Fortnow, Lance

The golden ticket. P, NP, and the search for the impossible. (English) Zbl 1267.68003
Princeton, NJ: Princeton University Press (ISBN 978-0-691-15649-1/hbk; 978-1-400-84661-0/ebook). x, 176 p. (2013).

"The golden ticket" is your key to the fascinating world of computational complexity. It provides an in-depth, yet easily understandable treatment of one of the most famous problems of mankind: P vs. NP. The whole book is fun to read and can be fully appreciated without any knowledge in (theoretical) computer science. Fortnow's efforts to make the difficult material accessible to non-experts should be commended. He intersperses the technical parts with many anecdotes, some of which might even be news to researchers in theoretical computer science. The book thus caters to all audiences: from novices with an interest in computational problems to experts with knowledge in theoretical computer science.

Chapter 1 introduces the basic P vs. NP problem and presents the mundane search solution. At the same time, the reader is made aware of the limitations of exhaustive search by showing that even a moderately sized problem might yield a huge search space. Naturally, the chapter also presents the famous Clay Institute list of problems, of which solutions are worth 1 million (per problem) and the relation between P and NP made that list.

Chapter 2 presents the author's vision of a world in which P = NP. The Urbana program, the universal solution engine for NP-complete problems, is shown to solve a variety of hard optimization, scheduling, and analysis problems. The author touches on several interesting areas of life here and shows the developments that would ensue with the help of the Urbana program. While many improvements might be desirable, the authors also cautions that the same power can also be used towards less desirable goals. Overall, the vision shared here is interesting and very captivating.

Chapter 3 is the first main chapter and introduces the problem in more detail. In particular, it presents several problems set in our world and in Frenemy, in which two people hate each other unless they are best friends. The problems discussed here are: shortest distance, match-making, cliques, Eulerian and Hamiltonian cycles, and map coloring. The Frenemy Institute is then tasked with solving those problems and some of the problems indeed have efficient solutions. The author nicely shows that the fastest known algorithms for similar problems can behave vastly different. For example, switching from min-cut, which can be solved efficiently, to max-cut, for which no efficient algorithms are known, illustrates this point. The chapter is concluded with some examples how the P vs. NP problem permeated other disciplines such as biology, physics, economics, and last but not least mathematics.

Chapter 4 introduces the notions of reduction and NP-hardness in a way that is understandable to everyone with basic education in mathematical logic. It recounts the history of this fundamental notion with a strong focus on the reductions between clique and SAT and the history of the name NP-complete, which is used for NP-hard problems that are in NP. In addition, it gives a multitude of sometimes well-known and ubiquitous problems that are NP-complete. This is complemented by a selection of NP problems that are seemingly difficult (not known to be in P), but not known to be NP-hard (like factorization). It is nice to see that even this "middle-ground" is mentioned.

Chapter 5 goes back one step further. It recalls the efforts that eventually lead to the famous P vs. NP problem. Since there was a strong divide between the east (Russia) and the west (USA) in those days, it recounts the history of this fascinating problem in those two parts of the world. Especially the less well-known developments in Russia offer an excellent insight into the famous Russian mathematical research. Most mathematicians and computer scientists might be absolutely unaware of the efforts of the Russian scientists Sergey Yablonsky, Andrey Kolmogorov, and Leonid Levin, although they all made important contributions to complexity theory.

Chapter 6 shows how we currently deal with NP-complete problems. While computing advances have allowed us to solve small and sometimes even medium sized problems by brute-force search, the search space of large problems quickly grows beyond all reasonable limits. It might have similarly been unimaginable for researchers living in the 70s that medium sized problems can be solved, but the exponential progress in computing (speeds) allowed more and more complex problems. However, the speed game stopped a

while ago. The number of transistors still rises exponentially, but new paradigms (like parallelism) took over the lead. The author thus introduces techniques that guide the search (heuristics) or approximate the result. Finally, it reminds the reader that maybe he actually wants to solve another problem altogether.

Chapter 7 demonstrates tried approaches to proving the relation between P and NP. It shows how one can, in principle, prove properties about all imaginable algorithms. In addition, it warns the reader about the common pitfalls and recalls the interesting JACM submission policy for P vs. NP papers.

Chapter 8 deals with cryptography, which uses the fact that NP-hard problems are currently difficult to solve. The chapter first recalls the highlights of the history of secret codes and then recounts ubiquitous public-key cryptography. The currently used cryptographic systems would be easy to break if P = NP, so the author discusses the remaining provably secure system (one-time pad) and how this could be implemented in a P = NP world. Finally, zero-knowledge protocols, which can be used to convince people that one knows a secret without giving it away, are introduced on the Sudoku example.

Chapter 9 gives a short overview of quantum technology, which is the basis for quantum computing. It shows how this computational model affects the P vs. NP question and illustrate that the difficulty switches from the actual computation, which is now relatively easy due to inherent parallelism, to reading off (observing or recognizing) the final result. This observation problem is explained together with the important notion of entanglement, which currently is hard to maintain perfectly, which only adds to the complexity.

Chapter 10 is the last chapter and provides an outlook into the reasonable future. This world is very different from the world described in Chapter 2. It showcases the upcoming challenges like "Big Data" and the new technologies that still need to be fully utilized.

Reviewer: Andreas Maletti (Stuttgart)

MSC:

68-01	Introductory exposition (textbooks, tutorial papers, etc.) pertaining to computer science
68-03	History of computer science
68Q25	Analysis of algorithms and problem complexity
68W40	Analysis of algorithms
68Q15	Complexity classes (hierarchies, relations among complexity classes, etc.)

Keywords:

computational complexity; cryptography; NP-completeness; problem analysis; complexity theory

Full Text: DOI