello scienziato Turing come punto di partenza e ideale traguardo di arrivo.
Nel mezzo però c'è anche un Turing tecnologo coinvolto in attività pratiche e contingenti, partecipe di progetti di enorme respiro e che richiedono l'impegno e la collaborazione con più persone, capace in ogni contesto di dare il suo personale contributo, originale e, spesso, determinante.
Il ruolo di Turing criptoanalista e progettista dei primi calcolatori inglesi è raccontato seguendo quel percorso di continuità che lega le macchine protagoniste delle vicende della seconda guerra mondiale ai primi veri calcolatori moderni realizzati negli anni immediatamente successivi.

Un duello di macchine e metodi

Nel periodo della seconda guerra mondiale furono realizzate diverse macchine che, a pieno titolo, entrano nel novero dei precursori dei calcolatori moderni. Alcune fra le esperienze più interessanti si svilupparono a Bletchley Park, vicino Londra, dove aveva sede la Government Code and Cypher School, il centro che ospitava i criptoanalisti impegnati a decodificare le trasmissioni dell'Asse.
Turing, come matematico, fu da subito reclutato fra i tanti civili che si impegnarano su questo fronte, decisivo per le sorti del conflitto: la lotta contro i sommergibili tedeschi nell'Atlantico, molti scontri per il controllo delle isole del Pacifico, la preparazione dello sbarco in Normandia si risolsero a favore degli Alleati grazie anche alla capacità di leggere le comunicazioni del nemico. Turing per il suo servizio a Bletchley Park ricevette il titolo di Officer of the Order of the British Empire, ma i dettagli del suo contributo sono assai più interessanti delle onorificenze.
La battaglia dei cifrari fu un duello di macchine e di metodi. Le macchine usate dall'Asse per crittare i messaggi furono principamente due: l'*Enigma* e la *Lorenz Schlüsselzusatz*.
L'Enigma, nelle sue varie versioni, era un dispositivo portatile – poco più di una macchina da scrivere – usato per le comunicazioni tattiche fra i comandi e le unità dispiegate sugli scenari di battaglia. Trattava messaggi composti con le 26 lettere dell'alfabeto: usando una chiave stabilita, l'Enigma cifrava il messaggio lettera per lettera e il testo ottenuto veniva poi trasmesso per radio in Morse. La stazione ricevente, dopo aver trascritto il testo cifrato ricevuto via Morse, lo ribatteva su un'altra Enigma configurata con la stessa chiave, riottenendo così il messaggio in chiaro.
La Lorenz, anche questa realizzata durante la guerra in diverse versioni, era invece usata per le comunicazioni fra i centri di comando strategico. La Lorenz cifrava la trasmissione fra telescriventi trattando direttamente i segnali della codifica a 5 bit CCITT ITA 2, lo standard telegrafico allora in uso che comprendeva lettere, cifre e segni di punteggiatura. Una Lorenz, configurata con una chiave prestabilita, era collegata dopo la telescrivente mittente, un'altra Lorenz, configurata con la stessa chiave, era collegata prima della telescrivente ricevente. Il sistema era trasparente: gli operatori alle telescriventi inviavano e ricevevano il testo in chiaro, ma il messaggio su tutti i passaggi intermedi fra le due Lorenz, via radio o via cavo, viaggiava cifrato.
A grandi linee, l'attacco a un messaggio cifrato con l'Enigma o con la Lorenz era condotto con la stessa tecnica di base: si simulava la decodifica con una chiave dopo l'altra escludendo via via quelle che producevano messaggi senza senso. Per simulare la decodifica era però necessario conoscere le mac-



Criptoanaliste della U.S. Navy al lavoro con la macchina Bombe. Sul fondo si contano tre Navy Bombe (National Cryptologic Museum).

chine usate per cifrare, studiando gli esemplari catturati o ricostruendole per tentativi sfruttando la matematica degli algoritmi di cifratura. La lotta contro Enigma e Lorenz era poi una lotta contro il tempo. I messaggi dovevano essere decifrati e passati agli analisti che ne vagliavano la rilevanza strategica, infine dovevano arrivare ai comandi responsabili delle operazioni sui teatri di guerra. Il valore militare delle informazioni scendeva velocemente al passare del tempo.

