Foundations of Computing and Communication

Lecture 5

The Universal Machine

Based on *The Foundations of Computing and the Information Technology Age*, Chapter 4

Lecture overheads © John Thornton 2010
Lecture Objective

To gain an overview of the historical development of the electronic stored program computer in the first half of the 20th century.

Overview of Topics

- The Revolutions in 20th Science and Mathematics
- Early Punched Card Machines
- Electro-Mechanical Computing: Zuse, Stibitz and Aiken
- The First Electronic Machines: ABC and ENIAC
- Colossus and the War-Time Codebreakers
- The Post-War Stored Program Machines
The End of Certainty

- **Electrical innovation**: Samuel Morse’s telegraph (1837), Alexander Bell’s telephone (1876), Marconi’s first radio broadcast (1896) Thomas Edison, first recording of human voice (1877), first power station in NY (1882), first motion picture machine (1892).

- **Clouds on the horizon**: Working classes not sharing in prosperity. Attitudes of ruling classes have not caught up with the times. Technology delivers high explosives, machine guns and mass transportation.
The Seeds of Materialism

- **Faith challenged:** Science: Darwin’s Origin of the species (1859), geology, archaeology, History: Reformation, Counter Reformation, inquisitions, religious wars.

- **New ideas:** Marx’s Communist Manifesto (1848), Freud’s Interpretation of Dreams (1900), Socialism and Nationalism.

- **The old world ends:** millions die on the battlefields of Europe, industrial scale war and mechanised slaughter, European culture in ruins.
The Science of Uncertainty

- **Relativity**: Einstein’s Theory of Relativity (1905), dethrones Newton’s law of gravity, mathematical physics begins, four-dimensional space-time continuum moves beyond sense perception.

- **Quantum Mechanics**: Paradox of matter as both particle and wave. Matter controlled by laws of probability, Heisenberg’s Uncertainty Principle (1927), superpositions of states collapse into particles, classical and quantum levels, matter just a mathematical abstraction?
The Mathematics of Uncertainty

• **Logical foundations**: Set theory, Georg Cantor, Gottlob Frege gives definition of number as the set of all sets containing \( n \) elements; David Hilbert lays out program to unify mathematics in a logical system that is complete and consistent.

• **Paradox and uncertainty**: Russell’s paradox with sets as members of themselves (1902), fixed in *Principia Mathematica*, destroyed by Kurt Gödel’s incompleteness theorems, no interesting logical system can be both complete and consistent.
The Mechanisation of Abstraction

- **The Turing Machine**: Alan Turing formalises ideas of an “effective method” and computability with the Turing Machine, proves Halting Problem is undecidable using Gödel’s approach (1936), defines Universal Turing Machine - proposed first universal computing machine as by-product of mathematical work.

- **Mathematics comes of age**: From tally stick to Turing Machine, mathematics becomes a universal language of abstraction, Universal Turing Machine can speak that language, challenge is to build one.
Punched Card Machines

- **Hollerith and IBM**: Turn of the 20th century, most sophisticated calculators were punched card machines, Hollerith Electric Tabulating System used in 1890 US census, cards read electronically, totals added mechanically, machines can sort and print cards. IBM becomes leading manufacturer in 1920s.

- **Scientific calculators**: L. J. Comrie has tabulating machine modified, connects mechanical accumulators, simulates Difference Engine using electric plugboard, produces 1000 lines of table per hour. IBM produce multiplying machine in 1935 using telephone relay technology, one multiplication per second.
The Zuse Machines

- **Binary Numbers**: Konrad Zuse saw advantages of binary system: easy to construct, easy calculation, easy representation of numbers, operators and instructions. Used mechanical pins in slots to encode 0/1 and moving plates to act as logic gates.
- **The Z1** Mechanical binary computer, controlled by holes punched in movie film, mechanical arithmetic unit, conditional branching, pioneers use of floating point arithmetic and conversion of binary to decimal.
- **The Z2** Based on Z1 but uses telephone relay technology for arithmetic unit - makes construction much simpler - still mechanical in operation but controlled electrically - hence relays connected by wires, physical location not important.
The Zuse Machines

- **Schreyer**: Zuse’s assistant Schreyer works on vacuum tube technology, comes up with basic circuit designs that get rid of mechanical operation of relays. Work abandoned due to lack of funding and worries about reliability.

