

Languages and Computation (COMP2049/AE2LAC)

Turing Machine: Background

Dr. Tianxiang Cui

tianxiang.cui@nottingham.edu.cn

Hilbert's Problems

- In 1900, David Hilbert, the German mathematician, proposed 23 problems in mathematics
 - Ten of them were presented at the Paris conference of the International Congress of Mathematicians
 - Complete list was published later
 - The most important problems in mathematics – all unsolved at that time
- #2 – Prove that the axioms of arithmetic are consistent
- Reframed in 1928:
 1. Is mathematics complete?
 2. Is mathematics consistent?
 3. Is mathematics decidable?

Gödel's Incompleteness Theorems

- In 1931, Kurt Gödel, the Austrian mathematician, proposed the solutions to (1) and (2)
- Gödel's incompleteness theorems
- Is mathematics complete? (Can derive every formula that is true)
 - **If the system is consistent, it cannot be complete – there will always be statements that are true but not provable**
- Is mathematics consistent? (Does not contain any internal contradictions)
 - **The consistency of the axioms cannot be proven within the system (a system cannot demonstrate its own consistency)**

Entscheidungsproblem

- Is mathematics decidable? – now known as the **entscheidungsproblem** (German for "decision problem")
- Is there a general algorithm to determine whether a mathematical conjecture is true or false?
- Church & Turing (independently, 1935-1937)
 - Showed the “decision problem” is unsolvable
 - Turing proved this by imagining a “Universal Machine”
 - This result is now known as Church's Theorem or the Church-Turing Theorem

Turing Machine

- Theoretical machine (imaginary / pencil and paper)
- Infinite tape separated into positions (squares)
- Each position can contain a symbol or be blank
- Tape head points to current position
 - Can read symbol
 - Can alter symbol / move – following a rule
 - The set of “rules” is a “program”
- Given some input the Machine will halt (or not) in a particular state
- Used to show the decision problem can't be solved
 - E.g., the “halting problem”

The Halting Problem

- Determine, from a description of an arbitrary program and input, whether the program will finish running (**halt**) or continue to run forever (**not halt**)
- Turing 1936: a **general algorithm** to solve the Halting Problem for **all possible** program-input pairs **cannot exist**
- Key part of proof: mathematical definition of computer and program (Turing Machines)
- The Halting problem is **undecidable** over Turing Machines

Genius of Turing

- TM is a fantastic abstract idea to solve a difficult abstract problem
 - Things we have learned so far (DFA, NFA, PDA), none of them existed at that time (1936), they all developed in 1960s
- So, a small group of pure mathematicians (logicians) were very impressed...
- But who else cares? Or even understands?
- In 1936: not many people!
- In fact, it was possible that Turing's ideas would be lost in the pages of a pure mathematics journal for many years
- Until...

World War II

- In 1939, the WW2 began
- It involved the vast majority of the world's countries—including all of the great powers
- Majority of world's population directly affected
- Estimated that more than 50 million killed during WW2
- Main instigators:
 - Germany in Europe (with their allies, e.g., Italy)
 - Japan in Pacific region

