Prime Tests and Keeping Proofs Secret

Stanford, California. *On 29 July through 2 August, a group of computer scientists, mathematical physicists, and mathematicians met at Stanford University for a conference on Mathematics and Computers. It was a varied meeting—the talks ranged from the mathematics of chaos to a talk by the peripatetic Hungarian mathematician Paul Erdos on number theory problems that might be interesting to work on. In addition, software vendors set up shop, inviting investigators to bring their problems and try them on different systems.*

On the last day of the conference, when the talks were in the field of computational complexity—the difficulty of doing certain computer calculations—two new computer science tricks were presented and are recounted here.

The Theory of Computation Comes of Age

Testing for primes is one of the oldest mathematical problems, and it is, so far, impossible to solve—to find an easy and completely accurate test. But there are ways around this problem; for instance, two computer scientists described a new method that uses some very recent, very abstract mathematics. The method illustrates the changing nature of computer science research.

"In 1970, we were amateurs, living in fear that real mathematicians would come into the field and clean it up for us," says Leonard Adleman of the University of Southern California, who, along with his colleague Ming-Deh Huang, developed the new method. "As computer scientists, we really felt and probably were inferior."

"At first, we applied mathematics results from the 1800's," says Adleman. "Then we applied results from 1914. In the last few years we applied results from the 1950's." Now Adleman and Huang used the Fields Medal–winning result of Gerd Faltings of Princeton University, which was derived just 3 years ago and so is brand new as far as mathematicians are concerned (*Science*, 22 July 1983, p. 349).

Adleman and Huang decided to improve on a probabilistic test for primes that was developed about a decade ago by Michael Rabin of Harvard University and, independently, by Robert Solovay of the University of California at Berkeley and Volker Strassen of the University of Zurich. The idea was to circumvent the problem of testing to determine, for sure, whether a number is a prime. There is no short and simple way to do this, but these researchers did find a method that provides an almost certain answer. In particular, they found a mathematical test that either proves a number is not a prime or says that it has a 50% chance of being a prime.

To explain this test, Adleman provides an analogy. "Suppose you walk up with a number, say it is 1001. On the shelf is a bucket labeled 1001 that is filled with balls that are either all red or all black. You can reach your hand in the bucket to take out balls, but you can't look. If 1001 is a prime, all the balls in the bucket are red. If it is not prime, at least half of the balls are black and the rest are red. So you reach in the bucket and get a ball. If it's black, you're done. But it might be red. If it is, you reach in again. If it's black, you're finished, but if it is red again, you reach in again. If you reach in 100 times and pull out 100 red balls, it could be that you are astronomically unlucky and that 1001 is not a prime. But, most probably, 1001 is prime."

This method, says Adleman, is accurate enough to be useful for many practical purposes, such as cryptography. However, he says, "we would like to have an algorithm. We want a proof that a number is prime." As a step in that direction, he and Huang bring in a second bucket, this time one with green and yellow balls. If 1001 is not prime—if it is composite—all the balls in the bucket labeled 1001 are green. If it is prime, at least half of the balls are yellow. It is the reverse of the first bucket.

The game now is to reach in the bucket with red and black balls and see if the ball is black, which would prove that the number is not a prime. If you are uncertain because you got a red ball, then you can try the new bucket to see if you pull out a yellow ball, thereby proving that the number is in fact a prime. Of course, you can end up with a sequence of red balls pulled from the first bucket and green balls from the second, but the addition of the second bucket greatly increases your chances of getting a definitive answer.

In making up the mathematical analog of the new bucket with green and yellow balls, Adleman and Huang use mathematics from the theory of Abelian varieties, a subject in number theory. "Abelian varieties live in the complex numbers but they have images in finite fields," says Adleman. "It turned out that the only way to really propel the Abelian varieties into finite fields was to use Faltings' result."