- **Z3 and Z4**: Z3 uses relay technology for memory, Z4 supposed to be full-scale machine for German military but war ends before it is finished - Zuse completes Z4 in Switzerland in 1950. Zuse recognised as first to build fully automated binary computer.
The Bell Relay Machines

- **The Complex Number Calculator**: George Stibitz at Bell Labs builds a simple relay circuit for binary addition, in 1930s uses relays to perform addition, subtraction, multiplication and division of complex numbers.

- **Anti-Aircraft Work**: Stibitz builds Relay Interpolator and Ballistic Computer to solve wartime problems of shell trajectories, machines slow due to relays but reliable, used multiple paper tape inputs, worked with floating point arithmetic.
The Harvard Machines

- **Aiken and IBM**: Howard Aiken from Harvard University collaborated with IBM to produce electro-mechanical computer. Using ideas from Babbage, combined IBM mechanical accumulator registers with electrically controlled clutches - clutches engage decimal number wheels to motorised rotating shafts, used Babbage carry mechanism, IBM paper tape readers, Mark I machine had limited ability to perform conditional branching, completed 1944, many features are copied to ENIAC.

- **Mark II to IV**: Mark II used relay technology (1945), Mark III (1949) and IV (1952) combined vacuum tubes, relays and stored program technology - however first fully electronic machines are built earlier during the war....
The First Electronic Machines

- The ABC: Atanasoff-Berry Computer: vacuum tubes offer the promise of faster non-mechanical operation, in 1938 John Atanasoff and Clifford Berry start to develop ABC in USA, uses vacuum tubes for control and arithmetic unit, has regenerative memory built from capacitors mounted rotating drums, project abandoned in 1942 but ideas used in ENIAC (image courtesy of Iowa State University).
ENIAC

- **Ballistics:** U.S. Army needed accurate, up to date ballistics tables in Second World War. In 1934 already built a mechanical differential analyser in collaboration with Moore School, University of Pennsylvania. One trajectory takes human expert 20 hours, differential analyser 20 minutes (after set up). Still too slow.

- **Sharing of Ideas:** John Mauchy joins Moore School during war, meets Atanasoff and Berry in 1940-1941, produces paper in 1942 “Use of High Speed Vacuum Tube Devices for Calculating”, calculates time to calculate trajectories could be reduced to 100 seconds.
ENIAC

- **Crisis**: By 1943 production of ballistic tables fallen behind - new approach needed. Mauchy and J. Presper Eckert present their vacuum tube ideas to the Army “Electronic Numerical Integrator” stress general purpose nature of machine, add “and Computer” - ENIAC project is born.

- **The Project**: Clearly understood that this was most complex piece of electronic equipment ever conceived - required serious project management skills, Mauchy does conceptual design, Eckert does circuit design and Joseph Chedaker in charge of construction team.
ENIAC

- **The Machine**: 18,000 vacuum tubes, 1500 relays, 70,000 resistors, 10,000 capacitors, 8 ft high, 3 ft wide, 100 ft long, weighed 30 tons, consumed 140 kilowatts of power, cooled by two 12 hp blowers, cost $486,804, working by 1945.

- **The Architecture**: Paper tape input, decimal numbers, no general purpose memory, accumulators used for intermediate results, each program set up using a plugboard, very low level, no language in modern sense, paper tape too slow for control instructions, hence purpose built electronic control unit where branching and looping controlled by manually setting switches; basic calculation procedures based on Aiken’s earlier ideas, links to Babbage, especially anticipating carriage mechanism.
ENIAC

- **After the War**: ENIAC modified to act as stored program computer with 99 basic instructions, core memory added (100 words, 10 digits each), used portable “function tables” with switches to program machine, previously would take several days to rewire machine to perform new calculations. Shut down in 1955 (image courtesy US Army).
Colossus

• **Rule Britannia!**: Of course the first electronic computer was built in Britain, but the whole project was so secret that the machines were not admitted to until recent times. This was all part of the British attempt to break the German Enigma machine cipher.