1940

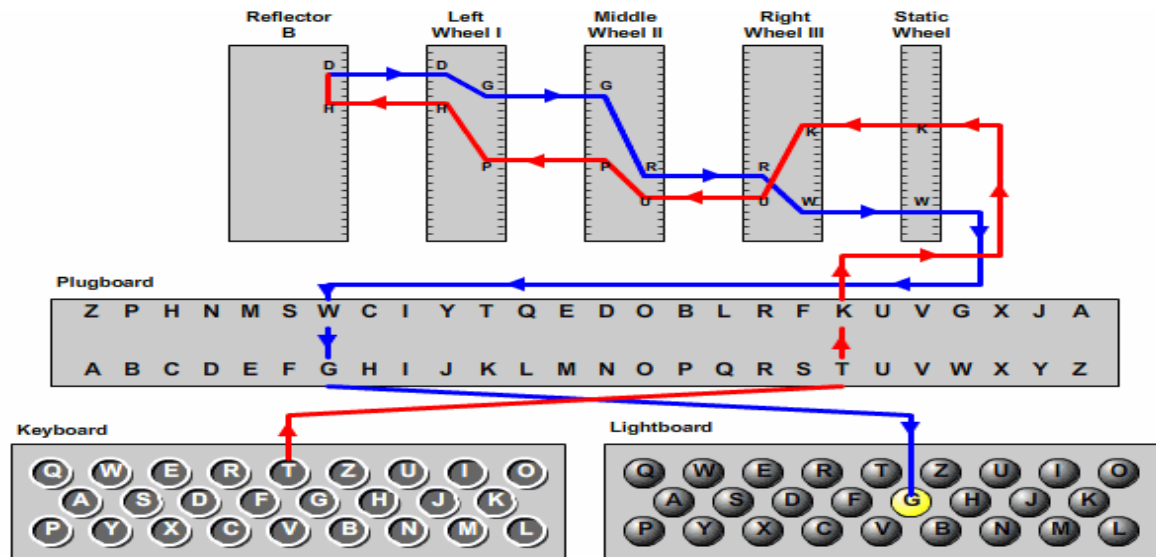
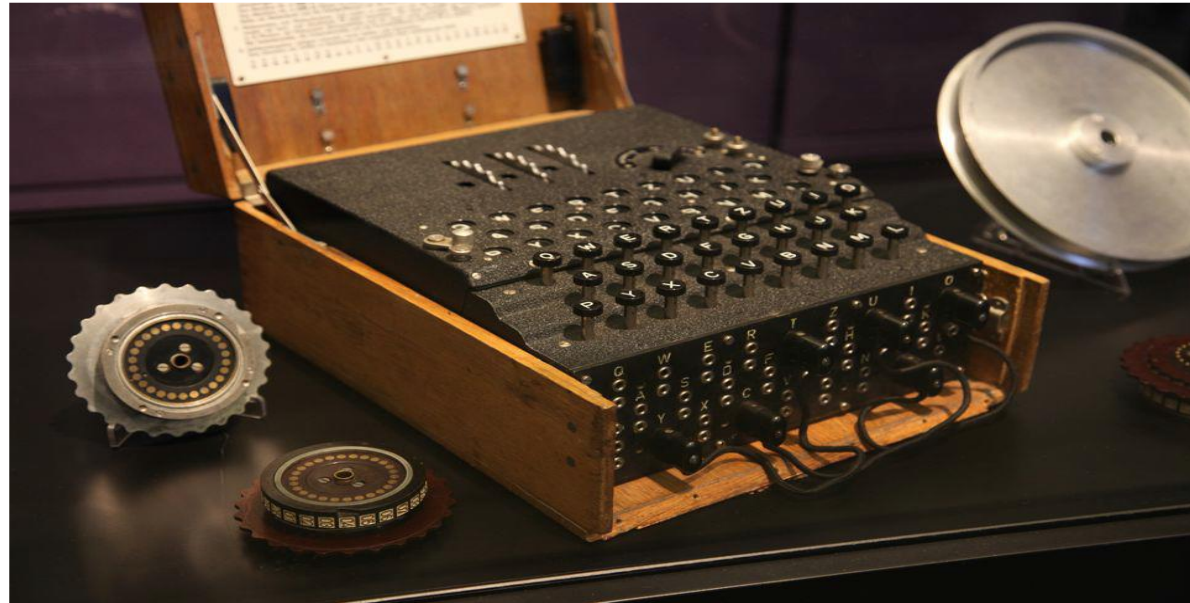
- The situation:
- Europe in hands of Germany (and their allies)
- Britain looking likely to fall next
 - “Battle of Britain” (1963 British planes against 4074 German planes)
- Japan dominating Pacific region
 - (China, Korea, Malaysia, Singapore, Vietnam, Thailand, Indonesia, etc...)
- USA, USSR (Russia) not yet involved
 - And do not want to get involved!

The Secret War

- While battle raged in the open a “secret” war was being fought
- Military messages are sent encrypted
- If messages can be deciphered, possible to know what the enemy is planning
- British (and their allies) goal: To decrypt German (and Japanese) code
- How hard can it be?

