Gödel's Lost Letter and P=NP

a personal view of the theory of computation

More on Mathematical Diseases

NOVEMBER 12, 2009
tags: Algorithms, breaking crypto-systems, Conway, Life, lower bounds, Problems, Proof
by rjlipton

*A summary of some **your** ideas on mathematical diseases*

John Conway is a world renowned mathematician, who defies a simple description. He has worked on countless games, puzzles, and easy to state, but often hard—if not impossible—to solve problems. These range from his classic game of *Life*, to his work on *Surreal* numbers; from his work on polyhedra, to his special notation for huge numbers. At the same time he has made deep contributions to many, if not most areas, of modern mathematics: from group theory, to number theory; from algebra, to geometric theory. There is only **one (http://en.wikipedia.org/wiki/John_Horton_Conway)** John Horton Conway.

Today I want to talk about some of the mathematical diseases that were raised by those who were kind enough to comment on my previous **discussion (http://rjlipton.wordpress.com/2009/11/04/on-mathematical-diseases/)**.

The response was so strong that I thought I would collect some of your comments in one place. I hope that this either helps someone to make progress on one of these diseases or to help spread them to others.

Conway was the source many of the popular MD's, which is probably not too surprising given his wide range of results, that includes many unusual problems.

He once gave the keynote address at SODA. This conference, the Symposium on Discrete Algorithms, is theoretical, but a bit more down to earth than FOCS, for example. Conway's presentation was a strange and wonderful one—at many levels. The main part of the talk was an impressive demonstration of his *Doomsday algorithm*. This algorithm allows one to calculate the day of the week from any date by a "simple" rule—Conway himself can do this in realtime. Thus,

$$\text{10 Nov, 2009} \rightarrow \text{ Tuesday.}$$

The funniest part of his demonstration was that people would ask dates and get back days of the week, but for many of them we had no idea if Conway was really correct or not. Oh well.

Personally, of his many theorems, his *15-Theorem* is one of the neatest:

> ***Theorem:*** *If a positive definite integral quadratic form represents all positive integers up to 15, then it represents all positive integers.*

Conway proved this with William Schneeberger in 1993: see this for a **overview (http://www.fen.bilkent.edu.tr/~franz/mat/15.pdf)** of the result. Forget how one proves such a theorem, my question is more basic: where do you get the intuition that such a theorem might even be true?

Let's turn now to the previous comments, with some extra annotation, here and there.

Some Mathematical Diseases (MD)

- **Conway's Thrackle Conjecture:** Joseph O'Rourke suggests this one: which he says *" bites me about once every two years$\dots$"*

I did not know this conjecture. See **this (http://en.wikipedia.org/wiki/Conway's_thrackle_conjecture)** for a description of this amazing simple sounding problem. László Lovász has worked on the problem so this disease can affect even one of the best mathematicians in the world.

- **Conway's Game of Life:** John Sidles suggest this one and, adds *"What a great subject!"* He says, *To lead off, a wholly benign, utterly useless, and wonderfully enjoyable MD is the study of self-replicating structures in Conway's Game of Life. The accomplishments of the Life community over the last 39 years are so amazing, that all one can say is $\dots$ Golly!*

The Game of Life is played on an infinite grid of squares. It is not really a game, it is a zero player game, one starts off by providing the *seed* — by marking some finite set of squares in the grid. Then the game is entirely deterministic, at each time instance, it evolves using 4 simple rules. Conway's original question was : Is there a seed which can grow indefinitely? For the answer to this, and a beautiful exposition on the game itself, please see the this **article (http://en.wikipedia.org/wiki/Conway's_Game_of_Life)** on the game.

- **Collatz Problem:** Akash Kumar suggests the famous $3x + 1$ conjecture, which is also called the Collatz Conjecture. He says, *"This `seemingly' toy problem has much to offer as shown by its resistance to attempts at solving it."*

I was introduced to this famous problem, while I was a graduate student, by Albert Meyer. I tried to show that the mapping had no cycles by a modular argument. It failed. Somehow the problem never has appealed to me again. Definitely, a simple to state, but very hard problem.

- **Palindromic Number Conjecture:** Ted Carroll suggests this one. He says, *"I suck non-mathematicians in with that one all the time—especially computer people because there's a proof that the conjecture holds for binary."*

Start with a number and reverse it, then add the two together. Repeat until a palindrome is reached. Does this always happen? See **this (http://members.cox.net/mathmistakes/palindromes.htm)** for an example and more:

1. $97 + 79 = 176$
2. $176 + 671 = 847$
3. $847 + 748 = 1595$
4. $1595 + 5951 = 7546$
5. $7546 + 6457 = 14003$
6. $14003 + 30041 = 44044$ which is a palindrome.

