XXIII

TWENTY-THIRD & PENULTIMATE LECTURE OF AUTOMATA & FORMAL LANGUAGES

26 NOVEMBER 2022

RECAP The Church-Turing Thesis allowed us to understand decision problems as concrete mathematical questions.

WORD PROBLEM $\{(w,v);\ w \in \mathcal{L}(G_v)\}$ $\{(w,v);\ w \in W_v\}$

EMPTINESS PROBLEM $\{w;\ \mathcal{L}(G_w) = \emptyset\}$ $\{w;\ W_w = \emptyset\}$

EQUIVALENCE PROBLEM $\{(w,v);\ \mathcal{L}(G_w) = \mathcal{L}(G_v)\}$ $\{(w,v);\ W_w = W_v\}$

↑ VIA ENCODING OF TYPE 0 GRAMMARS AS COMPUTABLY ENUMERABLE SETS

We proved: The WORD PROBLEM for type 0 grammars is unsolvable.

Remains to be proved:

Emptiness & Equivalence problems are unsolvable.

§4.11 Reduction functions & degrees of unsolvability

$A, B \subseteq \mathbb{W}$

Def. $f : \mathbb{W} \longrightarrow \mathbb{W}$ a REDUCTION FUNCTION FROM A TO B if

① f is total computable

② $w \in A \iff f(w) \in B$ for all w

Intuition If a reduction exists, A is "at most as complicated as B".

Write $A \leq_m B$ if there is such a reduction (many-one)

Properties of relation $\leq_m$:

(a) reflexive

(b) transitive

(c) If $A \leq_m B$, then $\mathbb{W} \setminus A \leq_m \mathbb{W} \setminus B$.

(d) ANTISYMMETRY ?

$\leq_m$ is NOT antisymmetric.

A reflexive, transitive relation is called a "partial preorder".

If $\leq$ is a partial preorder on X, then

$$x \equiv y \;:\Longleftrightarrow\; x \leq y \;\&\; y \leq x$$

is an equivalence relation and

$(X/_{\equiv}, \leq)$ is a partial order.

[ES#4 (54)]

Thus: a partial preorder looks like a partial order except that it has clusters consisting of $\equiv$-equivalence classes.

More properties

(e) If $A \leq_m B$ — $\exists f : \mathbb{N} \to \mathbb{N}$, $f^{-1}[B] = A$

- and B computable, then A is comp.
- and B c.e., then A is c.e.

[This is just $\chi_A = \chi_B \circ f$ if f is the reduction. $\psi_A = \psi_B \circ f$]

(f) Thus: if

$\mathbb{K} \leq_m A$, A is not computable

$\mathbb{W}\setminus\mathbb{K} \leq_m A$, A is not c.e.

Remark. Many proofs from the last few lectures are really "reduction function arguments".

E.g., the claim that solvability (= computability) of

$\{(w,v);\ w \in \mathcal{L}(G_v)\}$ and

$\{(w,v);\ w \in W_v\}$

is equivalent.

Proposition Suppose $B \neq \emptyset, \mathbb{W}$ and A is computable. Then $A \leq_m B$.

Proof. Since $B \neq \emptyset, \mathbb{W}$, let $v \in B$, $v \notin B$.