Adleman and Huang's 100-page proof of their prime-testing method is made up of 75 pages on the theory of Abelian varieties and only 25 pages of computer science theory. The abstract number theory was necessary, says Adleman, "to show the bucket has the right number of green and yellow balls."

The work by Adleman and Huang is currently the best that can be done to test for primes quickly. Since it is still a probabilistic method, says Adleman, "it raises the issue of when do you want to think you're done."

The reliance on Abelian varieties demonstrates not only the growing sophistication of computer science but also the interrelatedness of mathematical fields. "It is strange that the theory of Abelian varieties—the highest pinnacle of mathematics—hooks up to testing for primes—this most ancient math problem," Adleman remarks.

How to Keep Your Proof A Secret and Yet Convince Your Colleagues That You Have a Proof

Suppose you discover a proof of a major math problem. You want to get credit, yet you do not want to reveal the details of the proof before it is accepted by a journal. Manuel Blum of the University of California at Berkeley has the solution to your problem. His method, which at the moment is regarded by the computer science community as a clever trick, was described at the meeting by his colleague Richard Karp.

Blum's result is an application of the discovery, about 1 year ago, of so-called zero knowledge proofs. Shafi Goldwasser and Silvio Micali of the Massachusetts Institute of Technology and Charles Rackoff of the University of Toronto showed that, in principle, it is possible to convey that a theorem is proved without providing any details. The person who hears the proof is convinced the theorem is true but cannot convince anyone else. Then, a few months ago, Oded Goldreich of Israel's Technion University, Micali, and Avi Wigderson of the Hebrew University of Jerusalem showed

how to do a zero knowledge proof for any of a class of very difficult problems called NP. Now Blum showed how to do it for any math theorem at all.

Blum's idea is to make use of a fact that is well known to computer scientists: Every mathematical theorem can be converted to a graph—a set of points connected by lines—in such a way that if you actually have a proof of that theorem, you can also find in that graph a Hamiltonian circuit, which is a way of connecting the points so that you go through each point only once and then return to where you started from. Given a proof, you can quickly find a Hamiltonian circuit, and, given a Hamiltonian circuit, you can quickly find the proof. But because these graphs are incredibly complex jumbles of points and lines, it is virtually impossible to find a Hamiltonian circuit simply by inspection of the graph.

So the theorem prover would start out by converting his proof to a graph with a Hamiltonian circuit. He would then scramble the vertices by renaming them in a random way and draw the equivalent Hamiltonian circuit in his scrambled graph. Next, he would put each pair of vertices from his scrambled graph into separate boxes. In each box, along with a pair of vertices, would be either the number 1, indicating that those vertices are connected in the graph, or 0, indicating that they are not.

Now a skeptic comes by and asks to be convinced that the theorem prover actually has a proof. The prover tells the skeptic he has two choices. Either he can see the original graph and the scrambled graph or he can open a certain subset of the boxes that would allow him to see for himself that the scrambled graph, and thus the original, has a Hamiltonian circuit.

If the skeptic chooses the first option, he can verify that the prover is honest and did not cheat when he scrambled the graph. But he will not know the Hamiltonian circuit. If he chooses the second option, he can see that there really is a Hamiltonian circuit, but he will not know how or even if the original graph was scrambled and so he will not be able to go from the points making up a Hamiltonian circuit of the scrambled graph to the circuit in the original graph.

This game can continue as many times as is necessary before the skeptic is convinced. Each time, the prover would rescramble the original graph and offer the skeptic the same two options. "The theorem prover might get lucky and get away with cheating on a single trial, but if he comes through in a long series of trials, the skeptic would know that he could not be cheating and he must have the proof," Karp remarks. ■

GINA KOLATA

Briefing:

Mars Is Getting Wetter and Wetter

Ever since 1971 when the first spacecraft to orbit Mars sent back pictures of strikingly familiar though ancient valleys, planetary scientists have been trying to fathom the role that water has played in shaping a planet boasting huge channels, ancient catastrophic floods, and winding, braided drainage systems. At a symposium last month on the climate and atmosphere of Mars* held at the National Air and Space Museum, experts who have been poring over 5- and 10-year-old images from the Viking orbiters reported still more reasons to require water on the martian surface in the past, including a possible ancient sea, larger than ever estimates of the amount of water involved, and places large enough to store all that water below the now dry surface.

