Quantum Probabilistically Checkable Proofs

- Unproven
- Classical PCP proven

Classical PCP (or just PCP)

The New York Times

TUESDAY, APRIL 7, 1992

their power to force their young sons to leave their mates and return with their parent to help raise another brood.

New Short Cut Found For Long Math Proofs

A proof can be tested by checking just a part, inventors say.

By GINA KOLATA

IN a discovery that overturns centuries of mathematical tradition, a group of graduate students and young researchers has discovered a way to check even the longest and most complicated proof by scrutinizing it in just a few spots.

The finding, which some mathematicians say seems almost magical, depends upon transforming the set of logical statements that constitute a proof into a special mathematical form in which any error is so amplified as to be easily detectable.

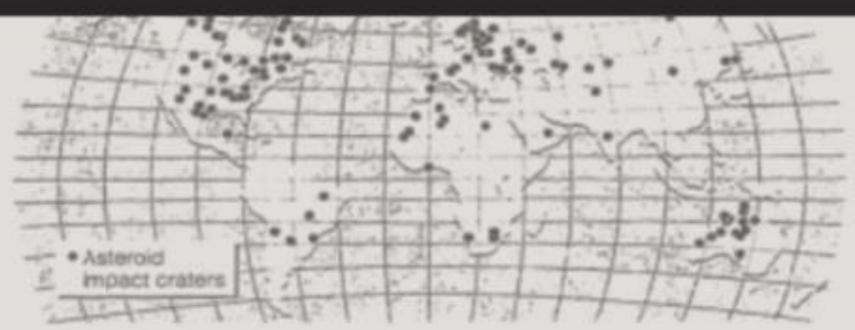
Using this new result, the researchers have already made a landmark discovery in computer science. They showed that it is impossible to compute even approximate solutions for a large group of practical problems that have long foiled researchers. Even that negative finding is very significant, experts say, because in mathematics, a negative result, showing something is impossible, can be just as important and open just as many new areas of research as a positive one.

The discovery was made by Sanjeev Arora and Madhu Sudan, graduate students at the University of California at Berkeley, Dr. Rajeev Motwani, an assistant professor at Stanford University, and Dr. Carsten Lund and Dr. Mario Szegedy, young computer scientists at A.T.&T. Bell Laboratories. Dr. Motwani, who is the senior member of the group, just turned 30 on March 26.

"With the conventional notion of a proof, you had to check it line by line," said Dr. Michael Sipser, a theoretical computer scientist at the Massachusetts Institute of Technology. "An error might be buried on page 475, line 6. A 'less than or equal to' should have been a 'less than.' That would totally trash the whole proof. But you'd have to dig through the whole thing to find it," Dr. Sipser said. Now, he added, "the new idea is that there is a way to transform any proof so that if there is an error, it appears almost everywhere. I'd say, 'You have a proof? Show me a page.' If there is an error, it will be there."

The finding, which is built on two and a one half years work by leading

Continued on Page C10



man of the study by nearly 100 scientists, said in an interview.

Skeptics disagree, dismissing the asteroid hazard as ridiculously small and belittling the NASA team as either laughably paranoid or, worse yet, conspiring for a lifetime of entitlements for astronomers and would-be makers of interceptors. What could be more suspicious, cynics ask, than astronomers offering to save the Earth from a cosmic disaster with just a few new telescopes?

In an editorial, The Washington Times scorned the NASA team's plan as a "scam to make away with taxpayers' money," adding that "there's no evidence that anyone in all of human history has ever been killed by an asteroid."

