WYATT SPREE

P versus NP

An “Unsolved” problem

Example

Consider Sudoku, a game where the player is given a partially filled-in grid of numbers and attempts to complete the grid following certain rules. Given an incomplete Sudoku grid, of any size, is there at least one legal solution? Any proposed solution is easily verified, and the time to check a solution grows slowly (polynomially) as the grid gets bigger. However, all known algorithms for finding solutions take, for difficult examples, time that grows exponentially as the grid gets bigger. So, Sudoku is in NP (quickly checkable) but does not seem to be in P (quickly solvable). Thousands of other problems seem similar, in that they are fast to check but slow to solve. Researchers have shown that many of the problems in NP have the extra property that a fast solution to any one of them could be used to build a quick solution to any other problem in NP, a property called NP-completeness. Decades of searching have not yielded a fast solution to any of these problems, so most scientists suspect that none of these problems can be solved quickly. This, however, has never been proven.

History

The precise statement of the P versus NP problem was introduced in 1971 by Stephen Cook in his seminal paper "The complexity of theorem proving procedures" (and independently by Leonid Levin in 1973).

Although the P versus NP problem was formally defined in 1971, there were previous inklings of the problems involved, the difficulty of proof, and the potential consequences. In 1955, mathematician John Nash wrote a letter to the NSA, where he speculated that cracking a sufficiently complex code would require time exponential in the length of the key.[5] If proved (and Nash was suitably skeptical) this would imply what is now called P ≠ NP, since a proposed key can easily be verified in polynomial time. Another mention of the underlying problem occurred in a 1956 letter written by Kurt Gödel to John von Neumann. Gödel asked whether theorem-proving (now known to be co-NP-complete) could be solved in quadratic or linear time,[6] and pointed out one of the most important consequences—that if so, then the discovery of mathematical proofs could be automated.

Context

The relation between the complexity classes P and NP is studied in computational complexity theory, the part of the theory of computation dealing with the resources required during computation to solve a given problem. The most common resources are time (how many steps it takes to solve a problem) and space (how much memory it takes to solve a problem).

In such analysis, a model of the computer for which time must be analyzed is required. Typically such models assume that the computer is deterministic (given the computer's present state and any inputs, there is only one possible action that the computer might take) and sequential (it performs actions one after the other).

In this theory, the class P consists of all those decision problems (defined below) that can be solved on a deterministic sequential machine in an amount of time that is polynomial in the size of the input; the class NP consists of all those decision problems whose positive solutions can be verified in polynomial time given the right information, or equivalently, whose solution can be found in polynomial time on a non-deterministic machine.[7] Clearly, $P \subseteq NP$. Arguably, the biggest open question in theoretical computer science concerns the relationship between those two classes:

Is P equal to NP?

Since 2002, William Gasarch has conducted three polls of researchers concerning this and related questions.[8][9][10] Confidence that $P \neq NP$ has been increasing – in 2019, 88% believed $P \neq NP$, as opposed to 83% in 2012 and 61% in 2002. When restricted to experts, the 2019 answers became 99% believe $P \neq NP$.[10] These polls do not imply anything about whether P=NP is true, as stated by Gasarch himself: "This does not bring us any closer to solving P=?NP or to knowing when it will be solved, but it attempts to be an objective report on the subjective opinion of this era."