SIGACT News Complexity Theory Column 36

Lane A. Hemaspaandra
Dept. of Computer Science, University of Rochester
Rochester, NY 14627, USA lane@cs.rochester.edu

Introduction to Complexity Theory Column 36

This current issue's guest column is by Bill Gasarch, and reports on a poll he has conducted on the most famous open question in complexity theory: P=?NP. If Mitsunori Ogihara's prediction that P-vs-NP will not be resolved until the year 3000 is correct, my guess is more than a few students of the history of computer theory will be visiting, long after all the contributors are gone, Bill's column, which will provide a time capsule into the thoughts of many in the field. Who knows? Perhaps there will even be Ph.D. theses devoted to figuring out who these people all are, and just who the (as the students will know from their history of science books) then-Turing/Fields/Nobel-laureate Bill Gasarch was making an exception of when he wrote below, "Almost all respondents are people whose opinions can be taken seriously," and great debates may rage over whether he actually meant, by "almost all," "all but a (large) constant number." In light of the fascinating opinions, though, I suspect that but little evidence will be found for that view—even by Ken Regan's Vegans. Surely some M.S. thesis will be written claiming that it was this column—and in particular the superfluous disjunct in Donald Knuth's claim that $x \leq 2048 \vee x \leq 4096$—that led, in the year $2^{10} + 2^{11}$, to Donald Knuth's Turing Award being posthumously rescinded and given to Bill Gasarch. However, the Knuth Cult will discover that Donald Knuth's words here are a numerical key that unlocks the secret of the Art of Computer Programming, which, it turns out, when decoded has nothing to do with computers but rather is a skillful telling of the life story of a Danish saint.

Warmest thanks to Bill and the dozens of contributors for their time, analyses, and prognostications.

Plugs for past and future issues: In 1996 and 1997, SIGACT News Complexity Theory Columns 14 and 15 collected various expert's opinions on the future of computational complexity. If you have not read those opinions already, they are worth a look. And coming in the next few issues we'll have Marcus Schaeffer and Chris Umans on completeness for higher polynomial hierarchy levels, Arfst Nickelsen and Till Tantau on partial information classes, and Ramamohan Paturi on the complexity of k-SAT.

Guest Column: The P=?NP Poll

William I. Gasarch[1]

Abstract

The P=?NP problem has been open since the early 1970's. When will it be solved? How will it be resolved? What techniques will be used? While it is impossible to answer these questions with any certainty, one can say for certain what one *thinks* may happen. We have taken a poll of theorists to see what they think. This is a report on that poll.

[1] © William I. Gasarch, 2002. Department of Computer Sciences, University of Maryland, College Park, MD 20742. E-mail: gasarch@cs.umd.edu.

1 Introduction

The P=?NP problem has been open since the early 1970's. Many people-hours have been spend thinking about it and many (perhaps irrelevant) things are known. Are we making progress? This is hard to say for sure. When will it be solved? Also hard to say. Lacking the mathematical tools to answer these questions rigorously we turn to rather non-rigorous means—polling. Almost all respondents are people whose opinions can be taken seriously.

Over the last 6 months I have asked various theorists these questions. I have cast a fairly wide net—posting to various theory newsgroups, emailing theorists whose email address I happen to have, and of course the ever-enlightening staff of SIGACT NEWS. A total of 100 people answered the poll.

This is a report on the poll. 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.

2 The Statistics and What They Mean

2.1 When Do You Think P=?NP Will Be Resolved?

79 of the respondents answered this one directly. I have broken down the data into 10-year intervals except at the beginning and the very end.

1. P=NP will be resolved between 2002-2009: 5
2. P=NP will be resolved between 2010-2019: 12
3. P=NP will be resolved between 2020-2029: 13
4. P=NP will be resolved between 2030-2039: 10
5. P=NP will be resolved between 2040-2049: 5
6. P=NP will be resolved between 2050-2059: 12
7. P=NP will be resolved between 2060-2069: 4
8. P=NP will be resolved between 2070-2079: 0
9. P=NP will be resolved between 2080-2089: 1
10. P=NP will be resolved between 2090-2099: 0
11. P=NP will be resolved between 2100-2110: 7
12. P=NP will be resolved between 2100-2199: 0
13. P=NP will be resolved between 2200-3000: 5
14. P=NP will never be resolved : 5.

The question was posed in its current form in the early 1970s by Cook and Levin (though it was mentioned in a letter between von Neumann and Gödel in the 1950s). Hence if it is solved before, say, 2070 we may think of that as "soon." With this definition we have the statistic that 57 people think it will be resolved soon and only 22 people think we are in for the long haul. On the other hand 21 people did not respond.