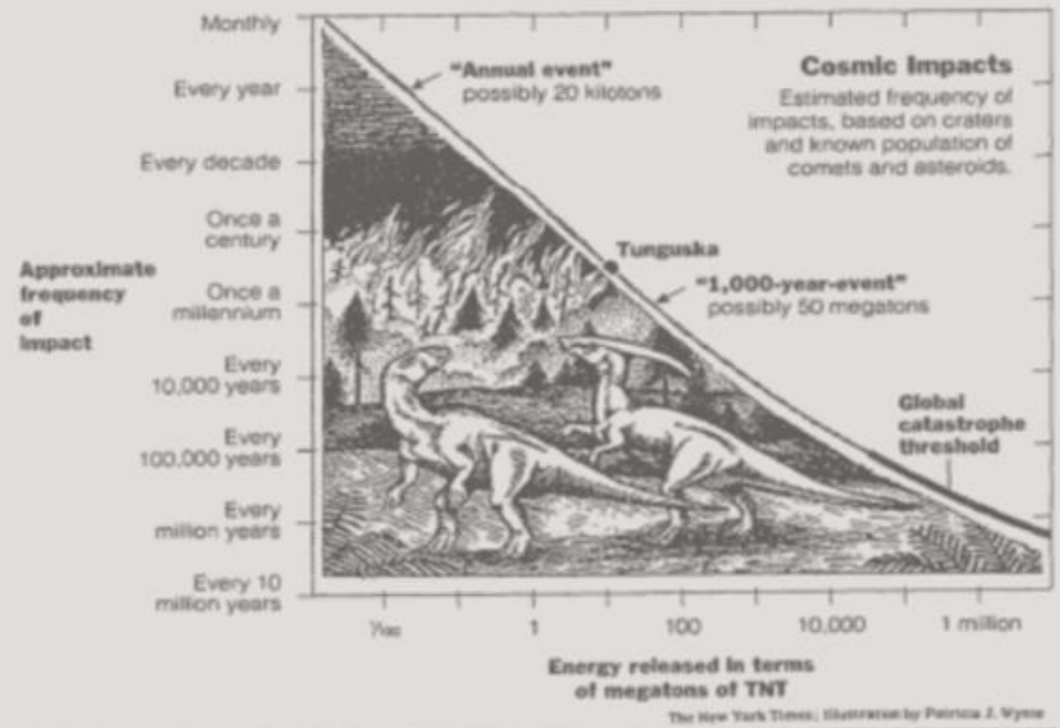
Continued on Page C7

0.62 miles and larger
Asteroids of this size are believed able to disrupt life on Earth because of the large amount of dust they throw into the atmosphere, changing the climate for years, maybe decades. They are estimated to strike land masses once every 300,000 years or so. The severity of the global effects increases with the asteroid's size, and in the modern world would at some point lead to widespread crop failures and starvation.

6.21 miles to 9.31 miles
About 65 million years ago, an asteroid of this size is believed by many scientists to have slammed into the Caribbean basin near present-day Mexico. It is the leading candidate for the asteroid presumed to have killed off the dinosaurs and 60 percent of all the Earth's life forms at that time.

Source: "The Spaceguard Survey," (NASA International Near-Earth-Object Detection Workshop).

The New York Times



The New York Times; illustration by Patricia J. Wynne

MUSIC
A concert honors German Resistance heroes of World War II. Page C13.

LITERATURE
In Dublin, some of James Joyce's papers go on display for the first time. Page C13.

DANCE
An unchastened Mark Morris returns to New York. Page C13.

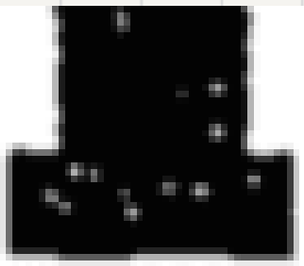
Original statement of PCP

.Any language in NP can be verified, up to a **constant** probability of error, by a randomised polynomial-time verifier who only reads a **constant** number of randomly chosen bits from a **polynomial-size** proof

