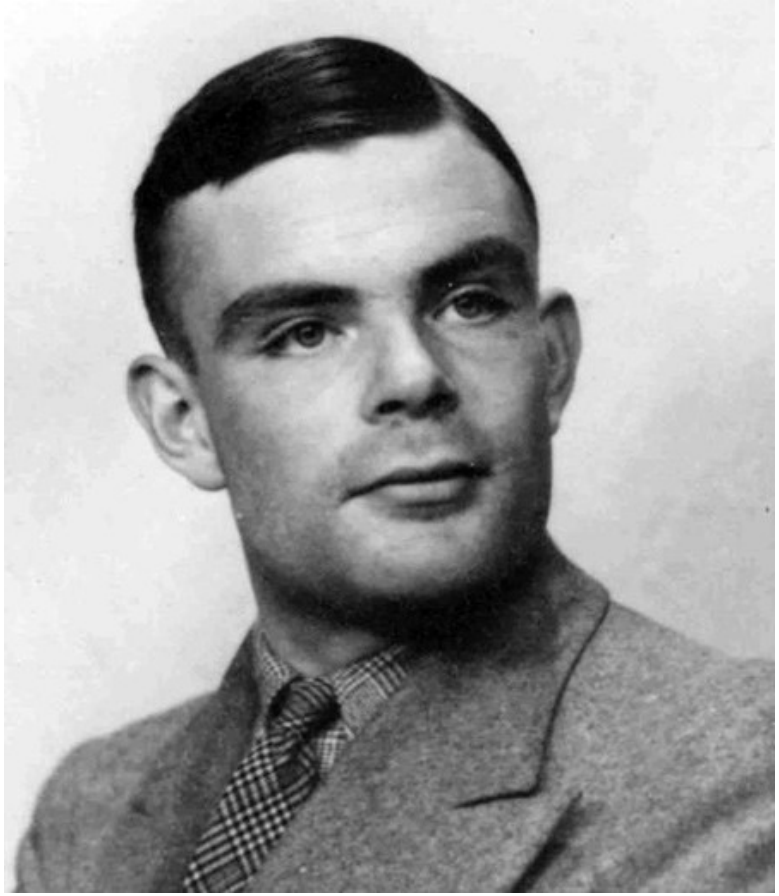
Turing's Real Machines



Michael R. Williams
Professor Emeritus
Department of Computer Science
University of Calgary

2012 - Turing centenary year

Some ground rules

- I am not a Turing expert, but I do know a lot about the man and his accomplishments.
- So do a lot of other people, but they are not here at the moment (or at least I hope they are not here to cause me embarrassment)
- I don't intend to say much about his mathematics – a substantial and lasting contribution!

Turing’s Real Machines

- I am old enough to knew many of the first generation of computer pioneers on a personal basis (few are now left alive – those that are in their 90s).

- I never knew Turing because I was only 12 when he took his own life.

- But I have talked to those who worked with him and collected stories, photos, etc.

Turing’s Real Machines

For example:

The house where Turing lived and died in Manchester

Turing's Real Machines

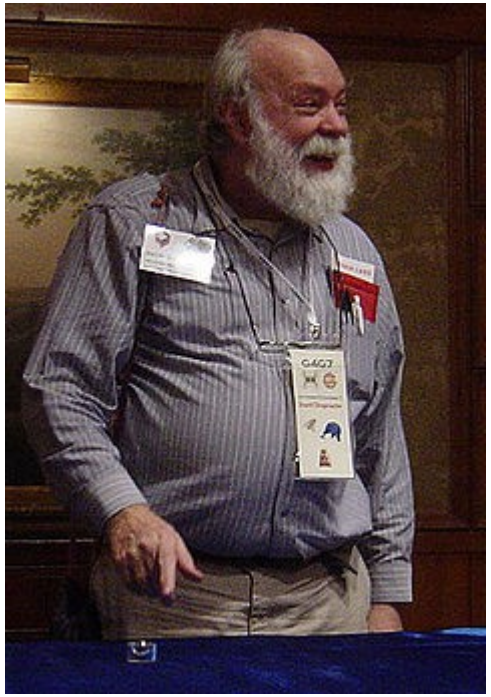
Mathematical Gazetteer of the British Isles

By David Singmaster

Retired mathematics prof

at London Southbank

University



Turing's Real Machines

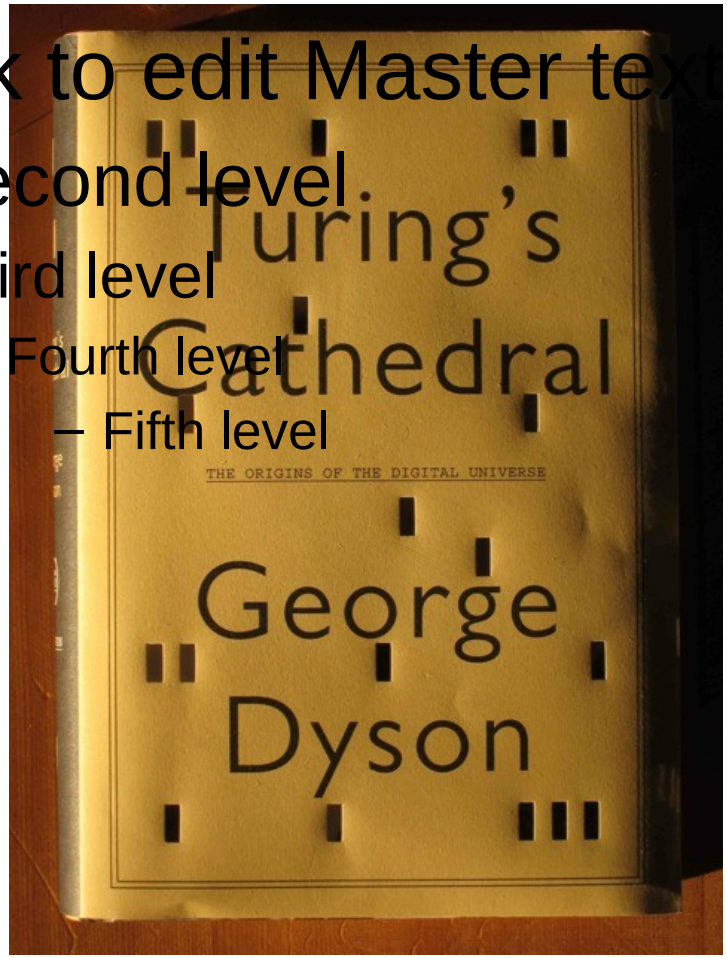
ck to edit Master text styles

econd level

hird level

Fourth level

– Fifth level



George Dyson's new book

GEORGE DYSON, a historian among futurists, is the author of *Darwin Among the Machines*; and *Project Orion: The True Story of the Atomic Spaceship*.

available March 6

Turing's Real Machines

- He had an impulse to build things and had done physical experiments since his youth

- But he was never any good at it
  - he could conceive of things and explain what he had in mind but his actual ability at construction was almost zero
  - "bird's nest" wiring and clumsy.

First attempt at a secret cypher machine

1936-37 (at Princeton) he attempted to build a cypher machine

- relay based multiplier
- would take binary message
- multiply it by “a horrendously long but secret number”
- transmit the product

Number was to be long enough that it would take 100 Germans, 8 hours per day, for 100 years to find the secret number by simple search.

Machine was never finished (typical).

