What Quantum Computing Can Do For You

Ronald de Wolf

Inaugural speech

September 20, 2012

UNIVERSITEIT VAN AMSTERDAM

Another inaugural speech

- John F. Kennedy, January 20, 1961:

  Ask not what your country can do for you,
  ask what you can do for your country

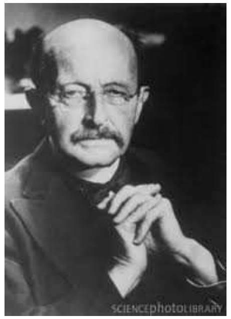
- The Ford Motor Company:

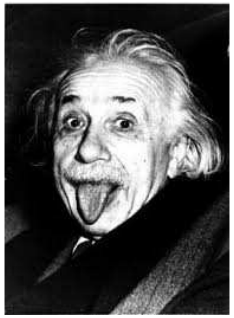
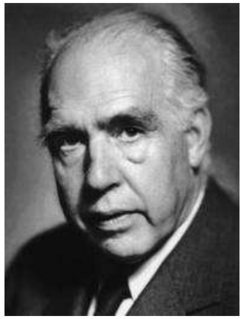
  Ask not what you can do for your Ford dealer,
  ask what your Ford dealer can do for you

- This lecture: *what quantum computing can do for you*

What is quantum mechanics?

- Our best physical theory of the world of “small” objects: electrons, photons, etc.
- Developed 1900–1925 by many people
Planck, Einstein, Bohr, Schrödinger, Heisenberg

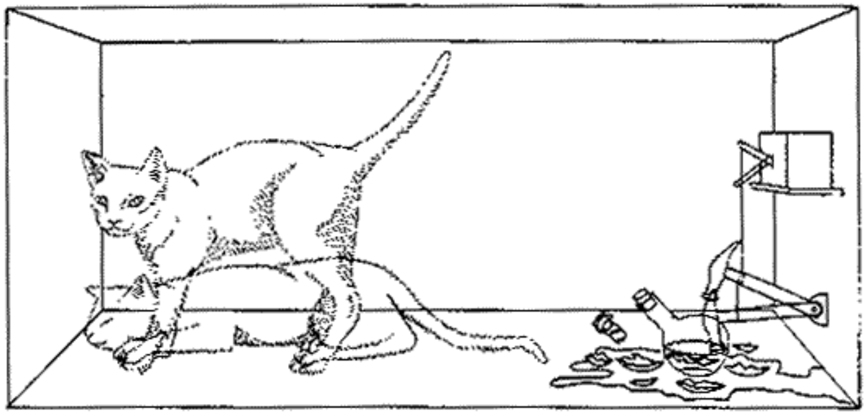


- Lots of weird things happen here:
  - Superposition of various states
  - Interference of states
  - Entanglement of different systems

Superposition

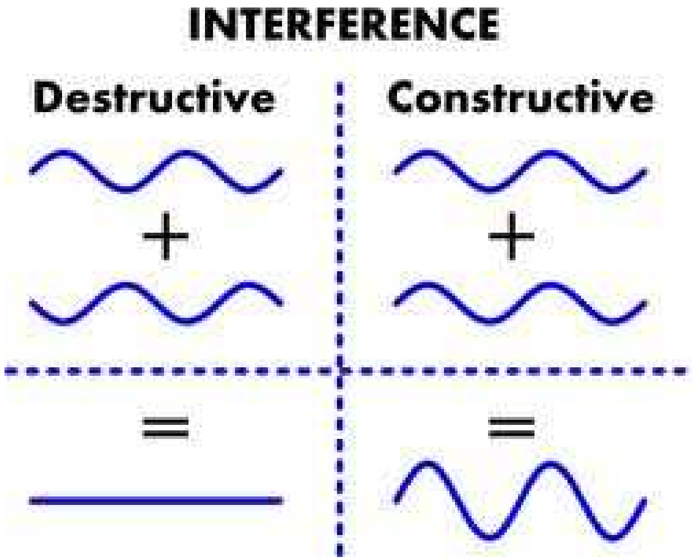
- Objects can be in superposition of different classical states simultaneously
- Example: the spin of an electron can be “up” or “down”, but can also be in a superposition of both
- In principle also larger objects can be in superposition Schrödinger’s cat is dead and alive “at the same time”



- Cats in superposition isn’t experimentally feasible (yet), but with large molecules this has already been done!

