Introduction

Theory of Computation

Objective

To give an overview of the class and what we are studying.

Proposed Problems

1901 mathematician David Hilbert

- proposed 23 problems to solve within next 100 years
- 10th problem: Given a polynomial with integer coefficients (called a Diophantine equation), does it have integer roots?

https://en.wikipedia.org/wiki/Hilbert%27s_problems

Assumption

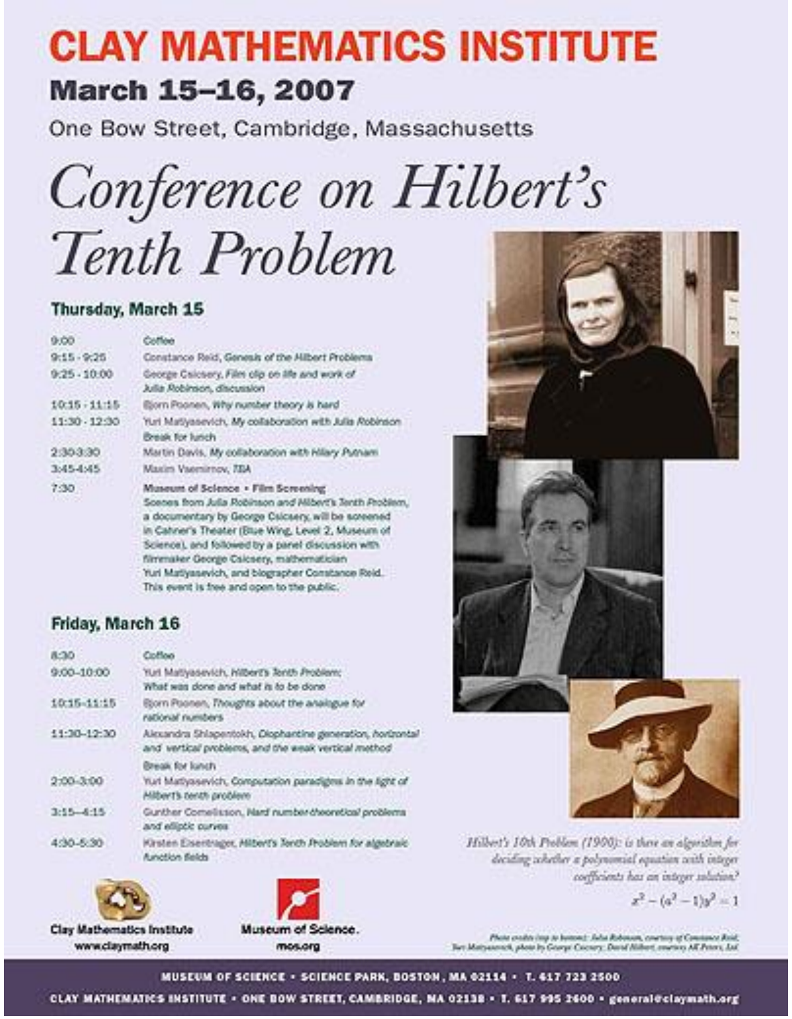
Assumption was that all 23 problems were solvable by some mechanical process (Hilbert said “process according to which it can be determined in a finite number of operations”)

Hilbert's 10th Problem is Not Solvable

Proof by Yuri Matijasevich

Picture (bottom up):

- David Hilbert
- Yuri Matijasevich
- Julia Robinson



CLAY MATHEMATICS INSTITUTE

March 15–16, 2007

One Bow Street, Cambridge, Massachusetts

Conference on Hilbert's Tenth Problem

Thursday, March 15

9:00	Coffee
9:15 - 9:25	Constance Reid, *Genesis of the Hilbert Problems*
9:25 - 10:00	George Csicsery, *Film clip on life and work of Julia Robinson, discussion*
10:15 - 11:15	Bjorn Poonen, *Why number theory is hard*
11:30 - 12:30	Yuri Matiyasevich, *My collaboration with Julia Robinson*
	Break for lunch
2:30-3:30	Martin Davis, *My collaboration with Hilary Putnam*
3:45-4:45	Maxim Vsemirnov, *TBA*
7:30	**Museum of Science • Film Screening** Scenes from *Julia Robinson and Hilbert's Tenth Problem*, a documentary by George Csicsery, will be screened in Cahner's Theater (Blue Wing, Level 2, Museum of Science), and followed by a panel discussion with filmmaker George Csicsery, mathematician Yuri Matiyasevich, and biographer Constance Reid. This event is free and open to the public.