Zeros of the Riemann Zeta Function

- He was interested in what was known as the zeros of the Riemann Zeta function – why is not important at the moment.

- He saw that any attempt at hand calculation was futile

- Knew of a mechanical tide calculating machine that he once saw at Liverpool

Tide Calculating Machine (invented by Lord Kelvin)

Zeros of the Riemann Zeta Function

- Kelvin's machine was analog – only did approximate calculations (good enough for tides and to find exceptions to Zeta function)

- When Turing returned to Cambridge he had help from a mechanical engineer (the brother of a Princeton friend) to design one for finding zeros of Riemann Zeta function

Zeros of the Riemann Zeta Function

- Asked for a 40 Pound grant to get it constructed
- Turing admitted in the grant application that it would have no other use.
- War started and machine never finished!

The War was a turning point

- World War II changed everything for Turing.
- Took him out of Cambridge and the academic life and put him into a less tolerant society
- unfortunate because of his lifestyle, but fortunate for the experience it gave him.

Three truths

- **Turing was an original thinker!**
- **He had (an almost unique) ability to think through a problem from the beginning and not just rely on what other had done or thought.**
- **His contributions to the WWII code breaking effort were fundamental.**

Turing has become an icon - helped by his other contributions and his early death

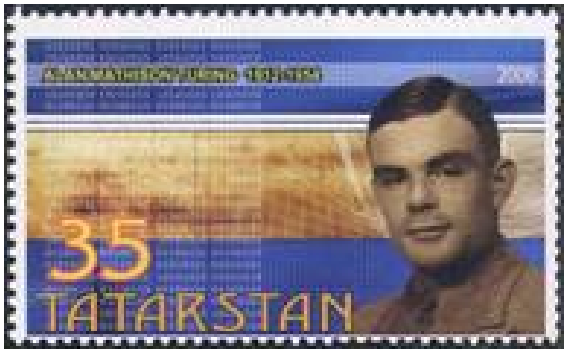
to edit Master text styles

cond level

d level

ourth level

– Fifth level



A lot of what we think about Turing is only partly true

His mathematics and personal life are well known

His code breaking work was unknown to most until the 1970s when it began to leak out

Some of what has been written about him is based on (now) questionable sources

Complete declassification only took place about 10 years ago (some stuff might still be unavailable)

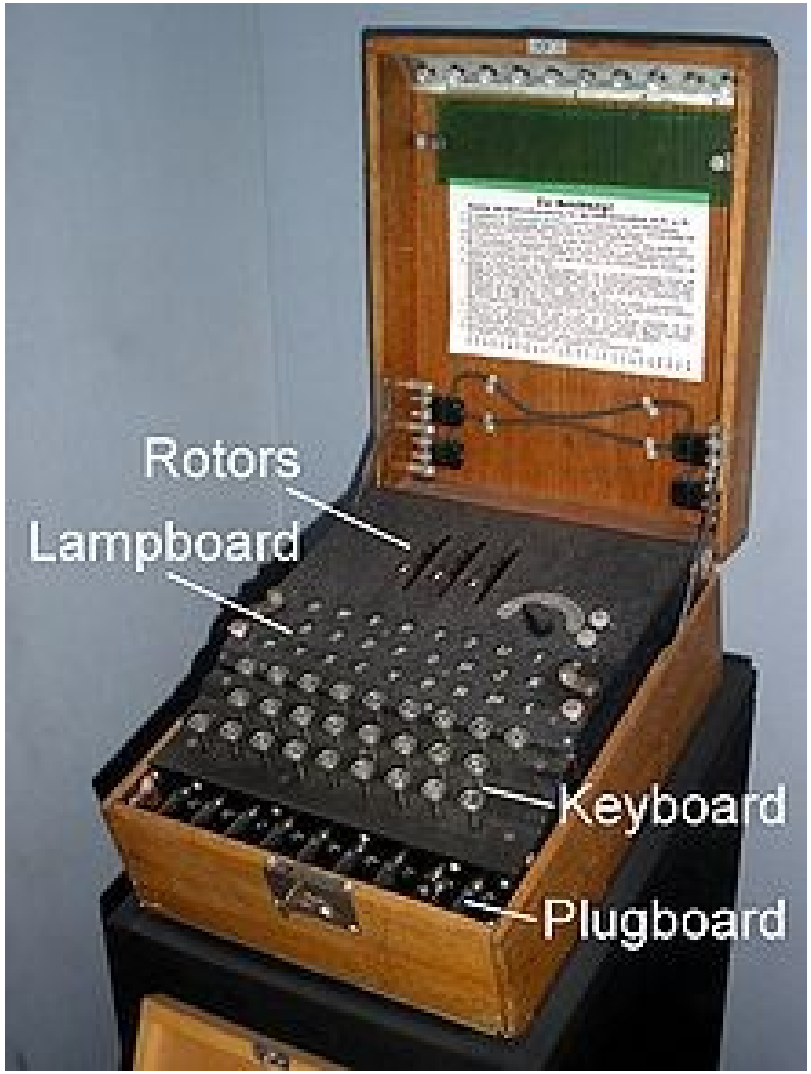
Like all icons/heros, the stories get confused and embellished

Most people think that

- The German military invented the Enigma code machine
- Turing single-handedly broke the Enigma code
- Turing invented the Colossus machine to break the Enigma code
- Turing was the inventor of the modern computer
- And a lot of other stuff – most of it **wrong**

The first thing I am going to do is to disabuse you of some of your misconceptions

Enigma encoding machine



Enigma encoding machine

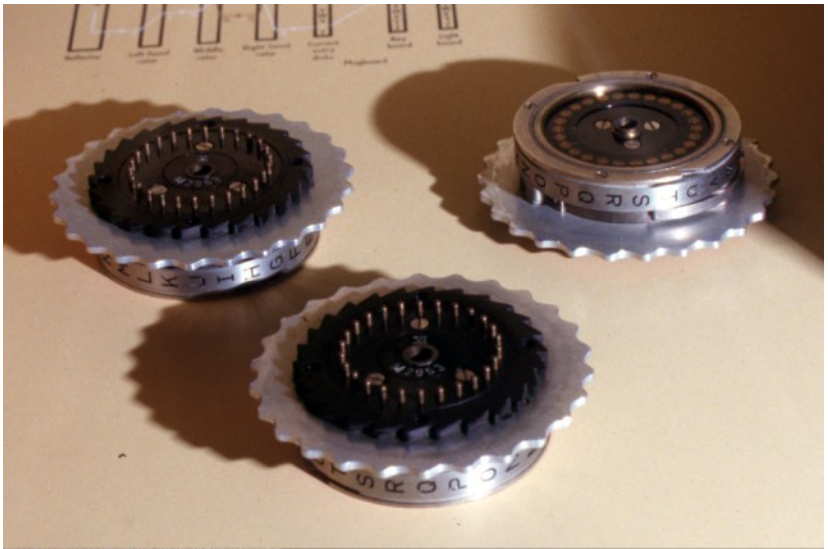
o edit Master text styles
ond level
level
urth level
- Fifth level

