

COMMENT

INTELLIGENCE Four experts compare brains with machines **p.462**

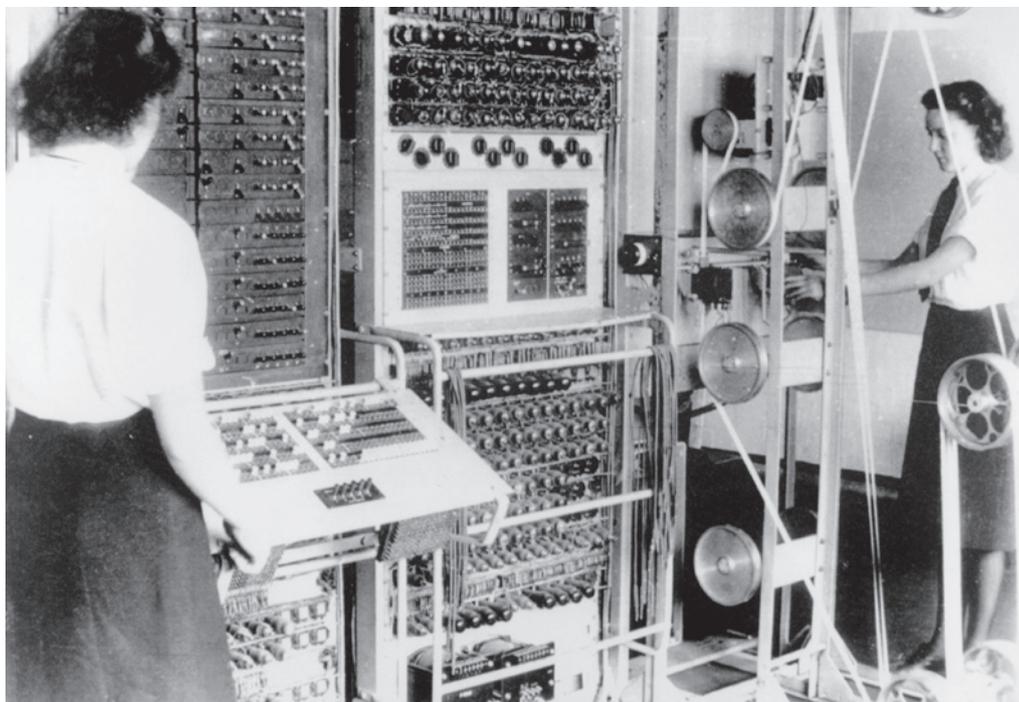
MATHEMATICS What lies beyond the limits of computability? **p.465**

THEATRE How actors use empathy to seduce an audience **p.466**

VIROLOGY Three books explore 30 years of developments in HIV/AIDS research **p.468**



BLETCHLEY PARK TRUST/S&SPL/GETTY



Using techniques developed by Alan Turing, the Colossus was able to decode German wartime communications.

The dawn of computing

Alan Turing's bridging of logic and machines laid the foundation for digital computers, says **George Dyson**.

The history of digital computing can be divided into an old testament and a new testament. The prophets of the old testament, led by Gottfried Wilhelm Leibniz in the 1670s, supplied the logic; those of the new testament, led by John von Neumann in the 1940s, built the machines. Alan Turing, born on 23 June 1912, falls in between. His paper 'On computable numbers, with an application to the *Entscheidungsproblem*', written in 1936 while he was a fellow at the University of Cambridge's King's College, UK, and published shortly after his arrival as a graduate student at Princeton University, New Jersey, in October 1936, led the way to the implementation of mathematical logic in machines¹.

Turing was aiming to solve German mathematician David Hilbert's 1928

Entscheidungsproblem — the 'decision problem' of whether a mechanical procedure could determine the validity of any logical statement in a finite number of steps. Turing took the 1930s concept of a computer — a person equipped with pencil, paper and instructions — and deconstructed it by removing all traces of intelligence except for the ability to follow instructions and read and write a finite alphabet of symbols on an unbounded paper tape.

The result was the Turing machine: a mathematical black box that obeys preset instructions, represented by symbols encoded

on the tape or stored in the machine's internal 'state of mind'. At any moment, the machine can read, write or erase a symbol from a square; move a square to the right or left; or change its state of mind. Complex symbols can be represented by strings of simpler ones, the limit being the binary distinction between two symbols (or the presence or absence of a hole in the tape). These 'bits' of information can take two forms: patterns in space that are transmitted across time, termed memory; or patterns in time that are transmitted across space, called code. For a Turing machine, time exists not as a continuum, but as a sequence of changes of state.

Turing then demonstrated the existence of a single machine that could "compute any computable" sequence¹. Such a 'universal computing machine' could mimic any ▶



TURING AT 100

A legacy that spans science:
nature.com/turing

▶ other machine by executing an encoded description of it. Thus, he foresaw the concept of software.

Finally, Turing answered Hilbert's conundrum. He identified a question that could not be answered by any machine in a finite number of steps: will a given encoded description come to a halt or run forever when executed by the universal computing machine? The answer to the *Entscheidungsproblem* was, therefore, no.

"You can build an organ which can do anything that can be done," explained von Neumann, paraphrasing Turing, in a lecture in 1949, "but you cannot build an organ which tells you whether it can be done"². Sensing the limits of deterministic machines, Turing began to explore non-deterministic computation by 'oracle' machines. These proceed step-by-step, but occasionally make unpredictable leaps by consulting "a kind of oracle as it were"³.

