The Structural Complexity Column

Juris Hartmanis

TR 89-994
April 1989

Department of Computer Science
Cornell University
Ithaca, NY 14853-7501

*This research was supported by the National Science Foundation research grant DCR 85-20597.

J. Hartmanis*

Department of Computer Science

Cornell University

Ithaca, New York 14853

Gödel, von Neumann and the P=?NP Problem

Abstract

In a 1956 letter, Gödel asked von Neumann about the computational complexity of an NP complete problem. In this column, we review the historic setting of this period, discuss Gödel's amazing letter and why von Neumann did not solve the P=?NP problem.

Historic Setting

It is interesting to recall that the motivation for the development of the theory of computation, on which theoretical computer science is based, came from purely mathematical considerations. The paradoxis emerging from Cantor's set theory emphasized the need to clarify the foundations of mathematics and, under Hilbert's leadership, concentrated attention on axiomatic proof systems. The quest to understand the power and limitations of axiomatizable systems led directly to the questions about all possible formal (mechanical) ways of deriving proofs (sequences with desired properties). In modern terms, it led to the search for *what is and is not effectively computable.*

This search intensified after 1931, when Gödel sent shock waves through the mathematical community with his independence result, showing that number theory can not be

*This research was supported by NSF Research Grant DCR 85-20597

completely and consistently axiomatized [Go, Da]. This result destroyed Hilbert's grandiose (and in retrospect, startingly naive) program to axiomatize ever larger parts of mathematics and prove these axiomatizations to be complete and consistent.

Gödel's work also scooped Emil Post, who had convinced himself in the 1920's that the Whitehead and Russell system presented in Principia Mathematica must contain unprovable propositions. Unfortunately for Post, he considered this result "fundamentally weak in its reliance on the logic of Principia Mathematica". Post realized that his result required "for full generality a complete analysis ... of all possible ways in which the human mind could set up finite processes for generating sequences" [Da]. Gödel was not bothered by such considerations and published his famous paper explicitly mentioning Principia Mathematica in its title: "Uber formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme" [Go].

In retrospect, we know that Post was trying to accomplish single handedly, in one blow, what was accomplished by Gödel, Church, Kleene and Turing from 1930 to 1936. He wanted to determine what is and is not effectively computable and then, with this general definition in hand, prove the incompleteness of all axiomatizations of sufficiently rich mathematical systems. After Gödel's incompleteness paper appeared, Post sadly concluded that his "plan, however, included prior calisthenics at other mathematical and logical work, and did not count on the appearance of a Gödel". He had hoped that the "incompleteness of the logic of Principia Mathematica would be a corollary of the more general result" [Da].

This search for a proper formulation of effective computability succeeded with a surprising emergence, almost simultaneously, of several equivalent formulations by Church, Kleene, Turing and Post in 1935-36. Turing's formulation finally convinced even the skeptical Gödel that a "minor miracle" had occurred; such an ill defined concept as effective computability could have a beautifully simple and precise formulation in terms of Turing machine computability.

Though the original motivation for the development of the theory of computation was purely mathematical, it is impressive how quickly and effectively some of the leaders of these developments participated in the practical development of electronic computers during and after World War II. The enigmatic Turing, after two years in Princeton where he worked with Church and met von Neumann, returned to England in 1939 and effectively participated in the highly successful effort of cracking German military codes and the construction of electronic devices for this purpose. After the war, Turing designed the ACE computer at the National Physics Laboratory in Teddington and then moved on to the University of Manchester to make further contributions to the development of computers and programming.

Von Neumann's intellectual and physical path to Princeton, computers, and computer science is quite different. While Post, in the 1920's was struggling to show formally that under all possible proof techniques there must be unprovable mathematical statements in any sufficiently rich, effectively axiomatized system, von Neumann was actively working with Hilbert on the grandiose project to prove the opposite. The super quick and technically superb von Neumann shared Hilbert's belief that mathematics could be consistently and completely axiomatized and, in this direction, he made profound contributions to the axiomatization of set theory and quantum mechanics. These achievements brought him to Princeton University in 1930 as a visiting professor which led to a professorship in 1931. He moved to the Institute for Advanced Study (IAS) in 1933 as the youngest member of its permanent faculty. Gödel achieved the equivalent rank at the IAS only in 1946, after several extended visits followed by six consecutive years at the institute.

