Hilberts Entscheidungsproblem, the 10th Problem and Turing Machines

Nitin Saxena (Hausdorff Center for Mathematics, Bonn)

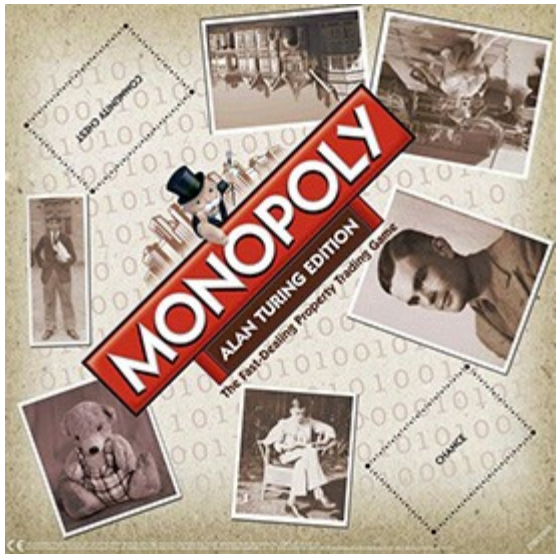
[Happy] [100th] [Alan] [Mathison] [Turing!][][][]...

**all pictures are works of others.

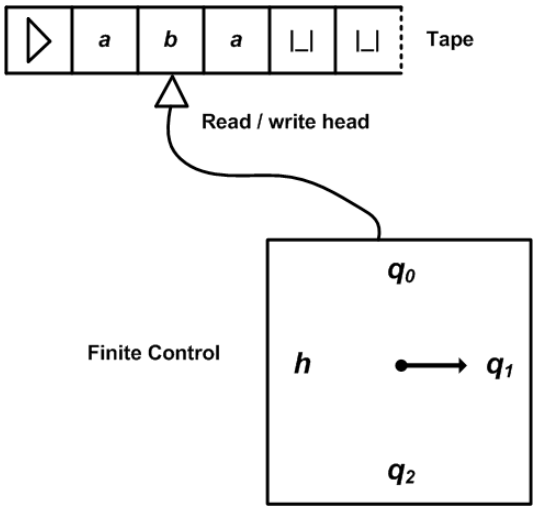
2012

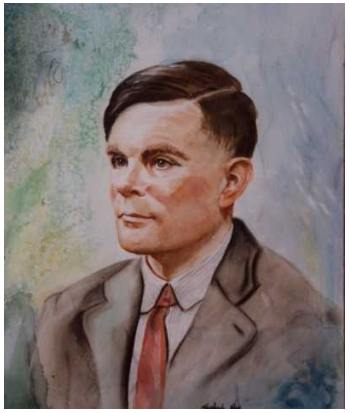
Contents

Prologue



- Turing did many things... (including winning **WW2** !)
  - But we focus on his *abstract* contributions.
- Postulated a simple, most general, mathematical model for computing – Turing machine (TM).
- How this postulation, together with Hilbert's dreams and Matiyasevich's realizations, led to some fundamental physical/ mathematical phenomena...





Turing (1912-1954)

Prologue

- Turing machines first appeared in the paper:

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

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

[*Extracted from the Proceedings of the London Mathematical Society, Ser.* 2, *Vol.* 42, 1937.]

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

Contents

- Prologue
- *Before Turing*
- Hilbert challenges
- Turing's first paper
- Matiyasevich solves the 10^{th} Problem
- Epilogue

Before Turing

- Gottfried Leibniz dreamt of building a machine that could check the truth of math statements.
- David Hilbert posed ***23*** problems in ICM Paris (1900) with the speech
  "*...**What methods, what new facts will the new century reveal in the vast and rich field of mathematical thought?**...*"
  - Only **3** are still unresolved!
- This talk is about one of the resolved ones: the 10th problem.

