Anyons and quantum computation

Alexei Kitaev

Microsoft, Caltech

Main topics

1. What is quantum computation?
2. Fault-tolerance: error-correcting codes vs. physical (topological) protection
3. Abelian and non-Abelian anyons
4. Special properties of $\nu = 5/2$ anyons
5. Anyonic qubits

Quantum vs. classical (discrete systems)

- Computer memory (bits): **0 0 1 0 1**
- Microscopic system (spins): $\Uparrow \Uparrow \Downarrow \Uparrow \Downarrow$

  But spins are quantum: $|\Rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\Uparrow\rangle + |\Downarrow\rangle\right)$

- Quantum memory (*qubits* (made of spins, atoms, etc.)):

$$|\Psi\rangle = c_{000}|000\rangle + c_{001}|001\rangle + c_{010}|010\rangle + \dots$$

complex numbers

In general, $|\Psi\rangle = \sum_{x_1,\dots,x_n} c_{x_1,\dots,x_n}|x_1,\dots,x_n\rangle$ (2^n terms)

Some assumptions

1. The system consists of well-separated subsystems

2. Each subsystem is a qubit, i.e., it has only two basis states

   n qubits $\Longrightarrow$ 2^n-dimensional state space

3. Time is discrete:

   $|\Psi_t\rangle = U_t|\Psi_{t-1}\rangle$, where U_t is a unitary operator

4. The evolution is time-dependent, i.e. U_t depends on t.

How difficult is it to simulate quantum mechanics?

$$|\Psi_{\text{out}}\rangle = U_L \ldots U_1 |\Psi_{\text{in}}\rangle$$

$2^n \times 2^n$-matrices

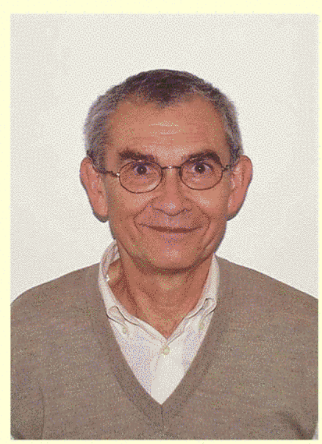
Exponentially long computation – bad news…

But let us be optimistic: this difficulty just means that quantum mechanics is computationally powerful (indeed, any quantum system performs the hard computational task of simulating itself).

Let the nature compute for us: one quantum system can likely simulate another; maybe we can arrange it to do even more.

The idea of quantum computation was born

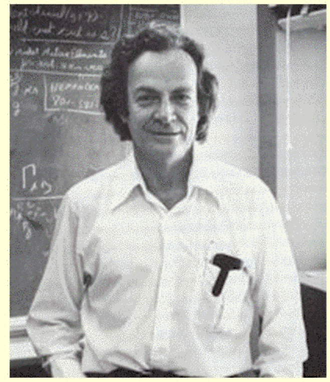
Yuri Manin, "Computable and uncomputable" (1980)



One difficulty in carrying out this program is to find the right balance between mathematical and physical principles. The quantum automaton should be abstract: its mathematical model should only use general quantum-mechanical principles, not specifying the physical realization. Thus, the model of evolution is a unitary rotation in a finite-dimensional Hilbert space, and the model of subdivision into subsystems is splitting the space into tensor factors. Somewhere in this picture there should be a place for interaction, which is conventionally described by Hermitian operators and probabilities.

Pioneering work on quantum computation

- Richard Feynman:



"Simulating physics with computers" (1982);

"Quantum mechanical computers" (1985)

- David Deutsch:

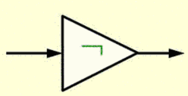
"Quantum theory, the Church-Turing principle, and the universal quantum computer" (1985);

"Quantum computational networks" (1989)

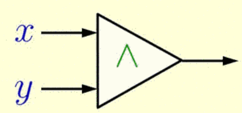
Classical and quantum gates

- Boolean gates (classical):

NOT gate



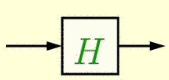
AND gate



x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

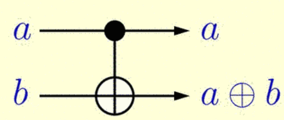
- Unitary operators (quantum):