Interference

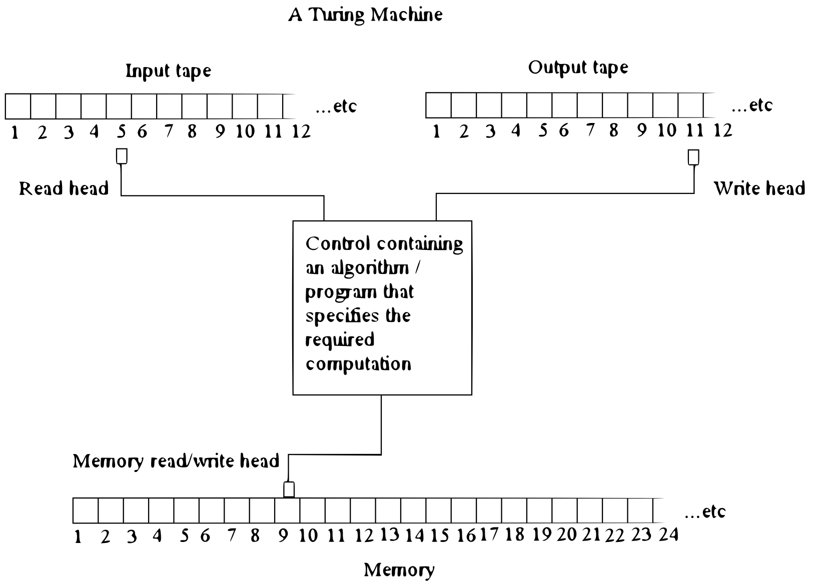
- Waves can strengthen and weaken each other

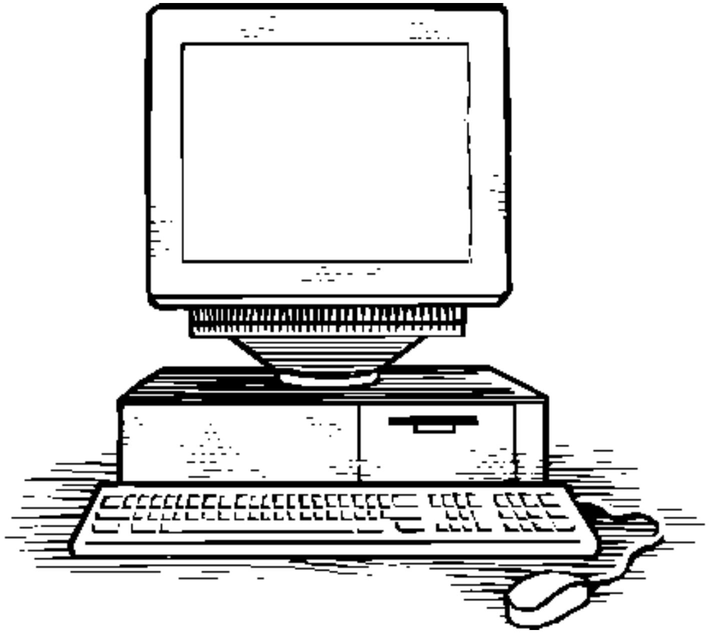


- Quantum superposition is similar to a wave, and combinations of different superpositions give similar interference-effects

Computers

- Our society runs on computers
- Modern computers are based on classical physics, in theory (Turing machine) and practice (PC, iphone)





- Memory-locations have specific value (0 or 1), the processor acts on a specific location, . . .

Quantum bits

- Richard Feynman,
  David Deutsch
  in the 1980s:

  Let's do useful computation with quantum effects!