Friday, March 16

8:30	Coffee
9:00–10:00	Yuri Matiyasevich, *Hilbert's Tenth Problem: What was done and what is to be done*
10:15–11:15	Bjorn Poonen, *Thoughts about the analogue for rational numbers*
11:30–12:30	Alexandra Shlapentokh, *Diophantine generation, horizontal and vertical problems, and the weak vertical method*
	Break for lunch
2:00–3:00	Yuri Matiyasevich, *Computation paradigms in the light of Hilbert's tenth problem*
3:15–4:15	Gunther Cornelisson, *Hard number-theoretical problems and elliptic curves*
4:30–5:30	Kirsten Eisentrager, *Hilbert's Tenth Problem for algebraic function fields*

Hilbert's 10th Problem (1900): is there an algorithm for deciding whether a polynomial equation with integer coefficients has an integer solution?

$$x^2 - (a^2 - 1)y^2 = 1$$

Clay Mathematics Institute
www.claymath.org

Museum of Science.
mos.org

Photo credits (top to bottom): Julia Robinson, courtesy of Constance Reid; Yuri Matiyasevich, photo by George Csicsery; David Hilbert, courtesy AK Peters, Ltd

MUSEUM OF SCIENCE • SCIENCE PARK, BOSTON, MA 02114 • T. 617 723 2500

CLAY MATHEMATICS INSTITUTE • ONE BOW STREET, CAMBRIDGE, MA 02138 • T. 617 995 2600 • general@claymath.org

Polynomials and Integer Roots

Do the following polynomials have integer roots?

- $x^2 – x = 0$
- $3x^2 – 7x - 40 = 0$
- $5x^4 + 2x^2 + 52 = 0$
- $3x^2y – 7xy + 40 = 0$
- $10x^3y^2 - 9x^2y – 3xy + 29 = 0$

Polynomials and Integer Roots

Do the following polynomials have integer roots?

- $x^2 - x = 0$ Yes, x=1
- $3x^2 - 7x - 40 = 0$ Yes, x=5
- $5x^4 + 2x^2 + 52 = 0$ No, no negatives
- $3x^2y - 7xy + 40 = 0$ Yes, x=5, y=-1
- $10x^3y^2 - 9x^2y - 3xy + 29 = 0$?

Can you write a program which takes an arbitrary polynomial as input and correctly outputs "yes, the polynomial has integer roots" or "no, the polynomial does not have integer roots"?

10th Problem is Not Decidable

- Hilbert’s 10th problem is not decidable (i.e. not solvable by any computing machine)

Decidable	Not Decidable
Determining if a polynomial on one variable has integer roots Many cases of polynomial s on multiple variables	Determining if a polynomial on an arbitrary number of variables has integer roots

Mechanical Process

Mechanical Process, M, for achieving some desired result:

- M is set out in terms of a finite number of exact instructions (each instruction being expressed by means of a finite number of symbols)
- M will, if carried out without error, produce the desire result in a finite number of steps;
- M can (in practice or in principle) be carried out by a human being unaided by any machinery save paper and pencil;
- M demands no insight or ingenuity on the part of the human being carrying it out.

Definitions of Mechanical Process

- Alan Turing (1912–1954) English computer scientist, mathematician, logician, cryptanalyst and theoretical biologist who in 1936, defined "mechanical process" using the Turing machine

- Alonzo Church, (1903-1995) American mathematician and logician science defined "mechanical process" differently in the same year

The Imitation Game

Benedict Cumberbatch as Alan Turing with the code-breaking machine Turing calls Christopher. Jack English/The Weinstein Company

Church-Turing Thesis

The Church-Turing Thesis:

