MATHEMATICS

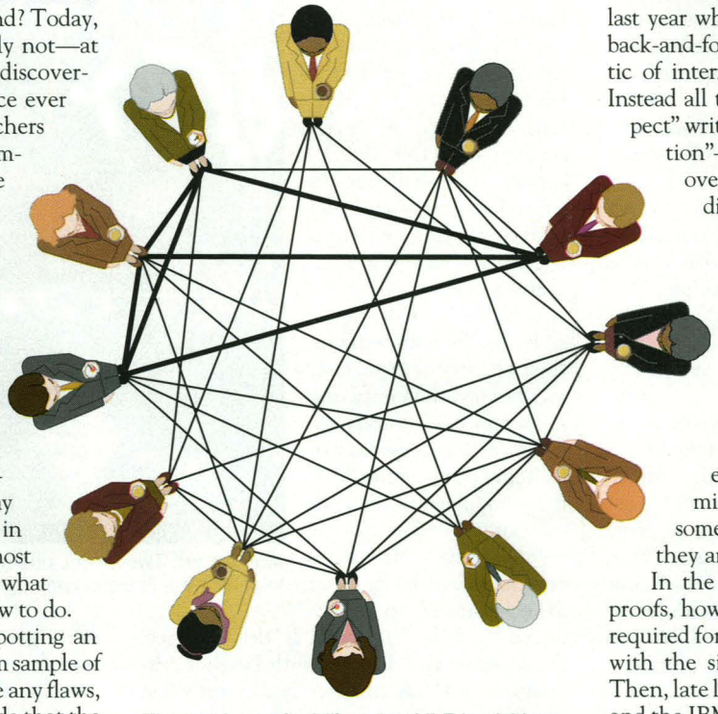
'Transparent' Proofs Help Solve Opaque Problems

Imagine a tired judge who's been handed a stack of legal papers and then been asked for his ruling. Instead of reading the complex briefs carefully from beginning to end, the judge thumbs through them idly, reading a line here and a line there. After a few minutes, he sets the papers aside and renders judgment. Grounds for a reprimand? Today, yes. But in the future, conceivably not—at least not if repercussions of recent discoveries in theoretical computer science ever reach the halls of justice. Researchers in the field of computational complexity have found a way that one computer can—at least in principle—quickly judge the logical correctness of another computer's long-winded computational solution to a problem by asking for an even longer version and them simply spot checking what amounts to a deposition on a disk.

The trick is that the requested deposition—or "transparent proof," to use the new theory's parlance—must be written in such a way that any mistake or inconsistency in the original solution shows up almost everywhere in the deposition. That's what researchers have now found out how to do. Since there's a good chance of spotting an error wherever you look, if a random sample of the transparent proof fails to expose any flaws, the reader can confidently conclude that the purported solution is correct—beyond, as they say, any reasonable doubt. Researchers have now shown that transparent proofs can be written in such a way that a small number of spot checks will produce a high degree of confidence no matter how long or complex the original solution.

That finding has some interesting implications, both in the real world and in the world of mathematical theory. In the real world, techniques based on transparent proofs could be used to identify "smart cards" for transactions like drawing money out of bank accounts—somewhat in the manner of an expanded personal identification number. And in the world of theory, mathematicians have already found a surprising result: Many computational problems are no easier to solve in an approximate form than they are in an exact form. This implication came as "a big shock" to complexity theorists, says Lance Fortnow of the University of Chicago.

The "shock" now rippling through the mathematics community is the result of a bit of serendipity. At the heart of the story of these latest results is a tale of how work in one area detoured into another. One strand of the work originated 2 years ago, when Laszlo Babai, Fortnow, and Carsten Lund at the University of Chicago determined the full range of power



The mathematical "in crowd." Friendships between people at a party are indicated by line segments. Heavy lines indicate a "clique" of people all of whom know each other. But is there a bigger clique hidden somewhere in this crowd? All known mathematical methods for finding the largest clique rapidly become unwieldy for large gatherings.

ILLUSTRATION: J. CHERRY

of a precursor to transparent proofs, a technique called multiprover interactive proofs. Unlike ordinary mathematical proofs, which guarantee the correctness of a solution by a strict line of logical reasoning, interactive proofs use random questioning to probe for weaknesses in a purported solution. The single-prover version, which was introduced in 1985 by Shafi Goldwasser and Sylvio Micali at MIT, and Charles Rackoff at the University of Toronto, can be likened to a police interrogator trying to shake a suspect's alibi. Multiprover interactive proofs could be compared to an interrogation of two suspects who have been separated for questioning.

