AUTOMATA & FORMAL LANGUAGES

PART II
MATHEMATICAL TRIPOS
MICHAELMAS 2022

FIRST LECTURE

6 October 2022

AUTOMATA AND FORMAL LANGUAGES (C) **24 lectures, Michaelmas Term**

Part IA Numbers and Sets is essential.

Recursively enumerable languages
Register machines. Recursive functions. Recursively enumerable sets. Church's thesis. Undecidability of the halting problem. Universal register machines. The recursion theorem. The s-m-n theorem. Reductions. Rice's theorem. Degrees of unsolvability. Hardness and completeness. [10]

Regular languages
Deterministic and non-deterministic finite-state automata. Regular languages. Regular expressions. Limitations of finite-state automata: closure properties; the pumping lemma; examples of non-regular languages. Minimisation. [3]

Context-free languages
Context-free grammars. Context-free languages. Chomsky normal form. Regular languages are context-free. Limitations of context-free grammars: the pumping lemma for context-free languages; examples of non-context-free languages. [5]

Appropriate books

S.B. Cooper *Computability theory (CRC Mathematics Series)*. Chapman Hall 2003
J.E. Hopcroft, R. Motwani and J.D. Ullman *Introduction to automata theory, languages and computation, 3rd ed.* Pearson 2013
P.T. Johnstone *Notes on logic and set theory (Chapter 4)*. CUP 1987
D.C. Kozen *Automata and computability*. Springer 1997
R.I. Soare *Turing computability: theory and applications (Theory and applications of computability)*. Springer 2016
M. Sipser *Introduction to the theory of computation, 3rd ed.* Cengage 2012

COMPUTATION

COMPUTABILITY

EXISTENCE VS ALGORITHMIC ACCESS TO WITNESS

DAVID HILBERT
1862-1943

ICM 1900 Paris

Hilbert Problems

"Hilbert 10"

$\mathbb{Z}[X]$

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.*

David HILBERT

Wilhelm ACKERMANN 1896–1962

1928: H-A

Grundzüge der theoretischen Logik

§ 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.

Given a formula, determine whether it is a tautology.

POSITIVE SOLUTION:

Positive solutions do not require a definition of

ALGORITHM

PROCEDURE

If presented & everyone agrees, leave fine.

NEGATIVE SOLUTION:

Negative solutions ("there is no algorithm") require a definition of ALGORITHM.

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 ENTSCHEIDUNGS-PROBLEM.

HILBERT 10

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

Martin DAVIS
born 1928

Yuri MATIYASEVICH
born 1947

Julia ROBINSON
1919-1985

Hilary PUTNAM
1926-2016

§ 1.1 BASIC DEFINITIONS

What is the object of computation?

Naïve answer: numbers.

?? $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Our examples don't even have numbers as input:

ENTSCH. : Formula φ.

H10 : Polynomial.

The idea of modern computation is to encode everything as strings of symbols.

Basic idea: A set (finite) Ω of symbols and then we consider Ω-strings Ω^* : the set of finite sequences from Ω

Recollect some things from N&S (Part IA).

A set X is called **COUNTABLE** if there is a surjection $\mathbb{N} \longrightarrow X$.

It is called **INFINITE** if there is an injection $\mathbb{N} \longrightarrow X$.

UNCOUNTABLE = NOT COUNTABLE
FINITE = NOT INFINITE

Proposition 1.1. If $X \neq \emptyset$ and countable, then X^* is infinite and countable.

PROOF INFINITE. Since $X \neq \emptyset$, take $x \in X$.

Then $n \longmapsto (\underbrace{x, \ldots, x}_{n \text{ times}})$

is an injection.

COUNTABLE Pick $\pi : \mathbb{N} \longrightarrow X$ surjection.