Given any effective procedure, it can be calculated by a Turing machine

and

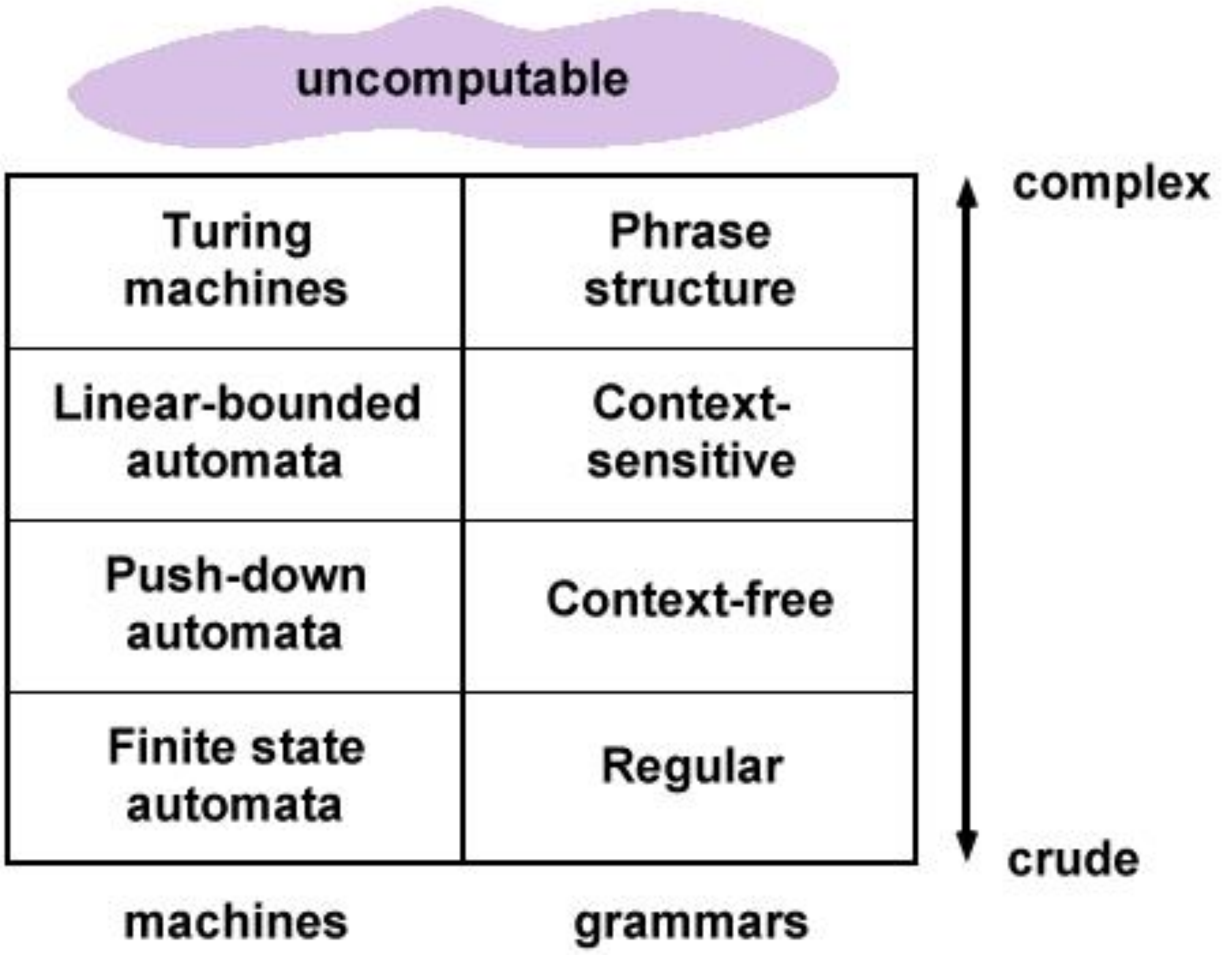
Anything that can be computed by a Turing machine is an effective procedure.

This is a thesis. It hasn't been proven, it is seen as a natural law.