Leibniz (1646-1716)

Hilbert (1862-1943)

Before Turing

- Here is the list of the 23 problems:

1) Cantor's problem of the cardinal number of the continuum.
2) The compatibility of the arithmetical axioms.
3) The equality of the volumes of two tetrahedra of equal bases and equal altitudes.
4) Problem of the straight line as the shortest distance between two points.
5) Lie's concept of a continuous group of transformations without the assumption of the differentiability of the functions defining the group.
6) Mathematical treatment of the axioms of physics.
7) Irrationality and transcendence of certain numbers.
8) Problems of prime numbers.
9) Proof of the most general law of reciprocity in any number field.
10) Determination of the solvability of a diophantine equation.
11) Quadratic forms with any algebraic numerical coefficients.
12) Extension of Kronecker's theorem on abelian fields to any algebraic realm of rationality.

Before Turing

13) Impossibility of the solution of the general equation of the 7^{th} degree by means of functions of only two arguments.
14) Proof of the finiteness of certain complete systems of functions.
15) Rigorous foundation of Schubert's enumerative calculus.
16) Problem of the topology of algebraic curves and surfaces.
17) Expression of definite forms by squares.
18) Building up of space from congruent polyhedra.
19) Are the solutions of regular problems in the calculus of variations always necessarily analytic?
20) The general problem of boundary values.
21) Proof of the existence of linear differential equations having a prescribed monodromic group.
22) Uniformization of analytic relations by means of automorphic functions.
23) Further development of the methods of the calculus of variations.

Contents

- Prologue
- Before Turing
- *Hilbert challenges*
- Turing's first paper
- Matiyasevich solves the 10^{th} Problem
- Epilogue

Hilbert challenges

- Hilbert (1928) further asked for
  "***an algorithm to decide whether a given statement is provable from the axioms using the rules of logic***".
  - Known as the *Entscheidungsproblem*.
- He "believed" there exists no *undecidable* problem!
- Answer first requires defining 'algorithm' & 'computation'.
- Done by Alonzo Church (1935-6).
  - Using effective computability based on his λ-calculus.
  - Gave a negative answer!


Church (1903-1995)

Hilbert challenges

- Church showed that there is no algorithm to decide the *equivalence of two given λ-calculus expressions*.
- λ-calculus formalizes mathematics through *functions* in contrast to *set theory*.
- Eg. natural numbers are defined as
  - $0 := \lambda fx.x$
  - $1 := \lambda fx.f\ x$
  - $2 := \lambda fx.f\ (f\ x)$
  - $3 := \lambda fx.f\ (f\ (f\ x))$
- Addition, multiplication, recursion, substitution, evaluation are defined...

Contents

- Prologue
- Before Turing
- Hilbert challenges
- *Turing's first paper*
- Matiyasevich solves the 10^{th} Problem
- Epilogue

Turing's first paper

- Soon after Church, Turing (1936-7) gave his own proof.
  - Inventing the more tangible – Turing machines.
- Showed the uncomputability of the Halting problem.
  - Deciding whether a given TM *halts* or not.
- He also realized that Turing machines and λ-calculus are equivalent models of computation.
- After studying the equivalence of several such models, they made the Church-Turing thesis
  "***a function is realistically computable if and only if it is computable by a Turing machine***".

Turing's first paper

- Both the proofs were motivated by Kurt Gödel's work.
  - Gödel (1931) invented a numbering to logical formulas in order to reduce logic to arithmetic, and prove his incompleteness theorem.


Gödel (1906-1978)

- Turing's proof idea for Entscheidungsproblem:
  - Enumerate the TMs as $\{M_1, M_2, M_3, \ldots\}$.
  - Let M_i be the one solving the Halting problem.
  - Consider the TM M: On input x, if M_i rejects $x(x)$ then ACCEPT else $NOT(x(x))$.
  - What is $M(M)$??
  - Thus, Halting problem is uncomputable.
  - Express Halting problem as a first-order statement. ■

Contents

- Prologue
- Before Turing
- Hilbert challenges
- Turing's first paper
- *Matiyasevich solves the 10th Problem*
- Epilogue