2.2 How Will it Be Resolved?

1. 61 thought P≠NP.
2. 9 thought P=NP.
3. 4 thought that it is independent. While no particular axiom system was mentioned, I assume they think it is independent of ZFC.
4. 3 just stated that it is NOT independent of Primitive Recursive Arithmetic.
5. 1 said it would depend on the model.
6. 22 offered no opinion.

These statistics indicate (not surprisingly) that *of those who answered* most thought P≠NP. Most of the 9 who thought that P=NP were respectable members of the community. All of them recognized that their opinion is a minority viewpoint. A few even said they took it just to be contrary. However, the fact that 22 people did not venture an opinion indicates more uncertainty on this then one would have thought.

2.3 What Techniques Will be Used?

52 people answered this one.

1. **Combinatorics and Complexity:** 11 people thought that combinatorics or complexity theory (or a combination of the two) is the key. Of those who thought so, 2 mentioned the PCP machinery, 1 mentioned Resolution theorem proving lower bounds, and 1 mentioned circuit lower bounds.
2. **Logic:** 9 people stated that logic is the key. Of those, 3 mentioned E-F games and finite model theory, 1 mentioned thought Paris–Harrington type Independence results, and 1 mentioned an arithmetic form of Berry's Paradox.
3. **Math:** 10 people stated that math (of the type not usually studied by theorists) is the key. 3 of these mention algebraic techniques, 1 mentions continuous techniques, and one mentions higher cohomology (in fact, he stated that the use of higher cohomology is inevitable).
4. **Misc:** 1 person each said computer assisted (like the proof of the four color theorem), contradiction, induction, information-theoretic argument, general-purpose lower bounds first, and not-probability. Two people (who stated P=NP) say it will be done by an algorithm for an NPC problem (this is not obvious—if P=NP then it is possible it will be done by some nonconstructive technique).
5. **New:** 16 people said it will take new techniques. Of course, the people who said "logic" or "funky math" may also have new techniques in mind.

It is notable that 36 people stated that the technique is known to us now, but not the way to apply it. This is higher than I would have thought, but is consistent with the notion that it will be resolved before 2070 (i.e., soon).

3 Some Notable Comments

This section contains some of the comments offered on the P=?NP problem. Next to everyone's name I put a brief summary of their views before their quote. Everyone is in a Computer Science department unless otherwise noted.

1. **Jamie Andrews:** (University of Waterloo, 2015, P=NP) There will be an $O(n^{\log^*(n)})$ algorithm for an NP-complete problem, rendering the whole P vs. NP question essentially irrelevant. :-)

2. **Eric Bach:** (University of Wisconsin, 2100, P≠NP) I can't say it better than Robin Hartshorne (Algebraic Geometry, p. 55) did:

   In any branch of mathematics, there are usually guiding problems, which are so difficult that one never expects to solve them completely, yet which provide stimulus for a great amount of work, and which serve as yardsticks for measuring progress the field.

   Clearly P vs NP is our guiding problem.

   We should be careful to distinguish between faster ways of doing essentially the same thing (Moore's law being the great example) and fundamental progress in our understanding of computation (knowing WHY we can or cannot do certain things). The first is easy, the second hard. It's perfectly all right for a field to have questions that will take more than a few years to solve. In fact, I would argue that the recent popularization of computing (with the attendant explosion of the computer business) has not necessarily been good for computer *science*. There is the temptation to expect quick easy answers to all technical problems.

3. **David Barrington:** (University of Mass., 2030, P≠NP) Razborov-Rudich suggests we need to get better at breaking pseudo-random generators before we get close to lower bounds putting natural problems outside of P

4. **Bela Bollobas:** University of Memphis, Math Dept, 2020, P=NP) I think that in this respect I am on the loony fringe of the mathematical community: I think (not too strongly!) that P=NP and this will be proved within twenty years. Some years ago, Charles Read (of the invariant subspace (rather, lack of it) fame) and I worked on it quite bit, and we even had a celebratory dinner in a good restaurant before we found an absolutely fatal mistake. I would not be astonished if very clever geometric and combinatorial techniques gave the result, without discovering revolutionary new tools. A bit like Tim Gowers's solutions to major sixty-year old questions of Banach. P vs NP may not be that much harder than the invariant subspace problem for Hilbert spaces (but that, of course, may be terribly hard). Sadly, we haven't returned the P vs NP question since that unfortunate experience fifteen years ago. The danger of wasting a year for no return is rather off-putting.

