

Q&A: Expert discusses how to realistically achieve quantum speedups beyond the hype





Compared to classical computers, quantum computers have advantages in computing speed when it comes to big computational problems on small amounts of data. Credit: ETH Zurich, Microsoft, ACM

In theory, quantum computers vastly outperform classical computers in terms of computing speed. For them to do so in practice, it is necessary to design more and novel high-speed algorithms, says ETH supercomputing specialist Torsten Hoefler.



ETH Zurich sat down with Hoefler to discuss his recent review article, published in *Communications of the ACM*

Quantum computers promise to be capable of solving some computational problems much faster than classical computers. To what extent is this true, or at least realistic?

Hoefler: In general, this statement is true. Quantum computers can indeed solve some computational problems fundamentally faster than classical computers do. I would say they really are capable to reduce the computational time from decades or years to hours or even minutes. Although this is true, it is not realistic for all <u>computational problems</u>.

For what problems are quantum computers not faster?

Hoefler: For example, if we want to make weather prediction or climate simulation much faster, then I wouldn't know by today how to accelerate these applications considerably with a quantum computer. In the same way, I wouldn't know how to significantly speed up machine learning with a quantum computer today. Also, for <u>fluid dynamics</u> in the turbulent regimes, we will most likely not achieve practical advantage with current quantum algorithms in the foreseeable future.

Do you see any areas of application in basic research or industry where quantum computers can display their advantages in the near future?

Hoefler: So far, we know for sure that quantum computing is extremely relevant to a huge range of research and development. I am thinking of



problems such as breaking the known cryptographic schemes based on prime factorization. Or, when it comes to simulating chemical systems at a very high precision, then quantum computing has an amazing impact potential.

Furthermore, quantum computing is very promising for research areas such as simulating material properties that are due to <u>quantum effects</u>, new medications for the future, inventing new fertilizers or understanding how biological systems work. In all these fields, quantum computers can play a crucial role to speed up computation time.

But this is still a vision for the future?

Hoefler: Yes, but even if quantum computing is not yet applicable to every open question in these fields, we clearly see a path towards how to better exploit the potential of quantum computers. But this is not true for all algorithms. You can't just take any algorithm, run it on a quantum computer and your computations become automatically faster. In principle, quantum computers might solve any computational problem, but the decisive question for their application is which problems do they practically solve faster or at lower cost than classical computers.

To what extent do you revise the assumption that quantum computers are always faster than classical computers?

Hoefler: Some people assume that quantum computers are fundamentally faster because they are capable to solve many problems in quadratically fewer steps. But a single quantum computational step is much slower than a classical one. Due to the principles of quantum mechanics such as superposition, interference or entanglement, fewer computational steps are necessary to solve a given problem. This is the



reason why quantum computers promise to solve certain problems faster than classical computers. Nevertheless, it would be a fallacy to believe that quantum computers may solve any problem supremely faster than conventional ones do.

Why is that?

Hoefler: Given the current design of quantum computation, each computational step will be slower than a corresponding classical one. This is due to the high complexity of error correction and other systems effects in quantum computation today. Furthermore, in conventional computing the industry has been driving the technologies since 60 years to an extent that they have become extremely fast. Today, a classical computer can execute millions up to billions of steps per second. A quantum computer on the other hand can only execute hundreds of thousands up to maybe millions of steps per second. For this reason, quantum computing is not inherently superior in every case. This misconception of an all-encompassing quantum supremacy is what we try to dispel. Nonetheless, I am very optimistic that we will build reliable quantum computers.

What scientific findings did you come to in your study? For what types of problems are quantum computers most likely to be faster?

Hoefler: We compared the performance of a market-leading classical chip to an optimistically designed quantum chip, each for the same problem. This way, we are the first to have identified what exactly is required for quantum computers to achieve real speed advantage. Our analysis shows that with pretty much all algorithms, the classical computer is faster for very small problem sizes and the quantum computer is faster for very large problem sizes.

This is because the time to solve certain problems on a quantum



computer grows more slowly with the size of the problems than on classical computers (see graphic). That's what we call quantum speedup. We also see that, in general, quantum computers are comparatively faster and more practical for "big compute" problems on small data, but they are not practical for big data problems.

Due to limitations of input and output bandwidth, big data is a problem which classical computer calculate faster. Furthermore, classical computers also solve a search problem in a database faster than a quantum computer. Therefore, <u>quantum computing</u> has been falsely hyped in the context of big data.

One of your findings is that 'quadratic speedup' is not good enough for quantum computers to really take advantage of their potential speedup advantages.

Hoefler: In our study we show that quadratic speedups, which reduce computation time by taking the square root of an algorithm's running time, are insufficient for practical quantum advantage in the foreseeable future. We see that if only quadratic speedup is implemented, then for many problems quantum computation will still take several months, which would be too slow and too expensive in practice.

From this, we derive that at least cubic or quartic speedups based on the third and fourth roots are required, because only then thousands or millions of computing operations are feasible. But even cubic or quartic speedups are only the lowest requirement. It is necessary to focus on exponential speedups, where the running time of the quantum algorithm is the logarithm of the running time of the classical algorithm. Therefore, the most promising candidates for achieving real practical quantum advantages are small-data problems with exponential speedup.



What needs to be done differently to eventually achieve true high-speed quantum computation?

Hoefler: One decisive key to realizing quantum speedup are more novel quantum algorithms. Without significant algorithmic improvements, a wide range of often-cited applications is unlikely to result in practical quantum advantage. From a practical perspective, most of the quantum algorithms we have today are not enabling real quantum speedups.

Even if we know that cubic, quartic, or exponential algorithms result in higher quantum speedups than quadratic algorithms, the real situation still is, that by today we just don't know many cubic or quartic speedup algorithms. Currently, many quantum speedup algorithms rely on quadratic quantum speedup, based on the well-known Grover algorithm.

We argue that designing more Grover style algorithms is not enough. For developing new quantum algorithms that really make a difference, algorithmic research needs to focus on algorithms that enable high quantum speedup in practice. Otherwise, quantum computers might not outperform the fastest devices of <u>classical computers</u>.

What is required from computer scientists to achieve real quantum speedup?

Hoefler: We need to invent novel high-speed quantum algorithms. The big challenge is that now we only have a handful of fundamental quantum algorithms, like Grover's algorithm or Shor's algorithm, which are widely used in chemistry or cryptography. Obviously, it is very difficult to develop new fundamental algorithms. Since quantum mechanics is a complex mathematical concept, understanding how to translate it into useful quantum algorithms is quite an undertaking. As a rule of thumb, a fundamental algorithm is developed about every decade.



What are next steps in the design of quantum algorithms, especially at ETH Zurich?

Hoefler: We need more computer scientists and mathematicians to research new quantum algorithms. So far, it's very hard to find excellent quantum algorithm scientists. A huge opportunity is to combine this need with ETH Zurich's teaching mission and to encourage the next generation of scientists to delve into quantum algorithm design. And to have a Quantum Center allows us to naturally cluster mathematicians, computers scientists around physicists and engineers to collaborate on quantum computers. This is the opportunity for ETH Zurich.

More information: Torsten Hoefler et al, Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage, *Communications of the ACM* (2023). <u>DOI: 10.1145/3571725</u>

Provided by ETH Zurich

Citation: Q&A: Expert discusses how to realistically achieve quantum speedups beyond the hype (2023, May 26) retrieved 28 April 2024 from <u>https://techxplore.com/news/2023-05-qa-expert-discusses-realistically-quantum.html</u>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.