CODE BREAKING

Having completed his PhD, Turing returned to England in July 1938. The outbreak of the Second World War soon sparked demand for his ideas, and he was sequestered at the Government Code & Cypher School at Bletchley Park. There, Turing and his colleagues, including his mentor, topologist Maxwell 'Max' Newman, deciphered enemy communications, including messages encrypted by the German Enigma machine — a Turing machine with an internal mechanism that shifted through 10²⁰ possible configurations to scramble the input text.

Starting with a set of electromechanical devices called bombs, each of which could emulate 36 suspected Enigma configurations at a time, the researchers at Bletchley Park, assisted by engineer Thomas Flowers at the General Post Office Research Station in Dollis Hill, London, developed a machine called Colossus — a sophisticated electronic digital computer. A 1,500-vacuum-tube internal memory provided Colossus with a programmable state of mind that searched for clues in coded sequences scanned from punched paper tape.

Colossus was swiftly improved and duplicated, producing a second generation of 2,400-tube machines that influenced the outcome of the war and the development of modern computers, although Britain's Official Secrets Act kept the details embargoed for more than 30 years. When the war ended, the push for more powerful computers shifted from cryptanalysis to the design of nuclear weapons, and the United States, which had declassified its wartime computer, the ENIAC (Electronic Numerical Integrator and Computer), in February 1946, assumed the lead.

At the Institute for Advanced Study in Princeton, and with funding from the US Army, the Office of Naval Research and

the US Atomic Energy Commission, von Neumann set out to build an electronic version of Turing's universal computing machine. He wanted a Turing machine with a memory that was accessible at the speed of light, and he decided to build it himself. The US government wanted to know whether a hydrogen bomb was feasible, so von Neumann promised it a machine, with 5 kilobytes of storage, that could run the required hydrodynamic codes. The computer's design was made public so that copies could be freely duplicated — and commercialized by IBM. "Words coding the orders are handled in the memory just like numbers," von Neumann announced at the first project meeting, on 12 November 1945 (ref. 4). This mingling of data and instructions was central to Turing's model. Most computers today are the direct offspring, in terms of their logical architecture, of a Turing machine built from war-surplus components in an outbuilding on a former New Jersey farm.

Turing and von Neumann first met in Cambridge in 1935, and subsequently spent two years together in Princeton, where Newman joined them for 6 months. How

"Most computers today are the direct offspring of a Turing machine built from war-surplus components."

much Turing and von Neumann collaborated during the war remains unknown, but we do know that Turing was in the United States between November 1942 and March 1943, and that von Neumann was in England between February and July 1943. During the war, British physicists, in consultation with von Neumann, made important contributions to the atomic bomb project at Los Alamos in New Mexico; and US cryptanalysts, in consultation with Turing, contributed to the effort at Bletchley Park. Although they could not communicate them openly in writing, Turing, von Neumann and Newman probably shared their ideas verbally, both during and after the war.

Turing's model was one-dimensional: a string of symbols encoded on a tape. von Neumann's implementation was two-dimensional: the random-access address matrix that underlies most computers today. The Internet — many Turing machines with concurrent access to a shared tape — has made the landscape three-dimensional. Yet the way in which computers work has remained fundamentally unchanged since 1946.

LEARNING FROM MISTAKES

Both Turing and von Neumann were conscious of processing errors in their machines. Early codes could be fully debugged, but the hardware was more unreliable, giving inconsistent results — a problem that has since

been reversed. Both men knew that biology relied on statistical, fault-tolerant methods for processing information (such as pulse-frequency coding in the brain) and assumed that technology would follow nature's lead. If "every error has to be caught, explained and corrected, a system of the complexity of the living organism would not run for a millisecond", von Neumann commented⁴.

"If a machine is expected to be infallible, it cannot also be intelligent," Turing noted in 1947 (ref. 6). When Turing joined Newman's group at the University of Manchester, UK, the following year and began designing the Manchester Mark 1 (a prototype for the Ferranti Mark 1, the first commercial stored-program electronic digital computer), he included a random-number generator, which allowed the computer to make guesses and learn from its mistakes.

Turing's deterministic universal machine receives the most attention, but his non-deterministic oracle machines are closer to the way in which intelligence really works: intuition bridging the gaps between logical sequences. Turing's oracle machines are no longer theoretical abstractions — an Internet search engine, for instance, operates deterministically until a person clicks on a link, adding non-deterministically to the search engine's map of where the meaningful information is.

Turing wanted to know how molecules were able to collectively self-organize, and whether machines could think. Von Neumann wanted to know how the brain worked and whether machines could reproduce. Turing, who died at the age of 41, left behind an unfinished theory of morphogenesis, and von Neumann, who died aged 53, left an unfinished theory of self-reproduction — a model inspired by the Turing machine's ability to generate copies of itself.

Had Turing and von Neumann lived longer, we can only imagine how their ideas might have merged. Their lives were both cut short just as the mechanism underlying the translation between sequence and structure in biology was revealed. ■

George Dyson is a writer based in Bellingham, Washington, and author of Turing's Cathedral.

e-mail: Gdyson@ias.edu

1. Turing, A. M. *Proc. Lond. Math. Soc.* **s2-42**, 230–265 (1936–37).
2. von Neumann, J. In: *Theory of Self-Reproducing Automata* (ed. Burks, A. W.) 42–56 (Univ. Illinois Press, 1966).
3. Turing, A. M. *Proc. Lond. Math. Soc.* **s2-45**, 161–228 (1939).
4. Minutes of the Institute for Advanced Study Electronic Computer Project, Meeting 1, 12 November 1945.
5. von Neumann, J. In: *Theory of Self-reproducing Automata* (ed. Burks, A. W.) 74–87 (Univ. Illinois Press, 1966).
6. Turing, A. M. Lecture to London Mathematical Society 20 February 1947. Turing archive held at King's College, Cambridge.