5. **Stas Busygin:** (2010, P=NP, continuous techniques) An embryonic form of such a technique is already described in the paper "A New Trust Region Technique for Maximum Weight Clique Problem." (available at http://www.busygin.dp.ua/npc.html and http://www.optimization-online.org/DB$_{\text{HTML}}$/2002/01/430.html) As well, there are impressive numerical experiment results on max clique instances seemingly hard for any combinatorial approach.

6. **Jin-yi Cai:** (University of Wisconsin, 2100, P≠NP, algebraic) No true substantial progress toward P vs NP is visible in the last 30 years since NP-completeness was formulated. I am

pessimistic on its quick resolution any time soon. This is not necessarily a bad thing. Look at the Riemann Hypothesis.

7. **Richard Chang:** (Univ of MD Balt County, 2066, P$\neq$NP) In the year, 2066 the idea that computers will double in speed every 18 months (Moore's Law) has been ludicrous for 50 years. As such, no one uses asymptotic analysis anymore. Programs are written in assembly language to shave the running time. Some poor assistant professor will prove that P != NP and fail to get tenure for it.

8. **Hubie Chen:** (Cornell University) Proof at http://www.cs.cornell.edu/hubes/pnp.htm

9. **John Conway:** (Princeton University, Math, 2030, P$\neq$NP, Conversion to some arithmetized form of the Berry paradox) In my opinion this shouldn't really be a hard problem; it's just that we came late to this theory, and haven't yet developed any techniques for proving computations to be hard. Eventually, it will just be a footnote in the books.

10. **Francisco Antonio Doria:** (University of Sao Paulo, Sao Paulo, Brazil, Math, 2005, Ind) There will be two steps. First, one will show surprisingly that P=NP is consistent with ZFC (if ZFC is consistent).

    Then one will show that P$\neq$NP is also consistent with ZFC, and so both are independent. It will also turn out to be true of the standard model for arithmetics. Finally, one will show that ZFC + some large cardinal hypothesis proves P¡NP. The idea will be similar to the proof of the Paris-Harrington theorem. But a surprising Busy Beaver like function will suddenly appear.

    This class of problems will turn out to be precisely in the limit, so to say, between time-poly problems and time-exp problems.

11. **Ron Fagin:** (IBM Almaden Research Center) I feel that theoretical computer scientists should devote a constant fraction of their lives to trying to resolve the P vs. NP question. I personally spend a few days each year thinking about it. I've proven (at least twice) that NP does not equal co-NP (and hence P does not equal NP). I've also proven (also at least twice) that NP equals co-NP. My most recent proof that NP does not equal co-NP occurred about a week ago as I write this, and the proof survived for about half an hour (not quite long enough for me to run it by someone else). My longest-surviving proof that NP does not equal co-NP (about 5 years ago) survived for about 3 days and fooled some very smart people into believing it. Each of my proofs that NP does not equal co-NP was via logic (descriptive complexity). I feel that descriptive complexity has as good a chance of resolving the P vs. NP problem as any other approach. In fact, it can be shown that, in a precise sense, if NP does not equal co-NP then there is a proof of this using descriptive complexity tools.

12. **Stephan Fenner:** (University of South Carolina, Never, P$\neq$NP) Even though I think it will never be resolved, I do not think it is independent of ZFC or anything like that. Simple questions may be decidable but have very long proofs (e.g., Fermat's Last Theorem). FLT is the exception rather than the rule; many simple decidable statements in number theory will never be proved because their proofs are just too long for anyone to find.

    (a) I'd bet 5,000 current dollars that PvsNP is not solved within 5 years
    (b) I'd bet 1,000 current dollars that PvsNP is not solved within 10 years

(c) I'd bet 500 current dollars that PvsNP is not solved within 20 years

(d) I'd bet 200 current dollars that PvsNP is not solved within 40 years

13. **Lance Fortnow:** (NEC, 2050, P$\neq$NP) At this moment, I believe we have no techniques that get us even close to a solution. Thus any attempt to guess when or how the problem will be solved is meaningless. The solution may come in 5 years or 500 years; it is just impossible to tell.

14. **Harvey Friedman:** (Ohio State, Math, 2050, P$\neq$NP) Detailed combinatorial work on easier problems, leading up to the full result. P=PSPACE will be refuted first.

15. **William Gasarch:** (Univ of MD, 2100, P$\neq$NP) NP-completeness is important since (as we tell our students) if a problem is NP-complete you look for other ways to attack it rather than seek an exact solution in poly time. Similarly, independent results (from restricted systems) are important in that they tell us that we should look for other ways to solve the problem.