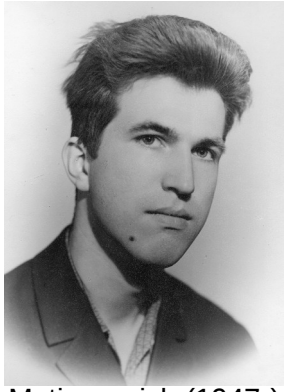
Matiyasevich

- We saw two uncomputable problems. How about a more *natural* (number theoretic) problem?
  - Hilbert's 10th problem: Deciding solvability of an integral polynomial (aka Diophantine solvability).
- Ancient mathematicians have spent much time looking at such “toy” equations.
  - **Univariate:** linear, quadratic, cubic, quartic, quintic,...
  - **n-variate:** $x^2-Dy^2=1$, $x^3+y^3=z^3$, $x^{100}+y^{100}=z^{100}$, $y^2=x^3+Ax+B$,...
- Hilbert asked if one could automate the study of solvability.
  - Answer (after a long time in 1970): NO!
  - Meta-Claim: Rarely can humans discern Diophantine equations.

Matiyasevich

- A large body of work towards Hilbert's 10th problem – Emil Leon Post (1940), Martin Davis (1949-69), Julia Robinson (1950-60), Hilary Putnam (1959-69).

- Yuri Matiyasevich (1970) provided the last crucial step, giving a negative answer to the 10th problem.


Matiyasevich (1947-)

- The Theorem: If R is a computably enumerable (ce) language then there exists $P \in \mathbb{Z}[x,x_1,\ldots,x_n]$ such that: $x \in R$ iff $P(x,x_1,\ldots,x_n)$ has an integral root.
  - A language $R \subseteq \{0,1\}^*$ is ce if there is a TM that accepts *exactly* R.
  - P is called a Diophantine representation of R.

- => Halting problem has a Diophantine representation!

Matiyasevich (Prime formula)

- Before the PROOF, a fun implication:
  ∃ *integral polynomial whose positive values are primes!*
  - Proof: PRIMES is clearly ce.
  - Thus, ∃ Diophantine representation $P(x,x_1,\ldots,x_n)$.
  - Consider $Q(x,x_1,\ldots,x_n) := x(1-P^2)$.
  - $Q>0$ iff $P^2<1$ iff $P=0$ iff $Q=x$ is prime! ■

- There has been much work to discover this prime formula.
  - (Jones, Sato, Wada & Wiens 1976) gave a 26-variate polynomial of degree 25.
  - (Matiyasevich 1977) gave a 10-variate polynomial of degree 10^{45}.
  - (Jones 1982) gave a 58-variate polynomial of degree 4.

Matiyasevich (Prime formula)

DIOPHANTINE REPRESENTATION OF THE SET OF PRIME NUMBERS

JAMES P. JONES, DAIHACHIRO SATO, HIDEO WADA AND DOUGLAS WIENS

1. Introduction. Martin Davis, Yuri Matijasevič, Hilary Putnam and Julia Robinson [4] [8] have proven that every recursively enumerable set is Diophantine, and hence that the set of prime numbers is Diophantine. From this, and work of Putnam [12], it follows that the set of prime numbers is representable by a polynomial formula. In this article such a prime representing polynomial will be exhibited in explicit form. We prove (in Section 2)

THEOREM 1. *The set of prime numbers is identical with the set of positive values taken on by the polynomial*

$$(1)\quad (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)\cdot(h+j)+h-z]^2-[2n+p+q+z-e]^2$$
$$-[16(k+1)^3\cdot(k+2)\cdot(n+1)^2+1-f^2]^2-[e^3\cdot(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2$$
$$-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2$$
$$-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2$$
$$-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}$$

as the variables range over the nonnegative integers.

(1) is a polynomial of degree 25 in 26 variables, $a, b, c, \ldots, z$. When nonnegative integers are substituted for these variables, the positive values of (1) coincide exactly with the set of all prime numbers 2,3,5,.... The polynomial (1) also takes on negative values, e.g., -76.

Matiyasevich (Proof)

- The proof of "***every ce language has a Diophantine rep.***" is fairly tedious.
  - We will discuss only the basic ideas and steps involved.