- Classical bit is either 0 or 1

- Quantum bit is a superposition of 0 and 1
  For example, we can use an electron, with
  0 = "spin up" and 1 = "spin down"

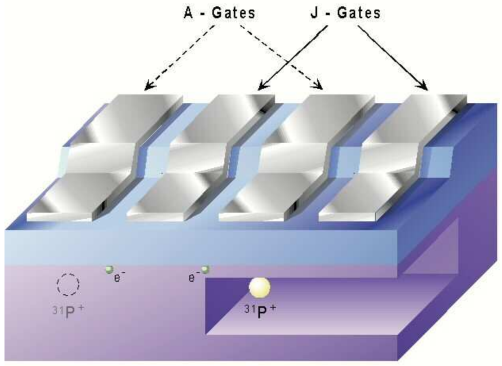
- 2 qubits is a superposition of 4 states (00, 01, 10, 11)
  3 qubits is a superposition of 8 states (000, 001,. . .)
  . . .
  1000 qubits: superposition of 2^{1000} states

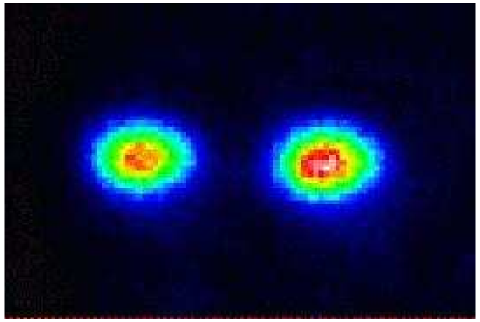
- More than the number of particles in the universe!

Quantum-mechanical computers

- Quantum computer:
  1. Start with qubits in simple state (for instance 0)
  2. Engineer the right kind of interference:
     paths of the superposition leading to solution should interfere constructively, paths that don’t lead to a solution should interfere destructively
  3. A measurement of final state should give a solution

- So far, this has only been realized on a few qubits



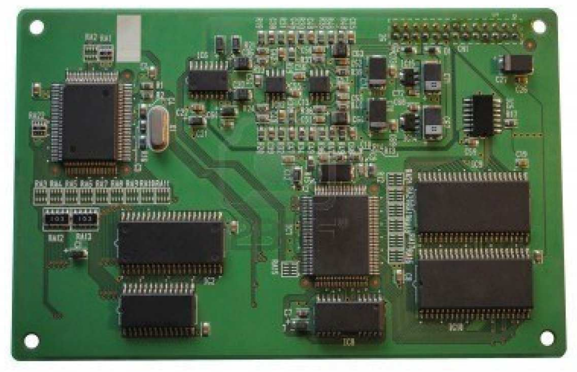


What can quantum computing do for you?

That depends on what you want. . .

If you want a faster computer. . .

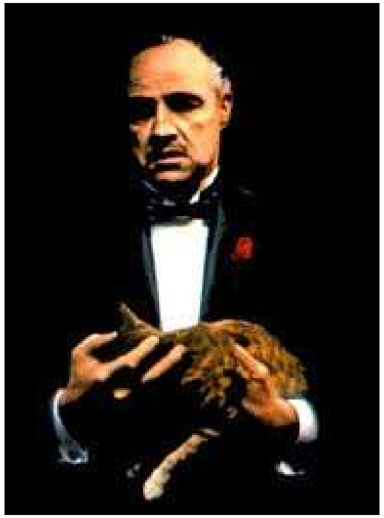
- Computers are getting faster and faster
  Main reason: miniaturization. Every 2 years, number of transistors on given area of chip doubles (Moore's law)



- Transistors are now so small that quantum effects are hard to suppress
- Why not use those effects instead of suppressing?
- Continuing miniaturization ⇒ faster computers
- But there are more fundamental advantages. . .

If you want to steal something. . .

- Crytpography: the art of hiding information
- Most practical cryptography is based on assumption that it’s hard to factor large numbers
  $15 = 3 \times 5$
  $12140041 = 3413 \times 3557$
  A 400-digit number takes years to factor today, even on a very large cluster of computers
- Shor’94: efficient quantum algorithm for factoring!
- Quantum computer can break your bank’s security



If you want to hide something. . .

- What if you *really* need to communicate securely?
- Quantum cryptography to the rescue! (BB’84)
- Already commercially available!
- Based on the Heisenberg uncertainty principle: some quantities cannot both be measured very accurately, for example *position* and *momentum* of a particle

At home with the Heisenbergs
I can't find my car keys.
You probably know too much about their momentum.