Definitions of Mechanical Process

- Later
  - Gödel with recursive functions
  - Post’s canonical and normal systems (rewriting systems)

Chomsky Hierarchy



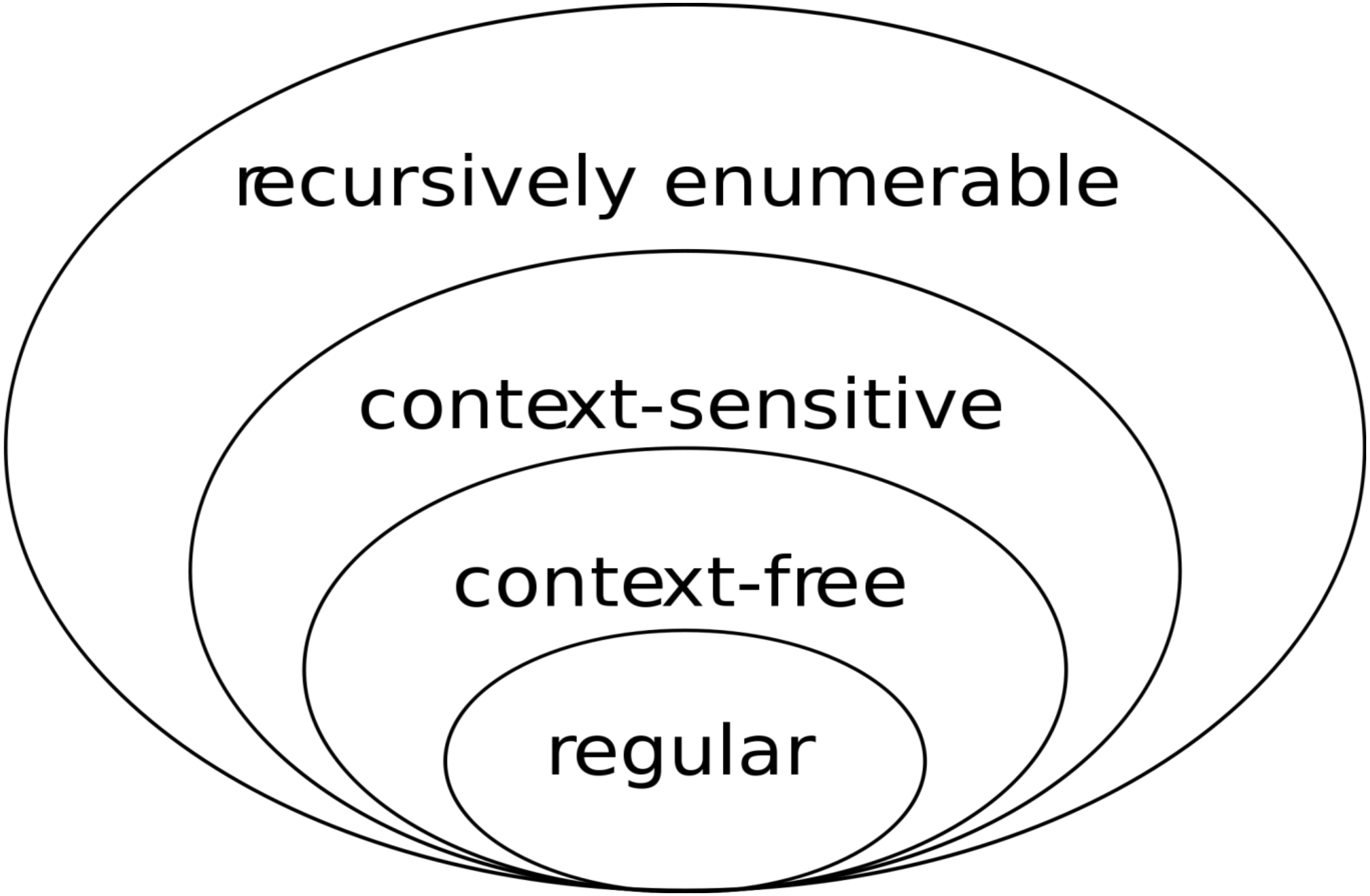
uncomputable

