
Contribution ID: **194** Type: **Plenary reports**

# From Quantum Speed-up to Supremacy and Advantage

*Wednesday 7 July 2021 09:00 (45 minutes)*

Quantum computing began in the early 1980s when physicist Paul Benioff constructed a quantum mechanical model of Turing machine and physicist Richard Feynman and mathematician YuriManin discussed the potential of quantum computers to simulate phenomena a classical computer could not feasibly do.
In 1994 Peter Shor developed a polynomial quantum algorithm for factoring integers with the potential to decrypt RSA-encrypted communications.
In 1996 Lov Grover developed a quantum algorithm for unstructured search in time O(√N) and proved that the time of any classical algorithm solving the analogous problem cannot be less than O(N). Grover's algorithm is provable faster than any classical competitor, so it has achieved a quantum speedup; this success led to a surge of theoretical and experimental results in the new field. However, after 30 years no new quantum algorithms had achieved a speedup . . .
In 2011 physicist John Preskill proposed and discussed the syntagm "quantum computational supremacy"–a significantly weaker form of speedup –at a Solvay Conference of Physics:
We therefore hope to hasten the onset of the era of quantum supremacy, when we will be able to perform tasks with controlled quantum systems going beyond what can be achieved with ordinary digital computers.
A quantum computational supremacy is achieved when a formal computational task is performed with an existing quantum device which cannot be performed using any known algorithm running on an existing classical supercomputer in a reasonable amount of time.
In recent years, investment in quantum computing research has increased in the public and private sectors. After a false start, on 23 October 2019, Google AI, in partnership with the NASA claimed to have performed a quantum computation that was infeasible on any classical computer.
The field captures the interest and imagination of the large public and media, and not surprisingly, unfounded claims about the power of quantum computing and its applications proliferate.
In this talk we will discuss the merits and limits of pursuing the goal of achieving a quantum advantage.

## Summary

**Author:** CALUDE, Cristian (University of Auckland)

**Presenter:** CALUDE, Cristian (University of Auckland)

**Session Classification:** Plenary reports