Dall'altra parte, il nemico contava proprio sulle quantità astronomiche di combinazioni da provare: per l'Enigma erano circa 10^{114}, per la Lorenz circa 10^{151}, numeri che facevano confidare nell'impossibilità di decodificare i messaggi in tempo utile. La decifrazione è infatti difficile ma non impossibile: specialmente se si conosce la macchina o se chi la usa commette errori, come sin dalla fine dell'Ottocento Kerckhoffs aveva sancito nei suoi principi di crittografia. Parte fondamentale dell'uso di Enigma e di Lorenz erano i complessi – e segretissimi – sistemi di regole che, sulla base del calendario, stabilivano le chiavi con cui configurare le macchine. Lo scopo era permettere di sincronizzare le coppie di macchine coinvolte nella trasmissione dei messaggi cambiando però frequentemente le chiavi: così attaccare un messaggio cifrato era ogni volta una storia nuova.

Bombe *vs* Enigma

I messaggi cifrati con Enigma erano attaccati con una macchina elettromeccanica chiamata *Bombe*. La prima versione della Bombe era stata realizzata già nel 1938 in Polonia da Marian Rejewski usando la conoscenza dell'Enigma, che in origine era una macchina commerciale. A Bletchley Park, Alan Turing lavorò al primo progetto per la costruzione della Bombe inglese, che fu successivamente migliorata da Gordon Welchman e da Harold Keen e aggiornata rispetto alle nuove versioni di Enigma che, essendo in dotazione alle unità impegnate nelle azioni di mare e di terra, furono più volte catturate.

La velocità delle Bombe nell'eseguire i tentativi e confrontare i risultati per escludere, con ragionevole certezza, le chiavi inutili era certamente un fattore importante. Ma, visti i tempi strettissimi delle operazioni di guerra, era comunque insufficiente a garantire il successo anche migliorando continuamente le prestazioni delle singole macchine e usandone molte in parallelo – a Bletchley Park arrivarono a funzionare fino a 200 Bombe. C'era anche il problema che, essendo Enigma usata per le comunicazioni tattiche, il traffico generato era molto elevato e molti messaggi erano, di fatto, informazioni di scarsa o nulla rilevanza militare.

Molto più rilevanti furono perciò le soluzioni algoritmiche. A Turing in particolare è dovuto il *Banburismus*, il metodo di costruzione e di analisi dei tentativi che veniva applicato a mano, ma che permetteva di scartare blocchi di chiavi inutili e ridurre enormemente il lavoro delle Bombe. Il nome curioso deriva da Banbury, la sede della tipografia che stampava le griglie cartacee usate dai criptonalisti. Sviluppato da Turing sulla base di un precedente metodo dovuto a Rejewsky, il Banburismus fu la soluzione "software" che permise agli Alleati di rispondere efficacemente anche alla più sofisticata delle versioni di Enigma: quella a quattro rotori introdotta dalla Kriegsmarine tedesca e usata per coordinare gli attacchi dei temibili U-Boot ai convogli che attraversavano l'Atlantico per portare truppe e mezzi dagli Stati Uniti in Inghilterra.
Nel dicembre 1942 Turing partecipò alla British Joint Staff Mission che si unì al gruppo che a Washington lavorava alla progettazione di una nuova versione della Bombe per la US Navy. Il contributo di Turing fu ancora una volta decisivo: con l'applicazione del Banburismus fu necessario costruire molte meno macchine. La stima iniziale di 336 Navy Bombe fu ridotta a 96, con notevoli benefici sui tempi di operatività di questa particolare macchina bellica.

