**Open Problems Column**
**Edited by William Gasarch**

Request for Columns!

I invite any reader who has knowledge of some area to contact me and arrange to write a column about open problems in that area. That area can be (1) broad or narrow or anywhere in between, and (2) really important or really unimportant or anywhere in between.

**This Issue's Column!**

This issue's Open Problem Column is:

**My Answers to My P vs NP Poll**
**By William Gasarch**

# 1 Introduction

There have been two polls asking theorists (and others) what they thought of P vs NP and related questions [**?**, **?**]. Both were written by me (William Gasarch) and appeared in the Complexity Column of SIGACT News, edited by Lane A. Hemaspaandra.

I have conducted a third poll. The results of that poll will appear in Lane's column in this issue (Volume 50, Number 1, March 2019). In the article I did not give my own answers [though I commented on other people's answers in square brackets]. By contrast, this column contains *my* answers about the status of P vs. NP. For information on what *is* the status of P vs NP see Scott Aaronson's article [**?**], Lance Fortnow's article [**?**], or (for the layperson) Lance Fortnow's book [**?**].

# 2 Questions and Answers

1. Do you think P = NP? No.

   I think P $\neq$ NP. I was once 200% sure, but now I am only 100% sure. The Graph Minor Theorem makes me ponder if some really hard math may all of a sudden have SAT $\in$ P pop out. One argument for SAT $\notin$ P is that people have been trying to prove that SAT is in P for 50 years and have not succeeded. But is 50 years (of 20th and 21st century mathematics) a long time or is it just a drop in the mathematical bucket? I do not know.

   There are people who think P = NP. I consider this a respectable viewpoint though I disagree with it. Knuth has a notion that P = NP, but the NP-complete problems will be somehow still harder. That might be true but hard to formalize.

   Lance Fortnow thinks that people who believe P = NP are like people who believe Elvis is alive. I think he is partially kidding; however, I think that he is wrong. We need to keep an open mind. It has been said: *If you think a conjecture is true spend half your time trying to prove it's true and half trying to prove it's false.*[1] I'll add to the quote by saying you need to really BELIEVE it is false when trying to prove it's false. (It's been said that when Bill Clinton talked to you he didn't just make you feel like the most important person in the world, he actually BELIEVED you were the most important person in the world. That may explain his success in politics and other endeavors.)

[1] One of my proofreaders, Clyde Kruskal, points out that this is equivalent to *if you think a conjecture is False spend half your time trying to prove it's true and half your time trying to prove it's false.* Touché!

2. When do you think the question will be resolved? In the year 2525.

   I will first address *who* might solve it.

   Hilbert's 10th problem was to find (in today's terminology) an algorithm that will, given $p \in \mathbb{Z}[x_1, \ldots, x_n]$, determine if $p$ has a Diophantine solution. Hilbert likely never considered that there would be no such algorithm. Hence it took *outsiders* to think *outside the box* and lay the groundwork for the solution. In those days Martin Davis (a logician), Hilary Putnam (a philosopher), and Julia Robinson (a logician and a woman) were outsiders for the (unfair) reasons given in parentheses. So — do we need an outsider for P vs NP?

   - YES — the current system rewards the-next-STOC/FOCS-paper more than long term thinking. So we need some outsider who is not in that mentality.
   - YES — the insiders are all stuck in a group think that focuses on the wrong issues (e.g., proving our techniques won't work instead of working on new techniques that will).
   - NO — the math needed to work on H10 was not that hard. The math needed to work on P vs NP seems like it will be quite hard. See next point.
   - NO — the genius-in-his-basement-solves-open-math-problem is mostly a myth. For hard pure math was it ever true?

   But there is a part 2 to the story of H10. Davis-Putnam-Robinson set the problem up, but then Matiyasevich solved it. He was a 23-years-old brilliant Russian mathematician. I suspect he was not in the STOC-FOCS mentality. His techniques were brilliant but not that far outside the box.

   Okay, so when? H10 needed a few new ideas plus the genius of seeing that there was no such algorithm. But I keep coming back to the fact that it didn't need that hard math and P vs NP almost surely does. Alas, Fermat's Last Theorem is a better analog and we are in the mid 1600's. Gauss, Euler, others, not only didn't solve FLT but, given how it was solved, probably could not have. (There is an episode of Dr. Who where The Doctor shows the proof that Fermat left out of the margin. Hence there is a proof using only the math of Fermat's day! Unfortunately Dr. Who is fictional.)