Since A is computable,

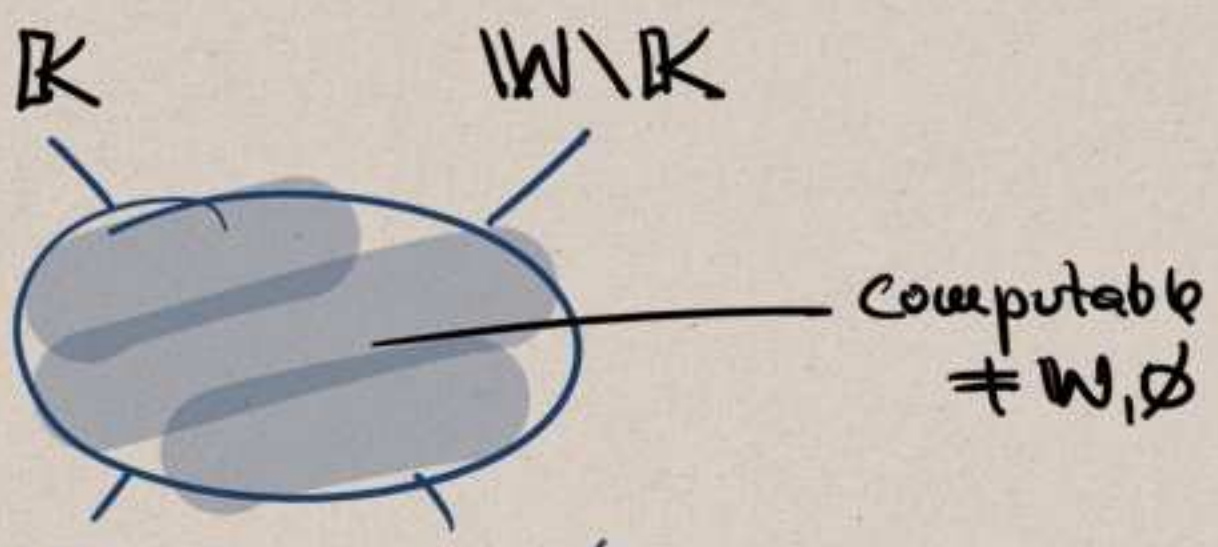
$$f : w \longmapsto \begin{cases} v & w \in A \\ u & w \notin A \end{cases}$$

is computable & it is a reduction from A to B. q.e.d.

We will look at $\emptyset$ & $\mathbb{W}$ on ES#4 (55).

Picture

DEGREES OF UNSOLVABILITY



Note that $K \not\equiv_m W \setminus K$ ← follows from the 2nd + complementation

$W \setminus K \not\equiv_m K$ ← o/w K is not c.e.

Do we think that this picture [ ] is all there is?

NO. If $A, B \subseteq W$, then define

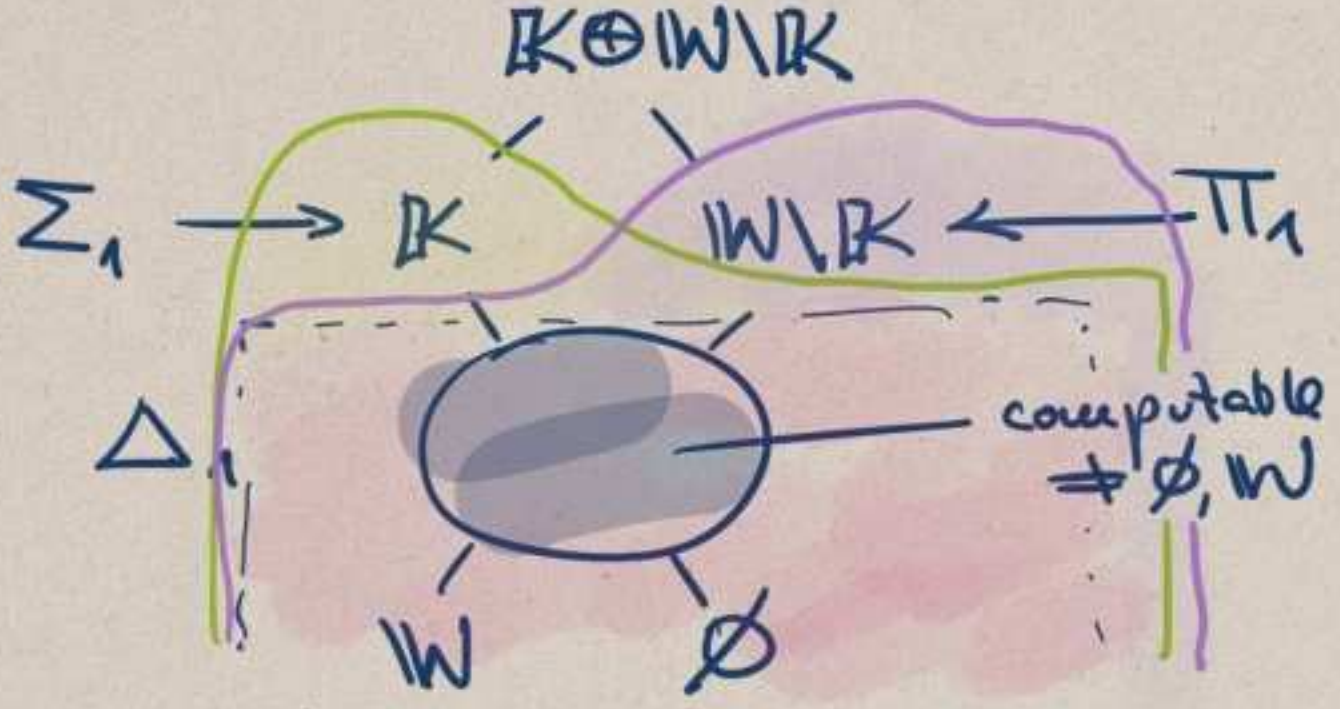
$\{0,1\} \subseteq \Sigma$ $A \oplus B := 0A \cup 1B$