Colossus *vs* Lorenz

Attaccare i messaggi cifrati con la Lorenz fu un problema ancora più arduo perché, al contrario dell'Enigma, nessun esemplare di Lorenz fu catturato dagli Alleati durante la guerra. Tuttavia, nel 1941 un operatore tedesco trasmise due volte un lungo messaggio impiegando la stessa chiave e usando nella seconda trasmissione alcune abbreviazioni: un'imperdonabile violazione delle regole che stabilivano come e quando cambiare le chiavi.
Il meccanismo di base delle macchine tipo Enigma e Lorenz è cambiare a ogni carattere lo schema di sostituzione secondo un algoritmo che ha la chiave come parametro ed è estremamente difficile da ricostruire. Però due testi quasi uguali codificati con la stessa chiave permettono di scoprire come cambia la codifica dei caratteri in funzione della loro posizione. Il vero regalo del pigro operatore tedesco furono proprio le abbreviazioni, dopo le quali si ritrova lo stesso testo ma codificato diversamente solo a causa della differente posizione. Fu la stele di Rosetta che bastò ai matematici di Bletchley Park, in particolare John Tiltman e Bill Tutte, per ricostruire dopo un lungo e paziente studio l'algoritmo della Lorenz. Compresa la macchina, la strada per decifrarne i messaggi era aperta.
Max Newman, un altro dei matematici di Bletchley Park, suggerì che anche la Lorenz poteva essere combattuta seguendo lo stesso schema adottato con la Bombe per l'Enigma. Sulle indicazioni di Newman, una prima macchina optomeccanica chiamata *Heath Robinson* fu progettata da Charles Wynn-Williams e realizzata in alcuni esemplari nel 1942. Non abbastanza veloce e poco affidabile, fu rimpiazzata alla fine del 1943 dal *Colossus*. Progettata da Tommy Flowers, Colossus era una macchina totalmente elettronica che leggeva direttamente i nastri perforati con i messaggi cifrati intercettati e ne tentava la decifrazione simulando la Lorenz con diverse chiavi e sottoponendo i risultati ad analisi statistica per scartare le chiavi inutili. Successivamente, il Colossus fu migliorato da Allen Coombs raggiungendo prestazioni cinque volte superiori alla prima versione. Alla fine della guerra a Bletchley Park c'erano dieci Colossus in funzione.
Ma, anche nella battaglia contro la Lorenz, i progressi più sostanziali si ottennero grazie a Turing, che di nuovo affrontò il problema dal lato software sviluppando una nuova tecnica di scarto di gruppi di chiavi capace di ridurre drasticamente il numero di tentativi da far provare ai Colossus. Questa volta il metodo fu direttamente chiamato *Turingery*.

Verso il calcolatore moderno

Né la Bombe né il Colossus erano però calcolatori moderni. Nonostante Turing lavorasse a Bletchley Park, fosse coinvolto nella prima progettazione della Bombe inglese e fosse autore dei metodi per usare efficientemente la Bombe e il Colossus, nessuna delle due macchine aveva la capacità di calcolo definita dalla macchina di Turing. La Bombe non era praticamente programmabile, il Colossus lo era, ma limitatamente alle funzioni neccessarie per l'analisi statistica dei risultati. D'altra parte, erano macchine dedicate a un compito particolare e urgente: nella contingenza della guerra non c'era motivo di progettarle diversamente.
Anche le macchine realizzate durante la guerra negli Stati Uniti non possono dirsi calcolatori moderni. L'Automatic Sequence Controlled Calculator (ASCC) costruito con un finanziamento dell'IBM all'Università di Harvard (e per questo noto anche come Harvard Mk1) lavorò all'US Bureau of Ships a partire dal 1944. L'ASCC era elettromeccanico, programmabile, ma non Turing completo. Fu però il primo calcolatore ad essere usato intensamente per il calcolo numerico durante la guerra.
L'Electronic Numeric Integrator and Computer (ENIAC) fu un progetto militare finanziato dall'US Army Ballistic Research Laboratory. Il contratto per la realizzazione da parte dell'Università della Pennsylvania fu firmato nel giugno del 1943, ma la macchina fu definitivamente completata solo nel 1946. ENIAC era un calcolatore elettronico digitale, era Turing completo, ma la sua programmazione avveniva tramite la configurazione di numerosi interruttori, cavi e spinotti.
Anche sul fronte opposto, in Germania, ci furono interessanti precursori. Le macchine su cui Konrad Zuse aveva cominciato a lavorare intorno al 1936 ottennero durante la guerra il finanziamento del Ministero dell'Aviazione. La Z3, completata nel 1941, era una macchina elettromeccanica programmabile tramite un nastro perforato. Nel 1998 è stato dimostrato che, adottando tecniche di programmazione molto particolari – e quasi impossibili da mettere in pratica – la Z3 poteva considerarsi Turing completa.
Il risultato più rilevante delle varie esperienze belliche è invece il consolidamento dell'elettronica digitale come la tecnologia di riferimento per la realizzazione dei calcolatori. La storia dell'elettronica digitale inizia con il *circuito di coincidenza* realizzato nel 1930 da Bruno Rossi: nell'ambito di un esperimento di fisica atomica il ricercatore italiano aveva usato le valvole termoioniche per realizzare delle semplici funzioni logiche e con-

