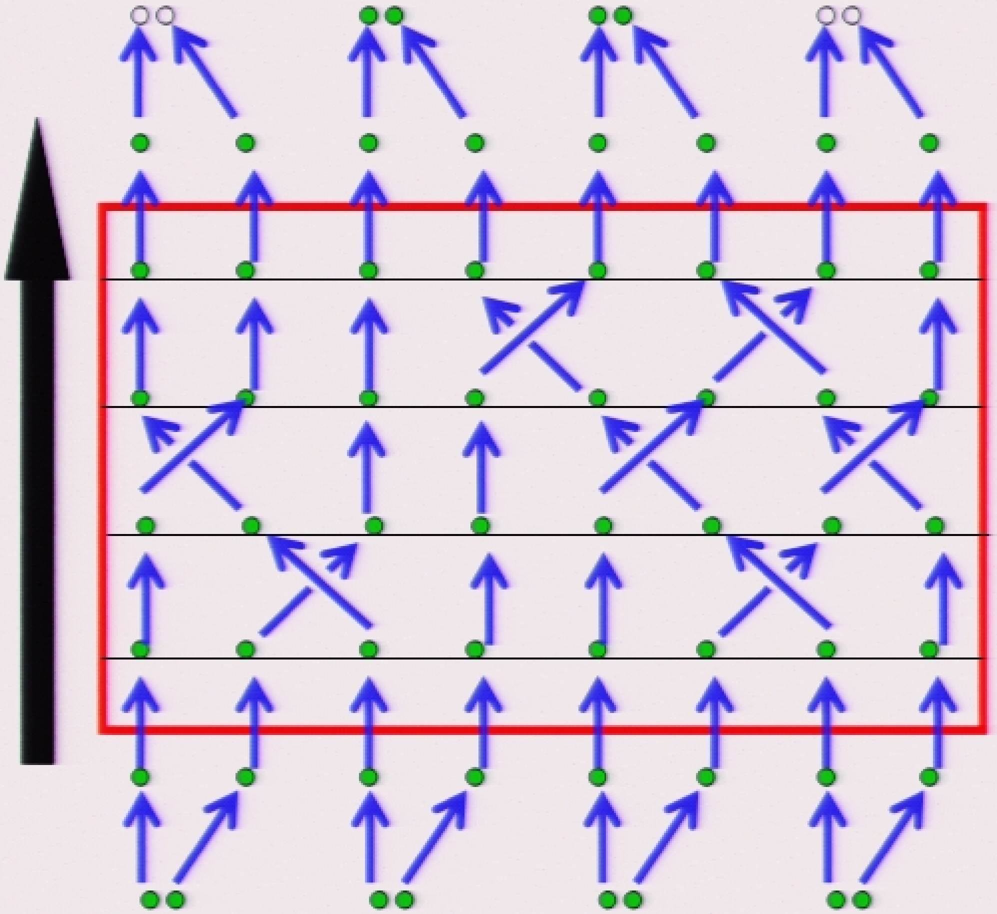
Topological quantum computing for beginners