Hadamard gate (one qubit)



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

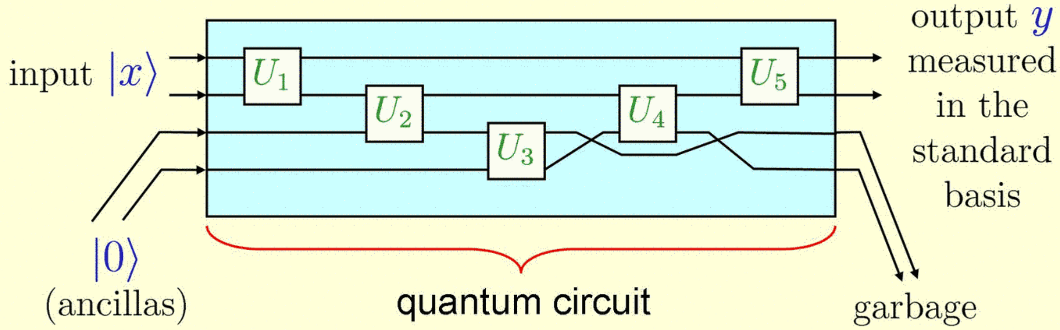
Controlled-NOT gate (two qubits)



$$|a, b\rangle \mapsto |a,\, a \oplus b\rangle$$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Anatomy of a quantum computer



The result is probabilistic!

We say that the computed value is $y = y(x)$ if it occurs with probability $\geq 2/3$ (any constant between $1/2$ and 1 will do)

What can quantum computers do?

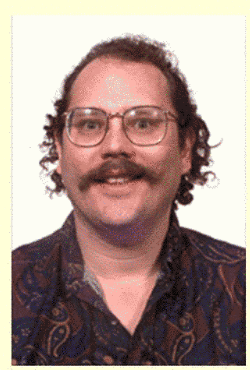
- Efficient simulation of quantum mechanics (molecules, crystals, nuclei, high energy physics) – every physicist's dream

- Great speedup for some number-theoretic problems

Factoring of an n-bit integer:

$\sim \exp(cn^{1/3})$ operations classically

$\sim n^3$ operations quantumly
(Peter Shor (1994))



There is a couple of problems though

- No scalable technology is presently available

Well, there was no scalable technology to build a classical computer at Charles Babbage's time (around 1840)...

- A fundamental problem: errors

– Systematic errors: each gate is implemented with certain precision, $\|U - \widetilde{U}\| \le \delta$

(U: ideal; $\widetilde{U}$: as implemented)

– Decoherence: interaction with the environment

A theoretical solution to the error problem

General idea: protection by redundancy

- Classical solution (primitive, but works):

Repetition code: $0 \mapsto 000, \quad 1 \mapsto 111$

- A quantum solution should be more tricky

Unfortunately, a quantum analogue of the repetition code does not protect from phase errors, like σ_j^z.

$$\left.\begin{array}{lcl} |000\rangle & \xrightarrow{\text{no error}} & |000\rangle \\ |111\rangle & \xrightarrow{\sigma_1^z} & -|111\rangle \end{array}\right\} \text{can distinguish (so far so good...)}$$

$$\left.\begin{array}{lcl} |000\rangle + |111\rangle & \xrightarrow{\text{no error}} & |000\rangle + |111\rangle \\ |000\rangle - |111\rangle & \xrightarrow{\sigma_1^z} & |000\rangle + |111\rangle \end{array}\right\} \text{can not distinguish}$$

Fault-tolerant quantum computation

- However, quantum error-correcting codes do exist!

The smallest one encodes 1 logical qubit into 5 physical qubits

- Quantum gates can be performed on the logical qubits without ever decoding them (or otherwise exposing them to error) – extremely tricky (P.Shor, 1996)

- This way, we can tolerate a constant, but sufficiently small error rate. The errors are constantly corrected, but we must correct them faster than they occur due to decoherence and imperfections in the correction circuit.