• **The Enigma Machine**: Developed by the German Arthur Scherbius, Enigma was an electro-mechanical cipher machine of great sophistication, adopted by German military in 1926 also available commercially. When machine arrived, British cryptanalysts were baffled. After open access to German communications during and after World War One, supply of intelligence dried up.
**Colossus**

- **Enigma’s Operation**: Fairly simple scheme of rotors each with 26 letters, type in one letter first rotor scrambles letter, electrical signal routes this letter through next rotor where it is transformed again, then through third rotor for final transformation - then after input rotor moves round one position - means same letter entered again will produce a different output, next input clicks rotor round again, in total $26 \times 26 \times 26 = 17,576$ settings. Rotors can also be placed in different orders + plugboard is added which allows swapping of six pairs of letters, makes for 10,000 million million possible settings. Beauty of system - all you need is another Enigma machine set up with same rotor and plugboard settings and message is deciphered.
An Enigma Machine (image courtesy of the Science Museum, London)
Colossus

**Poland to the Rescue:** The young Polish mathematician Marian Rejewski was able to break the early Enigma machines before the outbreak of war. The Germans used codebooks to set up their machines for each day, plus for each message they would transmit a new order for the rotors - this rotor order was repeated twice to avoid error. The Poles obtained a military enigma machine and used knowledge of the repetition to catalog a much smaller set of 105,476 possible settings for the rotors, after solving this the separate problem of the plugboard setting was relatively easy. To speed up searching the possible combinations the Poles built relay machines called *bombas.*
• **War begins**: In 1939 the Germans increased Enigma’s security, adding two extra rotors and extra plugboard capability to swap ten instead of six letters. Poland does not have resources to build enough *bombas* to crack the code. Just before the invasion of Poland, the *bombas* and all knowledge of Enigma are given to the allies.

• **Bletchley Park**: All British code-breaking work was based in a country house outside London. Many of great linguists and mathematicians were working here, including Alan Turing. Using the Polish start, more “bombs” were constructed and the German Airforce code was broken, but the navy and army codes remained secure.
Colossus

- **Electronic machines**: To search the enormous number of permutations of the Enigma code needed much faster machines - in 1943 the telephone division of the General Post Office are asked to start building a machine combining the use of relays and vacuum tubes - results in the Heath Robinson machines - 2,000 characters per second but unreliable - encouraged further work.

- **Tommy Flowers**: Tommy Flowers called in to fix up the Heath Robinsons, sees major problems in the design - suggests entirely new machine using 1500 valves - Bletchley Park do not approve, so Tommy goes ahead anyway with help of staff at Dollis Hill - Colossus is built and running by December 1943 - world’s first electronic computer.
Colossus

- **The Machine**: Colossus was purpose built for code breaking so had no arithmetic component but could have been wired to do arithmetic. Used photoelectric readers, 5,000 characters per second, decimal registers and internal clock with teleprinter output.

- **Victory!**: Colossus works! For most of the rest of the war German military communications are an open book to the allies. Considered to have shortened the war by more than a year.
Colossus

Work on ENIAC and Colossus forms basis of modern computer industry. John von Neumann involved in summarising work on ENIAC and suggesting the architecture for a stored program machine (image courtesy of the Science Museum, London).

This becomes the model for all future machines - the Universal Turing Machine becomes reality.
First Stored Program Machines

- **Manchester Baby**: Manchester University machine working by June 1948, used expertise gained from Colossus, but really only a prototype, unable to perform significant calculations.
- **EDSAC**: Cambridge University had first fully operational stored program machine working by May 1948, capable of solving realistic problems.
- **CSIRAC**: Trevor Pearcey in Australia works on world’s fifth stored program machine, operational by November 1949.
- **EDVAC**: Most famous American stored program machine not working until 1952 with involvement from von Neumann.
Lecture Exercise

Consider the following machines:

- Zuse’s Z1
- The ABC
- ENIAC
- Colossus
- Manchester Baby
- EDSAC

Each is considered to have been pioneering in some way - describe why.