   So when will P vs NP be resolved:

   > In the year 2525
   > If man is still alive
   > If women can survive
   > They may know that P $\neq$ NP.
   > But they might not know the status of Graph Isomorphism.

   (See *In the year 2525* by Zager and Evans, on You Tube. Alas, they do not mention P vs NP.)

3. (Answer this one only if you answered P $\neq$ NP above.) Sasha Razborov, Avi Wigderson, and Andy Yao (or three other wise people whose opinions on P vs NP you take seriously) all knocked at your door at 3:00 AM to tell you that P vs NP has been resolved — but after

announcing it dashed off to tell Lane the good news — without telling you in which direction or how it had been resolved! Which way do you think it went? (This question measures what is stronger: your belief that P $\neq$ NP or your belief that we are nowhere near proving P $\neq$ NP.)

I would think P=NP.

While I believe P $\neq$ NP, I have a stronger belief that we are nowhere near a proof. There has been little or no progress on the problem. We are not *just one genius away* or *just one new idea away*. See the answer to the last question for more on how hard I think it is.

So what would I do? I would think P = NP, cancel all of my credit cards, and go back to sleep.

4. What kind of mathematics will be used to resolve P vs NP? Hard Math.

   I separate what I hope is true from what I think is true. I *hope* it is solved using Ramsey Theory and Logic, since then I might be able to follow the proof. In my dreams the ideas come out of a RATLOCC (Ramsey Theory, Logic, and Complexity) meeting.

   Okay, now back to reality. I *think* it will be solved using very hard math that we do not know yet. In the 2012 poll Scott Aaronson summed up my view far better than I can:

   > The resolution will take many yellow books[2] including yellow books that haven't been written yet.

   It has been said that combinatorics is both the easiest and hardest field of mathematics. Easy since a lot of it requires no prerequisite knowledge. Hence a High School Student can do work in it. Hard because a lot of it requires no prerequisite knowledge. Hence you can't easily apply continuous techniques. As a concrete example, $\sum_{i=1}^{n} i^{100}$ is hard, whereas $\int_1^n x^{100}dx$ is easy.

   Having said that, continuous techniques have been used more and more in combinatorics. I believe they will continue to do so. So I'll go with some combination of combinatorics and continuous math. That probably covers all of mathematics.

   Another thought: Perhaps showing SAT $\notin$ P is hard but showing that factoring cannot be done in polynomial time is easier. It may be that factoring is the key problem, not SAT.

5. Do you think the polynomial hierarchy collapses to some level (e.g., there is an $i$ such that $\Sigma_i^p = \Sigma_{i+1}^p$)? No.

   I think $\Sigma_i^p \neq \Sigma_{i+1}^p$ and it will be proven the same time as P $\neq$ NP. Why are they different? Because of all those thousands of problems that are $\Sigma_{42}^p$-complete that mathematicians (even before the Cook-Levin Theorem) and Computer scientists have been trying to get into $\Pi_{42}^p$. Oh. There aren't any? Hmmm. Maybe I'm not that confident after all.

6. Do you think that SAT has polynomial-sized circuits? No.

[2]Springer-Verlag has two series of books *Undergraduate Texts in Mathematics* and *Graduate Texts in Mathematics* which have yellow covers. Hence the term *Yellow Books* indicates hard mathematics.

I think SAT does not have polynomial-sized circuits. That's my advice on advice. So why not? I can imagine advice helping factoring (e.g., a table of certain kinds of numbers). I just can't imagine advice helping with SAT.

I am more confident that SAT does not have poly-sized circuits than I am that PH does not collapse. Hence the Karp-Lipton Theorem:

$$\text{SAT} \in \text{P/poly} \rightarrow \Sigma_i^2 = \Pi_i^2$$

always looked odd to me. It says something really unlikely implies something less unlikely.

7. Do you think P = BPP? Yes.

   This is one of those rare statements that the community changed its mind on. In 1985 most people thought P $\neq$ BPP (alas I do not have a poll to prove it, but I was in the community at the time). Mike Sipser was an exception [**?**]. After the Nisan-Wigderson *Hard implies Random* results [**?**] the community shifted to thinking P = BPP. I can imagine this one being proved within the next 5 years; however, I said that 10 years ago.

