CMU professor honored for computational complexity breakthrough

May 21 2007

Computer scientists at Carnegie Mellon University and the Russian Academy of Science will share the Association for Computing Machinery's 2007 Gödel Prize for their seminal work on what many consider the most important unresolved question in theoretical computer science.

Steven Rudich, professor of computer science at Carnegie Mellon, and Alexander A. Razborov, a mathematician and computational theorist at the Steklov Mathematical Institute in Moscow, will receive the $5,000 prize at the ACM Symposium on Theory of Computing, June 11–13 in San Diego.

The ACM's Special Interest Group on Algorithms and Computing Theory recognized Rudich and Razborov for their work on the P vs. NP problem, a classic question concerning computational complexity that underlies the security of ATM cards, computer passwords and electronic commerce. It is literally a million-dollar question — one of seven Millennium Problems that the Clay Mathematics Institute has offered $1 million for solving.

The Gödel prize is named for Kurt Gödel (1906–1978), an Austrian-American mathematician and philosopher who had a major impact on the foundations of computer science and was among the first to puzzle over the P vs. NP problem.

"Of all of the prizes I could win, I would choose this one," Rudich said.

"Gödel has been my luminary hero since I was 12."

The P vs. NP question asks whether the class of problems with solutions that can be quickly recognized (complexity class NP) is the same as the class of problems with solutions that can be quickly generated (complexity class P). In human experience, it is intuitive that the ability to recognize something (like a good musical piece) is easy compared to being able to generate one yourself (like a good composer). People strongly suspect, based on a shared awe of creativity, that NP is a larger class than P. Cryptographers hope that is so; the security of all digital cryptographic systems requires it. At the same time, other computer scientists hope for the exact opposite — they hope to find unexpected shortcuts in the efficiency of creative problem-solving. To date, no one has formulated a mathematical proof that can answer the question one way or the other.

Findings by Rudich and Razborov brought decades of work to find such a proof to a screeching halt. In a paper presented at the Symposium on Theory of Computing in 1994 and published in 1997 in the Journal of Computer and System Sciences, they showed that a wide class of proof techniques they call "natural proofs" can't solve the P vs. NP question. What's more, they found that those previous results turned out to have an almost contradictory double life, providing methods for breaking a wide class of cryptosystems.

That's not to say that a mathematical proof for P vs. NP is impossible, Rudich said, but it will have to be very different from the natural proofs that mathematicians had been employing.

To date, no one has convincingly devised such a proof, but Rudich is among those who are trying. "I've devoted my life to this question," he said. And if he can't solve it, he's convinced someone will. "I'm a big believer in human creativity."

Rudich is editor of the Journal of Cryptology and was selected by the Mathematical Association of America as Pólya Lecturer for the 2004–2005 and 2005–2006 academic years. An accomplished magician, he also serves as director of Andrew's Leap, a highly selective summer program for Pittsburgh-area high school students interested in math and science.

Razborov is an editor of the Theoretical Computer Science journal and was awarded the Nevanlinna Prize of the International Mathematical Union in 1990 for his contributions to complexity theory.

Source: Carnegie Mellon University