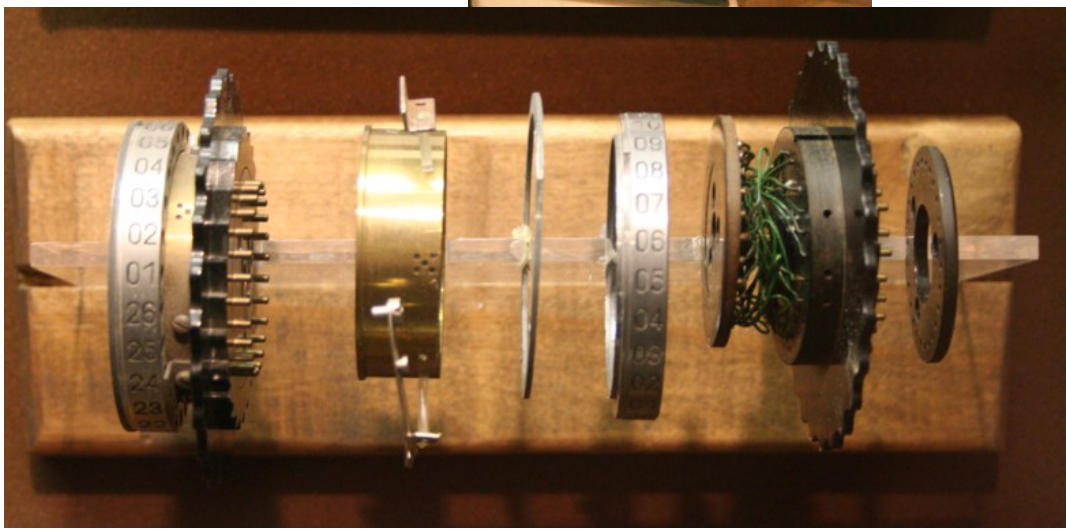
Enigma

- Invented in 1918 by German engineer Arthur Scherbius
- approached the German Navy and Foreign Office with the design, but neither was interested
- Sold many as a business communication encoding device for telegraph use (banks etc.)
- Replaced the telegraph code books then in use
- Enigma was no secret – you could buy one on the open market!

German Military Enigma

- Added a plug board to exchange 6 pairs of letters
- Devised new wiring for the rotors

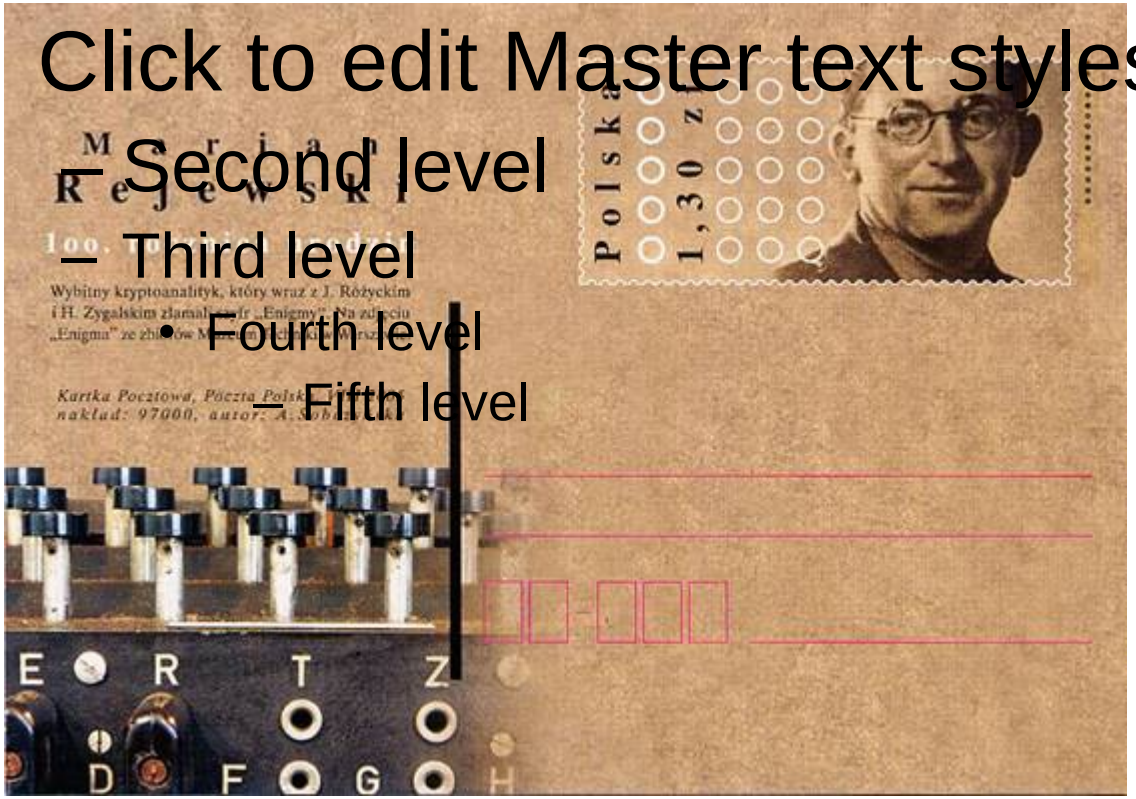




Poles break Enigma code before World War II

Click to edit Master text styles

- Second level
  - Third level
    - Fourth level
      - Fifth level



- Created the first Bombe to help break the code
- Pass the secret of the plug board, rotor wiring, and how they broke it to the British and French

German military made changes to Enigma

- Germans modify the plug board to exchange 10 (rather than 6) pairs of letters
- Introduce new rotors with different wiring
- Polish methods didn’t work anymore
- Alan Turing (aided by Gordon Welchman) try to figure out how to cope with the new situation

Turing's Real Machines

- Turing "designed" a more advanced version of the bombe to cope with German Enigma modifications
- 6' high, 7' wide – 1 ton
- simulated 30 Enigmas working at once - each with different rotor settings etc.
- Bombes actually built by trained engineers but Turing helped with the design and <u>found new creative ways of using them</u>.

Turing’s Bombe

US version of Turing’s Bombe

Much the same as the British version.

Turing's Bombe

Click to edit Master text styles

- Second level
- Third level
  - Fourth level
    - Fifth level

Didn't decipher Enigma messages

Was used to try and find the initial wheel settings of the Enigma for a given message.

Relied in knowing a "crib" of some kind

Turing's Bombe

- First one ("Victory") available in March 1940
- Second in August, others quickly thereafter
- Many produced
- By 1942 they were decoding 39,000 messages per month.
- Code breaking became routine and Turing went on to other projects

- Further German Enigma modifications made it impossible to decipher some messages.
- Extra interchangeable rotors added (different wiring)
- Some units used 4 rotor machines (instead of 3)

Turing's Real Machines

- 4 Rotor machines impossible to decipher with current bombe
- Enigma not the only coding system used
- German High Command used the Lorenz SZ40/42 (*Geheimschreiber*)
- Produced "Fish" ("Tunny")

Lorenz SZ40/42 (Geheimschreiber)

Lorenz internal workings

Transmitted binary code – not transmitted via Morse Code like Enigma

Note 12 rotors

Turing’s Real Machines

- The only possible way to deal with the more complex 4 Rotor Enigma and the Geheimschreiber codes was to speed up the process they already had in operation.

- Turing had once proposed that the setup time for a Bombe could be automated and this now seemed like something to do.