    We seem to have made no real progress on P vs NP; however we have made progress on proving what techniques do not work (Oracle results, Natural Proofs). I predict we will have some (weak) independence results in the next 20 years. This will be followed by 20 years of proving statements that nobody cares about independent of systems nobody cares about, results that will be obtained because they can be. Then researchers will return to the original problem and these independent results will help guide them to the solution. We're in for the long haul.

16. **Yuri Gurevich:** (Microsoft, 2060, P=NP) The positive solution will not make the standard NP problems worst-case feasible in the practical sense of the word. Cumbersome reductions to the very particular problem discussed above will exert a heavy price.

17. **Jeff Hirst:** (Appalachian State University, Math, 2100, P$\neq$NP) Assuming that P is actually not equal to NP, it seems that some sort of mathematical logic approach will have to be used. The computability theoretic analogs that have been tried seem to rely on P corresponding to the computable sets and NP corresponding to a jump. I think that progress will depend on adopting a different analog, using something like measure theory on Π^0_1 classes or perhaps Medvedev degrees.

    I remember telling Sam Buss in the mid-80s that I thought the problem would be solved by 1990 for sure.

18. **Neil Immerman:** (University of Massachusetts, 2017, P$\neq$NP, Finite Model Theory) No one knows, but I remain I hopeful that Ehrenfeucht-Fraïssé games will help, and that the main lemma will show something like that there is no first-order projection from 3 colorability to the circuit value problem.

    Yes, while I hope that the proof is clean and comprehensible once it is found, I suspect that computer generated constructions and lemmas will be very useful along the way.

19. **David Isles:** (Tufts University, Math) My guess is that the problem will be resolved not thru the development of new techniques but as a consequence of quite radical revisions in our way of conceiving of certain mathematical ideas. Such revisions will include an abandoning of the belief in a set of natural numbers unique up to isomorphism plus a recognition that there must be a more careful use of induction in reasoning about "natural numbers." One

consequence of this would be the recognition that exponential is, in general, not everywhere defined and can, depending on the context, be given different values.

20. **David Juedes:** (Ohio University, 2030, P≠NP) I am not completely sure what techniques will be used since most of the ones that I've seen do not seem to be leading to a resolution to this question. My intuition tells me that we need to be looking at techniques that examine both time and space simultaneously. When we solve the PSPACE vs EXP and the LOGSPACE vs P questions, then I believe that the P vs NP question will be resolved quickly thereafter using similar techniques. Furthermore, I think we need to build techniques to prove general purpose lower bounds, before we can get to the P vs NP question. For example, I do not believe that anyone has shown that Vertex Cover requires $O(n^3)$ steps on a Turing machine. If we can't do that, how can we expect to prove that P is not equal to NP?

21. **Sariel Har-Peled:** (University of Illinois at Urbana, 2525, P≠NP) There are good reasons to believe the question is NOT relevant. In particular, assume that tomorrow I came up with a $A(10) * n$ time algorithm for solving SAT, where $A(10)$ is Ackermann 10, and let us assume that this is tight. It is completely useless, as this implies that the problem can not be solved for any reasonable size instance, even assuming that we use Pentium 3000, although P=NP. We similarly have infinite number of examples of NPC problems that can be solved in practice (approximation algorithms, heuristics, you name it), so... Why is this question so important?

22. **Juris Hartmanis:** (Cornell University, 2012,P≠NP) I expect that the P vs NP will be solved during the next ten years and not much earlier. I hope that many other SEPARATION PROBLEMS, such as LOGSPACE, NLOGSPACE, P, PH; P, NP, PH, PSPACE; PSPACE, EXPTIME, NEXPTIME, will be solve once the first major SEPARATION result is obtained. I do not consider the possible separation of LOGSPACE from NLOGSPACE in the same class as the other SEPARATION PROBLEMS.

    My guess is that P will be shown to be different of NP. When I look at all the SEPARATION PROBLEMS below EXPSPACE, I believe that the first results may separate the bigger gaps, say, LOGSPACE from NP or PH, or P from PSPACE. Once one of these problems is solved, I expect that the rest will follow quickly, except that the separation or collapse of LOGSPACE and NLOGSPACE, may not cause or inspire directly any further collapses.

    I do not believe that the resolution of the SEPARATION PROBLEMS will be achieved by finding some existing deep mathematical results which can be applied directly to solve these problems, or any one of them. I expect that new techniques will have to be developed for the resolution of these problems. I also would not be very surprised if eventually we find a short proof that P is not NP.