Von Neumann met Turing in Princeton and eventually offered him to be his research assistant. Turing turned down this offer to return to war-threatened England in 1939. We have to assume that von Neumann had understood well Turing's work and that these ideas strongly influenced von Neumann's later work on computers. In 1944, von Neumann learned, from (then) Lieutenant Goldstine, about the ongoing work on the ENIAC project at the University of Pennsylvania and soon was actively involved in this project as a consultant.

From this collaboration emerged in 1946 the highly influential (and incomplete) report "Preliminary discussion of the logical design of an electronic computing instrument" with A.W. Burks and H.H. Goldstine. There is strong circumstantial evidence that the idea the internally stored program concept, proposed in this report and often attributed to von Neumann, was derived from Turing's universal machines. Von Neumann has never clarified the origin of these concepts.

After the ENIAC work, von Neumann participated in the design of the EDVAC and designed an built the JOHNNIAC at the IAS. Von Neumann made also extensive contributions to numerical computations, automata theory, and the study of self-reproducing systems.

Though Gödel's work gave an immense impetus to the search for the formulation of effective computability, it seemed that he had little interest and involvement in the development of computer science or practical computing. He took little interest in the development of the JOHNNIAC at the IAS, though he knew von Neumann well and respected him highly. (Von Neumann considered Gödel the greatest logician since Aristotle.)

In view of a recently rediscovered letter, we may have to reassess Gödel's interest in computational problems. A 1956 letter from Gödel to von Neumann reveals that Gödel was thinking about computational complexity of Turing machine computations. In this letter Gödel asks von Neumann about the computational complexity of an NP complete problem about proof systems and wonders if it could be solved in linear or possibly quadratic time ($c \cdot n^2$). He also asks von Neumann about the computational complexity of primality testing.

These are very likely the first questions ever asked about the time required to solve problems on a deterministic Turing machine and particularly about the computational complexity of an NP complete problem. Clearly, the problem is not referred to, in the modern terms, as NP complete; nor is there any discussion of reductions between combinatorial problems or the completeness of problems.

It is interesting to note Gödel's optimism (or naivity) that the NP cor problem could be solved in linear or quadratic time. He, who destroyed Hilbert's and umann's shared dream to consistently and completely axiomatize mathematics, seems not to have expected that this problem is not solvable in polynomial time (as most of us believe) and therefore it is not feasibly solvable. As a matter of fact, Gödel expresses the hope that many combinatorial problems can be solved much faster than by simply trying all possibilities (in his words "dem blossen Probieren").

We should recall that this optimism was not shared at this time, by the cyberneticists in the USSR. The Russians had convinced themselves that there are combinatorial problems whose solution require brute force or exhaustive search! They referred to this as *perebor* and worked hard to show that there were problems from which perebor could not be eliminated [Tr].

We do not know von Neumann's response to Gödel's question about the computational complexity of this NP complete problem. So far no letter responding to Gödel's query has been found. On the other hand, we know that at this time, von Neumann was already suffering from advanced cancer and that he passed away less than a year later on February 8, 1957 at the age of 53.

It is a pity that von Neumann was not challenged by Gödel to think about computational complexity when he was in good health. The development of theoretical computer science could have been substantially accelerated an the computer science intellectual landscape could be quite different today. A healthy, super-bright Johnny could have possibly solved the notorious $P = ?NP$ problem before it became notorious or made it even more notorious than it is today, as the problem, raised by Gödel, which defied von Neumann.

Gödel's Letter

In many regards, this is a fascinating letter in content and style. The letter is in German and hand written. Evan after decades in this country, Gödel, von Neumann and Einstein preferred German to English for their personal communication. Though Gödel and von Neumann had known each other a long time and had been colleagues at the IAS for more than a decade, the letter starts very formally with "Lieber Herr v. Neumann!" and is signed Kurt Gödel.