Suggested water-related features described at the symposium ranged from 2.6-kilometer-high volcanic edifices formed entirely beneath glacial ice to landslides that traveled 250 kilometers thanks to lubrication by the ice they carried. One of the most provocative suggestions, an ancient lake or sea, came from Timothy Parker and his colleagues at the Jet Propulsion Laboratory (JPL). They began their study of Viking images looking for the final resting place of sediments gouged away by the catastrophic currents whose flows approached 20 million cubic meters per second as they formed the 1000-kilometer-long outflow channels. But Parker, who had studied the shoreline deposits of Lake Bonneville, recognized something familiar—a variety of near-shore features around the smooth, low-lying northern plains.

Parker and his colleagues built their argument for ancient seas on three image mosaics. Viking images having typical resolution could not reveal an actual shoreline, which would be too narrow, but they do show features resembling those near the shores of terrestrial seas. Arcing ridges divide smooth plain and rougher, knobby terrain, sometimes enclosing higher standing massifs or linking isolated knobs, much the way offshore, wave-generated barriers link islands. A crater has been eroded to a string of debris-aproned knobs, in places linked by curvilinear ridges, that could have been cut by waves or wasted away by a rising sea. An area of fretted terrain—uplands cut by canyon-like lowlands—shows signs of progressive intrusion and alteration from south to north, including possible strandlines marking high-water stands.

The JPL group's "hypothetical lakes or a shallow sea or ocean" may have encompassed 10 to 15% of the planet's surface and a good portion of the northern plains 2 to 3 billion years ago, Parker says. He estimates that the water would have been about 100 meters deep or less, making the sea's volume equivalent to a layer about 10 meters deep covering the globe. Initial objections raised at the symposium included the possibility that lava rather than water formed some of the features and that any sea that young would need to have been frozen through. Much image analysis remains to be done, especially the difficult task of determining whether strandline-like features are all at the same altitude.

Such a sea by itself would equal all the water that geochemists allowed the whole planet on the basis of early post-Viking calculations, but Michael Carr of the U.S. Geological Survey (USGS) in Menlo Park reported that his latest estimates of the amount of water hidden beneath the surface are at least several times as large. By analogy with the moon, the upper 2 to 3 kilometers of Mars is assumed to be broken into rubble and porous soil capable of storing ice, water, or brine. Stephen Clifford of the Lunar and Planetary Science Institute in Houston estimated that this megaregolith has the capacity to hold water equivalent to a global layer 200 to 500 meters deep. The trick is to determine how much of that capacity is actually filled.

Carr checked the level of the subterranean martian water reservoir by looking at places where it had been opened to view. Debris falling off the canyon walls of the fretted terrain flows away as if it were lubricated. An obvious possible lubricant is ice that more than fills the pores of the debris. Because these canyons cut into the crust more than a kilometer, the reservoir of frozen water would seem to be at least a kilometer thick. Old craters at high latitudes seem to be fading away by the same ice-assisted degradation. The outflow channels also gave a measure of subsurface water, the presumed source of the channels themselves, if it is assumed that the volume of water that flowed through the channels at least equaled the volume of rock and soil removed to form them. All told, Carr finds at least 400 meters of water and that is "an extremely conservative estimate." One kilometer is possible. That hardly rivals Earth's nearly 3-kilometer storehouse, but it gives Mars experts plenty of water to shape the planet in every way so far imagined. ■ RICHARD A. KERR

*Symposium on Mars: Evolution of Its Climate and Atmosphere, held 17–19 July in Washington, DC. Extended abstracts available from Lunar and Planetary Institute, 3303 NASA Road One, Houston, TX 77058.