TURING JOIN OF A & B

Clearly $A \leq_m A \oplus B$ by $f(w) := 0w$

$B \leq_m A \oplus B$ by $f(w) := 1w$

The Turing join is actually the least upper bound in the degrees of unsolvability (CS#4).



COMPLETENESS

If $\mathcal{C}$ is a class of sets, we say that A is $\mathcal{C}$-hard if for every $B \in \mathcal{C}$, we have $B \leq_m A$.

We say A is $\mathcal{C}$-complete if it is $\mathcal{C}$-hard and $A \in \mathcal{C}$.

$\mathcal{C}$-complete means: the most complicated $\mathcal{C}$-set.

Corollary If A is Δ_1, $A \neq \emptyset, \mathbb{N}$, then A is Δ_1-complete.

Proof. Just the definition plus the earlier proof that every Δ_1 (= computable) set reduces to any set $\neq \emptyset, \mathbb{N}$.

q.e.d.

Goal: K is Σ_1-complete.

[will be proved today.]

EXCURSION

P = NP

Hilbert's Problems
1900

⇝

CLAY MILLENIUM PROBLEMS
2000

$1,000,000 per problem

CMI

ABOUT PROGRAMS PEOPLE MILLENNIUM PROBLEMS PUBLICATIONS EVENTS NEWS

Millennium Problems

Yang–Mills and Mass Gap

Experiment and computer simulations suggest the existence of a "mass gap" in the solution to the quantum versions of the Yang-Mills equations. But no proof of this property is known.

Riemann Hypothesis

The prime number theorem determines the average distribution of the primes. The Riemann hypothesis tells us about the deviation from the average. Formulated in Riemann's 1859 paper, it asserts that all the 'non-obvious' zeros of the zeta function are complex numbers with real part 1/2.

P vs NP Problem

If it is easy to check that a solution to a problem is correct, is it also easy to solve the problem? This is the essence of the P vs NP question. Typical of the NP problems is that of the Hamiltonian Path Problem: given N cities to visit, how can one do this without visiting a city twice? If you give me a solution, I can easily check that it is correct. But I cannot so easily find a solution.

Navier–Stokes Equation

This is the equation which governs the flow of fluids such as water and air. However, there is no proof for the most basic questions one can ask: do solutions exist, and are they unique? Why ask for a proof? Because a proof gives not only certitude, but also understanding.

Hodge Conjecture

The answer to this conjecture determines how much of the topology of the solution set of a system of algebraic equations can be defined in terms of further algebraic equations. The Hodge conjecture is known in certain special cases, e.g., when the solution set has dimension less than four. But in dimension four it is unknown.

Poincaré Conjecture

In 1904 the French mathematician Henri Poincaré asked if the three dimensional sphere is characterized as the unique simply connected three manifold. This question, the Poincaré conjecture, was a special case of Thurston's geometrization conjecture. Perelman's proof tells us that every three manifold is built from a set of standard pieces, each with one of eight well-understood geometries.