Intuitively, it would seem that the multiprover technique should be more powerful than the single-prover proofs—and that turns out to be correct. In late 1989, complexity theorists proved that single-prover interactive proofs could be used to verify the solution to any problem in a large class of computational problems called PSPACE (*Science*, 1 June 1990, p. 1079). Shortly thereafter, Babai, Fortnow, and Lund showed that multiprover interactive proofs could be used to verify solutions to problems in an even larger class called NEXP. "This is a class [of problems] you wouldn't even dream of approaching computationally—and still verification is possible," remarks Babai.

The next big step forward in the story came last year when researchers realized that the back-and-forth interaction that is characteristic of interrogations isn't strictly necessary. Instead all that's needed is to have the "suspect" write out a full and elaborate "deposition"—a complete account that goes over the details of an alibi in so many different ways that only a completely honest suspect can put together a consistent story. In joint work with Leonid Levin at Boston University and Mario Szegedy at the University of Chicago, Babai and Fortnow showed that each and every formal mathematical proof can be rewritten in this kind of transparent form, in which errors are virtually impossible to miss—all you need to do is sample some of the details and see whether they are consistent.

In the first incarnation of transparent proofs, however, the number of spot checks required for verification grew (albeit slowly) with the size of the proof to be checked. Then, late last year, Shmuel Safra at Stanford and the IBM Almaden Research Center and Sanjeev Arora, a graduate student at the University of California at Berkeley, made a significant modification in the theory that reduced the amount of spot checking to a level that grew far more slowly. And most recently, Arora, fellow graduate student Madhu Sudan, Rajeev Motwani at Stanford, and Lund and Szegedy, who are now at AT&T Bell Laboratories, have made further modifications that lower the amount of spot checking to a level that stays constant regardless of the size of the problem.

Our mutual friends. Surprisingly, these modifications in the theory of transparent proofs and the improvements in the spot-checking requirements were motivated by a second line of research, which initially appeared to be entirely unrelated. It is based on a longstanding question in complexity theory: Is it any easier to solve a particular computational problem approximately than it is to get an exact answer? In joint work last year with Uri Feige and Laszlo Lovasz at Princeton University and Goldwasser at MIT, Safra and Szegedy proved

that the answer to that question, at least for one important computational problem, is no. The kicker was that they did so using the theory of interactive proofs.

The problem they looked at is a counting problem in graph theory known as the "maximum clique problem." It can be described as the task of identifying the largest group of people who all know each other at a large party. Given any particular subgroup, it's easy enough to check whether they're all mutual friends. But the number of possible groups to consider increases exponentially with the size of the party, a pattern that makes finding the largest clique a daunting prospect.

Feige and his colleagues observed that separate statements in an interactive or transparent proof can be thought of as people at a party, with two statements being "friends" if they don't contradict one another. From this, they were able to show that any algorithm for estimating maximum clique size would, with just a small amount of extra work, make it possible to solve a large class of other problems—including the clique problem itself—exactly.

The modification by Safra and Arora removed the need for any extra work in obtaining exact solutions. In essence, they found that if there is an efficient way to solve the maximum clique problem approximately, then, in the lingo of computer science, P=NP. This equation—which no one believes is true—is considered the central question in complexity theory. Roughly speaking, P is the class of all problems that can be solved by an efficient algorithm. The class NP, on the other hand, contains thousands of problems for which no efficient algorithms are known. Since P is unlikely to equal NP, the proposition that gave rise to that result (that there is a way to solve the maximum clique problem efficiently in an approximate fashion) is probably false.

Interchangeable parts. The further modification by Arora *et al.* extended the connection between interactive proofs and approximation problems beyond the clique problem. For this they used work of Christos Papadimitriou at the University of California at San Diego and Mikalis Yannakakis at Bell Labs. Papadimitriou and Yannakakis had identified a class of problems that could be written in such a way that their approximate solutions were interchangeable. Arora and his colleagues appropriated one of these problems and proved that, like the clique problem, if it could be solved efficiently in approximate fashion, then P=NP. As a result, the dubious equation P=NP would be true if any of a vast number of problems have efficient approximation algorithms. The clear implication: These problems probably can't be solved efficiently by approximation.