More about fault-tolerance

- Threshold theorem:

Fault-tolerant computation is possible when the decoherence rate per gate and the systematic errors are smaller than $\delta \sim 10^{-3} - 10^{-2}$.

- To fight decoherence, we must perform error correction on all the qubits *in parallel*

- A sufficient level of protection will likely require *dozens* of physical qubit per logical qubit and *hundreds* of physical gates per logical gate.

- Most interesting algorithms do need a full scale error correction machinery.

Physical protection

- Classical:

Spins in a piece of magnetized material
(think of a single bit on the hard drive in your computer)

Ising Hamiltonian: $H = -\sum_{j,k} J_{jk} s_j s_k$ where $s_j = \pm 1$

...but this is just a physical realization of the repetition code!

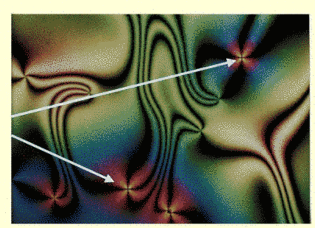
- Quantum:

The repetition code does not work.
We need to employ topology.

Classical topological defects

- Liquid crystals (e.g., nematics)
- Abrikosov vortices in superconductors

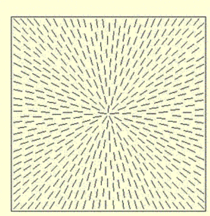
vortices



Texture in a nematic film (seen through crossed polarizers)

- A simple model of a vortex:

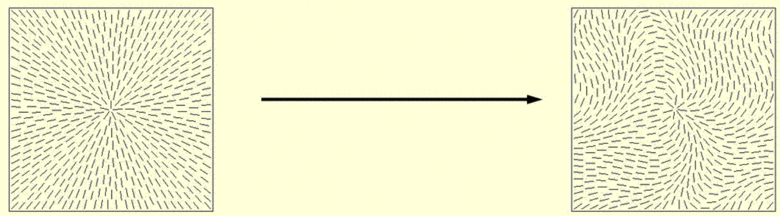
At each point x of the plane there is a *local order parameter* (orientation) $f(x) \in S^1$. The function $f : \mathbb{R}^2 \to S^1$ is continuous, except for the vortex points.



Vortices are *stable* and obey some *conservation laws*

Intuition about anyons: Quantum vortices

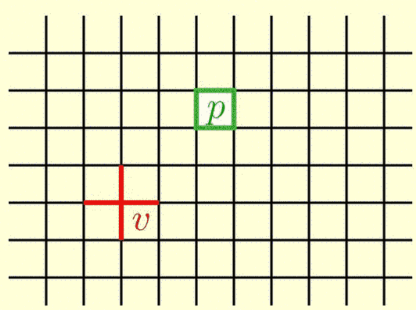
- First attempt: classical vortex distorted by quantum fluctuations



Idea: if the fluctuations are strong, the local order parameter disappears but the topological defect remains (like the Cheshire cat smile).

This doesn't actually work for S^1 vortices, but rather for $\mathbb{Z}_2$-vortices (see next slide).

The "toric code" model



Qubits at the lattice edges: $s_j = \pm 1$
(basis states are $|+1\rangle$ and $|-1\rangle$)

Vorticity at plaquette p:

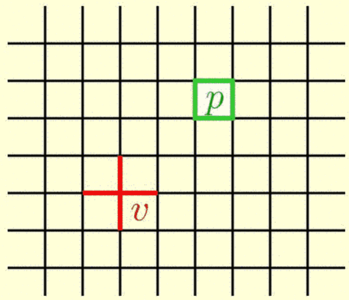
$$w_p = \prod_{j \in \text{boundary(p)}} s_j$$

Ground state: $|\Psi\rangle \sim \sum_{\substack{\mathbf{s}:\ w_p(\mathbf{s})=1 \\ \text{for all } p}} |\mathbf{s}\rangle$, for $\mathbf{s} = (s_1, \ldots, s_N)$ (vortex-free configurations)