Max Newmann

- First proposal was made by Max Newman – mostly because he found he disliked doing the hand stuff he had been assigned.
- Cambridge Math. Prof. who had given Turing the idea of proving things by mechanical process.
- Likely the one that suggested Turing join the code breaking group

Robinson machines

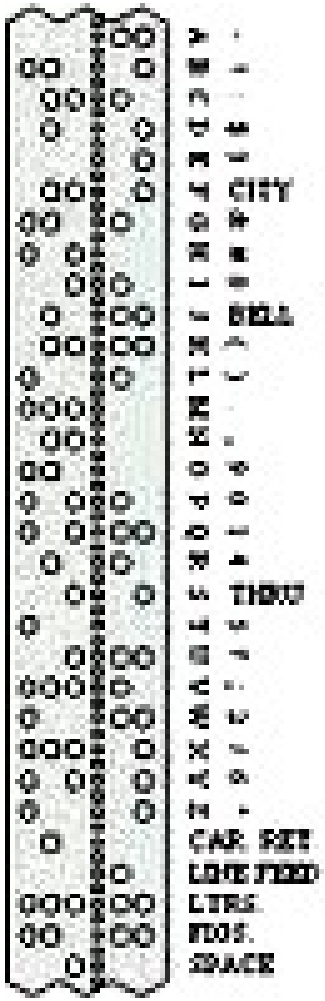
- Newmann suggested that they might use electronics and relays to create a more powerful machine to implement Turing's ideas.

- "Robinson" built by British Telecom Engineers under Newmann's direction.

- (Heath Robinson – cartoonist who created whimsical machines)

Robinson machines

- Machine set itself up and read encrypted message and possible rotor settings from tapes (1,000 c/s – 100 inches/sec. – later 2000 c/s)
- Tapes were driven by sprocket gears – regularly tore up tapes
- While trouble prone it proved Newmann's (and Turing's) ideas correct.



Robinson machines

- Incremental improvements were made to the Robinson
- named “Robinson and Cleaver” etc.

- problems keeping two paper tapes in synchrony

- Essentially performed correlations between the data on the encrypted message tape and one representing the Lorenz wheel settings

- Wheel setting then moved forward one place and the correlation ran again

- The code breaker was looking for the relative position which gave the highest cross-correlation score — which hopefully would correspond to the correct Lorenz wheel start position

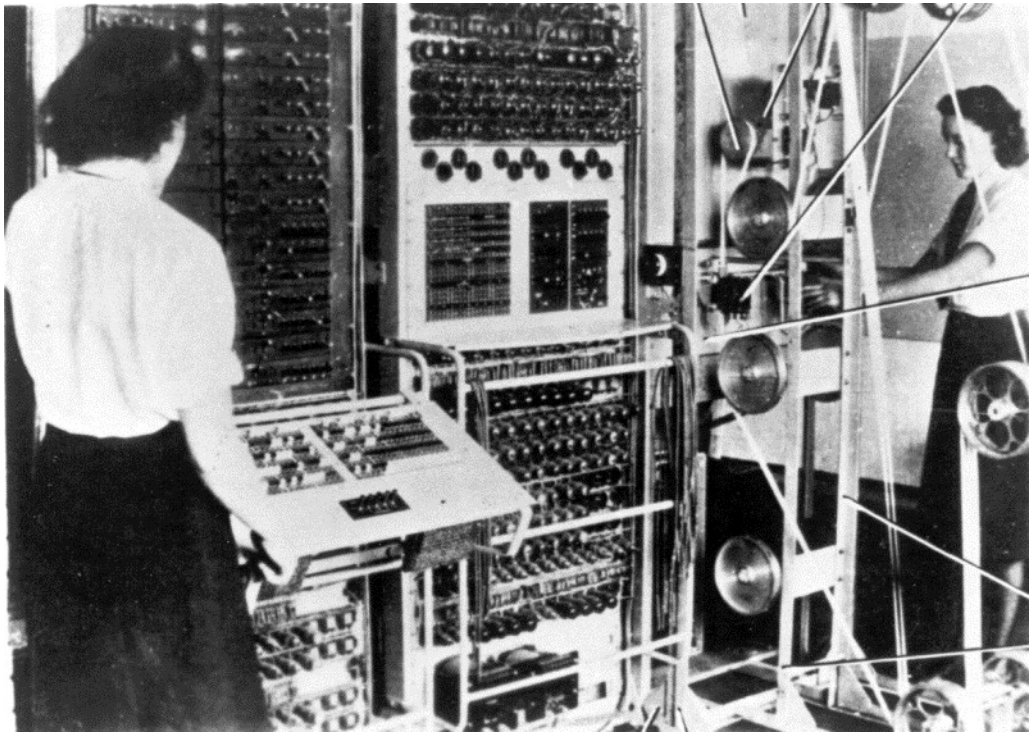
The Collossus

- Tommy Flowers became involved and realized that using vacuum tubes would permit a lot faster speed
- replaced sprocket tape with smooth drive rollers
- **Colossus** was finally created by the British Post Office Research Laboratory

Colossus

Used to break the Fish teleprinter code (Gehimschriber) not usually Enigma.

About a dozen were made – all destroyed to keep the secret.



Colossus

- Read tape at 5,000 c/s – could run through all the combinations of wheel settings (for some code machines) in 30 minutes

- printed out when it had found a setting that matched a potential key.

Bill Tutte

- Bill Tutte deduced the structure of the Lorenz machine
- devised the statistical method which made Heath Robinson and the Colossi possible
- invented a method to keep pace with the Germans' daily changes of the Lorenz code-wheel patterns.

After the War

- **Bill Tutte** later moved to Canada and became a distinguished math professor at Waterloo.

- **Max Newmann** became a math professor at Manchester and founded the Royal Society Computing Laboratory there.

- **Turing** had thought long and hard about computing.
- In **1945** he went to work at the National Physical Laboratory in Teddington to design and develop an electronic stored-program digital computer for scientific work (**a year before the Moore School Lectures**)

Turing’s Real Machines

- John Womersley, Turing's immediate superior at NPL, christened Turing's proposed machine the **Automatic Computing Engine**, or **ACE**, in homage to Babbage's **Difference Engine** and **Analytical Engine**.

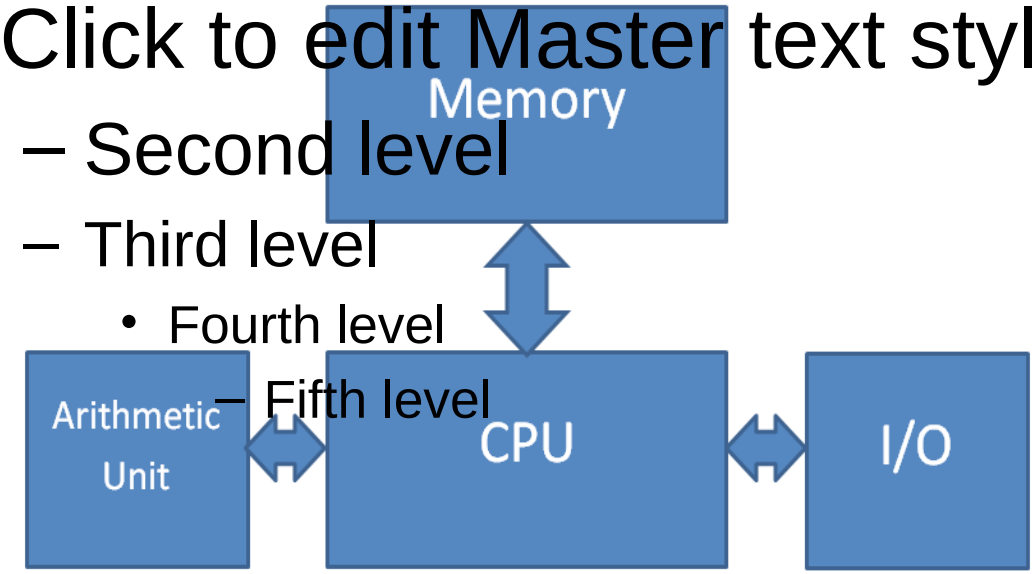
- Turing was in contact with others who were interested in building a computer – but did his usual rethinking the problem from scratch.