- Let $R \subseteq \{0,1\}^*$ be a ce language, and M be a TM that **prints** R one string at a time.

- At any point, M is in a configuration C described as $[s(C), p(C), q(C), a_0(C), \ldots, a_{q-1}(C)]$

  [state, head position, #used cells, bits in those cells]

- Overall, whether M will print a string b or not can be expressed as a first-order formula, $F_R(b) :=$ $\exists C_1 \exists C_2 (start(C_1) \,\&\, compute(C_1, C_2) \,\&\, stop(C_2, b))$.

Matiyasevich (Proof)

- $\mathrm{start}(C_1)$ asserts that C_1 is the *start* configuration.
- $\mathrm{compute}(C_1,C_2)$ asserts that in *finitely* many steps M moves from configuration C_1 to configuration C_2.
- $\mathrm{stop}(C_2)$ asserts that C_2 is the *stop* configuration.

- This gives us a first-order formula to express R, almost.
  - In quantification $\exists C$ we need to encode C as a *single* integer.
  - Idea: Chinese Remaindering (CR).
  - Encode $[a_0,\ldots, a_{n-1}]$ as two integers (x,y) such that $n = x \pmod{1+y}$ and $\forall i<n,\ a_i = x \pmod{1+(i+2)y}$.

- There is another, more serious, issue...

Matiyasevich (Proof)

- For CR to work we need $\{1+(i+2)y \mid -1 \le i \le n-1\}$ to be coprime numbers.
- Observe: $y=n!$ works.
  - How do we express $n!$ as a polynomial in n??
- Plan: Diophantine representations of
  1) Exponential y^z => Binomial coefficient ${}^yC_z$,
  2) Binomial coefficient ${}^yC_z$ => Factorial $y!$.
  3) Exponential y^z.
- The last step took the longest time!

Matiyasevich (Steps 1 & 2)

- Step 1: $(1+p)^y = \sum^y_{i=0} {}^yC_i\ p^i = u + ({}^yC_z + vp)p^z$.
  - For a large enough p, one can **extract** ${}^yC_z$ from $(1+p)^y$ by first dividing by p^z and then by p.
- Step 2: ${}^pC_y = p(p-1)...(p-y+1) / y!$.
  - For a large enough p, one can **approximate** $y!$ from $p^y / {}^pC_y$.
- These ideas can be easily worked out.
  - What remains is expressing the exponential y^z.

Matiyasevich (Step 3)

- Step 3: v^n is computed modulo $(v^2-2av+1)$ for large a.
- Observe: $v^n = x_n(a) + y_n(a).(v-a) \pmod{v^2-2av+1}$,
  - where $(a+\sqrt{(a^2-1)})^n = x_n(a) + y_n(a).\sqrt{(a^2-1)}$.
- We want a Diophantine rep. of $x_n(a)$ and $y_n(a)$.
- Observe: $(x_n(a), y_n(a))$ is a root of $X^2 - (a^2-1)Y^2 = 1$.
  - Known as Fermat's equation.
  - Its roots have nice periodic/ recurrence properties.
- Ultimately, this allows a Diophantine rep. of v^n !

Contents

- Prologue
- Before Turing
- Hilbert challenges
- Turing's first paper
- Matiyasevich solves the 10^{th} Problem
- *Epilogue*

Epilogue

- The 10th problem for $\mathbb{Z}$ is uncomputable.
  - (Shapiro & Shlapentokh 1989) showed it uncomputable for any *integer ring* of an alg. number field F, with abelian $\mathrm{Gal}(F/\mathbb{Q})$.
  - (Tarski 1930) showed it **computable** for *real closed fields* (eg. $\mathbb{R}$).
  - OPEN: For $\mathbb{Q}$?

- Thanks to Turing we understand *computability* better now.
  - What about *complexity*?
  - New versions of computation have propped up – *nondeterministic*, *randomized*, *quantum*, *bio/ DNA*,...

- "the evolution of the universe itself is a computation" – *Digital physics / pan-computationalism.*

Thank you!