Quantum Computing

Jan Plaza

Computer Science Department

SUNY Plattsburgh

March 24, 2009

A new revolution

Welcome. You can participate in a technological revolution that has just started. Feel the excitement experienced by inventors of electronic computers in 1940's! Quantum computing promises massively parallel computation with capability of attacking problems and making simulations which are out of reach for classical computers. Somebody will make billions. Some will become famous. Many will gain understanding of an essential truth about the Universe. Are you in?

Question 1

On a planet orbiting a star in a galaxy:

1. An alien leaves the room through two doors simultaneously, (but only if you do not watch).

2. A beam of light makes a spot on a screen.
   Two plates are placed and they block the light.
   A third plate is inserted between the two,
   and the light appears on the screen again.

What is the name of the planet?

Answer: EARTH

1. Aliens = photons, electrons, atomic nuclei:
   - behave like waves,
   - behave like particles (when you measure position).

2. Use polarization plates.
   Impossible to model using classical physics.
   Quantum mechanics can model it.

Double slit experiments

In early 1900's scientists thought:

- electron = miniature tennis ball;
- atom = miniature solar system.

An electron can pass through two slits in a wall at the same time, producing an interference pattern.
So, **electrons are not tiny tennis balls.**

If you shoot electrons one at a time
and test which slit each electron goes through,
there is no interference pattern.
So, **electrons are not just waves.**

Conclusion

Electrons are neither just particles nor just waves –
they exhibit a particle or wave behavior depending on what is measured.

The same about photons, neutrons, nuclei, atoms and small molecules.

The heavier the object, the less pronounced the wave-like behavior.

Classical physics fails

1. How is the particle-wave duality possible?
2. Why is diamond hard?
3. Why do magnetic properties diminish with increased temperature?
4. Why does conductivity of a semiconductor increase with temperature?

Classical physics does not provide an answer.

Quantum mechanics:

- was formulated in 1930's;
- **describes / models** the world on the subatomic scale;
- its calculations are compatible with experiments 1-4;
- **does not explain** the strangeness of the subatomic world.

Quantum world – a crazy one

“Reality is that which, when you stop believing it, does not go away.”

Philip K. Dick

“Though this be madness, yet there is method in it.”

William Shakespeare

Is it real? Is it useful?

Quantum mechanics:

- is the most thoroughly tested theory in physics;
- it withstood all the challenges.

We benefit from its applications in:

- nuclear engineering, isotopes,
- material engineering,
- electronics, lasers, semiconductors.

Question 2

On a planet orbiting a star in a galaxy:

1. In under a second a computer breaks an encryption scheme requiring 15 billion years for contemporary computers.

2. A computer runs (almost) without consuming energy and without giving off heat.

What is the name of the planet?

Answer: EARTH

1. A quantum computer will be able to do this.

2. A reversible computer will be able to do this.

Question 3

When?

“Prediction is always difficult, especially of the future”

Niels Bohr

Answer: Perhaps by 2050, as many experts believe.

Question 4: How?

Answer:

By taking physics seriously:

- **quantum mechanics,** and
- **thermodynamics,**

and by developing technology.

We stand on the shoulders of giants

Classical mechanics

- Nicolaus Copernicus (1473-1543): heliocentric system
- Galileo Galilei (1542-1642): trajectory of a cannon ball
- Johannes Kepler (1571-1630): laws of planetary motion
- Isaac Newton (1642-1727): classical mechanics
- Pierre Simon Laplace (1749-1827): mechanics is deterministic
- Joseph Louis Lagrange (1736-1813): coordinate space constraint
- William Rowan Hamilton (1805-1865): phase space constraints

Quantum mechanics

- Marie Curie (1867-1934): polonium, radium
- Max Planck (1858-1947): quantum = indivisible packet of energy
- Joseph John Thompson (1856-1940): electron
- Albert Einstein (1879-1955): photoelectric effect
- Ernest Rutherford (1871-1937): atomic nucleus
- James Chadwick (1891-1974): neutron
- Werner Heisenberg (1901-1976): matrix mechanics
- Wolfgang Pauli(1900-1958): exclusion principle
- Erwin Shrödinger (1887-1961): wave function
- Niels Bohr (1885-1962): Copenhagen interpretation
- Paul Dirac (1902-1958): antimatter

The place of quantum mechanics

		Speed comparable to light?	
		NO	**YES**
Molecule size or smaller?	**NO**	classical m.	relativistic m.
	YES	quantum m.	quantum field theory

While increasing the scale of objects, the laws of quantum mechanics morph into the laws of classical physics.