Hamiltonian: $H = -J_e \sum_{\text{vertices}} A_v - J_m \sum_{\text{plaquettes}} B_p,$

where $A_v = \prod_{\text{star}(v)} \sigma_j^x, \quad B_p = \prod_{\text{boundary}(p)} \sigma_j^z$

Excitations in the "toric code" model



Ground state:

$A_v|\Psi_{\mathrm{gr.}}\rangle = |\Psi_{\mathrm{gr.}}\rangle, \qquad B_p|\Psi_{\mathrm{gr.}}\rangle = |\Psi_{\mathrm{gr.}}\rangle$

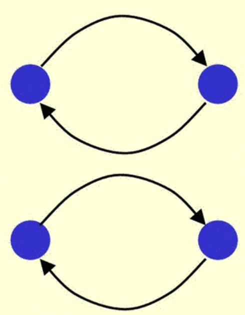
for all v and p

"Electric charge": $A_v|\Psi_v\rangle = -|\Psi_v\rangle$ for some v

"Magnetic vortex": $A_p|\Psi_p\rangle = -|\Psi_p\rangle$ for some p

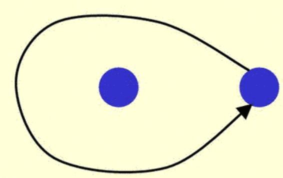
These may be regarded as charges and vortices for a $\mathbb{Z}_2$ gauge field.

Statistics and mutual statistics



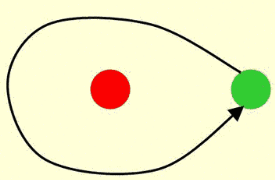
- Bosons: $= 1$
- Fermions: $= -1$

In both cases



$= 1$

But for the "electric charges" and "magnetic vortices",



$= -1$: Nontrivial *mutual* statistics!

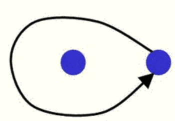
Particles with nontrivial statistics (neither bosons nor fermions) are called *anyons*. They only occur in two dimensions.

Abelian anyons

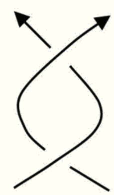
• The statistics is described by phase factors (a one-dimensional representation of the braid group)

Braids in space-time:

Top view (looking from the future)

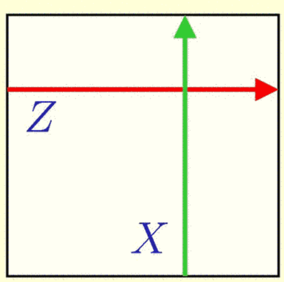


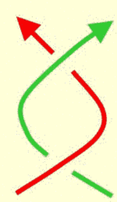
Side view (times goes up)



• The statistics on the torus is described by nontrivial operators (but still rather simple).

Ground state degeneracy on the torus



$Z^{-1}X^{-1}ZX$ =  $\neq 1$

X and Z do not commute, hence they act on a Hilbert space of dimension > 1 (Einarsson, 1990).

Quasiparticle tunneling may occur spontaneously, but it is exponentially suppressed: $\sim \exp(-L/\xi)$

torus size (L) — correlation length (ξ)

Non-Abelian anyons

A system of several non-Abelian quasiparticles has hidden degrees of freedom on which the braid group acts.

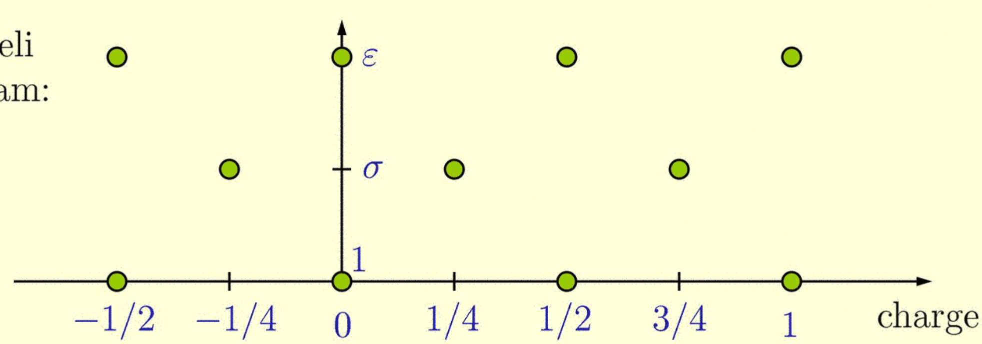
- Important algebraic structure in conformal field theory: final formulation by Moore and Seiberg (1989)
- Quantum Chern-Simons theory: Witten (1989)