If you’re looking for something. . .

- Suppose you lost your keys; you could find them by searching through all locations where they could be
- If there are N possible locations, you’ll have to inspect roughly $N/2$ locations on average
- Grover’s algorithm (’96): solve this search problem in roughly $\sqrt{N}$ steps

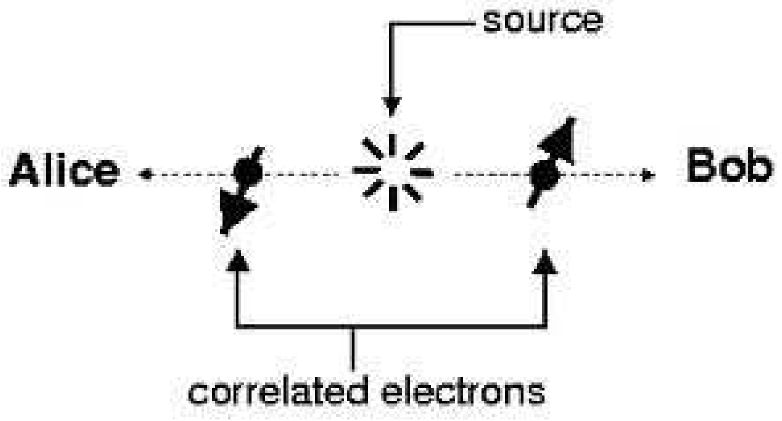
- Grover finds needle in haystack much faster than classical search

- This has many applications

If you’re a philosopher. . .

- Classical world is Local: no instantaneous action, and Realistic: objects have specific properties, even before they are measured
- If the world were classical, all non-communicating systems obey a “Bell inequality”
- Entangled quantum systems can violate Bell inequality.

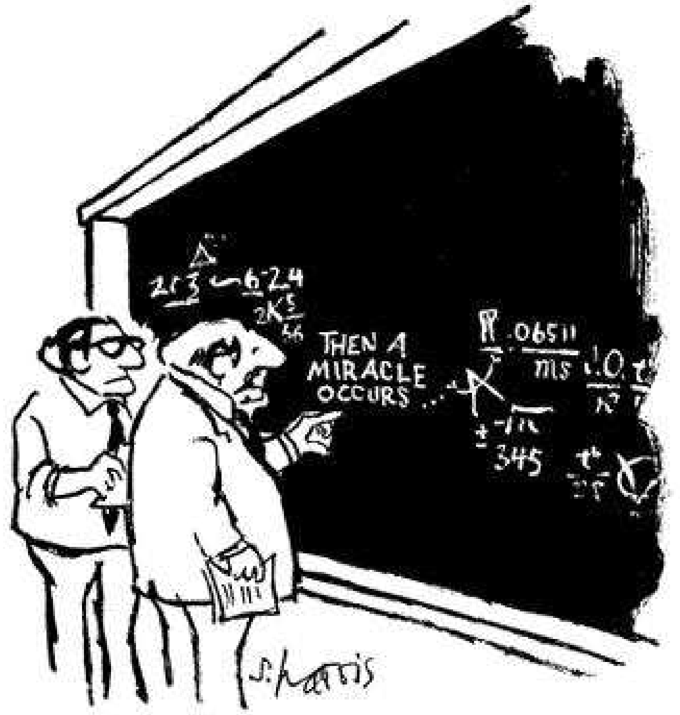
  In theory (Bell’64) and experiment (Aspect’81)



- This proves our world is not classical!
- Quantum computing results allow to design maximally non-classical experiments

If you want to prove something. . .

Mathematicians
need tools and techniques
to prove things



"I think you should be more explicit here in step two."

- Last few years: sequence of new results where crucial proof-ingredients come from quantum computing
  - Error-correcting codes
  - Linear programs for Traveling Salesman Problem
- Useful even if no large quantum computer is ever built!

Conclusion

- Quantum mechanics is best physical theory we have
- Fundamentally different from classical physics
- Quantum computing uses its non-classical effects for faster algorithms, more efficient/secure communication, …
- Useful for a lot of things
- What else? We'll see…

Many thanks!