If $k \in \mathbb{N}$ write $k = \prod_{i \in \mathbb{N}} p_i^{k_i}$

$p_0 = 2, \ p_1 = 3, \ p_2 = 5, \ p_3 = 7, \ p_4 = 11, \ \ldots$

$$k = \prod_{i \in \mathbb{N}} p_i^{k_i}$$

$k = 2^3 3^2 5^0 7^{10} 11^2 \cdot \underbrace{\quad}_{\text{all exp. } 0}$

LENGTH

$(2,0,10) \rightsquigarrow (\pi(2), \pi(0), \pi(10)) \in X^*$

The map that takes k, interprets k_0 as the length and then reads the next k_0 exponents and maps them by π to X is a surjection from $\mathbb{N}$ to X^*.

$$k \longmapsto (\pi(k_1), \dots, \pi(k_{k_0}))$$

q.e.d.

Proposition 1.2 If X is infinite, then

$$\mathcal{P}(X) = \{A ; A \subseteq X\}$$

POWER SET OF X

is uncountable.

[Numbers & Sets; but encouragement to revise and think about the proof method:

DIAGONALISATION]

Proposition 1.3 If X is countable, then the set $\mathrm{Fin}(X) \subseteq \mathcal{P}(X)$ of all finite subsets of X is countable.

PROOF It is enough to show that there is a surjection from X^* onto $\mathrm{Fin}(X)$. [By P 1.1]

Idea: If $\alpha \in X^*$ is a sequence, let $f(\alpha) \in \mathrm{Fin}(X)$ be the set of all elts of X occurring in it.

Claim: f is a surjection.

Since X is countable, we have

$$\pi : \mathbb{N} \longrightarrow X \quad \text{surjection.}$$

So for $x \in X$, $\pi^{-1}(x) \subseteq \mathbb{N}$.

$\neq \emptyset$

Therefore, let n_x be the least elt of $\pi^{-1}(x)$.

So, if given $F \in Fin(X)$, consider $\{n_x \mid x \in F\} \subseteq \mathbb{N}$, order it in the usual way. That's a sequence of nat. numbers with $|F|$ many elements. It's π-image is a seq. in X^* s.t.

$$f(\alpha) = F.$$

q.e.d.

NOTATIONS

1. $\mathbb{N} = \{0, 1, 2, \dots\}$!!!!!

2. Set-theoretic reconstruction of $\mathbb{N}$:

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

3. X^n set of X-strings of length n

These are functions

$$\alpha : n \longrightarrow X$$

$$\alpha \in X^n \rightsquigarrow \alpha = (x_0, x_1, \dots, x_{n-1})$$

length of α is n

$$|\alpha| = \mathrm{dom}(\alpha)$$

4. X^0 consists only of the empty sequence ε

5. $$X^* = \bigcup_{n \in \mathbb{N}} X^n$$

6. If $|\alpha| = n$, $k \leq n$

$\alpha \restriction k$ is the unique sequence of length k s.t.

$\alpha \restriction k \subseteq \alpha$

7. CONCATENATION

$\alpha, \beta \in X^*$ $|\alpha| = n$, $|\beta| = m$

$\alpha\beta$ is the concatenation of α, β and has length $n+m$.

8. By recursion, we define

$\alpha^0 := \varepsilon$

$\alpha^{n+1} := \alpha^n \alpha$

9. I identify the sequence of length one with symbol x with the symbol.

So x also means seq. of length one with x.

10. So, in particular

$x\alpha$ is α prefixed by x

αx is α postfixed by x

11. If $Y, Z \subseteq X^*$, we write

$$YZ := \{\alpha\beta \mid \alpha \in Y, \beta \in Z\}$$

12. If $Y = \{\alpha\}$, then we also write αZ for $\{\alpha\}Z$.

13. If $f : X \longrightarrow Y$, this function can be lifted to X^* by recursion

$$\hat{f}(\varepsilon) := \varepsilon$$

$$\hat{f}(\alpha x) := f(\alpha)\hat{f}(x)$$

Often, we just write f for this function.