- Pfaffian state: Moore, Read (1991) (believed to exist in FQHE at filling factor 5/2)
- Parafermion states: Read, Rezai (1998) (might exist in FQHE systems)

Anyons in the Pfaffian state

- Non-Abelian statistics is described by three particle types: 1, ε, σ.
- An excitation is characterized by one of the above labels as well as electric charge, which is a multiple of $1/4$.

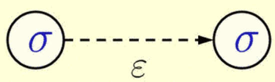
Bratteli diagram:



Fusion rules and hidden degrees of freedom

Three particle types: 1, ε, σ

Fusion rules: $\varepsilon \times \varepsilon = 1$, $\quad \varepsilon \times \sigma = \sigma$, $\quad \underline{\sigma \times \sigma = 1 + \varepsilon}$



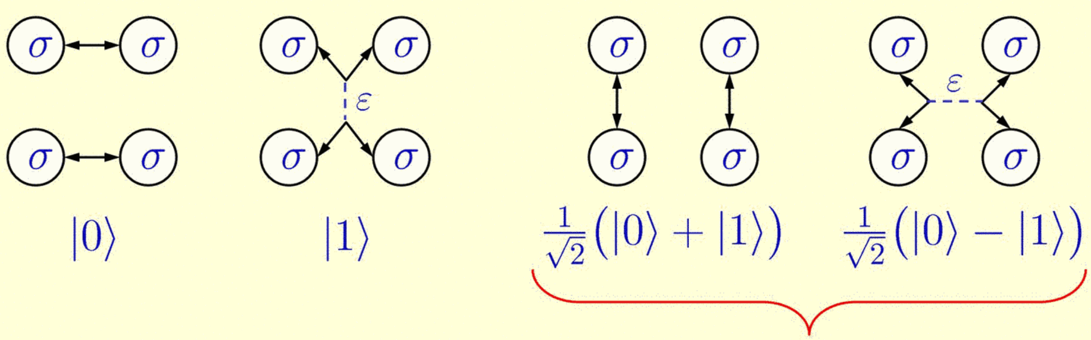
Total charge is 1 or ε? Cannot tell...

Any process that distinguishes the two states must involve quasiparticle tunneling (real or virtual). The tunneling is exponentially suppressed: $\exp(-L/\xi)$, where $\xi < \infty$ if the quasiparticles are gapped. Thus, the environment cannot distinguish the states, so it will not cause any phase error!

An anyonic qubit

Problem: The two fusion spaces cannot form superpositions because they belong to different superselection sectors.

Solution: Use four anyons instead on two



These relations follow from a full algebraic description of anyons

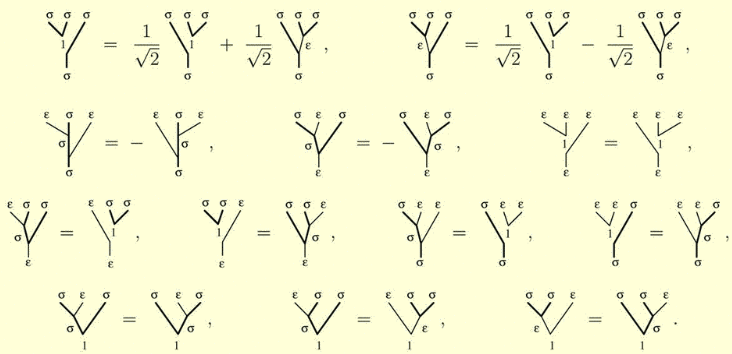
Superselection sectors: 1 (vacuum), ε (fermion), σ (vortex).

