Concluding remarks

Within the query model, Grover's algorithm is *asymptotically optimal*. What this means is that it's not possible to come up with a query algorithm for solving the *Search* problem, or even the *Unique search* problem specifically, that uses asymptotically less than $O(\sqrt{N})$ queries in the worst case. This is something that has been proved rigorously in multiple ways.

Interestingly, this was known even before Grover's algorithm was discovered — Grover's algorithm matched an already-known lower bound.

Grover's algorithm is also broadly applicable, in the sense that the square-root speed-up that it offers can be obtained in a variety of different settings. For example, sometimes it's possible to use Grover's algorithm in conjunction with another algorithm to get an improvement. Grover's algorithm is also quite commonly used as a subroutine inside of other quantum algorithms to obtain speed-ups.

Finally, the technique used in Grover's algorithm, where two reflections are composed and iterated to rotate a quantum state vector, can be generalized. An example is a technique known as *amplitude amplification*, where a process similar to Grover's algorithm can be applied to another quantum algorithm to boost its success probability quadratically faster than what is possible classically. Amplitude amplification has broad applications in quantum algorithms.

So, although Grover's algorithm may not lead to a practical quantum advantage for searching any time soon, it is a fundamentally important quantum algorithm, and it is representative of a more general technique that finds many applications in quantum algorithms.

Was this page helpful?

| Yes 👍 | No 👎 |

Report a bug, typo, or request content on GitHub ↗.

Previous page   Take the exam