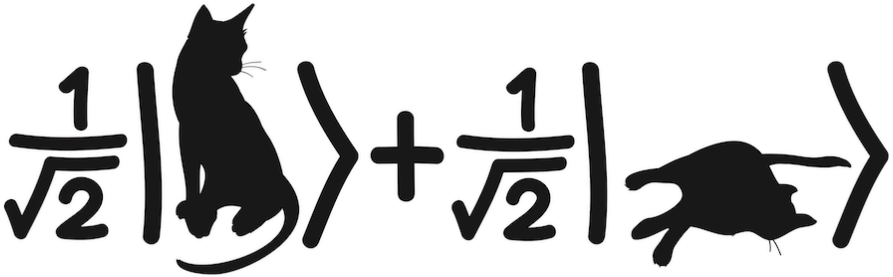
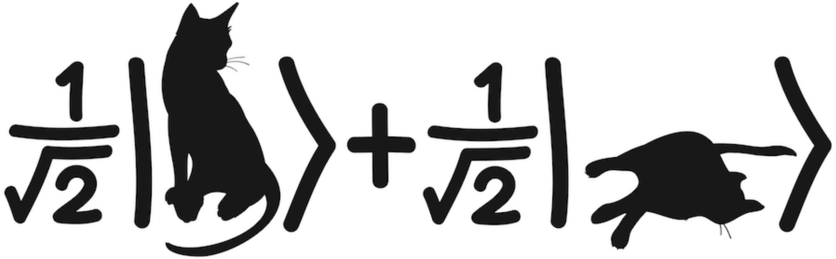
Quantum Mechanics
&
Quantum Computation



Overview

Quantum Computation

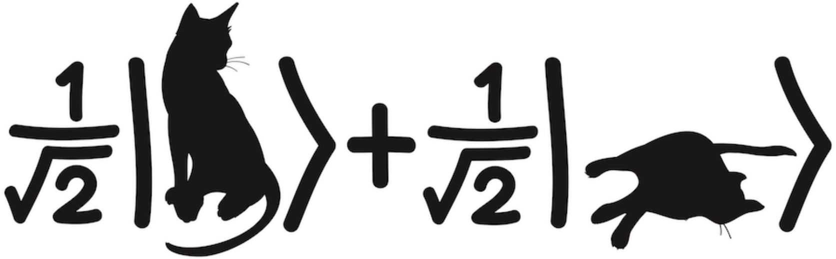


- Quantum systems are exponentially powerful.
  System of 500 particles has 2^{500} "computing power."
- Classically: either increase speed or parallelism:

  2^{500} >> # particles in the Universe x

  2^{500} >> Age of Universe in femtosecs.

Quantum Computation

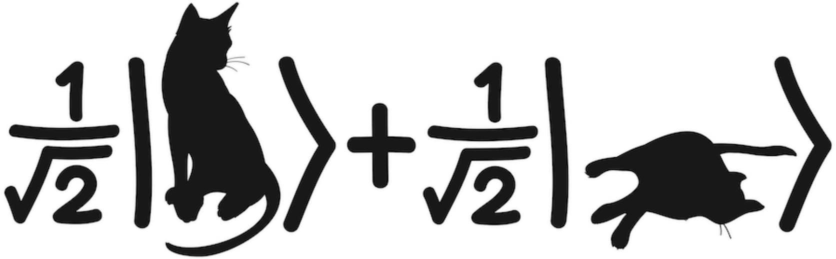


- Quantum systems are exponentially powerful.
  System of 500 particles has 2^{500} "computing power."

Have to work to channel this power towards solving a computational problem:

  – Pick the right computational problems
  – Design quantum algorithms.