The crucial thing

“The grand book of universe is written in the language of mathematics.”

Galileo Galilei

“One cannot understand the laws of nature, the relationship of things, without an understanding of mathematics.
There is no other way to do it.”

Richard Feynman

Complex numbers

"Whole numbers were created by God, all others are made by men."

Leopold Kronecker

- Imaginary unit, i: $\quad i \cdot i = -1$.
- Imaginary numbers: $\quad i,\ 2i,\ -5.3i$.
- Complex numbers: $\quad 12.4,\ -5.3i,\ 12.4 - 5.3i$.

"The only reason that we like complex numbers is that we don't like real numbers."

Bernd Sturmfels

Are complex numbers like reals?

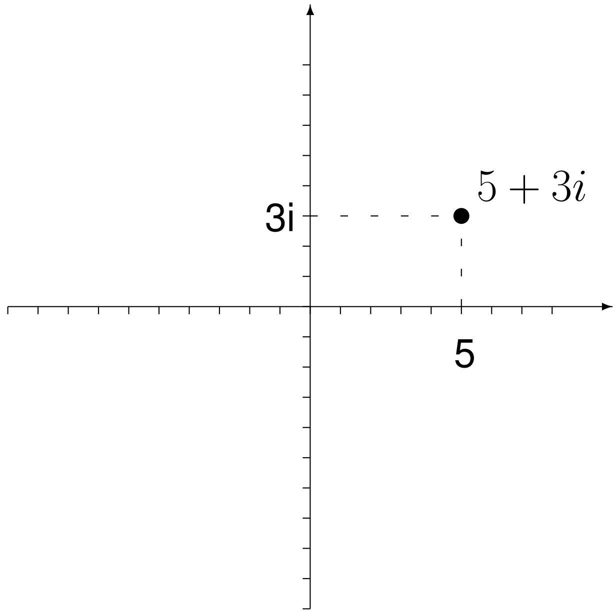
Similar:

- Can be added, subtracted, multiplied and divided;
- Powers, roots, logarithms can be calculated.

Different:

- the $<$ relation does not extend to complex numbers;
  while reals fill a line, complex numbers fill a plane (C.F. Gauss);
- given $a + bi$ its conjugate is $a - bi$; in general it is not equal to the original number.

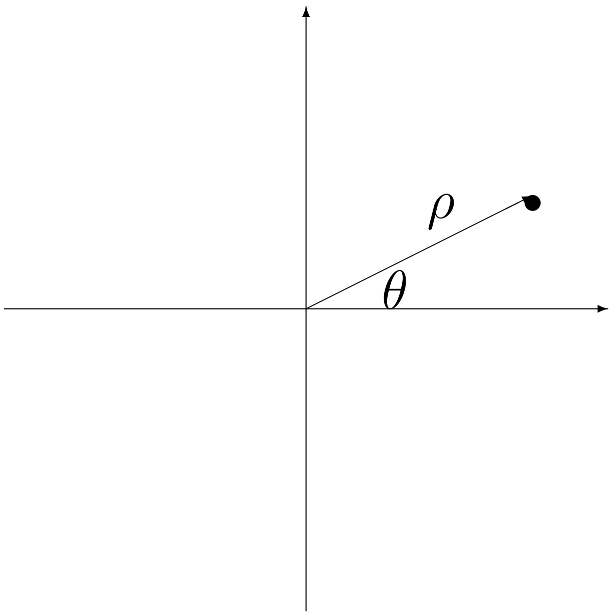
Cartesian representation



$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i$$

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$$

Polar representation



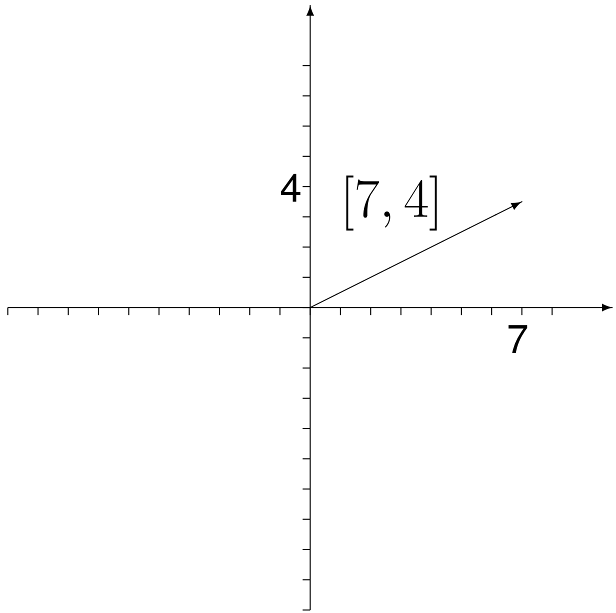
- ρ = magnitude
  (distance from (0,0))