Other people's computers

Often termed the "von Neumann model"

But he had nothing to do with its creation – but that is another story…

- Click to edit Master text style
  - Second level
  - Third level
    - Fourth level
      - Fifth level

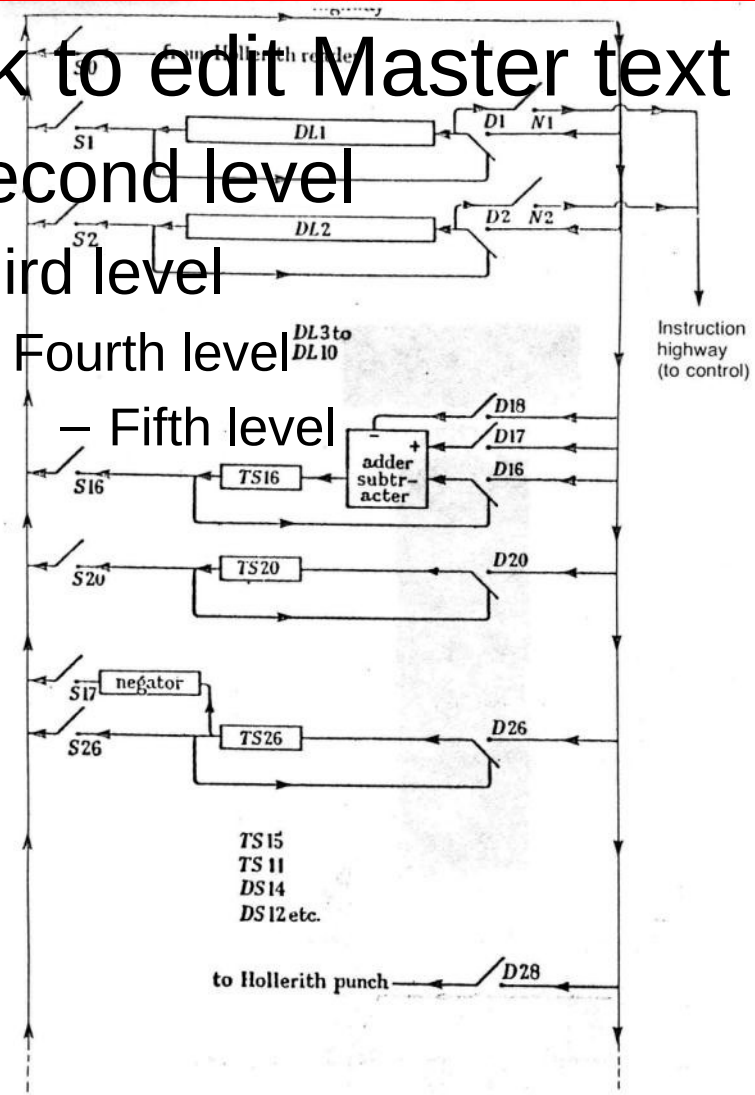


Turing's concept of a computer

Memory was not just a passive place to store numbers ("numbers live in houses")

Memory cells were active – some would add the incoming number to whatever was currently there, some would subtract, some multiply, some invert, etc., etc.

- Click to edit Master text st
  - Second level
  - Third level
    - Fourth level
      - Fifth level



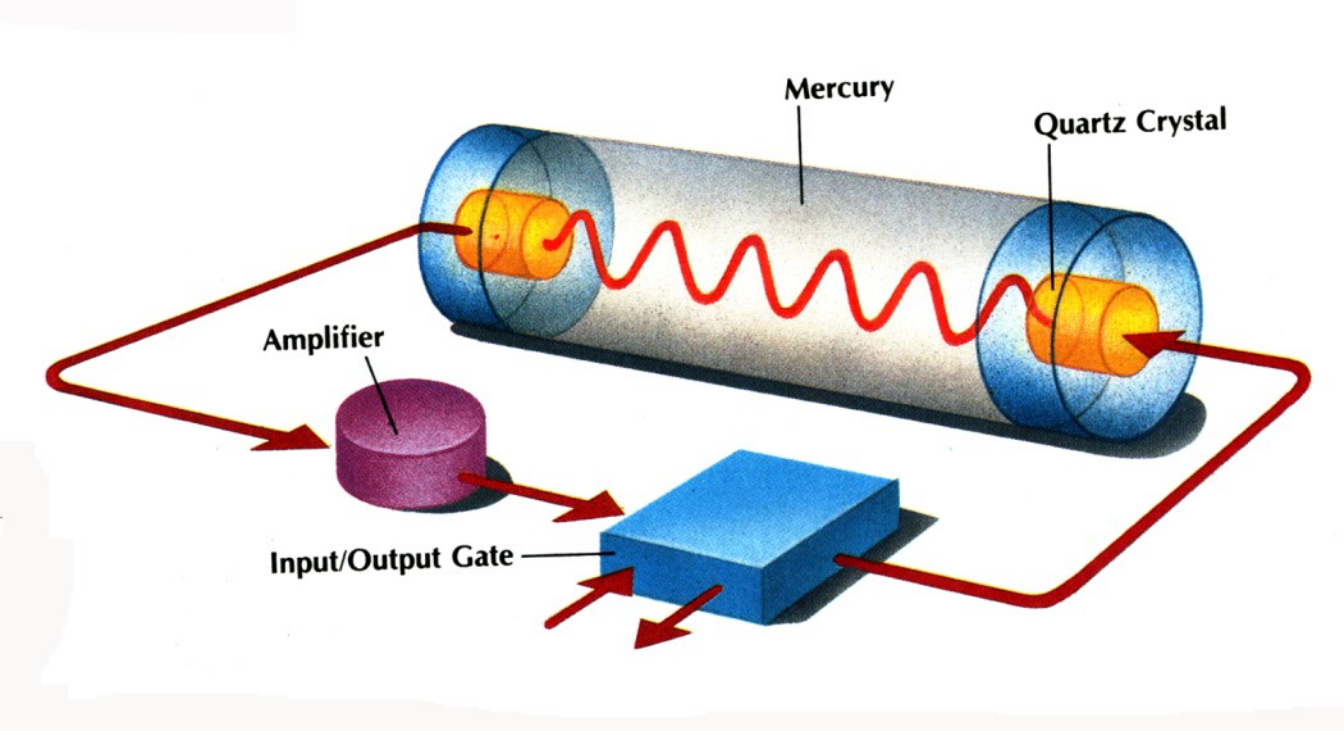
The ACE Computer

- Jim Wilkinson was hired to be Turing's assistant on the ACE project.
- He and Turing designed 7 versions of the machine.
- They wrote many programs to test out various configurations, instructions, etc. before anything was built

Turing's Real Machines

- Three different computer construction projects were going on in Britain
  - The Manchester "baby" computer – (1948)
  - The Cambridge EDSAC – (1949)
  - Turing's ACE (1950)
- Turing lectured at joint meetings of the three in London (1945 - 1948)