Quantum Computation

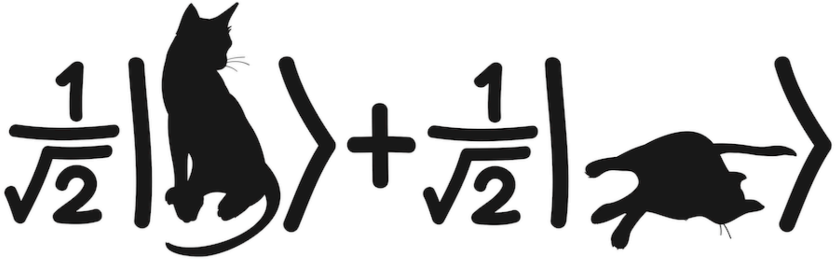


- Example: Factoring. $N = p_1^{e_1} p_2^{e_1} \cdots p_k^{e_k}$ $60 = 2^2 \times 3 \times 5$

RSA cryptosystem

- Shor's quantum algorithm for factoring integers in polynomial time.
- Breaks RSA cryptosystem.
- Quantum algorithms break most modern public-key cryptosystems!

Quantum Computation



- Quantum systems are exponentially powerful. System of 500 particles has 2^{500} "computing power."

To obtain exponential speedup must start with computational problem with right kind of structure.

Quantum computing

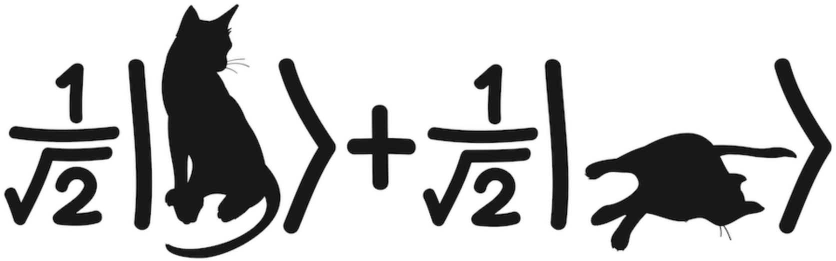
Orion's belter

Feb 15th 2007 | VANCOUVER
From *The Economist* print edition

The world's first practical quantum computer is unveiled

Quantum computers provide a neat shortcut to solving a range of mathematical tasks known as NP-complete problems. They do so by encoding all possible permutations in the form of a small number of “qubits”. In a normal computer, bits of digital information are either 0 or 1. In a quantum computer these normal bits are replaced by a “superposition” (the qubit) of both 0 and 1 that is unique to the ambiguous world of quantum mechanics. Qubits have already been created in the laboratory using photons (the particles of which light is composed), ions and certain sorts of atomic nuclei. By a process known as entanglement, two qubits can encode four different values simultaneously (00, 01, 10 and 11). Four qubits can represent 16 values, and so on. That means huge calculations can be done using a manageable number of qubits. **In principle, by putting a set of entangled qubits into a suitably tuned magnetic field, the optimal solution to a given NP-complete problem can be found in one shot.**

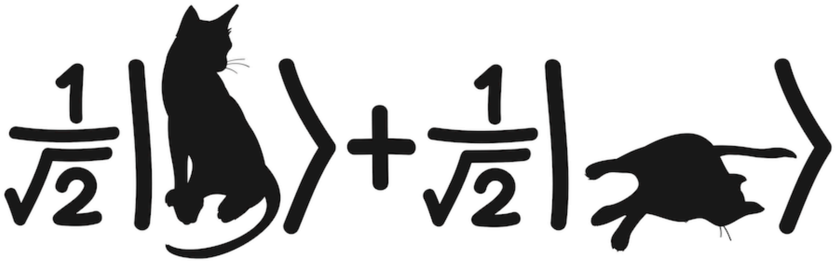
Quantum Computation



- Must understand the basic principles of quantum mechanics.
- Quantum mechanics is a very counter-intuitive theory:

  > "Anyone who is not shocked by quantum mechanics has not understood it." --- Neils Bohr.
- Quantum computing exploits the most counter-intuitive aspects of quantum mechanics.

Simple intro to basic Quantum Mechanics



- Simple building blocks – qubits, quantum gates.

- Emphasizes paradoxes and intuitive picture.

- More concrete.

- More fun.