The Golden Ticket
P, NP, and the Search for the Impossible*

Lance Fortnow

Georgia Institute of Technology

fortnow@cc.gatech.edu

As a reader of this bulletin you already understand the importance of theoretical computer science and why we care so much about the P versus NP problem. While the P v NP problem gets mentioned in the United States occasionally in television shows, video games, even the Unofficial Guide to Disney World [6] (for the traveling salesman problem of getting around the park), the general public knows little about this important problem. It's a rare popular science book that discusses P v NP, theoretical computer science or computer science at all.

In 2008, Moshe Vardi asked me to write a survey on the P versus NP problem for the Communications of the ACM. Instead of a typically technical survey, I focused on the ideas of P v NP and the challenges and opportunities that it affords us. That survey [2] would engender over a quarter million downloads. The broader computer science community wanted to understand the P versus NP problem, not as a technical relationship between deterministic and nondeterministic Turing machines, but as a concept that guides how we solve challenging algorithmic problems.

Given the popularity of the survey, I decided I could convert that survey into a book with each section of the survey expanded into a chapter for the book. Instead of aiming for a computer science savvy audience, like I did for the survey, I decided to write for the scientifically-interested general public. More specifically I aimed the book at a high school student who wanted to know more about computer science than just programming. When I went to high school I got inspired by books like Carl Sagan's *Cosmos* [5] or Douglas Hofstadter's *Gödel, Escher, Bach* [3]. I wanted to do the same, to inspire young adults to think about computer science through the lens of the P v NP problem.

Four years later I completed the book, *The Golden Ticket: P, NP and the Search for the Impossible*. The name refers to Roald Dahl's *Charlie and the Chocolate Factory* [1] where golden tickets hidden in candy bars gave admission

*Princeton University Press, 2013, 192pp, ISBN 978-0691156491, goldenticket.fortnow.com.

to a rare tour of the fabled Willy Wonka Chocolate Factory. The search for that golden ticket makes a great analogy to the P versus NP problem in many ways.

The Golden Ticket has done reasonably well for a popular science book with good reviews and some awards including being named one of Amazon's top 20 science books for 2013. The book has been translated into Chinese, Japanese, Finnish and Russian and a paperback edition will be released in spring 2017.

This book is not meant for the readers of the bulletin but perhaps your friends or family members that you would like to share the importance of what theoretical computer science is or better yet, a teenager who might be inspired by the excitement of our field.

To give a flavor of this book what follows is a summary of each chapter.

Chapter 1: The Golden Ticket

This introductory chapter sketches out the P versus NP problem through a series of examples, from the traditional traveling salesman to controlling a robotic hand.

Chapter 2: The Beautiful World

My science fiction chapter that looks at a world where P = NP, not just in the formal sense but supposing we had a truly efficient and practical algorithm for NP-complete problems. Instead of focusing on the negative (crypto is dead), I look instead to the positive (we cure cancer!).

Chapter 3: P and NP

We give examples of P and NP problems through several examples. Never in the book do I define P and NP in the formal sense–rather I go for intuitive notions of these concepts. I develop a world called Frenemy, where every pair of people are either friends and enemies and use that world to describe a series of graph problems, without actually talking about graphs.

Chapter 4: The Hardest Problems in NP

Focusing on NP-complete problems again in an intuitive way giving many examples (Rubik's Cube is easy, Sudoku is hard), as well as a short history of P, NP and NP-completeness and the naming of those classes based on Donald Knuth's wonderful and hilarious SIGACT News article [4].

Chapter 5: The Prehistory of P versus NP

What led up to the P v NP problem? I describe the history in the western world from Turing to Karp. I also talk about the development of the study of Perebor in Russia and how the cold war and mathematical politics made complexity research in the Soviet Union trickier and more dangerous.

Chapter 6: Dealing with Hardness

NP-completeness is not the death knoll for a computational problem, just an indication that we won't find an efficient algorithm that gives an exact solution all of the time. I discuss many approaches in dealing with hard problems including brute force, heuristics, small parameters and approximation. Sometimes you need to find a different problem or just accept that you cannot solve what you want to solve.

Chapter 7: Proving P $\neq$ NP

How have people tried to settle the P v NP problem and why haven't those techniques worked? This chapter discusses diagonalization and circuits, as well as reviewing the Deolalikar story and common mistakes made in the all too many P v NP "proofs" that get sent my way.

Chapter 8: Secrets

Cryptography from Ceasar to RSA, zero-knowledge via Sudoku, secure computation and pseudorandomness. Does P = NP kill cryptography? Not, but it will make it more challenging.

Chapter 9: Quantum

A very high level view of quantum physics, quantum computing, quantum cryptography and teleportation.

Chapter 10: The Future

What are the future challenges of computing (already dated), from parallelism, big data and the Internet of things. Final line of the book: As long as P versus NP remains a mystery we do not know what we cannot do, and that's liberating.

Conclusion

I truly aimed to tell the story of P and NP in an understandable and intuitive manner. How well I succeeded is not my call to make. I aimed for the book to help people understand this great question and get them interested in P v NP and theoretical ideas in computer science.

References

[1] R. Dahl. *Charlie and the Chocolate Factory*. Alfred A. Knopf, New York, 1964.

[2] L. Fortnow. The status of the P versus NP problem. *Communications of the ACM*, 52(9):78–86, September 2009. Review Article.

[3] D. Hofstadter. *Gödel, Esher, Bach: An Eternal Golden Braid*. Basic Books, New York, 1979.

[4] D. Knuth. A terminological proposal. *SIGACT News*, 6(1):12–18, 1974.

[5] C. Sagan. *Cosmos*. Random House, New York, 1980.

[6] B. Sehlinger and L. Testa. *The Unofficial Guide to Disney World 2010*. Wiley, New York, 2010.