Birch and Swinnerton-Dyer Conjecture

Supported by much experimental evidence, this conjecture relates the number of points on an elliptic curve mod p to the rank of the group of rational points. Elliptic curves, defined by cubic equations in two variables, are fundamental mathematical objects that arise in many areas: Wiles' proof of the Fermat Conjecture, factorization of numbers into primes, and cryptography, to name three.

Stephen Cook
born 1939

formulated P & NP in modern terminology

Sir Timothy Gowers will be lecturing INTRODUCTION TO COMPUTATIONAL COMPLEXITY in Lent term 2023 for Part II : TuTh 9–10 (MR 5)

Def. f is **polynomial-time** if it is

(a) total

(b) computable

(c) there is a polynomial p s.t. f.a. w, the computation of $f(w)$ halts in less than $p(|w|)$ steps.

Def. A is **polynomial-time** if χ_A is polynomial-time

COMP. Σ_1

$P := \{ A ;\ A \text{ is polynomial time} \}$

$NP := \{ A ;\ \text{there is } B \subseteq \mathbb{N}^2 \text{ polynomial-time s.t. } A = p(B) \}$

ANALOGUE

Q: $P \stackrel{?}{=} NP$ ← $1,000,000

Idea to prove that $P = NP$ would be to prove that an NP-complete problem is in P.

Write $A \leq_p B$ for "there is a poly-time reduction fn".

B is NP-complete if for all A NP, we have $A \leq_p B$ & B is NP

List of NP-complete problems

From Wikipedia, the free encyclopedia

This is a dynamic list and may never be able to satisfy particular standards for completeness. You can help by adding missing items with reliable sources.

This is a list of some of the more commonly known problems that are NP-complete when expressed as decision problems. As there are hundreds of such problems known, this list is in no way comprehensive. Many problems of this type can be found in Garey & Johnson (1979).

Contents [hide]

Graphs and hypergraphs [edit]

Graphs occur frequently in everyday applications. Examples include biological or social networks, which contain hundreds, thousands and even billions of nodes in some cases (e.g. Facebook or LinkedIn).

- 1-planarity[1]
- 3-dimensional matching[2][3]:SP1
- Bandwidth problem[3]:GT40
- Bipartite dimension[3]:GT18
- Capacitated minimum spanning tree[3]:ND5
- Route inspection problem (also called **Chinese postman problem**) for mixed graphs (having both directed and undirected edges). The program is solvable in polynomial time if the graph has all undirected or all directed edges. Variants include the rural postman problem.[3]:ND25,ND27
- Clique cover problem[2][3]:GT17
- Clique problem[2][3]:GT19
- Complete coloring, a.k.a. achromatic number[3]:GT5
- Cycle rank a.k.a. Rank coloring
- Degree-constrained spanning tree[3]:ND1

Back to Σ_1-completeness.

Theorem 4.42 K is Σ_1-complete.

Proof. K is Σ_1.

Take X arbitrary computably enum.

So fix f partial computable

$$X = \mathrm{dom}(f).$$

Goal: $X \leq_m K$.

Consider $g(w,v) := f(w)$. Clearly computable.

Apply s-m-n theorem to g: This is why totality was so important in the s-m-n theorem!

There is h total computable s.t.

$$f_{h(w)}(v) = g(w,v) = f(w).$$

Claim h is a reduction from X to K.

Assume $w \in X \longrightarrow w \in \mathrm{dom}(f)$

$\longrightarrow f_{h(w)}$ is the constant fn with value $f(w)$

$\longrightarrow W_{h(w)} = W$

$\longrightarrow f_{h(w)}(h(w)) \downarrow \longrightarrow h(w) \in K$.

Assume $w \notin X \longrightarrow w \notin \mathrm{dom}(f)$

$\longrightarrow f_{h(w)}$ is everywhere ~~undefined~~

$\longrightarrow W_{h(w)} = \emptyset$

$\longrightarrow f_{h(w)}(h(w))\uparrow \longrightarrow h(w) \notin K.$

q.e.d