8. Do you think that SAT $\in$ BQP (commonly called *Quantum P*) implies that the polynomial hierarchy collapses? Yes.

   I hope so, if only so when students claim they read on the web that SAT is in Quantum P I can tell them with more authority *SAT in Quantum P is very unlikely.* While we are here, will Quantum P be important? I think that in the future theorists will need to know quantum methods even if they work on classical, much like today theorists must know prob methods even if they only work on deterministic computation (are there people that only work on deterministic computation?).

9. Do you think P = NP $\cap$ coNP? No.

   Since I first cut my teeth on computability theory I was hoping the answer is yes. But since factoring is in NP $\cap$ coNP, and I think factoring is not in P, I am forced to think P $\neq$ NP $\cap$ coNP even though I don't want to. Darn logic!

10. Do you think Graph Isomorphism is in P? No but with no confidence.

    I think GI is in NP $\cap$ coNP by derandomization. I've heard that Babai's result [**?**] that GI is in quasipolynomial time $n^{(\log n)^{O(1)}}$ is as far as current methods can go. Hence it will be a long time before a new advance. Or it could be solved tomorrow. Or it may not be solved by the year 2525.

    As noted above, I hope that even after P vs NP is resolved the status of GI is unknown. That would be a hoot!

    Worst Case Scenario: GI $\in$ P and the proof uses the classification of finite simple groups. If so this might be the largest constant ever in an algorithm.

11. Do you think factoring is in polynomial time? No but with no confidence.

    This is probably the question where I am least confident of my answer. Contrast the following:

- A logician uses logic to show SAT $\in$ P. I rather doubt this will happen. I doubt that SAT is even a problem in logic. In fact, deep methods in logic have not given us *any* faster algorithms for SAT.
- A number theorist uses number theory to show factoring is in polynomial time. This is quite plausible. In fact, deep methods in number theory have given us faster algorithms for factoring.

Hence the notion that hard math gets factoring into P is quite plausible. So why do I think it won't happen? To paraphrase Samuel Wagstaff [**?**] (page 263–264)

> Why have no new factoring algorithms been discovered since 1995? There have been variants of Quadratic Sieve (QS), Number Field Sieve (NFS), and Elliptic Curve Methods (ECM) but they all have time complexity
>
> $$\exp(c(\ln N)^t(\ln\ln N)^{1-t}) = N^{c(\ln N)^{t-1}(\ln\ln N)^{1-t}}$$
>
> for some constant $0 < t < 1$. For QS and ECM $t = \frac{1}{2}$. For NFS $t = \frac{1}{3}$. The reason for this shape for the time complexity is the need to find smooth numbers (numbers with only small factors for some notion of small). Any new factoring algorithm that succeeds by finding smooth numbers will not be in P.

This quote cuts both ways – current techniques will not get Factoring into P, but a new idea might. I better move on before I change my mind again.

12. If you answered P $\neq$ NP above do you believe that an obstacle is "hard instances," for example, for any deterministic Turing machine $M$ accepting the language

$$L = \{(N, x, 1^t) : \text{Nondeterministic } N \text{ does not halt on input } x \text{ within } t \text{ steps }\}$$

there exists $(N', x')$ such that the runtime of $M$ on $(N', x', 1^t)$ is not bounded by a polynomial $t^c$?

Yes. SAT seems to be easy most of the time. So it's the hard instances that are ... hard. Also hard to find. Dang it!

13. If someone shows P = NP will this have a big effect on practical computing? Yes.

While the first algorithm for SAT $\in$ P may well be terrible, the ideas behind it will be used to get practical algorithms. It may be that these algorithms are hard to prove anything about; however, working well in practice will be awesome. We might even find out Ramsey of 5.

One chapter of Lance Fortnow's book [**?**] on P vs NP is a fictional story of what happens after P = NP is proven. Initially the algorithm is terrible. But since P = NP they use the algorithm to find a better one. After many iterations they have a really fast algorithm but have no idea why it works. If P = NP then this scenario is plausible.

14. If someone shows P $\neq$ NP will this have a big effect on practical computing? I originally thought YES but now I think NO.

I've had the following conversation with Darling:

**Bill:** If P $\neq$ NP then I can't imagine the insights will not have a drastic effect on real world computing. Hence I answer YES.