23. **John Kadvany:** (Policy and Decision Science, Menlo Park, 2010) The solution may involve an implicit informal foundational issue associated with the statement of the P vs NP problem. Speculative ideas include: alternative characterizations of the difference between polynomial and exponential computation similar to the intensional content of Godel's second incompleteness theorem; a close analysis of the relationship between addition and multiplication and the development of complexity at the lowest computational levels; a role for infinitary set theory via the association between computational complexity and countable ordinals; analogies between the infinitary power-set operation (and its problems) and exponentiation; a characterization of complexity involving an analysis of relative numerical clocks, analogous to that in

Einstein's special theory of relativity; a reformulation of the Turing machine concept in which tape geometry is varied, e.g. as compact sets supporting self-similar geometric computations; or computability assumptions for real numbers.

24. **Richard Karp:** (Berkeley, unsure, P≠NP) My intuitive belief is that P is unequal to NP, but the only supporting arguments I can offer are the failure of all efforts to place specific NP-complete problems in P by constructing polynomial-time algorithms.

    I believe that the traditional proof techniques will not suffice. Something entirely novel will be required.

    My hunch is that the problem will be solved by a young researcher who is not encumbered by too much conventional wisdom about how to attack the problem.

25. **Andy Klapper:** (University of Kentucky) I don't think these questions can be given anything like a reasonable response. It is apparent that it is a very hard question. To my knowledge there is no program in place which, if carried out (e.g., "if we could prove steps (a), (b), and (c) then it would be settled, and here are the techniques that must be developed to prove them") would settle the question. There have been several techniques developed that held some promise—circuit methods, measure theory, ...—in the sense that they seemed relevant, but to my knowledge none ever presented a program of attack such as the attack by Wiles on Fermat's theorem or the present attacks on the Riemann hypothesis or the classification of finite simple groups. So I think that we really haven't the slightest clue what it will take or how long it will take. But who knows, maybe there is a 17 year old Lithuanian mathematician who will emerge from his parents basement in 5 years with the answer using techniques we never expected.

    Also, I'd like to suggest calling it the "P and NP problem." P vs NP is too adversarial :-)

26. **Donald Knuth:** (Retired from Stanford) It will be solved by either 2048 or 4096. I am currently somewhat pessimistic. The outcome will be the truly worst case scenario: namely that someone will prove "P=NP because there are only finitely many obstructions to the opposite hypothesis"; hence there will exists a polynomial time solution to SAT but we will never know its complexity!

27. **Vladik Kreinovich:** (University of Texas at El Paso) My personal opinion is that it is more probable that P is different from NP. However, it is also highly possible that P will be proven to be equal to NP—but without the ability of solving all problems from NP easily.

    To be more precise, by definition, P=NP means that we will be able to solve NP-complete problems in time bounded by a polynomial $P(n)$ of the input's length, but it would still not enable us to solve NP-hard problems feasibly in practical sense of this word, because the coefficients of the corresponding polynomial $P(n)$ will likely be on un-physical (like 10^{40} or more).

    No objections to quoting me by name. Actually, Levin expressed similar opinion some time ago, you may want to cite him instead.

28. **Clyde Kruskal:** (University of Maryland, 2036, P≠NP) If P=NP then I think NP-complete problems will have very high degree polynomial times. Otherwise, it does not seem reasonable that we do not yet have a polynomial time solution.

    In an ideal world it would be renamed P vs VP (or maybe P vs PV).

29. **Stuart Kurtz:** (University of Chicago, 2050, P≠NP) Knowing Ketan Mulmuley, I live in fear that the solution will be via algebraic geometry, and it will come soon enough that I'll be expected to understand it. An alternative nightmare is that the undergraduate who solves it will publish his solution in French.

30. **Ming Li:** (Waterloo, P≠NP) For God's sake, let's keep it open for another 100 years! NSF needs to be convinced that theoretical CS is still relevant and supports it.

31. **Laszlo Lovasz:** (Microsoft, 2017,P≠NP) Probably some new math modeling the information flow through a boolean circuit. With luck, something like algebraic topology or algebraic geometry will be used.

32. **Dana Nau:** (Univ of MD) I have this wonderful proof that P≠NP, but it is to large to write in the margin of this email message!

33. **Anil Nerode:** (Cornell, Math) What techniques? Pure combinatorics if P=NP, Calculus estimates as in Hilbert's solution of Waring's problem if P≠NP.

    Being attached to a speculation is not a good guide to research planning. One should always try both directions of every problem. Prejudice has caused famous mathematicians to fail to solve famous problems whose solution was opposite to their expectations, even though they had developed all the methods required.

34. **Mitsu Ogihara:** (University of Rochester, 3000, P=NP) Connections to some algebraic hypotheses will be made and those hypotheses will be positively resolved. I think we are allowed to be very creative to answer this question. Here's a story I conjured up, which describes the progress towards the resolution (not brushed up).

