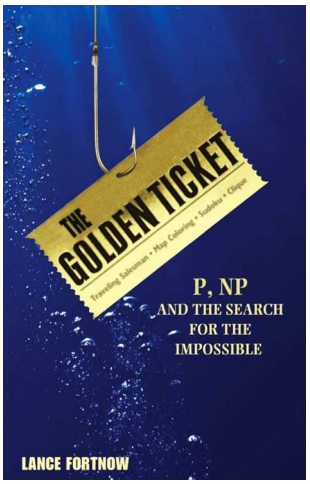
The Golden Ticket: P, NP, and the Search for the Impossible

Lance Fortnow
Princeton University Press, 2013, ISBN 978-0-691-15649-1

In the 1930s, Kurt Gödel and Alan Turing proved two unsolvability results that changed the face of mathematics forever. Gödel's theorem was syntactic: he showed that in any consistent formal theory strong enough to contain elementary number theory, there are propositions that can be neither proved nor disproved. Turing's theorem was semantic: he proved that in any reasonable model of computation there is no algorithmic procedure to solve Hilbert's *Entscheidungsproblem*, that is, to decide whether a statement of a first-order logic is valid in every structure satisfying the axioms.



Gödel's result led to unexpected developments in pure mathematics, for example independence results in set theory, algebra, topology, analysis and combinatorics.

Turing's result had similarly far-reaching consequences in applied mathematics, because it turned out to have economic and military implications.

The 40 years beginning in 1945 were those of the Cold War. Applied mathematicians in the sphere of the Soviet Union and those in the West worked independently of each other in the area of Operations Research, but not surprisingly came up with similar ideas. What evolved on both sides of the Iron Curtain in the 1970s was the notion of algorithmic complexity. Consider for example the problem of finding a clique of maximal size in a finite simple graph. The problem can be expressed as the disjunction of finitely many conjunctions of propositions stating that there is an edge between two vertices, so it is an instance of the Entscheidungsproblem involving a single binary relation. Since the graphs at issue are finite, any such instance can be solved by exhaustive enumeration. But what is at stake here is the 'cost' of the calculation, i.e. the number of elementary operations needed to solve an instance of given size. Even to determine by enumeration whether a graph with 100 vertices has a clique of size 50 is beyond the reach of computers today and in the foreseeable future. Other problems of a similar nature occur in graph theory, as well as in network design including the traveling salesman problem, partitioning sets into subsets with given properties, data storage and retrieval, biology including matching genome strings, number theory including factoring integers, economics including investment decisions and medicine including compatible kidney exchanges with multiple donors.

What ensued was a classification of finite combinatorial problems into a spectrum of types. The set of problems of a given type is parametrised by 'size', which we may take to be a positive integer n, representing the amount of data needed to describe a particular instance. At the hard end of the spectrum are the *perebor* problems, an adjective the Russians used to denote problems requiring brute force search. The solution of such a problem of size n has a cost which is of the order of C^n, where C is a positive integer independent of n.

At the easy end of the spectrum are the problem types for which the solution cost of a problem of size n is of the order of n^C. The latter problems are said to be in the class P, which stands for polynomial complexity. Floating between these two extremes are problems whose cost as a function of size n lies between polynomial and exponential in n. I say floating, because the solution cost depends on the choice of algorithm and even the software and hardware of the device used to compute the solution. A prominent example is linear programming: while it is known that there are instances of Dantzig's Simplex Algorithm not in P, Khachiyan showed in 1979 by the ellipsoidal method that the linear programming problem itself is in P. For another example, it was not until 2002 that Agrawal, Kayal and Saxena found an algorithm which demonstrated that the problem of deciding primeness of an integer is in P.