complex

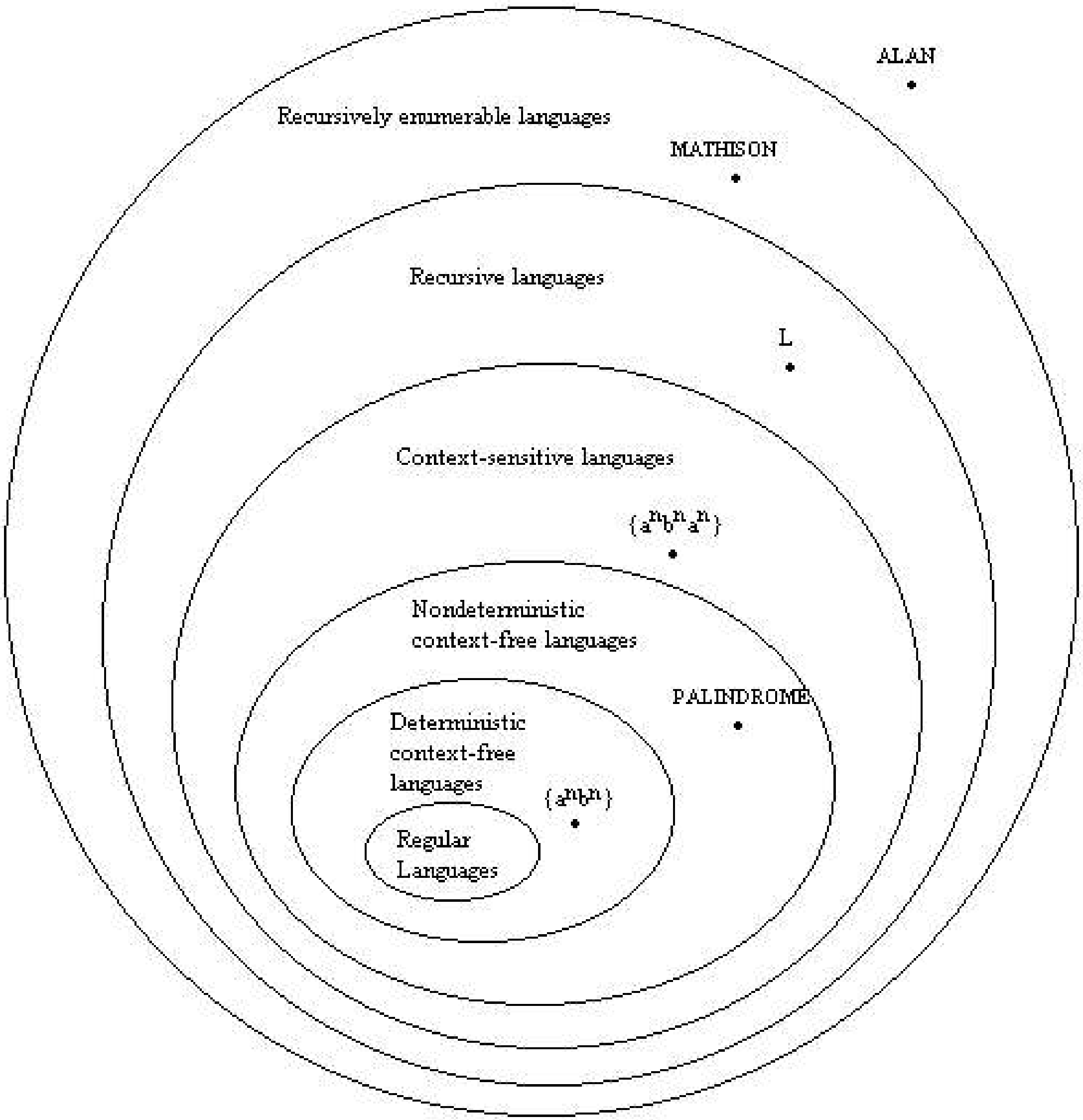
Turing machines	Phrase structure
Linear-bounded automata	Context-sensitive
Push-down automata	Context-free
Finite state automata	Regular
machines	grammars

