WHAT'S QUANTUM COMPUTING ANYWAY?

YURI GUREVICH
UNIVERSITY OF MICHIGAN

The following function inversion problem

> Given access to a Boolean oracle $f : \{0,1\}^n \to \{0,1\}$,
> solve equation $fx = 1$.

can be called searching for a needle in a haystack.

Example. Given access to an NYC phone directory, sorted by name as usual, find the name of a person by her phone number.

To simplify the exposition, we restrict attention to the case where equation $fx = 1$ has a unique solution. Let $N = 2^n$.

Claim. On average, any classical algorithm for the problem has to query the oracle at least $N/2$ times.

However, there is a quantum algorithm — Grover's algorithm, the second most famous quantum algorithm — that solves the problem with only $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ queries. How does it do that?

A quantum algorithm is an algorithm for quantum hardware. Separating the concerns, we first present Grover's algorithm in purely classical terms. We explain how it gets away with so (relatively) few queries and why one cannot do better yet. We also explain why the existence of Grover's algorithm does not contradict the claim above.

Then we explain how a quantum computer allows one to implement Grover's algorithm. No knowledge of quantum theory is assumed.

Finally, we will quickly address the current state of quantum computing.