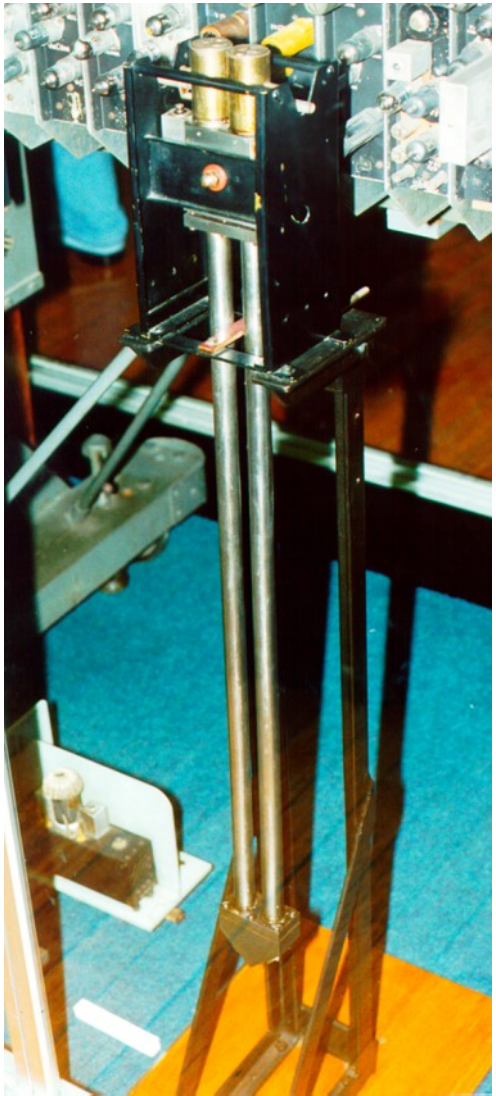
A Mercury Delay Line Memory



Mercury had its problems but it was used for many different early computers.

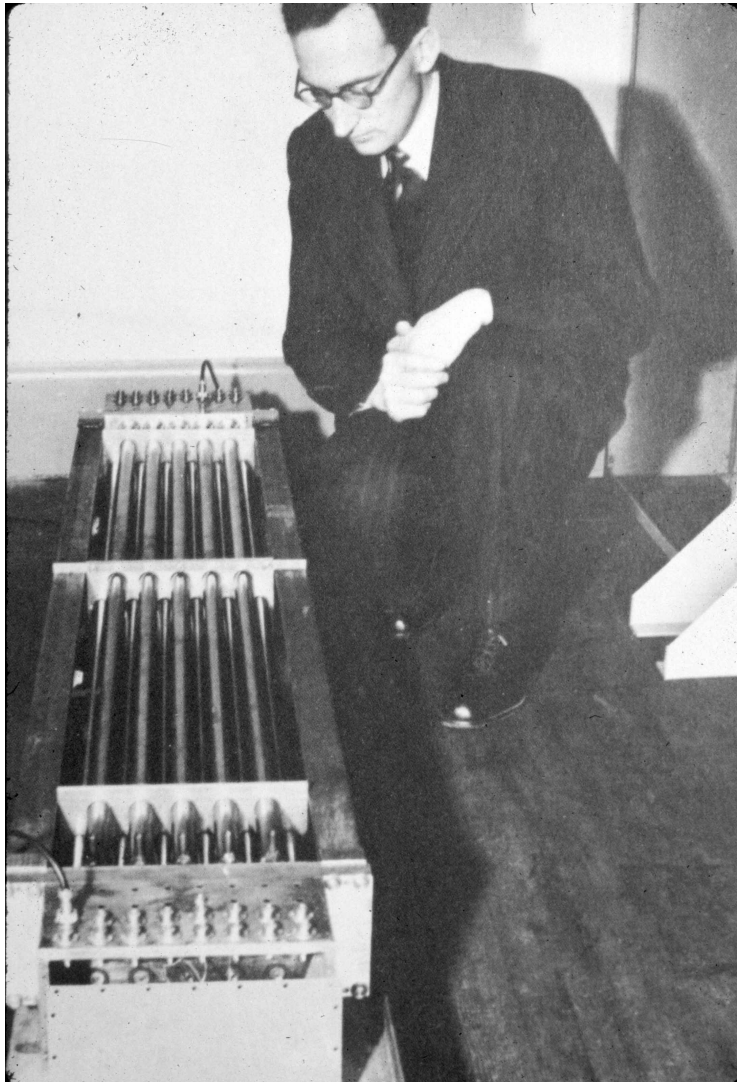
Turing had suggestions on using other media.

ACE mercury delay line



Turing's delay line

EDSAC (Cambridge) Delay line



Turing's Real Machines

- Harry Huskey came from the US (ENIAC project) to work with the group.
- Harry appreciated the design but gave Turing grief.

- Turing was frustrated at the slow progress on construction and this caused other problems with Charles Darwin (the Director of the NPL and grandson of the biologist).

Turing leaves NPL

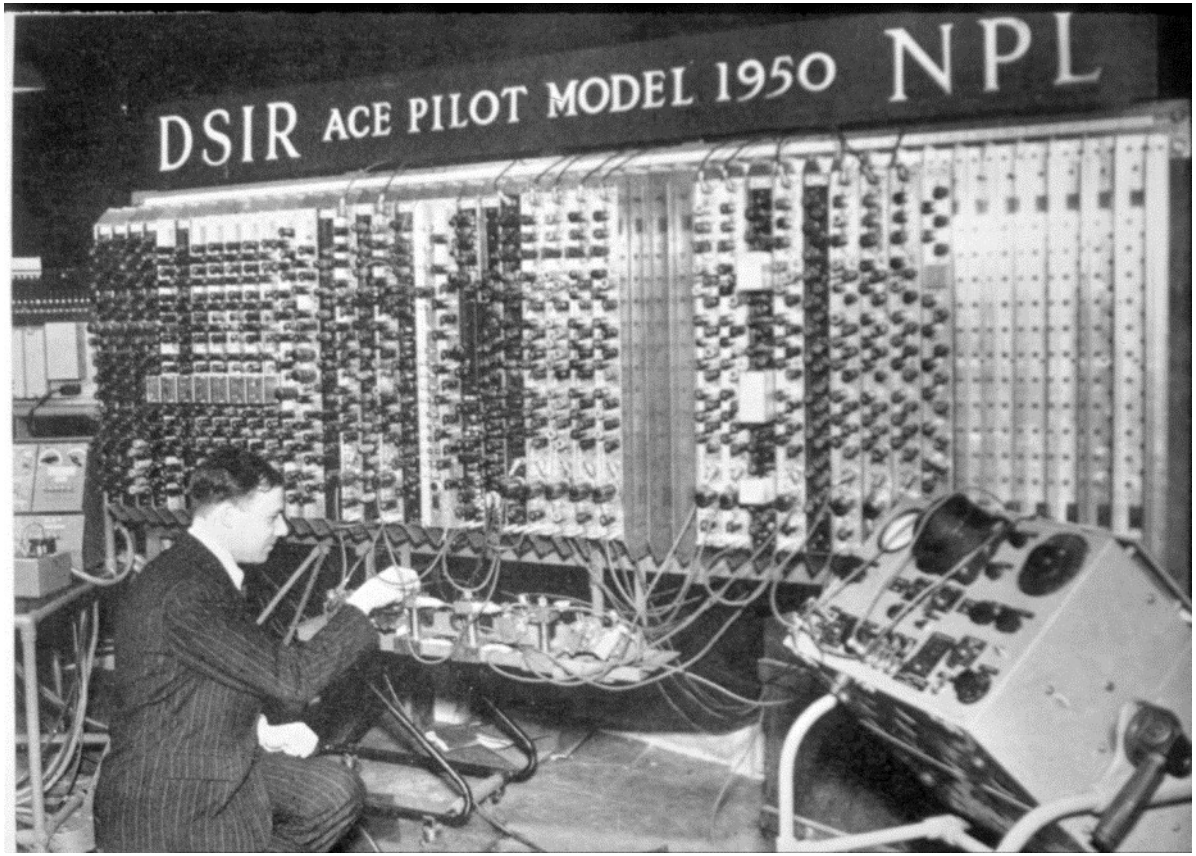
- Max Newmann offered Turing the job of Deputy Director at the Royal Society Computing Laboratory in Manchester.