ture gli impulsi simultanei di un rivelatore di particelle. Ma la prima applicazione al calcolo di un certo rilievo è merito di John Atanasoff e Clifford Berry, che fra il 1938 e il 1941, lavorando allo Iowa State College, realizzarono l'Atanasoff-Berry Computer (ABC) una macchina per la risoluzione di sistemi di equazioni lineari. L'ABC non era programmabile, quindi il problema della Turing completezza neanche si pone, ma fu la prima macchina a usare l'aritmetica binaria implementata con circuiti elettronici a valvole e ad avere una memoria elettronica per i dati intermedi. Saranno tuttavia le grandi macchine come l'ENIAC americano e il Colossus inglese a fugare gli ultimi dubbi sull'opportunità di usare le valvole in grandi numeri e per lunghi periodi di tempo. Il lavoro ininterrotto delle migliaia di valvole dei Colossus di Bletchley Park fu una dimostrazione di affidabilità inecepibile e, per certi versi, insperata.

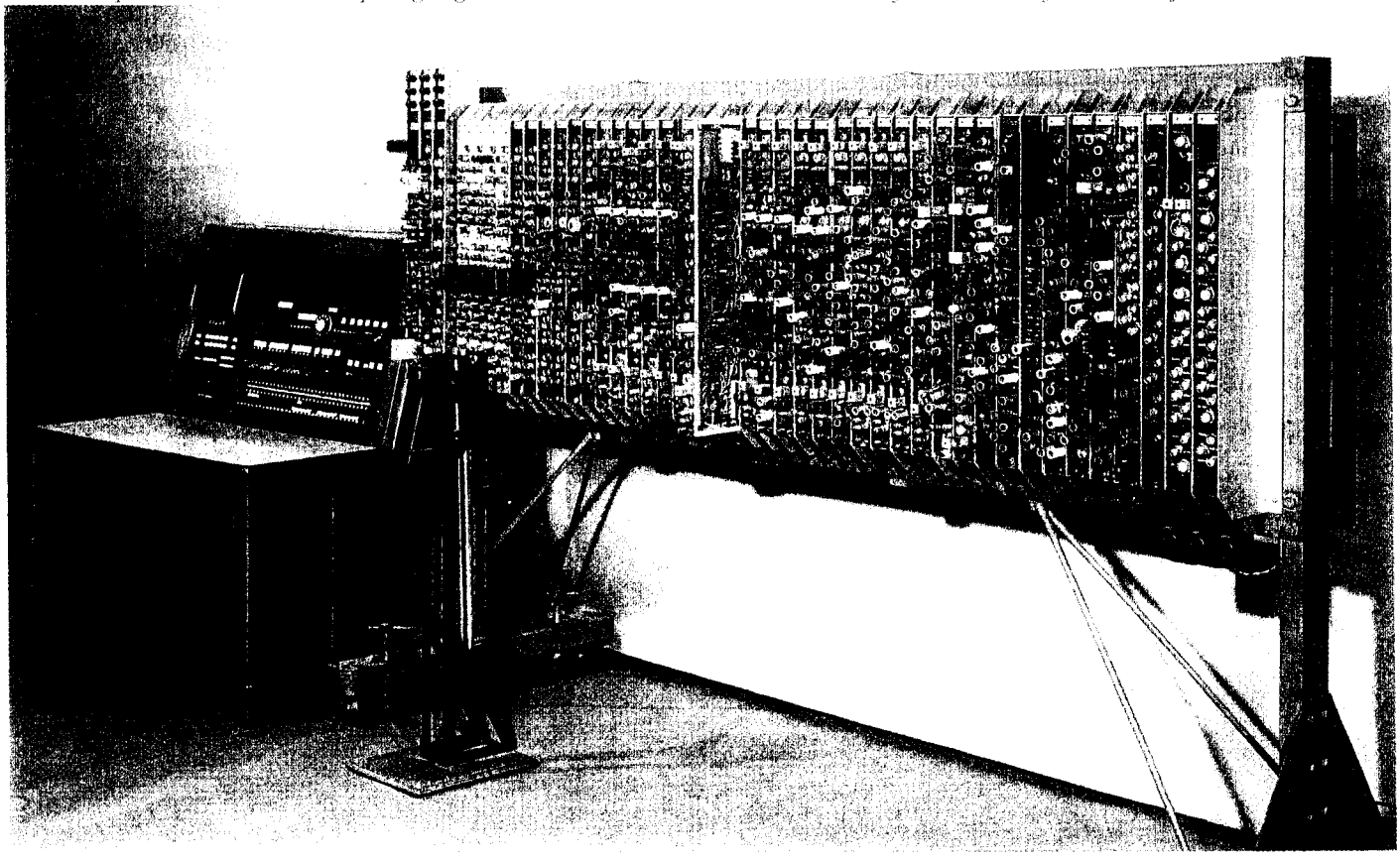
Il progetto ACE e la "corsa" con Von Neumann