- θ = phase (angle)

- multiplication = composition of rotations
  $(\rho_1, \theta_1) \cdot (\rho_2, \theta_2) = (\rho_1 \cdot \rho_2, \theta_1 + \theta_2)$

- conjugate = symmetry
  $(\rho, \theta)^* = (\rho, \pi - \theta)$

Vectors

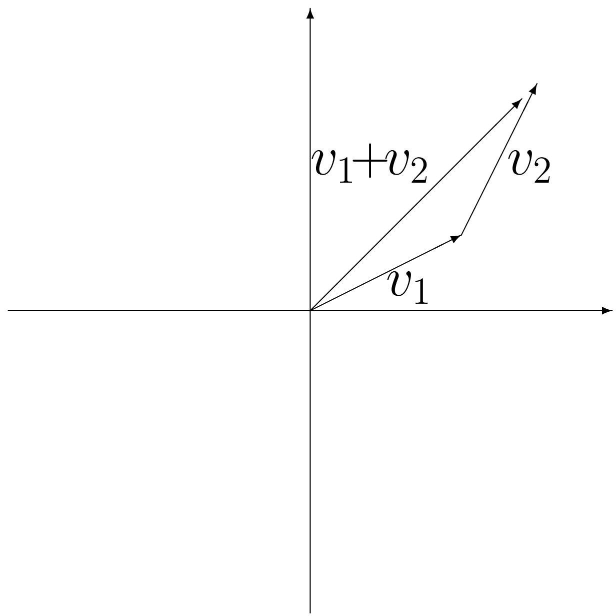


A (real) vector = any arrow starting at the point $(0,0)$

A vector from $(0,0)$ to (x,y) can be can be written as $[x,y]$ or $\begin{bmatrix} x \\ y \end{bmatrix}$.

Operations on vectors

- multiplication by a number (stretching),
- addition:



For real vectors:

Inner product of two vectors is a real number:

$$[x_1, y_1] \cdot [x_2, y_2] = x_1 x_2 + y_1 y_2$$

Norm (length) of a vector:

$$\|[x, y]\| = \sqrt{[x, y] \cdot [x, y]} = \sqrt{x^2 + y^2}$$

DIAGRAM (Pythagorean theorem)

Two vectors are **orthogonal** (perpendicular) if the innner product is 0.

Distance between vectors:

$$d([x_1, y_1], [x_2, y_2]) = \|[x_1, y_1] - [x_2, y_2]\| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

Superposition

$[1, 0]$ and $[0, 1]$ – base vectors.

$c_1[1, 0] + c_2[0, 1]$ – superposition of base vectors.

Quantum computing trick:
instead of performing operations on base vectors separately,
perform them at once on their superposition.

Quantum mechanics uses:

- n-dimensional vectors (with n components),
- complex vectors (with complex numbers as components).

Matrices

A matrix – a rectangular array of numbers.

	product1	product2
plates	2	3
bolts	1	0
connectors	4	5

We need m copies of product1 and n copies of product2.

$$\begin{bmatrix} 2 & 3 \\ 1 & 0 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = \begin{array}{c c} \begin{bmatrix} 2m + 3n \\ 1m + 0n \\ 4m + 5n \end{bmatrix} & \begin{array}{c} \text{plates} \\ \text{bolts} \\ \text{connectors} \end{array} \end{array}$$

A.k.a. multiplying a matrix by a vector.

Actually a vector is a (thin) matrix,
so this is a multiplication of two matrices.

Important matrices

Identity matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Unitary matrix = one that preserves vector length:

$$|Ax| = |x|$$

Hermitian matrix (after Charles Hermite, 1822-1901) = symmetric matrix (in the case of real numbers).

Matrix multiplication

There are:
trains between A and B,
trains between C and D,
flights between A and C,
flights between A and D.

Trains	A	B	C	D
A	0	1	0	0
B	1	0	0	0
C	0	0	0	1
D	0	0	1	0

Flights	A	B	C	D
A	0	0	1	1
B	0	0	0	0
C	1	0	0	0
D	1	0	0	0

$$T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad F = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Trips taking either one train **or** one flight (**matrix addition**).

$$T + F = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Trips taking one train **and then** a flight (**matrix multiplication**):

$$TF = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Trips taking one flight **and then** a train (**matrix multiplication**):

$$FT = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Trips taking one train, then two flights:

$$TFF$$

Transposition

Subway circle line: A to B , B to C, C to A but not back:

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

After extensive research sponsored by a $200 million grant a question arose if efficiency of the transportation can be improved. So, starting April 1 the trains will run in the opposite directions:

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

A.k.a. **transposed matrix**.