- A made-up job as there was no Director!

- Turing left NPL and Jim Wilkinson took over responsibility for the ACE.

The Pilot ACE

Jim Wilkinson decided to produce a "Pilot ACE" because of the construction difficulties.

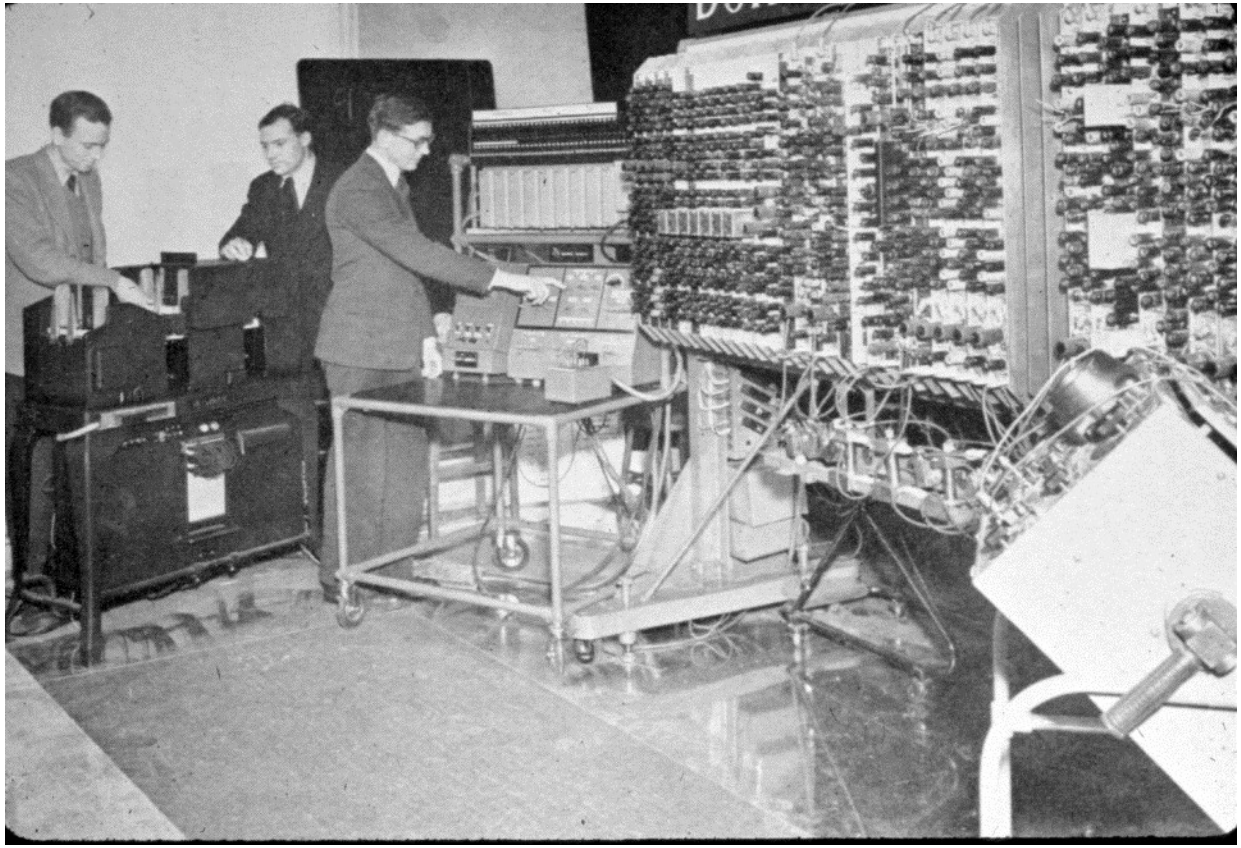


The Pilot ACE

Publicity photo at a press conference in 1950.

Machine unreliable

Power brownouts were a problem.



The Pilot ACE Spinoffs

English Electric Deuce (1955)

Harry Huskey's Bendix G15 (1956)

Pilot ACE remained in service until 1955

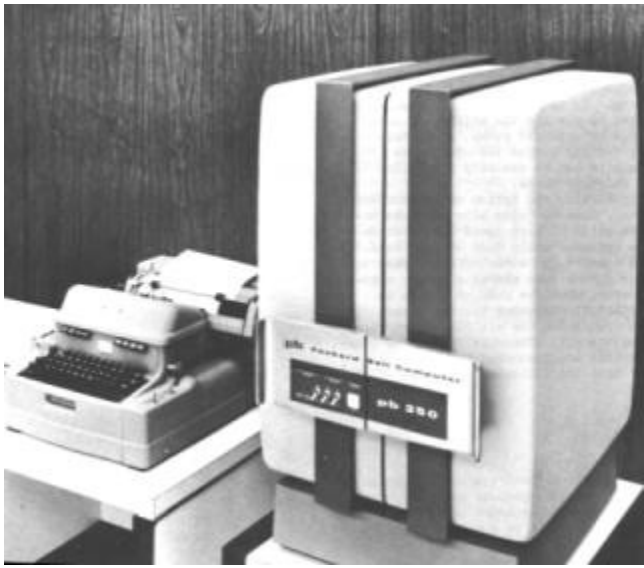
Pilot ACE in production mode in early 1950s
Fastest machine of its era.

ACE Spinoffs

The British air defense system used a MOSIAC computer (essentially an ACE) during the Cold War for radar tracking

The Packard-Bell PB250 (1961) was another.

- a bit-serial computer with acoustic delay line memory



Turing in Manchester

Alan Turing spent the rest of his life in Manchester.

He made several suggestions that changed the architecture of the Ferranti Mark I (“the Manchester machine”) and wrote its first programming manual.

University of Toronto got the second Ferranti Mark I.

“The programming manual was useless and had to be recreated entirely”

Turing in Manchester

He did some of the first work on proving programs correct via making assertions that can be checked – a technique still used.

He was not careful about his publishing and early conference papers are almost impossible to read because the number of errors in both text and mathematical notation.