Finita la guerra, Turing ottiene una posizione al National Physical Laboratory (NPL) a Teddington, alla periferia di Londra. Nel 1946 Turing propose alla direzione del NPL il progetto dettagliato dell'Automatic Computing Engine (ACE): una macchina – ovviamente Turing completa – da costruire con tecnologia digitale. Il progetto dell'ACE è anche interessante per l'architettura che Turing descrive per la realizzazione della macchina. Tale progetto fu presentato poco dopo il noto *preliminary draft* che John Von Neumann pubblicò nel 1945 sull'*Electronic Discrete Variable Automatic Computer* (EDVAC). EDVAC era il successore di ENIAC su cui all'Università della Pennsylvania avevano iniziato a lavorare in collaborazione con l'Institute of Advanced Study (IAS) di Princeton a cui Von Neumann afferiva e che pure aveva in corso un progetto per la realizzazione di un calcolatore digitale.

Il rapporto di Von Neumann è famoso per aver reso pubblica l'architettura a memoria unica su cui sono basati tutti i calcolatori moderni, e di conseguenza, aver influenzato molti progetti di quel periodo. Oltre all'EDVAC e alla macchina dell'IAS sono più o meno direttamente legati al rapporto Von Neumann un numero notevole di progetti sia negli Stati Uniti (per esempio AVIDAC all'Argonne National Laboratory, ILLIAC all'University dell'Illinois, JOHNNIAC alla RAND Corporation, MANIAC ai laboratori di Los Alamos, ORACLE all'Oak Ridge National Laboratory, ORDVAC ai laboratori di Aberdeen dell'US Army), sia nel resto del mondo (per esempio BESK a Stoccolma, BESM a Mosca, DASK a Copenhagen, PERM a Monaco, SILLIAC a Sydney, WEIZAC a Rehovoth in Israele).

Nel progetto dell'ACE si fa riferimento al rapporto di Von Neumann, ma nei dettagli e nella terminologia sembra che Turing

La versione pilota dell'Automatic Computing Engine (ACE) realizzata nel 1950 al National Physical Laboratory di Londra (foto Science Museum).