Enigma Machine

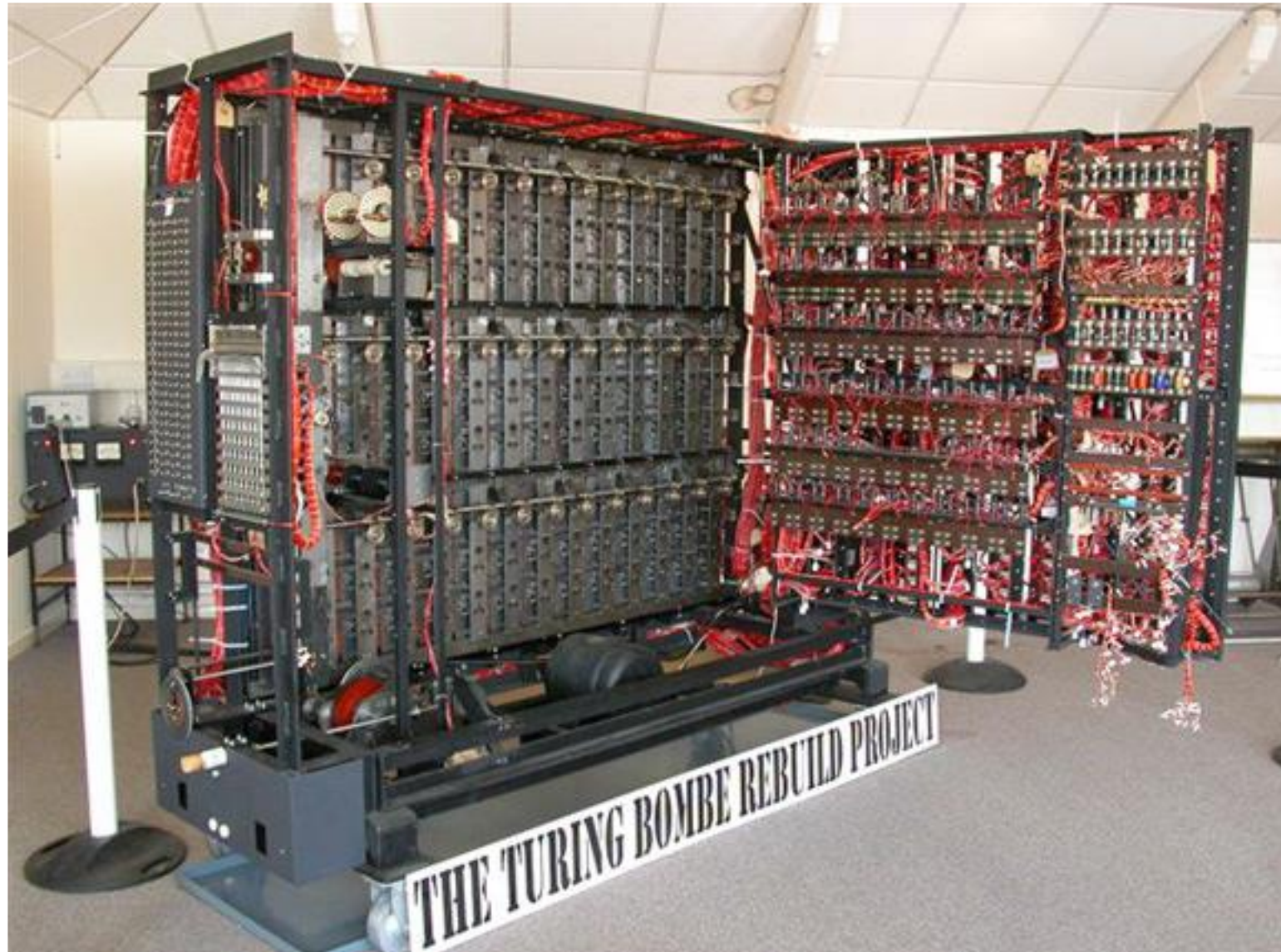
- To encrypt German messages
- “Unbreakable”
- 158×10^{18} (158 million million million) settings!
- Settings changed every day!
- Japan had something similar
 - Purple machine, based on Enigma



Breaking Enigma

- Bletchley Park was the central site for British codebreakers during WW2
- Teams of people (thousands):
 - Capturing German messages
 - Attempting to decrypt messages
- Top secret
 - Nobody knows this is happening
- Difficult problem. Struggling to succeed
- Turing and others (this was not done alone, despite what movies may say) built a machine to break the enigma code
 - Using abstract concepts from his Universal machine

Breaking Enigma



Breaking Enigma

- Breaking the “unbreakable” code
- Success! Enigma was broken
 - Japanese codes also broken
- Estimated shortening of war by 2 years
- Estimated 14-21 million lives saved!
- Outcome:
 - The first “computer”
 - An actual, physical computing device

Computer Science Born

- After the war ended (1945), computers began to be built and studied in universities
- Although the effort in Bletchley Park was secret
 - People who worked on breaking Enigma had learned a lot about how to build computing machines
 - They developed this knowledge at universities
 - Turing went to Manchester University, England, UK

Turing Test

- Turing had lots of visionary ideas
- Considered computer “intelligence”
 - One of the pioneers of Artificial Intelligence (AI)
- How to decide whether a computer is intelligent – the Turing Test
 - Identify whether you are talking to a computer or a person?
- One of the most important people in the history of computer science
- However...