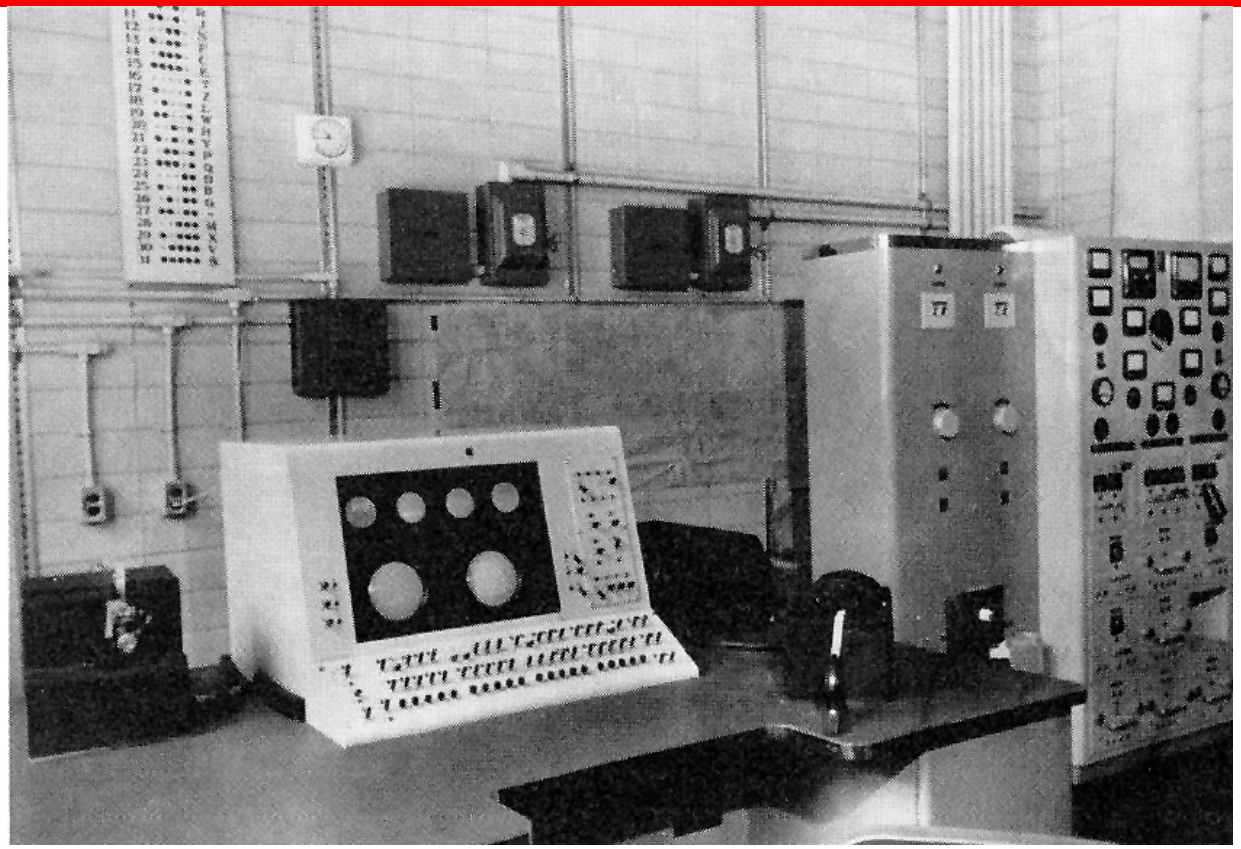
When asked what he was doing, he often replied “making plants grow”

Turing in Manchester

- Biologists associate Turing's name with his 1952 paper, "The chemical basis of morphogenesis"
  - pioneered the use of mathematical models in the study of pattern formation and advocated the application of computers to simulate biological phenomena

First simulation of nonlinear dynamics ever to be published!

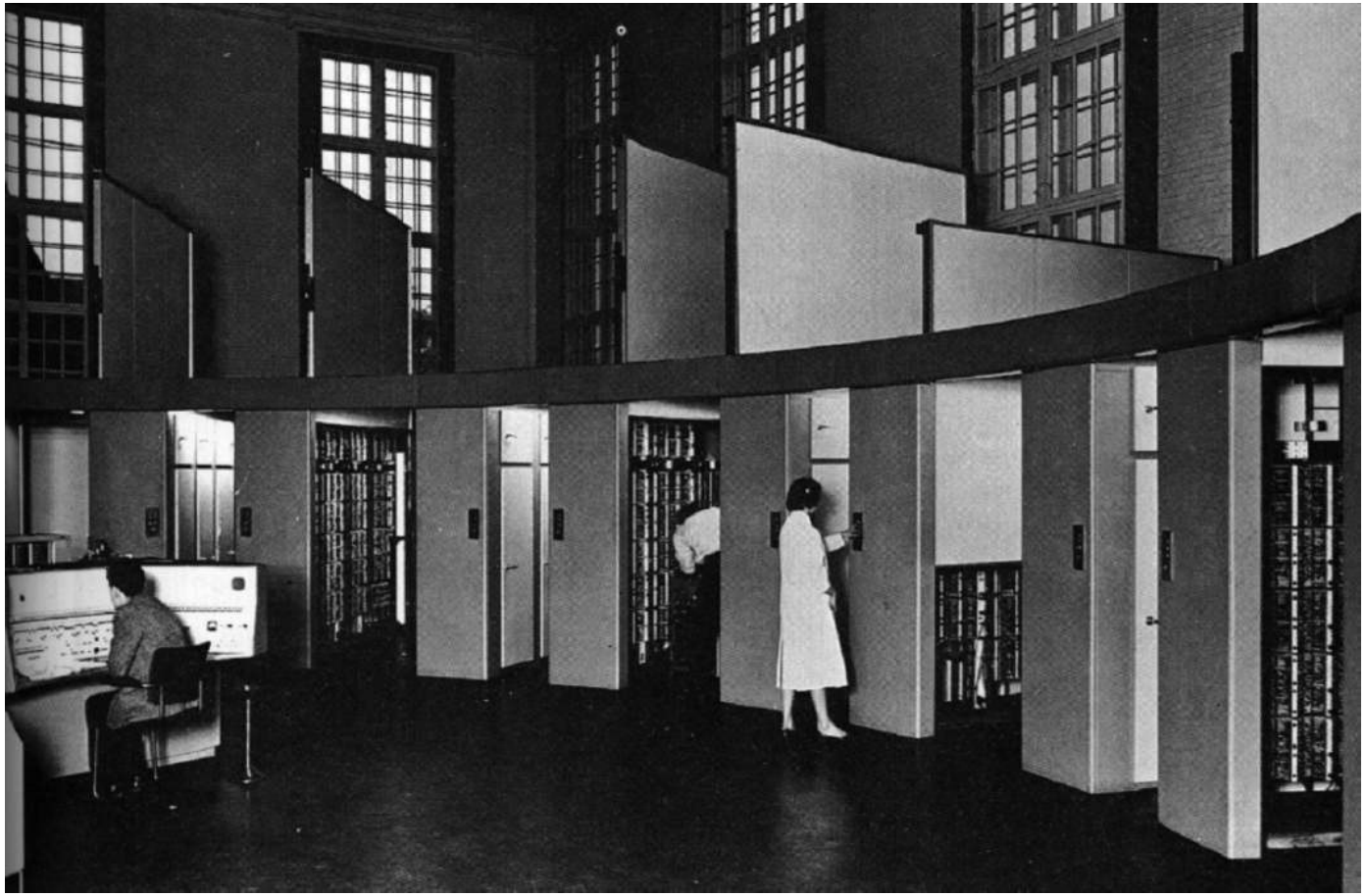
Turing’s ways of working



Turing simply assumed that his way of working was the most obvious – it was not to most of the human race!

Manchester Ferranti Mark I

Turing's Real Machines



The Full version of ACE was finally finished in 1957

Turing’s Real Machines

Thanks for listening!