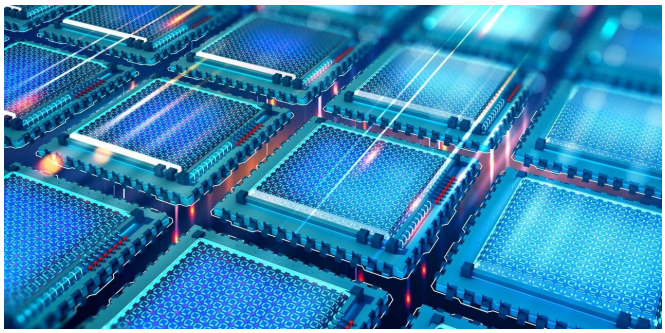
Major quantum computational breakthrough is shaking up physics and maths

17 August 2020, by Ittay Weiss



Quantum computers may be more trustworthy. Credit: Yurchanka Siarhei/Shutterstock

MIP* = RE is not a typo. It is a groundbreaking discovery and the catchy title of a recent paper in the field of quantum complexity theory. Complexity theory is a zoo of "complexity classes"—collections of computational problems—of which MIP* and RE are but two.

The 165-page paper shows that these two classes are the same. That may seem like an insignificant detail in an abstract theory without any real-world application. But physicists and mathematicians are flocking to visit the zoo, even though they probably don't understand it all. Because it turns out the discovery has astonishing consequences for their own disciplines.

In 1936, Alan Turing showed that the Halting Problem—algorithmically deciding whether a computer program halts or loops forever—cannot be solved. Modern computer science was born. Its success made the impression that soon all practical problems would yield to the tremendous power of the computer.

But it soon became apparent that, while some problems can be solved algorithmically, the actual computation will last long after our Sun will have engulfed the computer performing the computation. Figuring out how to solve a problem algorithmically was not enough. It was vital to classify solutions by efficiency. Complexity theory classifies problems according to how hard it is to solve them. The hardness of a problem is measured in terms of how long the computation lasts.

RE stands for problems that can be solved by a computer. It is the zoo. Let's have a look at some subclasses.

The class P consists of problems which a known algorithm can solve quickly (technically, in polynomial time). For instance, multiplying two numbers belongs to P since long multiplication is an efficient algorithm to solve the problem. The problem of finding the prime factors of a number is not known to be in P; the problem can certainly be solved by a computer but no known algorithm can do so efficiently. A related problem, deciding if a given number is a prime, was in similar limbo until 2004 when an efficient algorithm showed that this problem is in P.

Another complexity class is NP. Imagine a maze. "Is there a way out of this maze?" is a yes/no question. If the answer is yes, then there is a simple way to convince us: simply give us the directions, we'll follow them, and we'll find the exit. If the answer is no, however, we'd have to traverse the entire maze without ever finding a way out to be convinced.

Such yes/no problems for which, if the answer is yes, we can efficiently demonstrate that, belong to NP. Any solution to a problem serves to convince us of the answer, and so P is contained in NP. Surprisingly, a million dollar question is whether P=NP. Nobody knows.

Trust in machines

The classes described so far represent problems

faced by a normal computer. But computers are fundamentally changing—quantum computers are being developed. But if a new type of computer comes along and claims to solve one of our problems, how can we trust it is correct?

Imagine an interaction between two entities, an interrogator and a prover. In a police interrogation, the prover may be a suspect attempting to prove their innocence. The interrogator must decide whether the prover is sufficiently convincing. There is an imbalance; knowledge-wise the interrogator is in an inferior position.

In complexity theory, the interrogator is the person, with limited computational power, trying to solve the problem. The prover is the new computer, which is assumed to have immense computational power. An interactive proof system is a protocol that the interrogator can use in order to determine, at least with high probability, whether the prover should be believed. By analogy, these are crimes that the police may not be able to solve, but at least innocents can convince the police of their innocence. This is the class IP.

If multiple provers can be interrogated, and the provers are not allowed to coordinate their answers (as is typically the case when the police interrogates multiple suspects), then we get to the class MIP. Such interrogations, via cross examining the provers' responses, provide the interrogator with greater power, so MIP contains IP.

Quantum communication is a new form of communication carried out with qubits. Entanglement – a quantum feature in which qubits are spookishly entangled, even if separated—makes quantum communication fundamentally different to ordinary communication. Allowing the provers of MIP to share an entangled qubit leads to the class MIP^*.

It seems obvious that communication *between* the provers can only serve to help the provers coordinate lies rather than assist the interrogator in discovering truth. For that reason, nobody expected that allowing more communication would make computational problems more reliable and solvable. Surprisingly, we now know that $MIP^* = RE$. This means that quantum communication behaves wildly differently to normal communication.

Far-reaching implications

In the 1970s, Alain Connes formulated what became known as the Connes Embedding Problem. Grossly simplified, this asked whether infinite matrices can be approximated by finite matrices. This new paper has now proved this isn't possible—an important finding for pure mathematicians.

In 1993, meanwhile, Boris Tsirelson pinpointed a problem in physics now known as Tsirelson's Problem. This was about two different mathematical formalisms of a single situation in quantum mechanics—to date an incredibly successful theory that explains the subatomic world. Being two different descriptions of the same phenomenon it was to be expected that the two formalisms were mathematically equivalent.

But the new paper now shows that they aren't. Exactly how they can both still yield the same results and both describe the same physical reality is unknown, but it is why physicists are also suddenly taking an interest.

Time will tell what other unanswered scientific questions will yield to the study of complexity. Undoubtedly, $MIP^* = RE$ is a great leap forward.

Provided by The Conversation

APA citation: Major quantum computational breakthrough is shaking up physics and maths (2020, August 17) retrieved 18 September 2020 from https://phys.org/news/2020-08-major-quantum-breakthrough-physics-maths.html