The most important type within this spectrum is denoted NP, which stands for *non-deterministic polynomial*. These are problems, first described by Steve Cook in 1971, for which if a solution of an instance is proposed, the problem of deciding whether it is indeed a solution is in the class P. Thus $P \subseteq NP$ and the P versus NP problem is to determine whether this inclusion is proper. This is the fourth of the Clay Institute Millennium Problems, the only one of real interest to non-mathematicians. The point is that while it is (comparatively) easy to determine whether a class of problems is in P by finding an algorithm, it is difficult to prove that an NP problem is not in P.

In 1971 Cook and in 1972 Richard Karp in the USA, and at about the same date, Leonid Levin in the USSR found a special subclass of NP problems now known as *NP-complete*. These have the crucial property that any problem in NP can be reduced to an NP-complete problem. Thus if any NP-complete problem can be shown to be in the class P, then all NP problems are in P. The first NP-complete problem discovered both by Cook and Levin was the 3-satisfiability problem. This is a special case of the Entscheidungproblem which asks for an algorithm to decide whether it is possible to assign truth values to n propositions P_i so that a given conjunction of statements, each of which is a disjunction of three of the P_i or their negations $\neg P_i$, at least one of which is P_i, is true.

Other examples of NP-complete problems which are easier to describe (but not to solve) include deciding whether a graph has a Hamiltonian circuit, the clique problem of deciding whether a graph contains a clique of size k, the vertex cover problem of deciding whether a graph has a vertex cover of size k and the partition problem of deciding whether a finite set of positive integers can be partitioned into two subsets with equal sums.

It was only in the late 1980s that it came to light that Gödel in a 1956 letter to von Neumann discussed the satisfiability problem and formulated the P *v* NP problem in different terminology, suggesting that equality was within the realm of possibility.

I come now to the book under review. The author, Lance Fortnow, is a distinguished computer scientist at the Georgia Institute of Technology, and a specialist in computational complexity. His book is aimed at a lay audience with some experience in computation and networks. It is intended to outline the nature, history and importance of the P *v* NP problem. It contains no mathematical theory, but much discussion of algorithmic complexity and the intrinsic limits of computation. The 'Golden Ticket' of the title has two meanings; firstly it refers to a problem based on a Roald Dahl story, in which a wealthy man indulges his daughter whose wish is to win a competition of a chocolate bar manufacturer who has inserted a golden ticket into exactly one package. The millionaire buys the entire production and employs a team of workers to open every packet until they find the golden ticket. Of course this is not a decision problem and is solved in at most $n-1$ steps of a simple algorithm.

The second reference for the Golden Ticket is as a metaphor for the possible equality of P and NP. Fortnow outlines a possible scenario in which a mathematician wins a Fields Medal for a method to solve NP problems efficiently, whereupon various teams of computer scientists continually improve her algorithm until eventually a PhD student cracks the barrier by finding an algorithm in P. After several legal battles over copyright, the World Trade Organisation determines that the result is so important to human welfare that it belongs in the public domain. Fortnow continues with his fantasy by outlining how the algorithm is used to find a cure for cancer, a method to schedule major league baseball, and so on. All of this is almost believable, but I draw the line at the next step envisaged: Fortnow guesses that the Clay Foundation is forced to withdraw the remaining Millenium Problems, because they would all fall to the $P = NP$ result! Finally, however, Fortnow admits that most computer scientists suspect that $P \neq NP$, and that the resolution of the problem is far in the future.

While avoiding proofs and details of algorithms, Fortnow makes interesting observations on dealing with hard problems in operations research and cryptography by approximate methods and parallel and quantum computing. To summarise, this book is a lively popularisation of the P *v* NP problem for non-specialists, which could also be a suitable introduction to a serious study of the subject, such as the definitive 1979 text *Computers and Intractability* by M.R. Garey and D.S. Johnson, and to more recent research.