In the first part of the letter, Gödel expresses sadness about von Neumann's illness and hope that the modern medical treatment will fully restore his health. He then turns to mathematical problems. In short, he asks how many Turing machine steps are required to decide if there is a proof of length n for a formula F in predicate calculus ("Formel F des engeren Funktionenkalküls"). Loosely translated, the key sentences are:

> "Since, as I hear, you now are feeling stronger, I would like to allow myself, to write about a mathematical problem, about which I would like to know your opinion: Clearly we can construct a Turing machine, which for each formula F of the predicate calculus (engeren Funktionenkalküls) and every natural number n allows to decide if F has a proof of length n. [Length = number of symbols]. Let $\Psi(F,n)$ denote the number of steps required by the machine, let $\varphi(n) = \max_F \Psi(F,n)$. The question is, how fast grows $\varphi(n)$ for an optimal machine. One can show that $\varphi(n) \geq K \cdot n$. If in fact a machine with $\varphi(n) \sim K \cdot n$ (or even with $\sim K \cdot n^2$) existed, it would have very important consequences. It would apparently mean that in spite of the unsolvability of the Entscheidengsproblem, the reasoning of mathematicians about yes-or-no questions can be completely replaced by machines. One should just choose n so large that, if the machine does not yield a result, there is no reason to think about it. It seems quite possible to me that $\varphi(n)$ grows slowly".

He then observes that there are combinatorial problems for which the N steps of the simply trying ("dem blossen Probieren") can be reduced to $\log N$ or $(log\ N)^2$.

He continues:

> "It would be interesting to know, for example, what the situation is with the determination if a number is a prime, and *in general* how much we can reduce the number of steps from the method of simply trying for finite combinatorial problems".

Towards the end of the four page letter, Gödel discusses some recent developments in mathematics and asks if von Neumann has heard that Richard Friedberg has solved Post's problem. This was one of the outstanding open problems in recursive function theory and was solved independently by Friedberg and Muchnick of the Soviet Union.

Gödel concludes:

> "The solution is very elegant. Regrettably Friedberg will not study mathematics, but medicine instead (apparently under his father's influence)".

Clearly, Gödel's letter raises some key issues in complexity theory and we know that $P = NP$ if and only if his $\varphi(n)$ is polynomially bound. What a pity that von Neumann was in no condition to take up Gödel's challenge. What an interesting interchange of ideas this could have been between these two men. In this case, von Neumann could have evened the score with Gödel by proving that $\varphi(n)$ is not polynomially bounded and that therefore Gödel's problem is not feasibly computable.

From Gödel's work, we know that mathematics is too rich to be consistently and completely axiomatized. From Turing's and Church's work, we know that for sufficiently rich formal systems it is undecidable which statements are and are not provable. In this letter Gödel raised the next question about the fundamental nature of mathematics: how hard is it (computationally) to decide if a statement has a proof of length n in a formal system?

Though this question was raised by Gödel in a private letter in 1956, he does not seem to have publicized this as a great challenge nor was it so perceived until 1970. Only after Cook's work and extensive study of NP completeness do we now fully realize the importance of this problem to mathematics and computer science. We are also aware, after almost twenty years of struggle with $P = ?NP$, that it is a very difficult problem and that we very much need scientists of the Gödel and von Neumann calibre to seriously threaten this problem.

Acknowledgement

Gödel's letter was brought to my attention by Dr. Gerhard Heise.

References

[Da] Davis, M., ed. "The Undecidable". Raven Press, Hewlett, New York, 1965.

[Go] Gödel, K. "Uber formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme", In *Monatsheft für Mathematik und Physik*, 38(1931), 173-198.

[Tr] Trakhtenbrot, B.A. "A Survey of Russian Approach to Perebor (Brute-Force Search) Algorithms", *Annals of the History of Computing*, 6(October 1984), 384-400.

Recommended Historical-Biographical Reading

S. Feferman, ed., "Kurt Gödel: Collected Works, Volume I Publications 1929-1936", Oxford University Press, New York, NY, 1986.

H.H. Goldstine, "The Computer From Pascal to von Neumann", Princeton University Press, Princeton, NJ, 1972.

S.J. Heims, "John von Neumann and Norbert Wiener: From Mathematics to the Technology of Life and Death", The MIT Press, Cambridge, MA, 1980.

A. Hodges, "Alan Turing: The Enigma", Simon and Schuster, New York, NY, 1983.

G. Kreisel, "Kurt Gödel" Biographical Memoirs of the Fellows of the Royal Society, 26:149-223, 1980.

J.C. Oxtoby, B.J. Pettis, and G.B. Price, eds., "John von Neumann 1903-1957", Bulletin of the American Mathematical Society, Vol. 64, No. 3, Part 2, May 1958.

E. Regis, "Who Got Einstein's Office?", Addison-Wesley, Reading, MA, 1987. Contains a chapter about Gödel and a chapter about von Neumann.

Constance Reid, "Hilbert", Springer-Verlag, Heidelberg, Germany, 1970.