sia più consapevole sia dei meccanismi sia dell'utilità della nuova architettura. Tanto per fare un esempio, Turing prevede esplicitamente di mantenere l'indirizzo della prossima istruzione in un registro così da realizzare facilmente le istruzioni di salto. Una soluzione che diventerà ovvia in poco tempo e che sarà presente nei lavori di Von Neumann successivi al primo rapporto e coevi del progetto dell'ACE. Un segno di come la ricerca di quel periodo fosse particolarmente vivace e convergesse, più o meno indipendentemente, verso una soluzione condivisa.
Curiosamente, né Turing né Von Neumann, sicuramente protagonisti nell'aver fissato l'idea di calcolatore moderno, ebbero l'onore di tenere a battesimo la prima macchina pienamente conforme alle loro definizioni. Per vari motivi, i progetti a cui parteciparono di persona subirono ritardi.
L'EDVAC fu completato nel 1949, ma, per una serie di problemi (inclusa una disputa legale fra Eckert-Mauchly e l'Università della Pennsylvania), divenne operativo solo nel 1951. La macchina dell'IAS fu completata in quello stesso anno e divenne completamente operativa nel successivo. EDVAC e IAS furono anche precedute da alcuni dei loro "cloni" (AVIDAC e MANIAC per esempio).
Il progetto ACE di Turing fu inizialmente accettato. Il NPL ne diede anche pubblicità alla stampa definendolo come progetto di interesse nazionale. L'ACE era però un progetto ambizioso: Turing aveva intuito il ruolo cruciale della memoria e, di conseguenza, aveva definito requisiti esigenti in termini sia di quantità sia di tempi di accesso. Ma, in quel periodo, l'implementazione della memoria era ancora uno dei principali ostacoli tecnici. Inoltre Turing per la realizzazione dell'ACE confidava nelle competenze in elettronica digitale maturate a Bletchley Park. Ma, finita la guerra, i Colossus furono smantellati, i loro piani distrutti e la loro stessa esistenza secretata: nei nuovi scenari internazionali era meglio che nessuno sapesse che la Lorenz (ora in mano a Inghilterra e Stati Uniti) era stata battuta. La storia del Colossus comincerà a riemergere solo negli anni Settanta. Neanche fu possibile per il NPL reclutare gli ingegneri elettronici che avevano lavorato al Colossus, Flowers in particolare, troppo impegnato dalle sue responsabilità al Post Office nell'ambito della ricostruzione post bellica.
Di fronte a queste difficoltà la direzione del NPL bloccò il progetto; Turing ne rimase comprensibilmente contrariato. A parziale riscatto della delusione scientifica, sono di quegli anni i suoi maggiori successi da maratoneta: come socio del Walton Athletic Club partecipò a diverse manifestazioni locali arrivando a fare tempi da qualifica olimpica. Qualche tempo dopo, cambiati i vertici del NPL, il progetto ACE fu ripreso su scala ridotta e un *Pilot ACE* che usava memorie a linee di ritardo al mercurio (comunque lente per le specifiche di Turing) fu completato nel 1950.

La Baby Machine

La palma di primo calcolatore moderno spetta a una piccola macchina: la Small Scale Experimental Machine (SSEM) costruita dall'Università di Manchester e familiarmente chiamata Baby Machine.
Ma anche la storia della Baby affonda le sue radici a Bletchley Park, dove nel 1944 Max Newman aveva suggerito la realizzazione del Colossus e sovrainteso al suo uso. Al termine della guerra Newman diventa titolare della cattedra di Matematica Pura all'Università di Manchester. Insieme al fisico Patrick Blakett, Nobel nel 1948 e persona influente nel Governo, riescono ad ottenere un importante finanziamento per costruire un calcolatore elettronico. Newman ha una visione completa della situazione: nel 1935 aveva introdotto

I membri del Ratio Club, formato da biologi e ingegneri dell'Università di Manchester interessati alla cibernetica. Turing è il primo a sinistra, seduto.

Turing al problema di decisione di Hilbert ed era stato uno dei primi revisori dei suoi lavori comprendendo a pieno il valore della Macchina Universale; durante la guerra aveva constatato in pratica le potenzialità dell'elettronica digitale. Nel piano di Newman il punto critico era, al solito, l'implementazione della memoria.

Durante la guerra il Telecommunications Research Establishment (TRE) aveva investito notevoli risorse per lo sviluppo dei radar. Frederic Williams, in particolare, aveva lavorato sui tubi catodici per visualizzare le eco dei segnali. Venuto a conoscenza della sfida tecnologica rappresentata dalla memoria per i calcolatori, propose di usare la persistenza dei fosfori dei tubi catodici: i bit erano memorizzati come punti luminosi su uno schermo. Sulla base di questa idea, nel novembre 1946 fu chiamato da Newman per la cattedra di Ingegneria Elettrica e con il compito di sviluppare e provare la sua idea. Dopo il successo dei primi esperimenti, Williams fu raggiunto da Tom Kilburn, anch'egli proveniente dal TRE, e insieme iniziarono a lavorare al progetto di un semplice calcolatore costruito attorno al nuovo tipo di memoria e capace di dimostrarne i pregi. Il 21 giugno del 1948 la Baby eseguiva il suo primo programma per la ricerca del massimo fattore di un numero. La SSEM era un prototipo limitato: aveva una memoria di solamente 32 celle e un linguaggio macchina di appena 7 istruzioni, ma era Turing completa e aveva un'architettura Von Neumann. Il primo calcolatore moderno era in funzione.

