Vinay Deolalikar dit qu'il a démontré que P ≠ NP dans un article de 100 pages

- Les News de Buekenhout -

Date de mise en ligne : jeudi 12 août 2010

**
UREM :
Unité de Recherche sur l'Enseignement des Mathématiques**

<h3 class="spip">Researcher Claims to Prove that P Does Not Equal NP in 100-Page Paper</h3>

« Vinay Deolalikar, a principal research scientist at HP Labs, claims to have definitively proved that P`NP in a 100-page paper. As one of the six unsolved Millenium Prize problems and arguably the most important of the lot Deolalikar's proof, if true, would have important implications in the field of cryptography and in scientists' approach to research, and would entitle him to a $1 million prize to boot.

As the paper apparently was not peer reviewed, it'll probably be days before anyone, much less us, can provide anything approaching an assessment of its fundamental soundness. However, mathematicians like Richard Lipton who have glanced at the proof have generally agreed that this looks like a “long, well written paper, by a serious researcher [who] clearly knows a great deal of complexity theory and mathematics.”

Deolalikar sent the following letter announcing the “preliminary version” of the proof : (via Greg Baker)

Dear Fellow Researchers,

I am pleased to announce a proof that P is not equal to NP, which is attached in 10pt and 12pt fonts.

The proof required the piecing together of principles from multiple areas within mathematics. The major effort in constructing this proof was uncovering a chain of conceptual links between various fields and viewing them through a common lens. Second to this were the technical hurdles faced at each stage in the proof.

This work builds upon fundamental contributions many esteemed researchers have made to their fields. In the presentation of this paper, it was my intention to provide the reader with an understanding of the global framework for this proof. Technical and computational details within chapters were minimized as much as possible.

This work was pursued independently of my duties as a HP Labs researcher, and without the knowledge of others. I made several unsuccessful attempts these past two years trying other combinations of ideas before I began this work.

Comments and suggestions for improvements to the paper are highly welcomed.

Click for a full PDF of the 100-page paper.

You can learn more about the P versus NP problem on Wikipedia ; very briefly, P is polynomial time and NP is nondeterministic polynomial time. One fairly easy-to-follow summary, again from Wikipedia : “The question is whether, for all problems for which a computer can verify a given solution quickly (that is, in polynomial time), it can also find that solution quickly. The former describes the class of problems termed NP, whilst the latter describes P. The question is whether or not all problems in NP are also in P.”

If P did equal NP, it would have huge implications in the field of cryptography : A number of existing systems of cryptography most worryingly, many which we use to handle sensitive financial transactions would break down. On the flip side, scientific research dealing with NP-complete problems, like protein structure prediction, could proceed much faster.

While Deolalikar's credentials and the seriousness of his proof appear to check in, that doesn't mean that they haven't spurred any doubts among knowledgeable people. In the top-voted comment on a Hacker News thread

discussing Deolalikar's claims, Arvind Narayanan provides a measured assessment :

* It has been known that the straightforward combinatorial approaches to P = ? NP aren't going to work, and therefore something out of left field was required (http://web.cs.wpi.edu/ gsarkozy/3133/p78-fortnow.pdf). Mulmuley's plan of attack involved algebraic geometry.

* This paper uses statistical physics. This approach doesn't seem to have been talked about much in the community ; I found only one blog comment http://rjlipton.wordpress.com/2009/04/27/how-to-solve-pnp/#c... which mentions the survey propagation algorithm. (Deolalikar's paper also talks about it tangentially.)

* If the statistical physics method used here is powerful enough to resolve P != NP, then there's a good chance it is powerful enough to have led to many smaller results before the author was able to nail the big one. It's a little weird we haven't heard anything about that earlier.

* Finally, since the author is using physics-based methods, there's the possibility that he is using something that's a “theorem” in physics even though it is technically only a conjecture and hasn't actually been proven. Physicists are notorious for brushing technicalities under the rug. It would be very unlikely that the author didn't realize that, but still worth mentioning.

* If that is indeed what happened here, but the rest of the proof holds up, then we would be left with a reduction from P != NP to a physics conjecture, which could be very interesting but not ground breaking.

Conclusion : overall, it certainly looks superficially legit. But in non peer reviewed solutions of open problems there's always a high chance that there's a bug, which might or might not be fixable. Even Andrew Wiles's first attempt at FLT had one. So I wouldn't get too excited yet.

For what it's worth, MIT computer scientist Scott Aaronson is so confident that the proof is wrong, he's offered Deolalikar an additional $200,000 if he's awarded the $1,000,000 Clay Millenium Prize for the proof, though he hasn't exactly been transparent about his reasons. Aaronson : “I'm dead serious and I can afford it about as well as you'd think I can.”

(via Gödel's Lost Letter, Hacker News, Greg Baker via Slashdot) »

Source : Geekosystem Robert Quigley | 9:20 am, August 9th, 2010