Specifically, the number 196 has attracted lots of attention. Starting with 196, after being iterated to 300 million digits a palindrome is yet to be found. Curiously, in the binary case, there is a very short **counterexample (http://www.xs4all.nl/~itsme/projects/math/196/base2.html)** that can be shown to never reach a palindrome.

- **Goldbach Conjecture:** Akash Kumar and Tom both suggest this one. Akash says, *"I mean, I find it really amazing that this problem is accessible to people like me with a modest mathematical background and is so profound that it has avoided attacks by best brains."*

Tom says that *"Everyone has dreamed about solving these at least a little bit at some stage in their life. There's even a (fictional)* ***book (http://www.amazon.co.uk/Petros-Goldbachs-Conjecture-Apostolos-Doxiadis/dp/0571205119/)*** *written about this problem about a man obsessed with solving it."*

The book titled, "Uncle Petros and Goldbach's Conjecture" by Apostolos Doxiadis is well written and fun. I would definitely recommend it to you. See **this (http://en.wikipedia.org/wiki/Goldbach_conjecture)** for other examples of Goldbach's Conjecture appearing in popular culture.

The best known results about the Goldbach Conjecture are:

1. Every sufficiently large odd number is the sum of three primes. This result is due to Matveevich Vinogradov.
2. Every sufficiently large even number is the sum of a prime and the product of at most two primes. This **result (http://en.wikipedia.org/wiki/Chen%27s_theorem)** is due to Chen Jingrun. He proved it during the "culture revolution" in 1966, and at first the western mathematicians did not believe

that he had achieved this great result. He had.

● **Splay Conjecture:** Mihai Pătraşcu suggests this one. This conjecture concerns the behavior of certain tree data structures. See **this (http://en.wikipedia.org/wiki/Splay_tree)** for an introduction to the question. A real computer science question.

● **Graceful Tree Conjecture** Ibrahim Cahit and Shiva Kintali suggested this one. Cahit explains, *Let me give short explanation why GTC is a mathematical disease. Alexander Rosa has* ***identified (http://www.math.ilstu.edu/cve/speakers/Rosa-CVE-Talk.pdf)*** *essentially three reasons why a graph fails to be graceful: (1) G has "too many vertices and not enough edges," (2) G "has too many edges," and (3) G "has the wrong parity." If for any graceful tree an arbitrary vertex can be assigned the label 0 (rotatable tree) then the proof of the GTC would be piece of cake. Unfortunately not all trees are rotatable. Similarly if all trees are alpha-valuable (a kind of balanced labeling stronger than graceful (beta-valuable) labeling) then the proof of GTC follows easily. What remains is an algorithmic proof attempt based on the induction on the diameter d (the length of the longest path in a tree) of a tree. Unfortunately most of the trees with diameter greater than 4 have no alpha-labeling. In the past I have attempted twice (once in 1975, settled a class of symmetric trees and again 1980, settled all trees of diameter 4). I didn't give up, it is a disease after all.*

Despite of huge efforts very little known for about graceful trees e.g., any tree with < 34 vertices has a graceful labeling and all trees of diameter up to 5 are graceful.

● **Riemann Hypothesis:** Subrahmanyam Kalyanasundaram suggests this one. He says, *"Although not so easy to state, I think Riemann Hypothesis has attracted quite a lot of attention. See* ***here (http://secamlocal.ex.ac.uk/people/staff/mrwatkin/zeta/RHproofs.htm)*** *for a list of attempted proofs."*

Two mathematicians from Purdue recently made independent claims, incorrectly, that they have proved the famous theorem. The Riemann has been claimed many times previously by both amateurs and professionals. I asked some experts the other day what is up with this great problem. The answer was there seems to be no progress; the conjecture is still as unreachable as ever.

● **4-Color Theorem:** Gilbert Bernstein and Gil Kalai both suggest this one. Gilbert says that *"633 configurations is still too many!"*

Kalai adds, *Once I had some idea about 4CT (which asserts that every planar cubic graph is 3-edge colorable) and relating it to Tverberg's theorem, and I remember Laci Lovász asked me: "Can you use your approach to prove that a bipartite cubic graph is 3-edge colorable?" (Which is an easy graph theory result.) Dealing with bipartite cubic or even with bipartite planar cubic graphs looks like a good test-case for various hypothetical approaches.*

I have outlined an approach that we have suggested for a "human" proof in a previous **discussion (http://rjlipton.wordpress.com/2009/04/24/the-four-color-theorem/)**. Roughly, we show that even proving that every planar cubic graph is *approximately* 3-edge colorable, is enough to prove 4CT. Still we are unable to prove that this is true.

