Gödel's Lost Letter and P=NP

a personal view of the theory of computation

On Mathematical Diseases

NOVEMBER 4, 2009

tags: crypto, diseases, graph isomorphism, group isomorphism, Harary, jacobian conjecture

by rjlipton

Mathematical diseases: symptoms and examples

Underwood Dudley is a number theorist, who is perhaps best known for his popular books on mathematics. The most famous one is **A Budget of Trisections (http://www.abebooks.com/servlet/SearchResults?isbn=0387965688)**, which studies the many failed attempts at the ancient problem of trisecting an angle with only a ruler and a compass. This problem is **impossible (http://www.jimloy.com/geometry/trisect.htm)**, yet that has not stopped some people from working day and night looking for a solution. Trying to find such a solution is an obsession for some; it's almost like they have a malady that forces them to work on the problem.

Today I plan on talking about other mathematical obsessions. They are like diseases that affect some, and make them feel they *have* to work on certain mathematical problems. Perhaps P=NP is one?

Dudley's book is quite funny, in my opinion, although it does border on being a little bit unkind. As the title suggests, in "A Budget of Trisections," he presents one attempt after another at a general method for trisecting any angle. For most he points out that when the angle is equal to some value what the exact error is. For others he adds a comment like:

> *This construction almost worked, if only the points* A *and* B *and* C *had really been co-linear it would have worked. Perhaps the author could move . . .*

His book is about the kind of mathematical problems that I will discuss today: problems that act almost like a real disease.

I cannot resist a quote from Underwood that attacks bloggers. Note he uses "he" to refer to himself in this quote:

> *He has done quite a bit of editing in his time–the College Mathematics Journal for five years, the Pi Mu Epsilon Journal for three, the Dolciani Mathematical Expositions book series (six years), and the New Mathematical Library book series (three years). As a result he has a complete grasp of the distinction between "that" and "which" (very rare) and the conviction that no writing, including this, should appear before the public before passing through the hands, eyes, and brain of an editor.* ***Take that, bloggers!***

(Bold added by me.)

Oh well.

What Is a Mathematical Disease?

This is the flu season in Atlanta, and many are getting it. I hope you either miss the bug, or if you are unfortunate enough to get it, get a mild case.

There is another type of "bug" that affects mathematicians—the attempt to solve certain problems. These problems have been called "diseases," which is a term coined by the great graph theorist Frank Harary. They include many famous problems from graph theory, some from algebra, some from number theory, some from complexity theory, and so on.

The symptoms of the flu are well known—I hope again you stay away from fever, chills, and the aches—but the symptoms for a mathematical disease (MD) are less well established. There are some signs however that a problem is a MD.

1. A problem must be easy to state to be a MD. This is not sufficient, but is required. Thus, the **Hodge-Conjecture (http://en.wikipedia.org/wiki/Hodge_conjecture)** will never be a disease. I have no clue what it is about.
2. A problem must seem to be accessible, even to an amateur. This is a key requirement. When you first hear the problem your reaction should be: *that is open?* The problem must *seem* to be easy.
3. A problem must also have been repeatedly "solved" to be a true MD. A good MD usually has been "proved" many times—often by the same person. If you see a paper in arXiv.org with many "updates" that's a good sign that the problem is a MD.

Unlike real diseases, MD's have no known cure. Even the solution of the problem will not stop attempts by some to continue working on it. If the proof shows that something is impossible—like the situation with angle trisection—those with the MD will often still work hard on trying to get around the proof. Even when there is a fine proof, those with the disease may continue trying to find a simple proof. For example, Andrew Wiles' proof of Fermat's Last Theorem has not stopped some from trying to find Pierre de Fermat's "the truly marvellous proof."

Some Mathematical Diseases

Here are some of the best known MD's along with a couple of lesser known ones. I would like to hear from you with additional suggestions. As I stated earlier Harary was probably the first to call certain problems MD's. His original **list (http://www.math.ilstu.edu/cve/speakers/Rosa-CVE-Talk.pdf)** was restricted to graph problems, however.

• **Graph Isomorphism:** This is the classic question of whether or not there is a polynomial time algorithm that can tell if two graphs are isomorphic. The problem seems so easy, but it has resisted all attempts so far. I admit to being mildly infected by this MD: in the 1970's I worked on GI for special classes of graphs using a method I called the **beacon set method (http://www.cs.yale.edu/publications/techreports/tr135.pdf)**.