Original statement of PCP

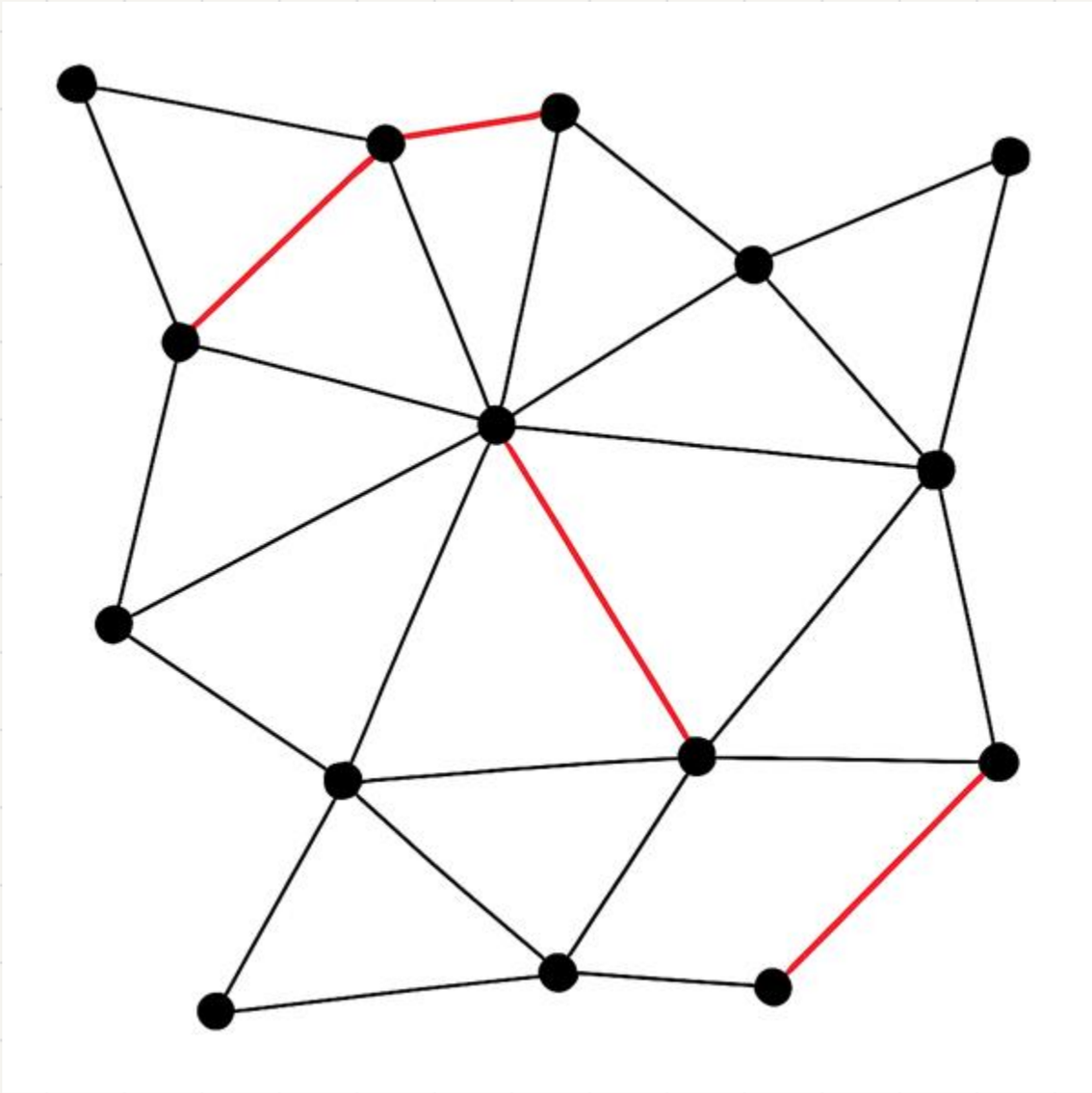
- (a v b) ^ (~a v c) ^ (~b v ~d) ^ ….
- a = 0, b = 1, c = 1, d = 1
- Verified by reading a **constant** number of bits in a **polynomial** length proof

Original statement of PCP



dition, a group of graduate students and young researchers has discovered a way to check even the longest and most complicated proof by scrutinizing it in just a few spots.

