Sketch of Lecture 37 Fri, 4/21/2023

P versus NP: A Millennium Prize Problem

The Clay Mathematics Institute has offered 10^6 dollars each for the first correct solution to seven **Millennium Prize Problems**. Six of the seven problems remain open.

https://en.wikipedia.org/wiki/Millennium_Prize_Problems

Comment. Grigori Perelman solved the Poincaré conjecture in 2003 (but refused the prize money in 2010).
https://en.wikipedia.org/wiki/Poincaré_conjecture

Example 220. (P vs NP) P versus NP is one of the Millennium Prize Problems that is of particular importance to cryptography.

"*If the solution to a problem is easy to check for correctness, is the problem easy to solve?*"

https://en.wikipedia.org/wiki/P_versus_NP_problem

Roughly speaking, consider decision problems which have an answer of yes or no. P is the class of such problems, which can be solved efficiently. NP are those problems, for which we can quickly verify that the answer is yes if presented with suitable evidence.

For instance.

- It is unknown whether factoring (in the sense of: does N have a factor $\leqslant M$?) belongs to P or not.

  The problem is definitely in NP because, if presented with a factor $\leqslant M$, we can easily check that.

- Deciding primality is in P (maybe not so shocking since there are very efficient nondeterministic algorithms for checking primality; not so for factoring).

- In the (decisional) travelling salesman problem, given a list of cities, their distances and d, the task is to decide whether a route of length at most d exists, which visits each city exactly once.

  The decisional TSP is clearly in NP (take as evidence the route of length $\leqslant d$). In fact, the problem is known to be NP-complete, meaning that it is in NP and as "hard" as possible (in the sense that if it actually is in P, then $\mathrm{P}=\mathrm{NP}$; that is, we can solve any other problem in NP efficiently).

- Other NP-complete problems include:

  - Sudoku: Does a partially filled grid have a legal solution?

  - Subset sum problem: Given a finite set of integers, is there a non-empty subset that sums to 0?

Comment. "Efficiently" means that the problem can be solved in time polynomial in the input size.

Take for instance computing $2^n \pmod{n}$, where n is the input (it has size $\log_2(n)$). This can be done in polynomial time if we use binary exponentiation (whereas the naive approach takes time exponential in $\log_2(n)$).

Comment. This is one of the few prominent mathematical problems which doesn't have a definite consensus. For instance, in a 2012 poll of 151 researchers, about 85% believed $\mathrm{P}\neq\mathrm{NP}$ while about 10% believed $\mathrm{P}=\mathrm{NP}$.

Comment. NP are problems that can be verified efficiently if the answer is "yes". Similarly, co-NP are problems that can be verified efficiently if the answer is "no". It is an open problem whether $\mathrm{NP}\neq\text{co-NP}$.

- Factoring is in both NP and co-NP (it is in co-NP because primality testing is in P).

- For all NP-complete problems it is unknown whether they are in co-NP. (If one of them is, then we would, unexpectedly, have $\mathrm{NP}=\text{co-NP}$.)