Sex

- Turing was homosexual
 - In 1950s it was illegal in Britain
 - Not any more (since 1967)
- Prosecuted and convicted of “indecent” in 1952
 - He lost his security clearance to work with government
 - His reputation as University Professor was damaged
- He (probably) committed suicide in 1954
 - Took a bite from a poisoned apple
- He died largely unknown (by the public)

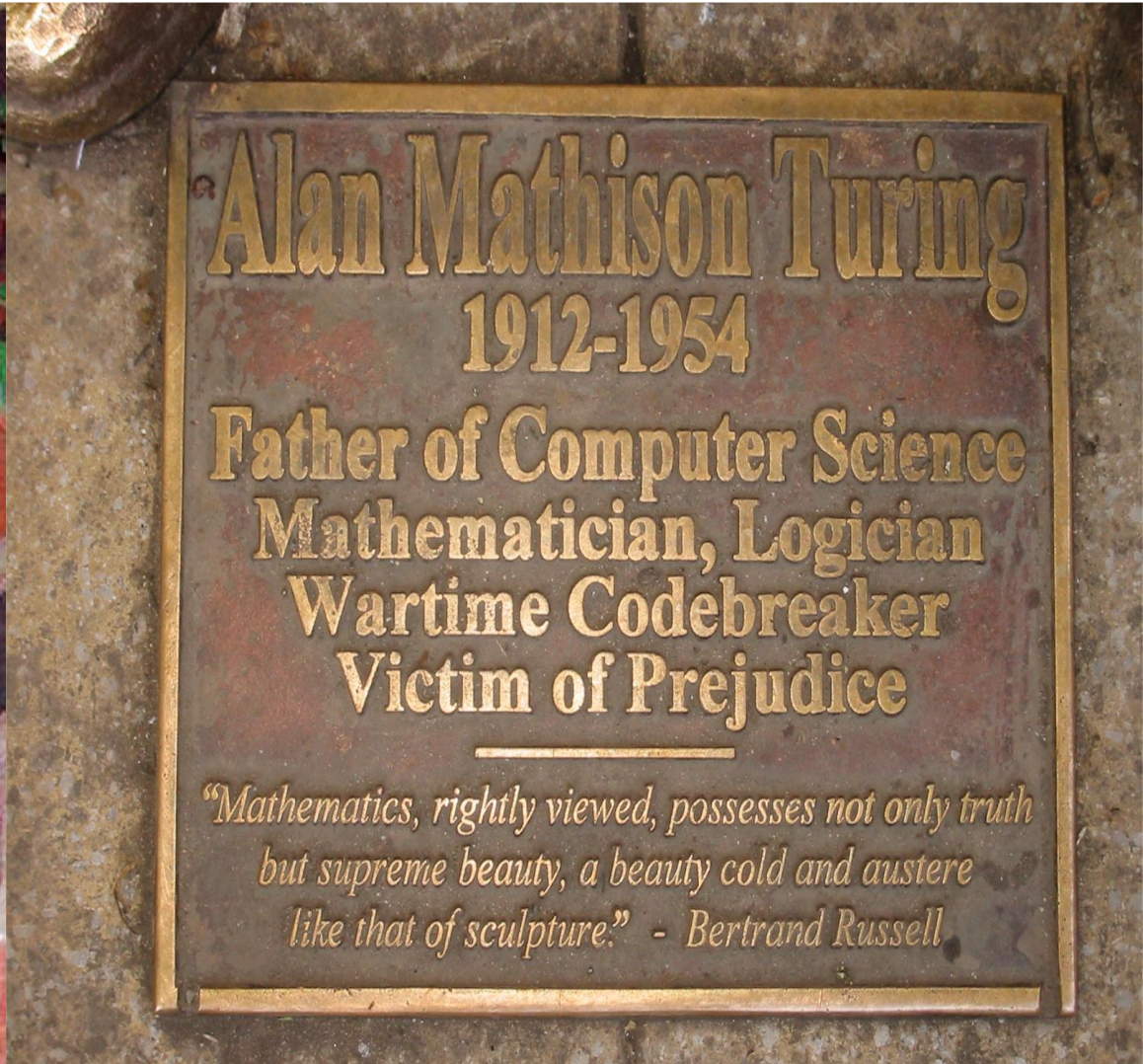
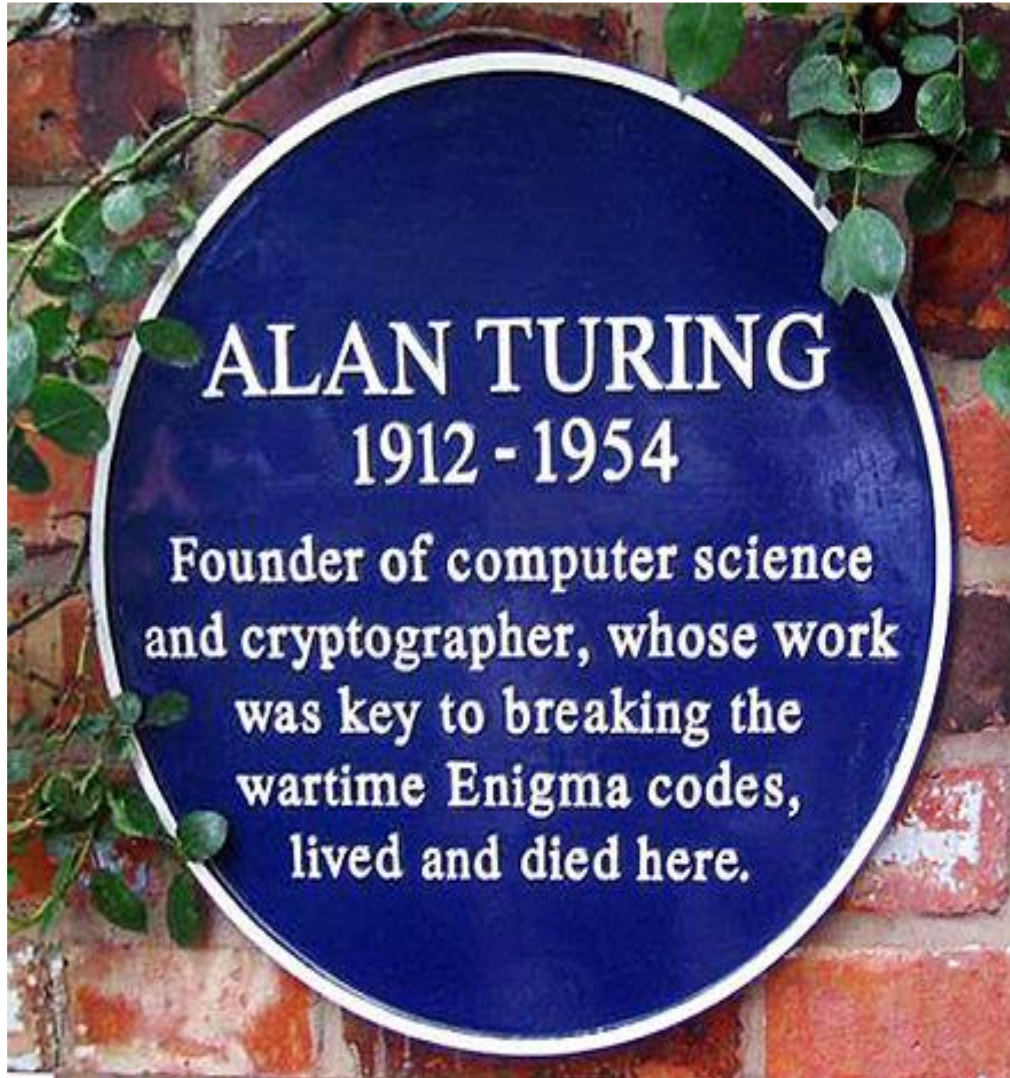


the bite of an apple

Secrets No More

- Eventually, work at Bletchley was revealed
 - Official secrets are released (after 50 years)
- Public opinion changes
 - Turing now largely regarded as a “national hero”
- 2009: British Government apologise for “the appalling way [Turing] was treated”
 - Following an internet campaign, Prime Minister Gordon Brown made an official public apology on behalf of the British

Now Remembered



Manchester



Aged 16

