Part II of the Mathematical Tripos

Automata & Formal Languages

MICHAELMAS TERM 2023

FIRST LECTURE : 6 October 2023

This course is about THEORY OF COMPUTATION

Typical questions

What mathematical question can be answered by computation?

How fast can you compute the solution?

Not a major theme of the course, but shows up from time to time.

Automata & Formal Languages
Michaelmas Term 2023
Part II of the Mathematical Tripos
University of Cambridge
Prof. Dr. B. Löwe

Automata & Formal Languages

Contents

Slightly more precisely:

DECISION PROBLEMS

Domain D of objects
Property P of elements of D,
i.e., $P \subseteq D$.

$\underline{Q^P}$ Can you decide whether $x \in P$?

Note that the answering mechanism for deciding Q^P could be nonuniform
(i.e., depend on x).

Therefore, we are more interested in uniform solutions:

$\underline{Q^P_x}$ Is $x \in P$?

Is there a uniform way with input x to solve Q^P_x?

"uniform way" is interpreted as ALGORITHM

DECISION PROBLEM FOR PROPERTY P

SOLVABLE
YES

UNSOLVABLE
NO

Example 1 $\quad D := \mathbb{N}$

$P := \{n \in D ;\ n \text{ is not prime}\}$

BRUTE FORCE algorithm is a solution to P

Example 2 $\quad D := \mathbb{Q}^{n \times n}$

$P := \{A \in D ;\ \exists B \ A \cdot B = \mathbb{1}\}$

Linear Algebra says:

$A \in P \iff rk(A) = n.$

And we have Gauß algorithm to determine $rk(A)$.

Remark. Note that we solved these without ever defining the word "algorithm".

David Hilbert

Hilbert in 1912

Born	23 January 1862 Königsberg or Wehlau, Prussia
Died	14 February 1943 (aged 81) Göttingen, Nazi Germany

1900

International Congress of Mathematicians in Paris

Hilbert : Mathematical Problems ("for the 20th century")

HILBERT 10.

10. DETERMINATION OF THE SOLVABILITY OF A DIOPHANTINE EQUATION.

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients : *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Is there an algorithm that on input $p \in \mathbb{Z}[X_1, \dots X_n]$ gives whether $p \in P := \{q \,;\, \exists \vec{z} \in \mathbb{Z}^n \; q(\vec{z}) = 0\}$

David Hilbert

Hilbert in 1912

Born	23 January 1862 Königsberg or Wehlau, Prussia
Died	14 February 1943 (aged 81) Göttingen, Nazi Germany

ENTSCHEIDUNGSPROBLEM
=
German for "decision problem"

Wilhelm Ackermann

Wilhelm Ackermann in c. 1935

Born	29 March 1896 Herscheid, German Empire
Died	24 December 1962 (aged 66) Lüdenscheid, West Germany
Nationality	German

§ 12. Das Entscheidungsproblem.

Aus den Überlegungen des vorigen Paragraphen ergibt sich die grundsätzliche Wichtigkeit des Problems, bei einer vorgelegten Formel des Prädikatenkalküls zu erkennen, ob es sich um eine identische Formel handelt oder nicht. Nach der in § 5 gegebenen Definition bedeutet die Identität einer Formel dasselbe wie die Allgemeingültigkeit der Formel für jeden Individuenbereich. Man pflegt deswegen auch von dem *Problem der Allgemeingültigkeit* einer Formel zu sprechen. Genauer müßte man statt Allgemeingültigkeit Allgemeingültigkeit für jeden Individuenbereich sagen. Die identischen Formeln des Prädikatenkalküls sind nach den Ausführungen des § 10 gerade die Formeln, die aus dem Axiomensystem des § 5 sich ableiten lassen. Zu einer Lösung des Problems der Allgemeingültigkeit vermag uns diese Tatsache nicht zu helfen, da wir kein allgemeines Kriterium für die Ableitbarkeit einer Formel haben.

