**Excerpt from**
**The Book Review Column**[1]
Vol 41, No. 4
Edited by William Gasarch
Department of Computer Science
University of Maryland at College Park
College Park, MD, 20742
email: gasarch@umd.edu

**Review of**[2]
**The P = NP Question and Godel's Lost Letter**
**by Richard J. Lipton**
**Springer, 2010**
**240 pages, Hardcover**

**Review by**
**William Gasarch (gasarch@cs.umd.edu)**

# 1 Introduction

I write this review in the form of a series of fictional blog posts. If there is a comment by, say, Lance F, then that does not mean that someone named Lance F actually thinks that. It may mean that I think that Lance thinks that.

Do not confuse this with my real blog.

**INTRODUCING LIPTON REVIEW BLOG**
**September 16, 2010**

This blog will be dedicated to reviewing Lipton's book **The P = NP Question and Godel's Lost Letter**. The book is based on his blog *Godel's Lost Letter and* P = NP. I wonder why he reversed the order going from blog to book?

**BLOGS INTO BOOKS? WHY? AND WHAT ABOUT KINDLE?**
**September 17, 2010**

I got a copy of Lipton's book in the mail today from Springer since I am the SIGACT NEWS book review editor.

Why make a blog into a book? Couldn't I just log on to read it? Not really. When I read a post on a blog I skim it and always mean to get back to it later for a careful read but tend not to. Having a book on your desk is calling to you to read it in a way that a blog cannot.

The book is not on Kindle. Would that make sense? Actually yes— I can imagine having a Kindle with me and not having my laptop with me. Especially since I have a Kindle but don't have a laptop.

**Comments**

**Anon 1:** On Amazon the book sells for $80.00 new but $120.00 used. What kind of sense is that?

**Anon 2:** Dear anon 1- this makes plenty of sense. I for one prefer to read a used book since its already broken in. And I am willing to pay more for the privilege.

**Anon 3:** Isn't $80.00 a lot for a book that you can get on the web anyway?

**Jin-Yi C.:** I think it is the single most interesting web blog I have seen on related topics. He has great insight and wit and beautiful ways to see things and explain them.

**Richard Lipton:** The book will be on Kindle soon. Perhaps by the time you read this.

**FIRST IMPRESSIONS LAST**

**September 20, 2010**

My first impressions are very good, though since I have already read many of his blog postings, its not clear these are my first impressions.

Lipton has been a professor since 1973 and hence has a long view of the field. He not only has many results but has seen many results and trends. His posts reflect a deep sense of history and where ideas come from. Where do ideas come from? People of course! And Lipton never loses sight of that. Most of his posts begin with a description of story of the people involved.

At the end of the posts he references people who made intelligent comments on that post. Gee, if I had known he would do that then I would have commented on his posts more often. Hopefully intelligently.

**DOES HE REALLY THINK** P = NP**?**

**September 21, 2010**

The book is in four parts (I) Introduction, (II) On the P = NP question, (III) On Integer Factoring, and (IV) On Mathematics. The P and NP chapter has 31 posts. His point (and his original motivation for the blog) can be summed up by the following manifesto:

*MANIFESTO I: We should have an open mind about the possibility that* P = NP*.*

There are those who disagree. I was one of them; however, in a series of posts he does much to support the manifesto. Here are some of his points.

1. We all thought that NSPACE($n$) was not closed under complementation but Immerman and Szelepcsenyi proved us wrong. The post was called *A Proof We All Missed*. He makes the point that not only was the result a surprise, but the proof is easy to follow (though clever to come up with). How easy? He includes a sketch that suffices to explain it.

2. We all thought that Bounded Width Branching Programs were not that powerful. Barrington proved us wrong as explained in the post *Barrington Gets Simple*.

3. What if P = NP but the algorithm is impractical?

4. What if P $\neq$ NP but the proof just shows that $SAT$ does not have $n^{O(\log \log n)}$ sized circuits? It is harder to make the case that this is interesting. Lipton also makes an analogy to the Riemann Hypothesis which, whether it is true or false, will tell us something interesting

**Comments:**

**Lance F:** I disagree.with the Manifesto. We should not have an open mind about the possibility that P = NP since clearly $P \neq NP$.

**Anon 1:** Lance, if its so clear then go ahead and prove it.

**Anon 2:** If I proved P = NP then I would title the paper *A new barrier to showing* P $\neq$ NP.

**Bill G:** I disagree about P = NP not being useful. I am sure that if P = NP then whatever technique was used would speed up lots of computations (perhaps not rigorously). There is a wonderful chapter in Lance Fortnow's upcoming book on Complexity Theory for the Layperson on the consequences of P = NP. They are Awesome! The notion of P $\neq$ NP not being enlightening I find more plausible and scary.

**Emily Litella** The papers that got into SODA are posted. They messed up some of the list! Some of the authors are not listed! Oh, they only list the contact author. Never mind.

**Anon 4:** Other results that may make us pause when we are so sure that P $\neq$ NP: IP = PSPACE = ZK and PH $\subseteq$ $\mathrm{P}^{\mathrm{PP}}$.

**Anon 5:** When NP was shown to be in PCP$(1, \log n)$ peoples reaction was *now we can show certain functions hard to approximate.* Why didn't they think *Gee, NP is easier than we thought.* Dr. Lipton is right- we are too tied to the mindset. Fortunately, since P $\neq$ NP, I don't think its really a problem.