Quantum dimension:	$d_1 = 1,$	$d_\varepsilon = 1$	$d_\sigma = \sqrt{2};$
Topological spin:	$\theta_1 = 1,$	$\theta_\varepsilon = -1,$	$\theta_\sigma = \exp\left(\frac{\pi}{8}i\right);$
Frobenius-Schur indicator:	$\varkappa_1 = 1,$	$\varkappa_\varepsilon = 1,$	$\varkappa_\sigma = 1.$

Global dimension: $\mathcal{D}^2 \stackrel{\text{def}}{=} \sum_u d_u^2 = 4.$

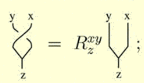
Fusion rules: $\varepsilon \times \varepsilon = 1, \quad \varepsilon \times \sigma = \sigma, \quad \sigma \times \sigma = 1 + \varepsilon.$

Associativity relations:



Braiding rules:

Definition of R_z^{xy}:

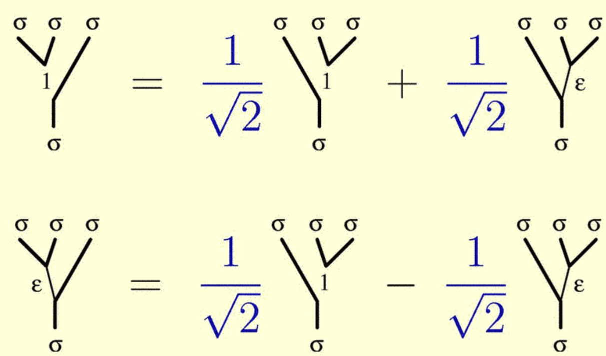


$R_1^{\varepsilon\varepsilon} = -1, \quad R_1^{\sigma\sigma} = \exp\left(-\frac{\pi}{8}i\right),$

$R_\sigma^{\varepsilon\sigma} = R_\sigma^{\sigma\varepsilon} = -i, \quad R_\varepsilon^{\sigma\sigma} = \exp\left(\frac{3\pi}{8}i\right).$

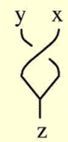
This algebraic structure is also found in the conformal field theory corresponding to the Ising model at the critical point.

Associativity relations



Each tree diagram represents a particular way of splitting $\sigma \to \sigma\sigma\sigma$.

Braiding rules

Notation: 

$= R_z^{xy}$ 

$$R_1^{\varepsilon\varepsilon} = -1, \qquad R_1^{\sigma\sigma} = \exp\left(-\frac{\pi}{8}i\right),$$

$$R_\sigma^{\varepsilon\sigma} = R_\sigma^{\sigma\varepsilon} = -i, \qquad R_\varepsilon^{\sigma\sigma} = \exp\left(\frac{3\pi}{8}i\right).$$

There are also Abelian phase factors associated with the charge.

Computation by anyons

- State preparation: the creation of particle-antiparticle pairs
- Unitary operators: braiding (by dragging the anyons with a moving potential well)
- Measurement: the fusion of two quasiparticles (we need to actually measure the type of the resulting particle).

All these operations are intrinsically fault-tolerant. But are they universal?

The answer depends on the type of anyonic theory

Not universal:

- Pfaffian state
- Quantum $\mathbf{SU}(2)$ at level 2
- The honeycomb lattice model

But all these systems are still good for the realization of decoherence-protected quantum memory. The computational univerality can be achieved using certain *ancillary states prepared by non-topological means* (see recent article by S. Bravyi).

Universal:

- Quantum $\mathbf{SU}(2)$ at level 3 (Freedman, Larsen, Wang 2000)
- Parafermions (FQHE at $\nu = 12/5$)
- "Fibonacchi theory" ($\mathbf{SO}(3)$ at level 3)
- Drinfeld double of S_5 (Kitaev 1997)
- Drinfeld double of S_3 (Mochon 2003)

Alternative approach:

Protected qubits in Josephson junction arrays

- Doucot, Vidal (2002); Ioffe, Feigelman (2002)
- Kitaev (work in progress)

Potential advantage:

Elements are connected by wires (like in conventional electronics).