crude

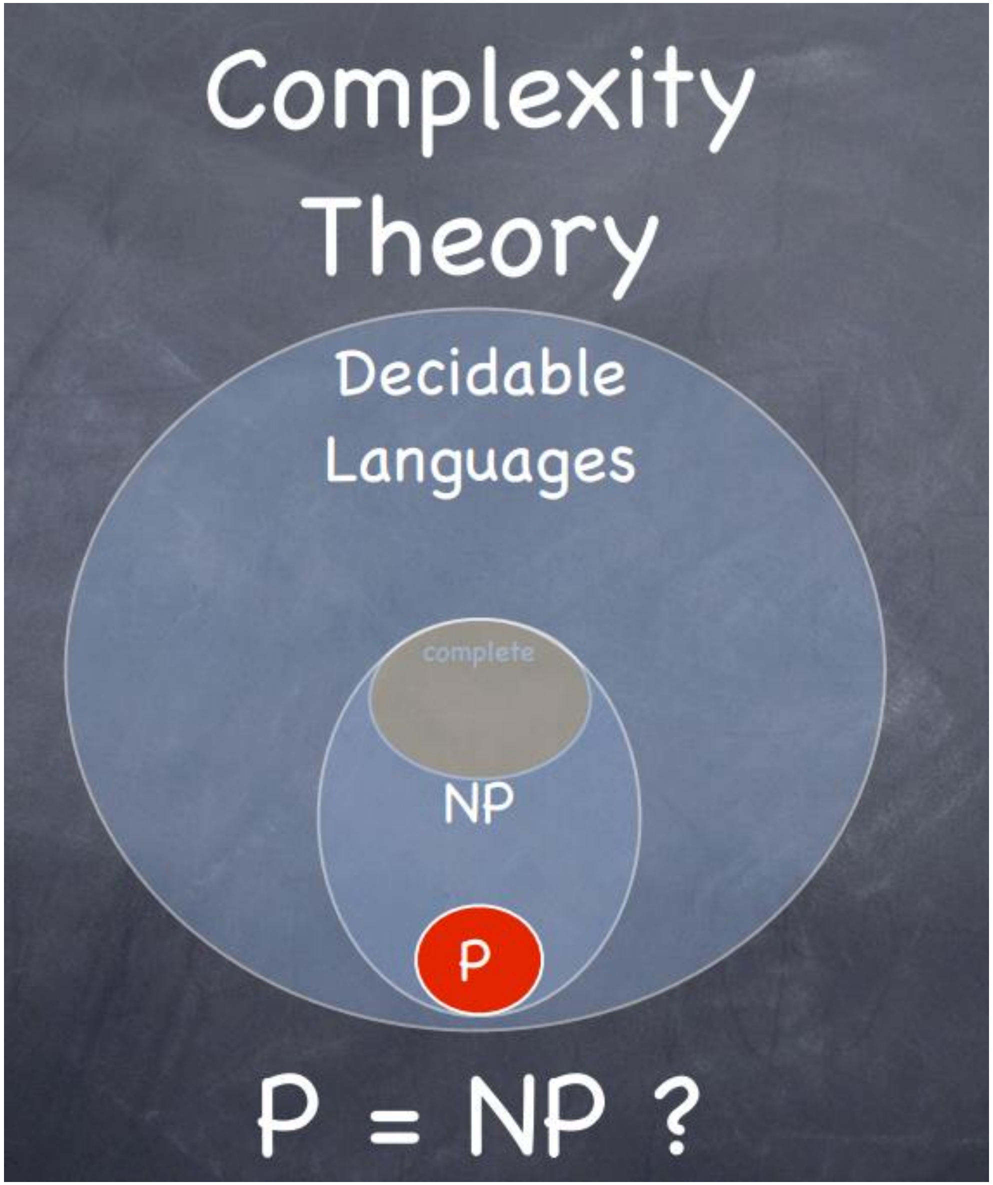
Chomsky Hierarchy



Chomsky Hierarchy


ALAN
Recursively enumerable languages
MATHISON
Recursive languages
L
Context-sensitive languages
$\{a^n b^n a^n\}$
Nondeterministic context-free languages
PALINDROME
Deterministic context-free languages
$\{a^n b^n\}$
Regular Languages

NP (and P) are Decidable


Complexity Theory
Decidable Languages
complete
NP
P
P = NP ?