**Darling:** I can imagine it.

**Bill:** Since you can imagine it, I'll change my answer to NO.

15. Given that SAT-SOLVERS are now quite good, will P vs NP become less relevant? No, it will still be relevant.

    A while back I had the $17 \times 17$-challenge on my blog: find a 4-coloring of the $17 \times 17$ grid that has no monochromatic rectangles and you'll get \$289.00. Many people said *just run a SAT Solver on it*. Several tried but despite only having $289 \times 4$ variables the standard SAT Solvers didn't work. (It was later solved by a much more sophisticated SAT Solver – see my blog and search for $17 \times 17$.) Factoring and BITCOIN and other problems can be phrased as Boolean Satisfiability problems. Finding Ramsey of 5 as well. Gee, I had heard that SAT Solvers do well with *millions of variables*. So why were these problems hard? I suspect that in my problem, and other hard problems, the clauses have a lot of overlap; and this makes them hard.

    Perhaps SAT SOLVERS have a good reputation because (1) they really are good on some problems people care about, and (2) they tend to be tested on problems they do well on (perhaps those with little overlap of clauses). More generally there may be a street-light-problem here. Recall the anecdote:

    **Alice to Bob:** Why are you looking for your keys under the street light when you dropped them a block away?

    **Bob to Alice:** The light is better here.

16. Aside from P vs NP which open problem do *you* most want to see solved?

    (a) The Erdos-Turan Conjecture: show that if $\sum_{x \in A} \frac{1}{x}$ diverges then $A$ has arbitrarily long arithmetic progressions.

    (b) The Erdos-Turan-Gasarch Conjecture: show that if $\sum_{x \in A} \frac{1}{x}$ diverges then, for all $p_1, \ldots, p_k \in \mathbb{Z}[x]$ with $p_i(0) = 0$, there exists $a, d$ such that $a, a + p_1(d), \ldots, a + p_k(d) \in A$.

    (c) Obtain tight asymptotic bounds on the Van Der Waerden numbers and the polynomial VDW numbers.

    (d) Prove that computing the Ramsey numbers is hard. This may require a new framework for complexity.

    (e) Resolve the difficulty of *The Muffin Problem* (There is an out-dated paper on arXiv on The Muffin Problem. I am also working on a book on it.)

    (f) The Unique Game Conjecture. When this first came out it seemed like there were no barriers to proving it and that it might be proven. There are still no barriers but its still open. Oh well.

    (g) Meta Problem – Provide proofs of any of the above that I can understand.

17. Anything else you want to comment on, feel free!

I wish that the popular media did a better job at portraying P vs NP. All mentions of it on TV that I have seen have been terrible. One problem is that we are trying to prove that problems are *hard*, which is not as sexy as proving that problems are *easy*.

18. Do I have permission to print your response with your name? Without your name? Not at all?

    Yes. Duh.

19. What is your highest degree? What is it in? Where is it from? When did you get it? The answer will not appear in the article; however, I want it for statistical use.

    PhD from Harvard in Computer Science in 1985.

    You can always tell a Harvard man, but you can't tell him much.

## 3 Wrap Up

Well, that's it for now. If P vs NP is not resolved within the next 10 years I may do another survey. Or maybe a robot will do it for me. In any case I will supply my own answers.

## 4 Acknowledgment

I want to thank Clyde Kruskal, David Sekora, Nathan Grammel, Justin Hontz, Karthik Abinav, and Josh Twitty for proofreading and discussion. And of course I want to thank Lane for giving me a forum to present my survey, which led to this open problems column.

## References

[1] S. Aaaronson. P=?NP. In J. Nash and M. Rassias, editors, *Open problems in mathematics*. Springer, 2016.

[2] L. Babai. Graph isomorphism in quasipolynomial time, 2016. `https://arxiv.org/abs/1512.03547`.

[3] L. Fortnow. The status of the P versus NP problem. *Communications of the ACM*, 86(8):78–86, 2009.

[4] L. Fortnow. *The golden ticket: P, NP, and the search for the impossible*. Princeton University, 2013.

[5] W. Gasarch. Complexity Theory Column 36: The P=NP poll. *SIGACT News*, 33(2):34–47, 2002.

[6] W. Gasarch. Complexity Theory Column 74: The P=NP poll. *SIGACT News*, 43(2):53–77, 2012.

[7] N. Nisan and A. Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49:149–167, 1994. Prior version in FOCS88. Full Version at `http://www.math.ias.edu/~avi/PUBLICATIONS/`.

[8] M. Sipser. Expanders, randomness, or time versus space. *JCSS*, 36:379–383, 1988. Earlier version in CCC 1986, then called Structures.

[9] S. Wagstaff. *The joy of factoring.* AMS, Providence, 2013.