Phill Schultz
School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009, Australia. Email: phill.schultz@uwa.edu.au

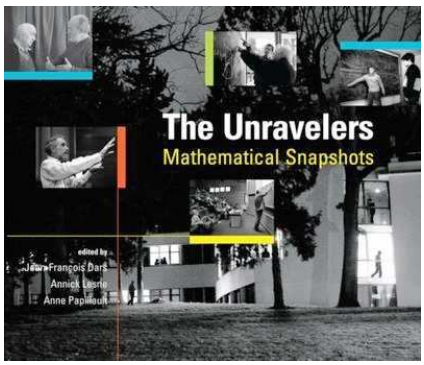
◇ ◇ ◇ ◇ ◇ ◇

The Unravelers: Mathematical Snapshots

J.-F. Dars, A. Lesne and A. Papillaut (Eds), V. Méla (Trans)
A.K. Peters, 2008, ISBN-13: 978-1-56881-441-4

The Institut des Hautes Études Scientifiques, modelled on the Princeton Institute of Advanced Studies, was founded in 1958 by businessman and mathematical physicist Léon Motchane. Situated in bucolic environs in the village of Bures-sur-Yvette, 15 km south-east of Paris, the IHES allows mathematicians and theoretical physicists to immerse themselves in research without administrative and teaching duties. In recent years, theoretical biologists have been added to the list. The early years of the Institute were fashioned by the strong personalities of Alexandre Grothendieck, René Thom and Dennis Sullivan. More recently, it has hosted a roll-call of winners of Fields and Einstein medals, and Abel, Crafoord and Wolf Prizes.

While nonresidential, it provides a nurturing atmosphere accommodating the habits and working hours of everyone, from owls to fowls. The lecture halls and seminar rooms are old-fashioned enough to provide immense triptych blackboards as well as electronic projectors and the cafeteria is apparently all you would expect from a French Institute.



In 2006, the IHES invited a team of documentary filmmakers, one of them a mathematician, to visit the Institute and over the course of a year, to photograph the members and visitors. The photographs are exceptional, providing a penetrating view of scholars at work in their offices, walking in the woods, interacting at the blackboards or performing solo or ensemble music. Each batch of photos is accompanied by a text written by its subjects. There was no restriction, apart from length, on these contributions. They include reminiscences, tributes to previous Institute members, reflections on the nature and practice of mathematics, and even poems. Most are enlightening, some are banal, but none is pretentious. While the Prologue by the editors and many of the contributions were written in French, the English translations, by Vivienne Méla, are skillful; for example the choice of title in my opinion is better than the English cognate of the French title, *Les Déchiffreurs*.

The mathematical contributors to this book encompass a host of distinguished scholars, including Michael Atiyah, Jean-Pierre Bourgignon, Pierre Cartier, Yvonne Choquet-Bruhat, Alain Connes, Pierre Deligne, David Eisenbud, Mikhail Gromov, Victor Kac, Maxim Kontsevich, Bao Châo Ngô, Dennis Sullivan, Jacques Tits, and Minoru Wakimoto. In addition, there are scores of lesser-known scholars

including post-docs and other mathematicians on the threshhold of their careers. In particular, two Australians are included, the theoretical physicist Dirk Kreimer and the mathematical biologist Henry Tuckwell. The kitchen and domestic staff, so responsible for the smooth running of the Institute, are not neglected in the photographs.

Among the texts, I was particularly struck by Connes' description of his very personal relationship with mathematics; by Paolo Almeida's remarks, entitled 'Structured Fury', on the initial conflict but eventual synthesis of intuition and rigour in mathematical activity; and by the account by Cecile DeWitt, a member of the Administrative Council of IHES, of the founding of the Institute. A memorable account by Cartier concerns his dramatic visit to Poland with Laurent Schwartz, Marcel Berger and Alain Guichardet on the eve of Jaruzelski's 1981 putsch.

This book is a fitting celebration of the first 50 years of the IHES, and a captivating answer to the question: what is it that mathematicians do?

Phill Schultz
School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009, Australia. Email: phill.schultz@uwa.edu.au

◇ ◇ ◇ ◇ ◇ ◇