Original statement of PCP



Gap statement of PCP

- the PCP theorem states that it is NP-hard to distinguish between the cases when an instance of 2-CSP is completely satisfiable, or when no more than 99% of its constraints can be satisfied
- Approximation is hard

Equivalence of original statement and gap view

- any language in NP can be verified, up to a constant probability of error, by a randomized polynomial-time verifier who only reads a constant number of (randomly chosen) bits from a polynomial-size proof
- it is NP-hard to distinguish between the cases when an instance of 2-CSP is completely satisfiable, or when no more than 99% of its constraints can be satisfied

Putting the q in qPCP

- NP → QMA
- CSP → Local Hamiltonian
- Constraint → k-local Hermitian
- Number of constraints violated → ground state energy

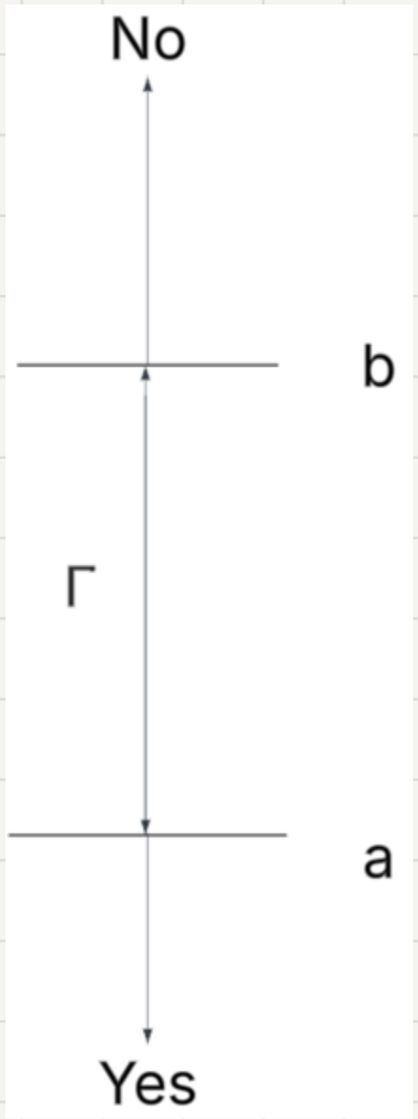
QMA recap

Definition 1.2 (The complexity class QMA) *A language $L \subseteq \{0,1\}^*$ is in* QMA *if there exists a quantum polynomial time algorithm V (called the* verifier*) and a polynomial $p(\cdot)$ such that:*

- *$\forall x \in L$ there exists a state $|\xi\rangle$ on $p(|x|)$ qubits such that V accepts the pair of inputs $(x, |\xi\rangle)$ with probability at least $2/3$.*
- *$\forall x \notin L$ and for all states $|\xi\rangle$ on $p(|x|)$ qubits, V accepts $(x, |\xi\rangle)$ with probability at most $1/3$.*

qPCP gap view

- Increases the absolute promise gap to be proportional to the number of “constraints”



qPCP gap view

$$\Gamma = \Omega(1/poly(m)) \rightarrow \Gamma = \Omega(m)$$

qPCP proof verification view

Conjecture 1.4 (Quantum PCP by proof verification) *For any language in* QMA *there exists a polynomial time quantum verifier, which acts on the classical input string x and a witness $|\xi\rangle$, a quantum state of poly$(|x|)$ qubits, such that the verifier accesses only $\mathcal{O}(1)$ qubits from the witness and decides on acceptance or rejection with constant error probability.*

qPCP proof verification view

- Verifier → quantum verifier
- Witness → quantum witness
- O(1) bits sampled → O(1) qubits sampled
- Last we'll see of this view…

qPCP proof verification view

- Verifier → quantum verifier
- Witness → quantum witness
- O(1) bits sampled → O(1) qubits sampled
- Last we'll see of this view…