The recent results are still being assimilated by the computer science community, and researchers aren't sure what other surprises might be in store. Enthuses Arora: "This is opening up a whole lot of directions." One new direction lies in finding out whether transparent proofs can be shortened to a practical length (so they could fit onto a "smart card," for example). Another is to find the precise limits of approximation techniques, since the recent results don't rule out approximations in all cases but place limits on the accuracy that can be attained by efficient algorithms. But aside from new research directions, some of the pleasure the math community is deriving from these findings is simply the astonishment that two apparently unrelated areas of mathematics could suddenly coincide.

–Barry Cipra

ASTROPHYSICS

Sightseeing at a Black Hole Gets Easier

As any science fiction buff knows, diving into a black hole means a quick and messy death. According to the standard scenario, tidal forces—the same phenomena that produce the earth's tides, but infinitely stronger—would stretch out both rocket ship and occupants like taffy, pulling them apart long before they reached the core of the black hole.

But now sci-fi writers—not to mention theoretical astrophysicists—may have to redo their scripts. Caltech's Amos Ori reports in the 6 April *Physical Review Letters* that the approach to a giant black hole's inner core should actually be quite peaceful. Indeed, a space traveler should be able to proceed comfortably all the way to the singularity that lurks near the center of the black hole. At that point, though, things could get quite nasty—although, to be honest, science still hasn't a clue about what would happen: total destruction, passage to a new universe, or perhaps something that no one, not even science fiction authors, has yet imagined.

What new understanding tamed the ride in? Scientists have studied and speculated about black holes for decades, and their essence is well known: A massive star collapses in upon itself, creating a gravitational pull so intense that nothing, not even light, can escape once it gets within the black hole's "event horizon"—the point where, as astrophysicist Werner Israel of the Canadian Institute for Advanced Research in Edmonton, Alberta, describes it, you've reached "the last outpost from which you can send news to the outside world [since no information can exit from inside the event horizon]." So much was a given, but Ori, expanding on work by Israel and his student Eric Poisson, showed that if the black holes were very old and very large—hundreds of millions of suns in mass, such as the black hole thought to be at the center of our galaxy—the tidal forces would be so small that a traveler would not even feel them as he came right up to the "inner boundary." That's "the last place you can receive news from outside," says Israel: Past the inner boundary (assuming there is anything past it), the outside universe disappears.

Ori arrived at his conclusion working from the Kerr model of a rotating black hole, which assumes the black hole to be perfectly symmetric and featureless—and thus easy to analyze mathematically, but physically unrealistic. He then added perturbations to the model to make it more realistic. Israel and Poisson had already shown that once the perfect symmetry of the Kerr model was lost, tiny perturbations would be infinitely amplified at the inner boundary, causing space there to be infinitely curved. But Ori found that outside the inner boundary, conditions would be surprisingly smooth. The result has astounded some astrophysicists, such as Caltech's Kip Thorne, who calls the calculated tidal forces "disturbingly gentle."

That doesn't mean it's time to book a ticket for the next black hole express, however. Israel, for instance, suspects that even if the tidal forces don't rub out a singularity sightseer, the concentrated radiation near the boundary would. Ori, on the other hand, doesn't think that's a problem. Although there is an infinite amount of energy at the boundary, his analysis finds that an observer diving into the boundary would be moving so quickly that he would be exposed to only a small part of it.

Even so, it would be a wild ride. Here's how Israel envisions the tour: If an intrepid space traveler were to pass through the event horizon and head for the inner boundary, events in the outside universe would appear to move faster and faster, Israel says, and in the few seconds or minutes before hitting the inner boundary, "the entire future of the outer universe is flashed before your eyes."

Then comes the real enigma: what happens at the inner boundary? In the simple Kerr model, passing through the boundary leads to another universe, and Ori holds out hope that this could still be true for real black holes. Others, such as Thorne, think such speculation is best left for science fiction. But there is general agreement on two points: Past the inner boundary (assuming there is anything past it), the outside universe disappears, and general relativity does not hold the answer to what would happen at the boundary and beyond. It remains for the much sought-after theory of quantum gravity, or perhaps some as yet undreamed-of theory, to reveal the secrets at the heart of the black hole.

–Robert Pool