Il successo della Baby e delle memorie a "tubi Williams" portarono nuovi fondi ed energie al progetto dell'Università di Manchester che si mise al lavoro per realizzare un calcolatore di maggiori dimensioni. Giocò un ruolo importante anche la volontà dell'Inghilterra di proporsi come potenza nucleare nei nuovi scenari che si stavano delinenando con i primi segni della Guerra Fredda. E lo sviluppo della bomba richiedeva molti calcoli.

Newman offrì una posizione a Turing che accettò di buon grado visto anche il suo disappunto con i vertici del NPL per la vicenda ACE. Nel 1948, con un finanziamento della Royal Society, Turing assunse il ruolo di *Deputy Director* del Computing Machine Laboratory: lavorò allo sviluppo delle librerie software del nuovo calcolatore e curò la redazione del manuale di programmazione.

In poco tempo fu realizzato il Manchester Mark 1 dal quale, con la partecipazione industriale di Ferranti Ltd., derivò il primo calcolatore moderno commerciale, il Ferranti Mark 1 che fra il 1951 e il 1957 fu realizzato in nove esemplari, uno dei quali arrivò in Italia all'inizio del 1955 acquistato dall'Istituto Nazionale delle Applicazioni del Calcolo di Roma (vedi *Sapere*, aprile 2005, p. 42).

Il cerchio si chiude

Il lavoro di Turing sul software della macchina di Manchester è particolarmente significativo di come la sua figura di scienziato si completi nelle due anime teorica e applicativa. Uno dei programmi che Turing sviluppò per il Mark 1 serviva a studiare la funzione $\zeta(s)$ di Riemann, un vecchio interesse matematico su cui aveva lavorato già nel 1939. Il programma fu, quasi certamente, realizzato soprattutto a scopo dimostrativo per illustrare le potenzialità del Mark 1, ma è anche uno dei primi usi di un calcolatore per una ricerca in matematica teorica – se non proprio il primo.

Ancora più interessante è il fatto che nel 1939 Turing, proprio per quell'obiettivo di ricerca, aveva proposto e progettato un calcolatore meccanico dedicato. L'aver infine risolto il problema con un programma è la miglior dimostrazione dell'importanza dell'idea di Macchina Universale e dell'utilità della sua realizzazione come strumento concreto.

BIBLIOGRAFIA

L'opera completa di Turing sui calcolatori è stata raccolta in [1] e molti documenti originali sono disponibili in rete [2]. Sempre in rete esiste un escursus biografico dettagliato e agganciato alle fonti originali [3]. Le pagine web [4] create da Tony Sale, curatore del progetto che ha recentemente ricostruito il Colossus, sono probabilmente le più esaustive per tutto quel che concerne la battaglia dei cifrari. Infine, [5] consente di confrontare il progetto di Turing dell'ACE [6] con il rapporto di Von Neumann sull'EDVAC [7].

[1] **Turing A.M.**, «The Collected Works of A.M. Turing – Vol. 1 Mechanical Intelligence», (D. Ince ed.), North Holland, 1992.

[2] «The Turing Digital Archive», www.turingarchive.org, Archive Centre at King's College, Cambridge.

[3] **Hodges A.**, «Alan Turing Internet Scrapbook», www.turing.org.uk/turing/scrapbook.

[4] **Sale T.**, «WWII Codes and Ciphers», www.codesandciphers.org.uk.

[5] **Carpenter B.E., Dorant R.W.**, «The Other Turing Machine», in *The Computer Journal*, v. 20 n. 3, Oxford University Press, 1977.

[6] **Turing A.M.**, «Proposal for Development in the Mathematics Division of an Automatic Computer Engine», Report E882, National Physical Laboratory, 1946.

[7] **Neumann J. Von**, «First Draft of a Report n the EDVAC», Moore School of Electrical Engineering, University of Pennsylvania, 1945.

Giovanni Antonio Cignoni
è docente di Simulazione presso il Dipartimento di Informatica dell'Università di Pisa.