**Anon 6:** My PhD was on Oracles for Space Classes. While I was proving that proving things about space classes would be hard to prove, Immerman and Szelepcsenyi were proving things about space classes. Oh Well.

**Luca T.** People forget that at one time the conventional wisdom was that P $\neq$ BPP. And now the conventional wisdom is that P = BPP. Could the same happen to P and NP. NO!

**I SHOULD POST ON THAT! OH.**
**September 22, 2010**

Upon reading the post *Ramsey's Theorem and NP* my first thought was *what a great idea! I should post about it on complexity-blog!.* This is of course silly since it was already posted on Lipton's blog. Nevertheless, I will discuss it here, as it is my favorite post in the book (so far). Recall the following subcase of Ramsey's theorem:

*For all $k$ there exists an $n = f(k)$ such that, for all 2-colorings of the edges of $K_n$ there is a monochromatic $K_k$. (It is known that $2^{k/2} \leq f(k) \leq 2^{2k}$.)*

Let us turn this around.

*For all $n$ there exists an $k = g(n)$ such that, for all 2-colorings of the edges of $K_n$ there is a monochromatic $K_k$.* (It is known that $\frac{1}{2} \lg k \leq g(k) \leq 2 \lg(k)$.)

Let $G$ be a graph. We want to know if $G$ has a clique of size $m$. KEY: If $G$ does have a clique of size $m$ then, if we randomly color the edges of $G$ we will *always* find a monochromatic clique of size $g(m)$. We can use this to obtain the following randomized algorithm for clique

1. Input$(G, m)$.
2. Randomly 2-color the edges of $G$.
3. By brute force check if there is a monochromatic clique of size $g(m)$.
4. If there is not one then you KNOW that $G$ does not have a clique of size $m$.
5. If there is one then you do not know anything; however, if you repeat this many times your confidence in $G$ having an $m$-clique may increase.

It is unlikely that anything can be proven about this algorithm. In fact, a graph with many cliques of size $g(m)$ will fool it (though perhaps we can get around this). But this shows the power of the blog– he can toss out ideas of interest without worrying about referees, editors, journals, or paywalls.

**Comments:**

**Bill G:** If you fix $m$ then this looks like a randomized sub-exp algorithm for Clique-of-size-$m$. Sort of a fixed parameter tractability thing.

**DOES HE REALLY THINK FACTORING IS IN P?**

Lipton seems to believe the following:

*MANIFESTO II: We should have an open mind about the possibility that factoring is in* P.

Logically MANIFESTO I implies MANIFESTO II, though he seems to be more emphatic about MANIFESTO I.

There are three postings about factoring. They offer some very interesting ideas. One of them is that if factorial was easy to compute then factoring would be easy.

**Comments:**

**Larry W:** If factoring is easy then we will all switch to Elliptic Curve Crypto. That's good news for me since my book on the topic will sell better.

**Lance F:** If factoring is easy then we'll just all go back to private keys. This won't be a big deal with today's technology.

**Anon 1:** If factoring is easy then I will take my credit card off of amazon.com and then I can't buy this great book. Oh well.

**Bill G:** I think its more likely that we show factoring is hard and thus that P $\neq$ NP.

**MATHEMATICAL EMBARRASSMENTS, DISEASES, AND SURPRISES**

There are nine posts on Mathematics in the chapter called *On Mathematics*. There is more variety here then in the other chapters since mathematics is so large. Of particular interest are the three posts on mathematical embarrassments, diseases, and surprises.

A mathematical embarrassment is a math problem that is open but should really be closed. They just don't sound that hard. Perhaps when we solve them we will see that they aren't that

hard. Here is an example from Terry Tao (from his blog which is also a book which I will also review).

*The Linear Recurrence Problem:* Given integers $c_1, \ldots, c_d$ and numbers $a_0, \ldots, a_{d-1}$ consider the recurrence

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d}.$$

Is there some $k$ such that $a_k = 0$? It is not known if this is decidable.

I agree- this is embarrassing. This should be known. My intuition is that we just solve the recurrence and get good enough approximations (hmmm- that could be the problem) for the roots of the char equation then we can determine if the recurrence ever gets to 0.

A mathematical disease is a problem that obsesses the math community without much success. I give one example due to Ulam.

*The Reconstruction Conjecture:* Let $G$ be a graph on $n \geq 3$ vertices. Given all of the vertex-deleted subsets of $G$, can you uniquely determine $G$. The good money says that you can; however, the conjecture is open.

A mathematical surprise is just what it sounds like- a result that surprised people. We have already mentioned above the closure of NSPACE(n) under complementation and Barrington's result on Bounded Width Programs. The negative solution to Hilberts' tenth problem was also a surprise. This post also goes into what causes a surprise: connecting two fields, incorrect proofs, and asking a new problem can all cause surprises.

**Comments:**
**Bill G:** The following surprised me: Let

$$VC_{17} = \{G \mid G \text{ has a vertex cover of size 17 }\}.$$

I would think this would take roughly $O(n^{17})$ steps. I first learned that by the Graph Minor Theorem you can get it into $O(n^3)$. This algorithm is not practical for a variety of reasons. However, later it was down to $n + O(k^k)$ (which is practical). Its even better now. But this all surprised me. This gave birth to the field of Fixed Parameter Tractability.

**Anon 1:** I am not surprised that this book is so awesome!

**Bill G:** So, who should read this book? If you do better reading books than blogs, and you know some (not even that much) theoretical computer science then you should buy this book. Certainly get it for your school's library.