    The path towards the positive resolution of the P vs. NP problem was created when unpublished notes of FOO, one of the 20th century's math geniuses, were discovered in the late XX00's. The notes were very sketchy. They were written in an attempt to formulate a new theory on some algebraic structure. Apparently, FOO gave up on that early on and never returned to the subject. The notes were trapped in the cracks on the floor of FOO's bedroom. The notes were found by builders working on a renovation project of the house in which FOO lived.

    The notes themselves did not create much immediate sensation because they were so sketchy. However, decades later, a group of mathematicians found that if a variation of one of the hypotheses FOO made on the notes holds then a number of interesting statements can be said. Although the hypothesis is not in the form that FOO intended, it was called FOO's Conjecture, to give an honor to this genius.

    Almost a hundred years later, a group of computer scientists found that if FOO Conjecture holds, then a certain algebraic problem, called QQQ, which is not known to be NP-complete, is NP-complete. Also, a few years later, groups computer scientists found that if one of the then-famous mathematical conjecture, the BAR Conjecture, holds then Q is polynomial time solvable. Combination of these two pieces of work established the goal for resolving the infamous problem, i.e., if FOO and BAR both hold, then P = NP.

    In the next two centuries, both conjectures were intensely studied. Many partial resolutions were given to them and the remaining special cases were transformed into new forms. Those modifications narrowed down to both conjectures to very small, specialized statements. Finally, two groups reported that the specialized statements are valid. The first report, which resolved the specialized BAR conjecture, was made three weeks before FOO's birthday and the other report, which resolved the FOO conjecture, came out just three months later.

35. **Jim Owings:** (Univ of MD, Math, maybe never, P≠NP) I had thought that it would be solved by the year 2000. But that was in 1975. I am now guessing that it will not be solved in the next fifty years, and maybe never. I think the answer is that P not= NP. Perhaps there is some very clever algorithm that puts some NP complete problem in P, but why hasn't it been found yet? How clever can it be? There is something very strange about this problem, something very philosophical. It is the greatest unsolved problem in mathematics, better than the Riemann hypothesis. It is the raison d'etre of abstract computer science, and as long as it remains unsolved, its mystery will ennoble the field.

    Another possibility- someone comes up with an algorithm for SAT that is in P but cannot be proven to be in P.

36. **Karl Papadantonakis:** (Caltech, 2025) Characterization of what happens to a logic system when you assume P=NP, and what happens when you assume P≠NP. I don't think that inconsistency has to result in either case; rather there is some property that we can't quite put a finger on yet...

    Complexity theory, model theory, and programming language models. These techniques probably need to be refined and even unified somehow. People in different areas of research will need to join forces.

    Clearly these are just quick opinions. Nobody really knows.

37. **Ian Parberry:** (University of North Texas, 2050, P≠NP, Weird Math)

    It will be solved by a mathematician, not one of us. Probably somebody in a discrete area of math that nobody in our community has ever heard of and may not even exist as a field of study yet.

38. **Chris Pollett:** (San Jose State University, 2020, P≠NP, Complexity Theory)

    (a) P=BPP will be shown first.

    (b) The inability to prove P=NP will be demonstrated in stronger and stronger systems of arithmetic before then.

    (c) Within a year of P≠NP the polynomial hierarchy will be proven infinite.

39. **Ranu Raatikainen:** (University of Helsinki, 2030, P≠NP)

    (a) It may be solved in the next 10-20 years, but this depends on many issues: modes can change, and the problem may become less trendy etc.—if practically nobody works with the problem and related issues, it may take ages; or, if people approach it only with "wrong" tools.

    (b) I believe it will be solved indirectly by solving the spectrum problem, which is in my mind a very natural problem in logic.

    (c) I believe that actually the P≠NP problem in itself is not very important, and that P is not as good substitute for the intuitive notion of feasibly computable as many seem to think.

40. **Charles Rackoff:** (University of Toronto, 2004, PCP etc. stuff) Uniformly, P is not equal to NP; Nonuniformly, P=NP. I actually believe that (uniform) exponential time is contained in nonuniform polynomial size. It is not hard to prove that this implies (uniformly) NP is unequal to P. My goal, therefore, is to show how to get small circuits for exponential time.