Other operations on matrices

- Inverse:
  B is an inverse matrix to A if AB=BA=I,

- Tensor product.

Postulates of quantum mechanics

- At any moment a quantum system is in a state.
- The system evolves in a reversible way.
- A state may become a superposition of basic states
  (e.g. a particle present at the same time
  a little bit in position1 and a little bit in position2 .)
- The observation/measurement irreversibly destroys the state.
- The result of the measurement is non-deterministic
  but statistically predictable.

"We all agree that your theory is crazy, but is it crazy enough?"

Niels Bohr

Representation:

- State – vector,
- Change of the state – multiplying by a unitary matrix,
- Result of the measurement – an eigenvalue of a hermitian matrix.

Bits and qubits

Bit = unit of information:

- yes or no,
- on or off,
- 0 or 1,
- vectors $[1,0]$ or $[0,1]$.

Qubit:

- an electron in one of two orbits,
- a photon in one of two polarized states,
- a subatomic particle with one of two spin values,
- a complex vector $[c_1, c_2]$ – a superposition of $[1,0]$ and $[0,1]$.

Exponential blowout

Byte = 8 bits
it can be in $2^8 = 256$ different classical states
00000000, 00000001, 00000010, ..., 11111111;
it is described by 8 Boolean values.

Qbyte = 8 qubit system
it can be in $2^8 = 256$ different **basic** quantum states
and in their superpositions;
it is described by 256 complex numbers.

A 64 bit system is described by 64 Boolean values.
A 64 qubit system is described by 18446744073709551616 complex numbers.

The idea of quantum computation

In 1970's it was clear that no electronic computer can simulate a 64-piece quantum system.
In 1982 Richard Feynman put the complexity concern on its head; a disadvantage turned into an advantage:

If simulating a quantum process
requires an exponential number of computation steps
then perhaps a quantum process
can perform an exponential number of steps.

Classical vs. quantum computation

Instead of considering 2^{64} different states one by one, put 64 qubits in a superposition of all these states and process them at once.

However, classical algorithms are **not** easily adaptable:

- Computation must proceed only by applying unitary operations;
- Once in a superposition, data cannot be copied (no-cloning theorem);
- The final measurement of the qubits (by a hermitian operator) is not deterministic;
  It must represent a deterministic result or
  indicate a deterministic result under repetitions.

Algorithms

	Search	Factorization
Classical	$O(n)$	exponential
Quantum	$O(\sqrt{n})$ – Grover 1997	$O(n^2+)$ – Shor 1994

Shor's algorithm achieves an exponential speedup and can break some public key encryption schemes such as RSA.

Grover's algorithm can reduce search time from years to seconds; it can be applied to solve NP-complete problems faster.

Do NP-complete problems have polynomial quantum algorithms? Nobody knows but probably not.

Current quantum hardware

What hardware has been constructed?

- Fixed computing networks
- For a small number of qubits.

Is it significant?

- Toy calculators!
- But they work!

Future

“Where a calculator like the ENIAC today is equipped with 18,000 vacuum tubes and weighs 30 tons, computers in the future may have only 1,000 [more specialized] vacuum tubes and perhaps weigh only 1.5 tons.”

Popular Mechanics, 1949

Goals:

- **Programmable computer**:
  perhaps a classical master and a quantum slave,
  capable of arbitrary initialization of qubits,
  applying an arbitrary unitary operation
  and performing measurement;
- **Managing de-coherence.**

Reversible computers

1960's, Rolf Landauer:
Erasing information (not writing) causes energy loss and heat.

1970's Charless L. Bennett:
In theory, a computing process that is reversible and does not erase can run without consuming any energy and giving off heat.

"In theory, there is no difference between theory and practice. But, in practice, there is."

Jan L.A. van de Snepscheut

An arbitrarily close approximation should be possible.

Want to study?

It is just a matter of time before quantum computing becomes a standard subject in undergraduate computer science curricula.

Prerequisites:

1. open mind – to accept the strangeness of the quantum world,
2. brave heart – not to be scared of mathematics.

How difficult is it?

	Quantum mechanics	Quantum computing
Time	continuous	discrete
Number of dimensions	infinite	finite

“Everything should be made as simple as possible, but not simpler”.

Albert Einstein