Open Problems Column
Edited by William Gasarch

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 other questions) [6, 7]. Both were written by William Gasarch (me) and appeared in the Complexity Column of SIGACT News, edited by Lane A. Hemaspaandra. They were in 2002 and 2012. Since William Gasarch is fond of Van der Waerden’s theorem, you would think the next poll would be 2022; however, Notorious LAN asked if it could be a bit earlier so, to coincide with his 100th column, and I agreed.

The results of that poll will appear in Notorius’s column in this issue. That article is written objectively – I report on what people responded without comments like Lance, really, there are intelligent people who think P = NP but do not think Elvis is alive. By contrast, this column will be my answers and perhaps some commentary on the answers others gave.

This column is about what I think the status of P vs NP is and will be. For information on what is status of P vs NP see Scott Aaronson’s article [1], Lance Fortnow’s article [4], or (for the layperson) Lance Fortnow’s book [5].

2 Questions and Answers
1. Do you think P = NP? I think P \neq NP. I was once 100\% sure now I am only 100\% sure.

The Graph Minor Theorem makes me ponder if some really hard math theorem may all of a sudden, and perhaps by accident, get SAT \in P. Also, people have been trying to get SAT into P for only about 50 years. A drop in the mathematical bucket? Or since they were 1970-2018 and not 1670-1718, perhaps more of a splash?

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 things 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.” I’ll add to the quote by saying you need to really BELIEVE it is false when trying to prove its 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 himself believed you were the most important person in the world. That may explain his success in politics and other endeavors.)

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

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), Julia Robinson (a logician and a women) were outsiders for the reasons given in parenthesis. So – do we need an outsider for \( P \neq NP \)?

- **YES-** the current system rewards the-next-STOC/FOCS-paper more than long term thought. 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 (possibly proving our techniques won’t work instead of working on new techniques that will).
- **NO-** the math needed to work on H10 was not much. The math needed to work on \( P \neq NP \) seems like it may be quite formidable. See next point.
- **NO-** the myth of the genius-in-his-basement is no longer true. For hard pure math was it ever true?

But there is a part 2 to the story of H10. David-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 much math and \( P \neq NP \) does. So when will it be solved:

\[
\begin{align*}
\text{In the year 2525} \\
\text{If man is still alive} \\
\text{If women can survive} \\
\text{They may know that } P \neq NP. \\
\text{But they still won’t know the status of Graph Isomorphism.}
\end{align*}
\]

(The original song by Zager and Evans is better – see it on You Tube)

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 \( P \neq NP \) you take seriously) all knocked at your door at 3 a.m. to tell you that \( P \neq NP \) 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 believe that we are no where near proving \( P \neq NP \).) In the actual poll more people thought \( P \neq NP \) then I would have thought. This
may be because the three wise men all think $P \neq NP$. If I ask this question again on my next poll I may make it a group with people on both sides of the issue.

While I believe $P \neq NP$, I have a stronger believe that we are nowhere near a proof. Hence I would think $P = NP$. Therefore I would cancel all of my credit cards and go back to sleep.

4. What kind of mathematics will be used to resolve $P$ vs $NP$? Let us separate out what I want to see happen vs what I think will happen.

I hope the answer depends on Ramsey Theory and Computability theory since that way I might be able to understand it. In my dreams the ideas come out of a RATLOCC (Ramsey Theory, Logic, and Complexity) meeting.

Okay, now back to reality.

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. Hardest because a lot of 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 $\int_{1}^{\infty} x^{100} dx$ 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 $\Sigma^p_i = \Sigma^p_{i+1}$)? I think $\Sigma^p_i \neq \Sigma^p_{i+1}$ 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 $\Sigma^p_5$-complete that mathematicians (even before Cook’s Theorem) and Computer scientists have been trying to get into $\Sigma^p_4$. Oh. There aren’t any? Hmmm. Maybe I’m not that confident after all.

6. Do you think that $SAT$ has polynomial-sized circuits?

I think $SAT$ does not have polynomial-sized circuits. Thats 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:

$$SAT \in P/poly \rightarrow \Sigma^2_i \Pi^2_i$$

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 [9]. After the Nisan-Wigderson Hard implies Random results [8] 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.
In this year's poll the trend seems to be reversing- 60% thing $P \neq BPP$. This surprised me.

8. Do you think that SAT $\in$ BQP (commonly called Quantum P) implies that the polynomial hierarchy collapses? 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 NO. 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 P, and I think factoring is not in P, I am forced to think $P \neq NP \cap$ coNP.

10. Do you think Graph Isomorphism is in P? No; however, I do think it is in P $\cap$ coNP by derandomization. I've heard that Babai's result [2] that GI is in quasipolynomial time ($n^{(\log)^{O(1)}}$) 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. If so will people lose interest?

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. 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 theorists 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 [10] (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 the all have time complexity

$$\exp(c(\ln N)(\ln \ln N))^{1-t}$$

for some constant $0 < t < 1$. For QS $t = \frac{1}{2}$. For NFS $t = \frac{1}{4}$. 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. As I write this I may even be changing my mind. So let’s move on to the next question.

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 $t^c$?

Not sure this is a YES or a NO but I do think that it is hard to generate natural hard instances of SAT and this is a problem with pinning down its complexity.

13. If someone shows $P = NP$ will this have a big effect on practical computing? While the first algorithm for $SAT \in P$ may well be terrible, the ideas behind it will be used to get practical algorithms

One chapter of Lance Fortnow’s book [5] 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. While I doubt that will happen, something similar might.

14. If someone shows $P \neq NP$ will this have a big effect on practical computing?

Maybe. Sorry for the cop-out answer. The techniques may give us such great insights into computation that they are used to solve other problems. Or not.

I’ve had the following conversation with my darling

BILL: If $P \neq NP$ the proof can’t help but have such great insights that will help real world programmers write better and faster code.

DARLING: I think it can help it

She may be right.

15. Given that SAT-SOLVERS are now quite good, will $P$ vs $NP$ become less relevant?

Yes. SAT-SOLVERS are great on some problems; however, my own experience with trying to use them on Ramsey Theory problems indicates that they have their limits.

The premise that they are “now quite good” was challenged by some of the people who answered the poll. Factoring can be phrased as a problem in SAT, and they haven’t done well there. 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 Warden 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 (see [3]).

(f) 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 the problem. All mentions of it in fiction have been terrible. One problem is that we are trying to prove that problems are hard which is not as sexy as proving problems are easy.

18. Do I have permission to print your response with your name? without your name? not at all? 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.

References