41. **Alexander Razborov:** (Institute for Advanced Study) Well, this problem is (at the moment) very unique since we seem to be missing even the most basic understanding of the nature of its difficulty. Neither we currently have any ideas of what approach might turn out to be viable and lead us to the solution (or at least to a better understanding of the problem). All approaches tried so far probably (in some cases, provably) have failed. In this sense P=NP is different from many other major mathematical problems on which a gradual progress was being constantly done (sometimes for centuries) whereupon they yielded, either completely or partially. Perhaps, although, the key word in this difference is "century", and the P=NP problem has simply not aged enough yet (by mathematical standards).

42. **Ken Regan:** (University of Buffalo, P≠NP) Assuming the Vegans hold to the treaty of 1979 and don't tell us the answer, humanity will solve it between 2030 and 2040. The trail seems to have gone "cold" since 1993, but will pick up publicly later this decade. Thirty-plus years now represents the same integral of brain-hours as over the 300-plus years it took to get Fermat. P≠NP: SAT cannot be done in time $2^{o(n/\text{polylog} n)}$.

    Higher cohomology seems inevitable, and damn hard... it will need something besides linear algebraic groups and the level of stuff I've tried as a supporting cast, too. Somewhere inside the reams and folds of the math is a dynamic rather than static information theory trying to get out.

43. **Mike Robson:** (Universite Bordeaux in France, 2020, P≠NP) Maybe the question will be obsolete when we all have quantum computers.

44. **Rocky Ross:** (Montana State University) I don't think I'm close enough to the recent research to give an opinion that would be worth anything. However, I can give you a cautionary anecdote. In about 1976 when I was a graduate student in Germany I bumped into a new professor who had been a particularly bright student of my major professor in Germany. He had been given a full professorship at another university pretty much right after receiving his Doctorate. He told me straight out that he was going to solve the P=NP problem. He exuded confidence in his abilities and fairly gloated over the fact that he had a leg up on his American counterparts, because, as a German professor, he could pretty much dictate his schedule. That is, he could go into his room, lock his door, and focus on The Problem.

    Many years later I asked about this person, and I got answers indicating that no one really knew anything about him. He was still a professor as far as anyone could tell, but he had turned into a recluse and virtual hermit, which seemed to baffle everyone. Maybe he just hadn't expressed his aspirations to anyone else. I haven't asked about him in years, so I'm not sure what has evolved since.

45. **Pannagadatta Shivaswamy:** (Cisco Systems) The person will be richer by one Million Dollars—courtesy Clay math institute, and the world will be richer by one more proof (see www.claymath.org/prizeproblems/).

46. **Peter Shor:** (Bell Labs, P≠NP, hard math)

(a) Possibly the right question for practice is whether NP is contained in BPP or BQP (my response to both of these questions is "no."

(b) I would love to see a survey of how many people think P = BPP.

(c) My answer to (b) is that I think P = BPP but P ≠ BQP.

47. **Michael Sipser:** As you may know, when I was a graduate student in the mid 1970s I predicted that it would be solved by the century's end. I also bet Len Adleman an ounce of gold that I would be right. Now that I've paid off, I'm more reluctant to make a prediction once again. But I'll go out on a limb and give it another 25 years, so by around 2025. And I'll stick with my earlier prediction that the resolution will be a proof that P ≠ NP. The technique would be combinatorial, but that isn't saying much. No more bets, however.

48. **Steve Skiena:** (SUNY at Stonybrook, 2025, P≠NP, Complexity theory) I fear a result akin to the proving of Fermat's Last Theorem, where I one morning I read the great news that the problem has been solved, and I never get much insight into how beyond mumbled references to elliptic curves in the popular media.

49. **Carl Smith:** (University of Maryland, 2025, model-dependent, novel diagonalization) Before the Berlin wall fell I had thought it would be solved by a young eastern block mathematician who didn't have to worry about tenure and could hence spend his best years thinking about P≠NP for hours, days, weeks, months, years, decades, until he either solved it or became an old Eastern block mathematician. Now that the Berlin wall has fallen, the number of young mathematicians who can afford to not worry about tenure and just think deep thoughts has fallen so it may be longer then it would have been to solve it. In any case, the solution will not be as enlightening as the problem has been.

50. **Bob Tarjan:** (Princeton) In my view, there is no way to even make intelligent guesses about the answer to any of these questions. If I had to bet now, I would bet that P is not equal to NP. I estimate the half-life of this problem at 25 - 50 more years, but I wouldn't bet on it being solved before 2100. Its solution will require unforeseen new techniques.

51. **Luca Trevisan:** (Berkeley, 2100, P≠NP, hard math) I fear that the solution will come by someone recognizing a completely unexpected connection to some really weird mathematics, and then by working out the weird mathematics. Those of us that understand only combinatorics will have no clue.

