10-year-old problem in theoretical computer science falls

July 30 2012, by Larry Hardesty

Thomas Vidick. Photo: M. Scott Brauer

(Phys.org) -- Interactive proofs, which MIT researchers helped pioneer, have emerged as one of the major research topics in theoretical computer science. In the classic interactive proof, a questioner with limited computational power tries to extract reliable information from a computationally powerful but unreliable respondent. Interactive proofs are the basis of cryptographic systems now in wide use, but for computer scientists, they're just as important for the insight they provide into the complexity of computational problems.

Twenty years ago, researchers showed that if the questioner in an interactive proof is able to query multiple omniscient respondents — which are unable to communicate with each other — it can extract information much more efficiently than it could from a single

respondent. As quantum computing became a more popular research topic, however, computer scientists began to wonder whether such multiple-respondent — or "multiprover" — systems would still work if the respondents were able to perform measurements on physical particles that were "entangled," meaning that their quantum properties were dependent on each other.

At the IEEE Symposium on Foundations of Computer Science in October, Thomas Vidick, a postdoc at MIT's Computer Science and Artificial Intelligence Laboratory, and Tsuyoshi Ito, a researcher at NEC Labs in Princeton, N.J., finally answer that question: Yes, there are multiprover interactive proofs that hold up against entangled respondents. That answer is good news for cryptographers, but it's bad news for quantum physicists, because it proves that there's no easy way to devise experiments that illustrate the differences between classical and quantum physical systems.

It's also something of a surprise, because when the question was first posed, it was immediately clear that some multiprover proofs were not resilient against entanglement. Vidick and Ito didn't devise the proof whose resilience they prove, but they did develop new tools for analyzing it.

In an interactive proof, a questioner asks a series of questions, each of which constrains the range of possible answers to the next question. The questioner doesn't have the power to compute valid answers itself, but it does have the power to determine whether each new answer meets the constraints imposed by the previous ones. After enough questions, the questioner will either expose a contradiction or reduce the probability that the respondent is cheating to near zero.

Multiprover proofs are so much more efficient than single-respondent proofs because none of the respondents knows the constraints imposed

by the others' answers. Consequently, contradictions are much more likely if any respondent tries to cheat.

But if the respondents have access to particles that are entangled with each other — say, electrons that were orbiting the same atom but were subsequently separated — they can perform measurements — of, say, the spins of select electrons — that will enable them to coordinate their answers. That's enough to thwart some interactive proofs.

The proof that Vidick and Ito analyzed is designed to make cheating difficult by disguising the questioner's intent. To get a sense of how it works, imagine a graph that in some sense plots questions against answers, and suppose that the questioner is interested in two answers, which would be depicted on the graph as two points. Instead of asking the two questions of interest, however, the questioner asks at least three different questions. If the answers to those questions fall on a single line, then so do the answers that the questioner really cares about, which can now be calculated. If the answers don't fall on a line, then at least one of the respondents is trying to cheat.

"That's basically the idea, except that you do it in a much more high-dimensional way," Vidick says. "Instead of having two dimensions, you have 'N' dimensions, and you think of all the questions and answers as being a small, N-dimensional cube."

This type of proof turns out to be immune to quantum entanglement. But demonstrating that required Vidick and Ito to develop a new analytic framework for multiprover proofs.

According to the weird rules of quantum mechanics, until a measurement is performed on a quantum particle, the property being measured has no definite value; measuring snaps the particle into a definite state, but that state is drawn randomly from a probability

distribution of possible states.

The problem is that, when particles are entangled, their probability distributions can't be treated separately: They're really part of a single big distribution. But any mathematical description of that distribution supposes a bird's-eye perspective that no respondent in a multiprover proof would have. Finding a way to do justice to both the connection between the measurements and the separation of the measurers proved enormously difficult. "It took Tsuyoshi and me about a year and a half," Vidick says. "But in fact, one could say I've been working on this since 2006. My very first paper was on exactly the same topic."

Provided by Massachusetts Institute of Technology