There are some beautiful partial results: for example, the work of László Babai, Yu Grigoryev, and David Mount on the case where the graphs have bounded multiplicity of eigenvalues is one of my favorites. Also the **solution (http://ix.cs.uoregon.edu/~luks/iso.pdf)** by Eugene Luks of the bounded degree case is one of the major milestones.

I would like to raise one question that I believe is open: Is there a polynomial time algorithm for the GI problem for *expander graphs*? I asked several people at the recent Theory Day and no one seem to know the answer. Perhaps you do.

• **Group Isomorphism:** This problem is not as well known as the GI problem. The question is given two finite groups of size n are they isomorphic? The key is that the groups are presented by their multiplication tables. The best known result is that isomorphism can be done in time $n^{\log n + O(1)}$. This result is due to Zeke Zalcstein and myself and independently Bob Tarjan. It is quite a simple observation based on the fact that groups always have generator sets of cardinality at most $\log n$.

I have been affected with this MD for decades. Like some kind of real diseases I get "bouts" where I think that I have a new idea, and I then work hard on the problem. It seems so easy, but is also like GI —very elusive. I would be personally excited by any improvement over the above bound. Note, the hard case seems to be the problem of deciding isomorphism for p-groups. If you can make progress on such groups, I believe that the general case might yield. In any event p-groups seem to be quite hard.

• **Graph Reconstruction:** This is a famous problem due to Stanislaw Ulam. The **conjecture (http://en.wikipedia.org/wiki/New_digraph_reconstruction_conjecture)** is that the vertex deleted subgraphs of a graph determine the graph up to isomorphism, provided it has at least 3 vertices. It is one of the best known problems in graph theory, and is one of the original diseases that Harary discussed.

I somehow have been immune to this disease—I have never thought about it at all. The problem does seem to be solvable; how can all the subgraphs not determine a graph? My only thought has been that this problem somehow seems to be related to GI. But, I have no idea why I believe that is true.

• **Jacobian Conjecture:** This is a famous problem about when a polynomial map has an inverse. Suppose that we consider the map that sends a pair of complex numbers (x, y) to $(p(x, y), q(x, y))$ where $p(x, y)$ and $q(x, y)$ are both integer polynomials. The conjecture is that the mapping is 1-1 if and only if the mapping is locally 1-1. The reason it is called the Jacobian Conjecture is that the map is locally 1-1 if and only if the determinant of the matrix

$$\begin{pmatrix} p_x(x,y) & q_x(x,y) \\ p_y(x,y) & q_y(x,y) \end{pmatrix}$$

is a non-zero constant. Note, $p_x(x, y)$ is the partial derivative of the polynomial with respect to x. The above matrix is called the Jacobian of the map.

This is a perfect example of a MD. I have worked some on it with one of the experts in the area—we proved a small result about the problem. During the time we started to work together, within a few months the full result was claimed twice. One of the claims was by a faculty member of a well known mathematics department. They even went as far to schedule a series of "special" talks to present the great proof. Another expert in the area had looked at their proof and announced that it was "correct." Eventually, the talks were cancelled, since the proof fell apart.

• **Crypto-Systems:** This is the quest to create new public key crypto-systems. While factoring, discrete logarithm, and elliptic curves seem to be fine existing public key systems, there is a constant interest in creating new ones that are based on other assumptions.

Some of this work is quite technical, but it seems a bit like an MD to me. There are amateurs and professionals who both seem to always want to create a new system. Many times these systems are broken quite quickly—it is really hard to design a crypto-system.

A recent example of this was the work of Sarah Flannery and David Flannery in creating a new system detailed in their book **In Code (http://astore.amazon.com/sosmath/detail/1565123778)**. The book gives the story of her discovery of her system, and its eventual collapse.

• **P=NP:** You all know this problem. See **this (http://www.win.tue.nl/~gwoegi/P-versus-NP.htm)** for a nice list of attempts over the years to resolve the problem. Thanks to Gerhard Woeginger for maintaining the list.

Open Problems

What are other MD's? What is your favorite? Why do some problems become diseases? While others do not?

I would love to see some progress made on group isomorphism—I guess I have a bad case of this disease. I promise that if you solve it I will stop thinking about it. Really.

from → History, P=NP, People, Proofs

61 Comments leave one →