52. **Jeff Ullman:** (Stanford, 2100, P≠NP) I think the problem is comparable to some of the great problems of mathematics that lasted hundreds of years, e.g., the 4-color theorem. Thus, I'd guess 100 years. I'd bet we don't have the techniques, or even names for the techniques today. Again, that would be analogous to the situation for many of the great open problems of mathematics 30 years after they were posed.

53. **Moshe Vardi:** (Rice) A few years ago Ron Fagin collected "bets" on the outcome of the PvNP question. I believe that I am one of the very few people who placed nontrivial odds in FAVOR of the P=NP question. When asked to justify my bet, I answered that it is essentially a "protest vote." I do not really have any deep intuition in favor of P=NP. I do not, however, believe that the evidence in favor of P≠NP is as strong as it is widely believed to be. The main argument in favor of P≠NP is the total lack of fundamental progress in the area of exhaustive search. This is, in my opinion, a very weak argument. The space of algorithms is

very large and we are only at the beginning of its exploration. Witness the non-constructive tractability proofs in the area of graph minors and tractability proofs in the area of group theory that are based on the very deep classification of finite simple groups. The resolution of Fermat's Last Theorem also shows that very simply questions may be settled only by very deep theories. Over the two decades we have seen several major lines of attack on the PvNP question. I myself was involved on one of them, that of finite-model theory. All these lines of attack yielded beautiful theories, but there is little reason to believe that they led us any closer to resolving the problem.

In summary, I think it is impossible to give intelligent answers to questions such as when P=?NP will be solved, what the resolution will be, and what techniques will be used to resolve the question.

54. **Paul Vitanyi:** (University of Amsterdam, 2050, P=NP) I think R = P = NP.

55. **Avi Wigderson:** (Institute of Advanced Study) I think this project is a bit premature. I think we know too little of what is relevant to even guess answers to your questions, certainly if "we" is replaced by "I."

    The only thing I can definitely say, is that it is one of the most important and interesting questions ever asked by humans, and more people and resources should participate in filling up the holes that would allow better guesses of answers to your questions.

56. **Andy Yao:** (Princeton) It's hard to say when the question will be resolved. I don't have even an educated guess. Probably the resolution is that P is not equal to NP. I think the mathematical techniques used will be beautiful.

57. **Doron Zeilberger:** (Rutgers, Math, 2020, P≠NP, Computer-assisted and/or generated formal enumeration using ideas in the spirit of Razborov (as improved by Alon–Boppana) but instead of the counting sieve, using much more sophisticated, yet-to-be discovered computer-generated sieves, that only computers can analyze. At the end there be long computer checking like in 4CT and Kepler.

    It is only fair that computers will chip-in in solving the major problem of Computer Sci.

58. **Marius Zimand:** (Towson State) If P=NP then it will be proven within 10 years. If P≠NP then it will not be proven for at least 100 years.

59. **Anonymous1:** Only a few people will follow the proof. Whoever does will spend the rest of his life convincing people it is correct.

60. **Anonymous2:** The current level of research is inadequate; there is only a handful of researchers making a serious effort (that I am aware of). Most of structural complexity research seems to have lost sight of the big picture.

61. **Anonymous3:** (Names, schools, dates changed to protect the innocent) On Dec 14, 1991 it was shown that P=NP by undergraduate Mary Lou Koslowsky on her Algorithms final exam at The University of Southern North Dakota. Her ingenious but somewhat hastily written proof, establishing that 3-SAT could be reduced to 2SAT in $O(n^3)$ time, received only 2 points of credit out of a possible 25 and the comment "Wrong." She left computer science and became a pharmacist, working now at Osco Drugs in Lake Wobogon, where all problems have above average complexity.

62. **Anonymous4:** Even though P≠NP people should still work on trying to prove P=NP to see what goes wrong.

    I think the P=BPP question is almost as interesting. I am appalled that people take for granted that P=BPP.

4 Comments on the Comments

The comments were fairly diverse so trends are hard to spot.

1. 13 people stated that the solution would be hard—which is orthogonal to saying it will take a long time to find it.
2. 5 people thought the solution, once we have it, will be easy to follow.
3. 5 people stated that we are overestimating our confidence in P≠NP.
4. 4 people stated the problem will end up being irrelevant either because of large constants or large degree.
5. 3 people stated that issues involving randomization would be more interesting (one suggests that I do a poll on how many people think P=BPP).
6. 2 fear that a nonconstructive proof that P=NP will happen and is a worse case scenario.
7. 2 people stated the problem will end up being irrelevant because of quantum computing.
8. 2 sighted reasons of sociology of research as to why the problem remains unsolved—the tenure system in America being a problem, and the globalization leading to uniformity of thought.