

Vistula, IT Faculty, 2014

Algorithms and Complexity

Dmitry A. Zaitsev

<http://daze.ho.ua>

Lecture 4:

Undecidable problems

Self-applicability of TM

A TM M is a self-applicable TM if processing its own code $E(M)$ machine M stops after a finite number of steps; otherwise, if M never stops processing $E(M)$, TM M is named non self-applicable.

Theorem. The problem of TM self-applicability is undecidable.

Proof. Suppose the contrary then a TM MSA exists that solves this problem. Given $E(M)$, MSA stops in q_f having on tape “0” when M is self-applicable and “1” when M is not self-applicable.

We construct TM MP on MSA adding a state u and two following instructions $(q_f, 1, 1, S, q_f)$ and $(q_f, 0, 0, S, u)$ considering u a final state of MP.

A question: whether MP is a self-applicable TM?

Suppose MP is self-applicable then MSA halts in q_f with 1, then MP cycles in q_f and never halts; thus MP is non self-applicable.

Suppose MP is non self-applicable then MSA halts in q_f with 0, then MP halts in u ; thus MP is self-applicable.

Conclusion MSA does not exist.

Reduction technique

A mass algorithmic problem (MAP) Z consists of infinite number of individual problems z_1, z_2, \dots and supposes either positive or negative answer (Yes/No or 1/0).

Any problem can be represented in such form adding an assumed solution to the input data, for instance, " $x + y = ?$ " is represented as " x, y, z " which yields "Yes" for " $x+y=z$ " and "No" otherwise.

We say MAP Z is reducible to Z' if there is a passage, implemented with a certain algorithm, from each individual problem z to z' such that the answer for z' is positive if and only if the answer to z is positive. $Z \rightarrow Z'$

If it is proven that Z is undecidable then Z' should be undecidable too.

If we try to prove undecidability of Z' , we find some known undecidable problem Z and try to reduce it to Z' ($Z \rightarrow Z'$).

Undecidability of TM halting problem

TM halting problem – for a given TM M and input word w decide whether M halts processing w .

Theorem. TM halting problem is undecidable.

Proof. Putting $E(M)$ instead of w , we reduce the self-applicability problem to the halting problem.

Thus, supposing MH solving the halting problem exists, we solve MSA putting $E(M)E(M)$ on MH tape.

Enumeration of TM, TM and languages

Let us consider $E(M)$ as binary numbers. A given binary number N either correspond to a valid TM with $E(M)=N$ or not. Starting from $N=1$, trying it, and proceeding with $N=N+1$ we can find and enumerate all TM: M_1, M_2, \dots

TM work can be considered as a recognition of a language L over alphabet X .

For a given word w in X^* it always halts with 1 when w belongs to L or 0 otherwise – decidable (recursive)

For a given word w in X^* it either halts when w belongs to L or never halts otherwise – semidecidable (recursively enumerable)

List of undecidable problems

- Validity of formulas in elementary arithmetic
- Problem of words correspondence of Post
- Problem of matrices representation
- Solvability of algebraic Diophantine equations
- Wang's tiling problem (set of 13 tiles)
- etc

The mortal matrix problem. Determining, given a finite set of $n \times n$ matrices with integer entries, whether they can be multiplied in some order, possibly with repetition, to yield the zero matrix. (This is known undecidable for a set of 7 or more 3×3 matrices, or a set of two 21×21 matrices.)

Post correspondence problem. The input of the problem consists of a finite list of pairs of words (A_i, B_i) over some alphabet Σ having at least two symbols. A solution to this problem is a sequence of indices such that

$$A_{j_1}A_{j_2}\dots A_{j_k}=B_{j_1}B_{j_2}\dots B_{j_k}.$$

Hilbert's tenth problem. Given a Diophantine with rational integral numerical coefficients: whether the equation is solvable in rational integers. A Diophantine equation is an equation of the form

$$P(x_1, x_2, \dots, x_n)=0.$$

where p is a polynomial with integer coefficients

How to do with undecidable problems

- Try to find solutions for particular cases
- Use technique of randomization – solution with a certain probability

Other universal models of computations

- Partially recursive functions of Church
- Normal algorithms of Markov
- Tag rewriting systems
- Counter machines of Minsky
- Cellular automata
- Spiking neurons

etc