- **Reconstruction Conjecture:** Harrison and Ryan Williams suggest this one. Harrison explains why the conjecture is related to the GI conjecture:

As someone who's been bitten by the reconstruction bug, I'll tell you that it is indeed related to graph isomorphism on a fundamental level. Here's a brief sketch of why:

If we label the vertices of a graph, then reconstruction is trivial—we just glue the induced subgraphs together so that the labels match up, and in fact we only need three induced subgraphs to reconstruct our original graph. The reconstruction conjecture is that, if we forget the labels, then this "gluing" process is still unique (up to graph isomorphism, of course). This feels like it should be intuitively true, but there's a crucial problem: namely, if the graph has a large automorphism group, then its induced subgraphs can get "put into" the original graph in many different ways, and it's not clear that the global properties of the graph don't change.

So much of the work on graph reconstruction centers around understanding just how automorphism groups of graphs behave, and how they relate to combinatorial properties. (From the other direction, by the way, it's an old result of Béla Bollobás that almost all graphs are reconstructible, since random graphs don't allow us to embed large subgraphs into them in more than one way.)

Ryan Williams adds, *Allow me to get a little bit infected* $\dots$ *If we assume the graph reconstruction conjecture, does this imply anything interesting about the complexity of graph isomorphism? If you want to tell whether two* n*-node graphs are isomorphic, and you know that this "reduces" to checking whether there is an "isomorphism matching" between two sets of* n *graphs on* $n-1$ *nodes each, can you get a recursive algorithm?*

I have to say that I love this conjecture, but have some immunity—I have never thought about it all.

- **The Status of $\zeta(3)$:** This was suggested by Ninguem. He says:

Roger Apéry was a professor at a small French university. He was past the age most mathematicians prove big theorems, he had a history of bad proofs, not a big research output and, I was told, also an alcoholic. But he was a professional mathematician and not a crank. He showed that $\zeta(3)$ *is not rational. We still don't know whether* $\zeta(3)$ *is transcendental.*

An anonymous commenter adds, *The reason people were initially skeptical was that Apéry gave a very weird talk presenting the proof. In the talk, he stated some implausible-looking identities and recurrences, with no hint of how to prove them, and he showed that they implied the irrationality of* $\zeta(3)$. *He apparently didn't respond well to questions, and this led people to wonder whether he actually had a proof of the identities. Maybe he had just conjectured them based on numerical experiments, and perhaps they weren't even true. He eventually came out with a paper that proved everything, and he probably had the proofs at the time he gave the talk, but he certainly didn't explain it at all clearly at that time. I think it wasn't until Don Zagier came up with his own proofs of Apéry's assertions that everyone became convinced it definitely worked (although everyone got very excited even before that, once they checked everything numerically and found that it all seemed to work).*

I heard that when Apéry wrote on the board the key identity he needed,

$$\zeta(3) = \frac{5}{2}\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^3\binom{2n}{n}}$$

he gave a very strange answer to "where did this identity come from?" He is alleged to have answered, "**they grow in my garden**." Obviously, this did not help make people feel comfortable. The identity is wonderful, the proof is correct, and the values of the zeta function at other odd integers is still a mystery.

- **Finding New Crypto-Systems:** Chris Peikert suggests this one. He says: *As one of the many who search for new cryptosystems, allow me to defend the affliction (before someone develops a vaccine)! Sure, factoring- and discrete-log-based systems are great for Alice and Bob's everyday secret messages, but* $\dots$

1. *What if you don't believe that these problems are truly hard?*
2. *What if someone builds a quantum computer? (What if it happens sooner rather than later?)*
3. *What if your device is constrained and can't handle 2048-bit exponentiations?*
4. *What if you need "extra features," like delegation, revocation, or homomorphisms?*
5. *What if you want to be guaranteed security even if some/most of your secret key leaks out via a side channel?*
6. *Your standard-issue cryptosystems don't admit very satisfactory answers to these questions. That's why we need to look for more* $\dots$

I agree with all he says, but I still think the search for new systems has a bit of an MD flavor, however.

- **Rudrata Problem:** Proaonuiq suggested this one. He says, *In the Harary paper they cite the Rudrata disease, an old and widespread one. I like specially the RCD-variant (Rudrata problem for Cayley Digraphs), also old and widespread. Be aware: the later infection is harder to cure than the more general Rudrata disease, since the problem seems simpler!*

I was puzzled by the reference to the "Rudrata disease," since I had not heard of it before. I found out that it is another name for the *Hamilton cycle problem*, which is of course NP-complete. A special case of the Hamilton cycle problem is the famous knights tour **problem (http://en.wikipedia.org/wiki/Knight's_tour)** on a chessboard. The pattern of moving a knight on a half-chessboard was presented back in the 9^{th} century by the Kashmiri poet Rudrata in a Sanskrit poem. Hence the name "Rudrata disease."

Thus, this open question is about understanding the structure of Hamiltonian cycles on special graphs that arise from groups—Cayley Digraphs. I can see why this could be an MD.