D : set of formulas

$P := \{\varphi \,;\, \varphi$ is a tautology$\}$

= valid

= provable

[Details will require definitions from the Part II Logic & Set Theory Course]

1928: "The Old Testament of Logic"

It'll turn out that both Hilbert 10 & Entscheidungsproblem are both unsolvable.

Asymmetry between

POSITIVE solutions

only need to be able to ~~a~~ recognise an algorithm when we see it

and

NEGATIVE solutions

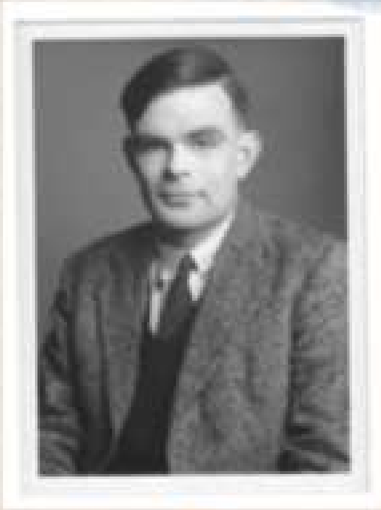
need a definition of "algorithm".

This lecture course is about:

- precise definition of algorithm
- how to prove negative results

NEGATIVE RESULTS:

ENTSCHEIDUNGSPROBLEM



Alan TURING
1912–1954

Alonzo CHURCH
1903–1995

230 A. M. TURING [Nov. 12,

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable numbers, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

There is no algorithm to solve the ENTSCHEIDUNGSPROBLEM.

HILBERT 10

There is no algorithm to determine whether a given polynomial in $\mathbb{Z}[x_1, \dots, x_n]$ has an integer root.

Martin DAVIS
born 1928

Yuri MATIYASEVICH
born 1947

Julia ROBINSON
1919–1985

Hilary PUTNAM
1926–2016

Most general setting:

STRINGS OF SYMBOLS

Fix a finite set Ω of SYMBOLS and let Ω^* be the set of finite strings of elts of Ω.

Then $D := \Omega^*$, $P \subseteq D$ is the general form of our decision problems.

This is most general since computing requires encoding in working memory, i.e. as a finite string of finite objects.

So, it is general enough to recapture all of the past example.

Ex. 1 Natural numbers written as strings of digits

Ex. 2 Rationals are $\pm a_0 \dots a_k / b_0 \dots b_l$

Then $A \in \mathbb{Q}^{2\times 2}$ is just

$\pm a_0 \dots a_k / b_0 \dots b_l \,\square\, \pm a_0' \dots$

Ex. 3 Polynomials are finite strings of their coefficients

Ex. 4 Formulas are finite strings of symbols.

NOTATION & REMINDER

(1) $\mathbb{N} = \{0, 1, 2, \dots\}$ 0 is included in $\mathbb{N}$

$n = \{0, \dots, n-1\}$

(2) ~~For~~ any set X, we write

X^n for the sequence/tuples/strings of length n of elts of X

(3) In particular, X^0 consists only of the empty string.

We call ~~this~~ ε (EPSILON).

(4) Note that if $\alpha \in X^n$, α is a function with $\mathrm{dom}(\alpha) = n$, $\mathrm{ran}(\alpha) \subseteq X$.

(5) If $\alpha \in X^n$ and $k \leq n$, then $\alpha \restriction k \in X^k$ is the unique initial segment of α of length k.

(6) $|\alpha| := \mathrm{dom}(\alpha)$.

length of α.

(7) $X^* := \bigcup_{n \in \mathbb{N}} X^n$ The set of finite X-sequences

(8) <u>Concatenation</u>:

$\alpha \in X^n$, $\beta \in X^m$, we can define $\alpha\beta \in X^{n+m}$ by

$$\alpha\beta(k) := \begin{cases} \alpha(k) & k < n \\ \beta(\ell) & k = n + \ell \text{ with } \ell < m \end{cases}$$

(9) Slightly incorrectly, I'll write x for the length one seq. with value x.

This means that αx is just

$$\underbrace{a_0 \dots a_n}_{=\alpha} x .$$