I have to add a comment on a related but completely different topic: **how good are you at chess?** Moving knights on a chessboard can be used to rate your chess ability. There is a simple test: One places four pawns on the chessboard at certain locations. Your job is to move the knight from one corner of the board to the other **as fast as possible**. You must visit all squares in a certain order, and can never visit the squares that are occupied by the pawns. You can have the knight visit a square more than once. The **time** that you take to do this task apparently correlates very well with your chess ability. I was given the test by a friend, and did not do very well.

- **Long List of Problems:** These were all suggested by Gil Kalai. He says the following: (I have made some minor edits—I hope that I have not changed any content by mistake.)

Let me adopt the MD term under a slight protest and mention some of my favorites MD's that I spent most time studying.

1. ***The rate of error-correcting binary codes (and spherical codes).***

   (Infected by Nati Linial) A very easy to describe problem. You want an error correcting binary code on n bits with minimal distance δn. What is the largest possible rate as a function of δ. (A closely related problem is about the densest sphere packing in high dimensional spaces.)

   Is the Gilbert-Varshamov lower bound the correct one? Can the MRRW upper bound (the best known one) be (even slightly) improved? A (somewhat) related (easier) problem: Can you find an elementary construction (not based on algebraic geometry) for large-alphabets codes with better rate than Gilbert-Varshamov. (The zig-zag success for expanders give some little hope.)

2. ***The g-conjecture for spheres:***
   *This is probably the first problem on my list. I started working on it the earliest and probably spent more time on it than on any other. It is a little hard to explain and motivate. But there are quite a few people who thought about the problem. (There are a few posts about it on my **blog (http://gilkalai.wordpress.com/tag/g-conjecture/)**).*

3. ***The Hirsch conjecture (and strongly polynomial LP)***
   *I wrote about it amply on my **blog (http://gilkalai.wordpress.com/tag/hirsch-conjecture/)**.*

4. ***The Erdös-Rado Delta system-conjecture***
   This is on Gowers's possible future polymath projects so let me not elaborate further here.

5. ***The Cap set conjecture***
   It is about the largest size of a subset A of $(\mathbb{Z}_3)^n$ not having three elements that sum to zero. Closely related to Roth's and Szemerédi's theorems.

6. ***Borsuk's conjecture.***
   I don't think Jeff Kahn and I were "obsessed" about the problem while working on it for quite a few years. It is not clear if an obsession mode is a good sign.

   Our approach to the problem is somewhat related to a famous open problem which is still open and is on Alexander Rosa's list and was always high on Jeff's list: The Erdös-Faber-Lovász conjecture. (Jeff settled the EFL conjecture skepticism and Jeff and Paul Seymour solved it fractionally.)

7. ***Bible codes***
   This represents an applied topic that I intensively (and obsessively) spent much time in the late 90's. At the end I was a coauthor of a 4-author paper containing a thorough refutation of the scientific evidence for the existence of bible codes. It was a good (while strange) introduction for me on various issues regarding statistics, science, Learnability, even philosophy of science.

8. ***Learnability vs rationality***
   One tempting "cure" for various diseases, especially of conceptual nature, is "learnability" via VC-dimension. I was very optimistic at some time about the usefulness of replacing "rational" by "learnable" in the foundations of theoretical economics.

9. ***Infeasibility of quantum computers***
   This represents a current main research interest.

10. ***P≠NP and related issues***
    It is probably a good instinct whenever you study some new notion about Boolean functions (or simplicial complexes which are just monotone Boolean functions) to spend a little (let me repeat: a little) time on thinking: does this new notion has bearing on P≠NP or other questions in computational complexity? Most often you can easily realize that the answer is no, and sometimes you realize that the answer is no after some more effort.

11. ***A little flirt with Poincaré***
    I was interested in triangulation of manifolds for which the links of vertices are of the simplest possible kind: stacked spheres. (They are the boundaries of a set of simplices glued together along facets.)

    For dimension greater than three, I proved that such a simply connected manifold is a sphere. For dimension three, I could not prove it and it is a very very very special case of the Poincaré conjecture. (I still cannot prove this special case directly.) If you drop the assumption that the manifolds are simply connected then for $d > 3$ you are left with very simple handle body manifolds. I do not know (and am curious to know) which 3 -manifolds have a triangulation where are links are stacked spheres.

Open Problems

Solve some of these MD's. Or suggest some others. One of my **favorites (http://wp.me/pr9Ir-L9)** that is missing is the power of polynomials over composite moduli.

from → History, P=NP, People, Proofs

49 Comments leave one →

1. **eqnets PERMALINK**
   November 12, 2009 4:57 pm
   There is a claimed human proof of 4CT from a few days ago: http://arxiv.org/abs/0911.1587

   I haven't looked at anything past the abstract though.