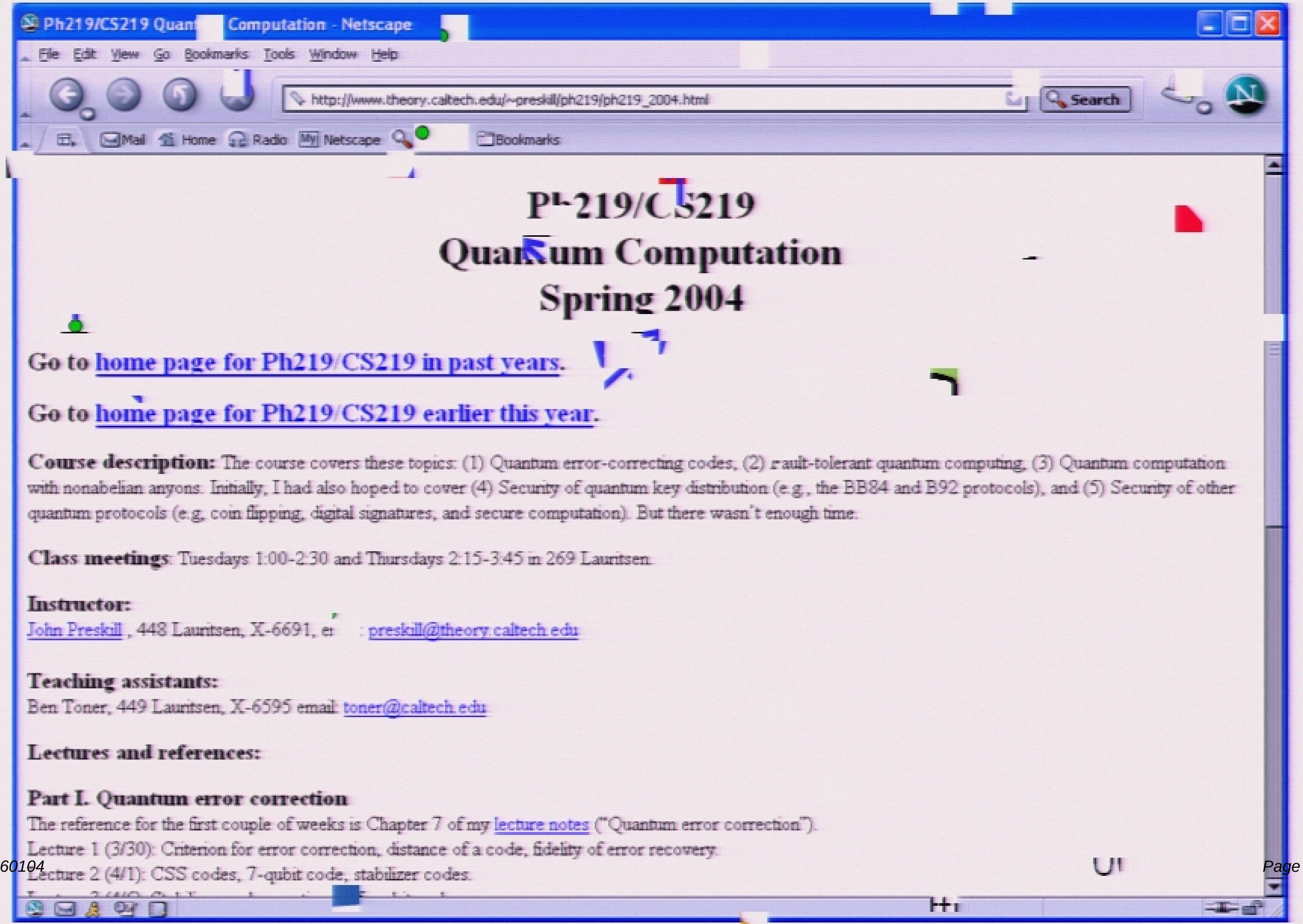


John Preskill, Caltech
Perimeter Institute
29 June 2005
http://www.iqi.caltech.edu/

IQI Institute for Quantum Information

Sponsored by the NSF

http://www.theory.caltech.edu/~preskill/ph219/ph219_2004.html


Ph219/CS219 Quantum Computation - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.theory.caltech.edu/~preskill/ph219/ph219_2004.html
Search
Mail Home Radio Netscape
Bookmarks

Ph219/CS219
Quantum Computation
Spring 2004

Go to home page for Ph219/CS219 in past years.

Go to home page for Ph219/CS219 earlier this year.

Course description: The course covers these topics: (1) Quantum error-correcting codes, (2) Fault-tolerant quantum computing, (3) Quantum computation with nonabelian anyons. Initially, I had also hoped to cover (4) Security of quantum key distribution (e.g., the BB84 and B92 protocols), and (5) Security of other quantum protocols (e.g, coin flipping, digital signatures, and secure computation). But there wasn't enough time.

Class meetings: Tuesdays 1:00-2:30 and Thursdays 2:15-3:45 in 269 Lauritsen.

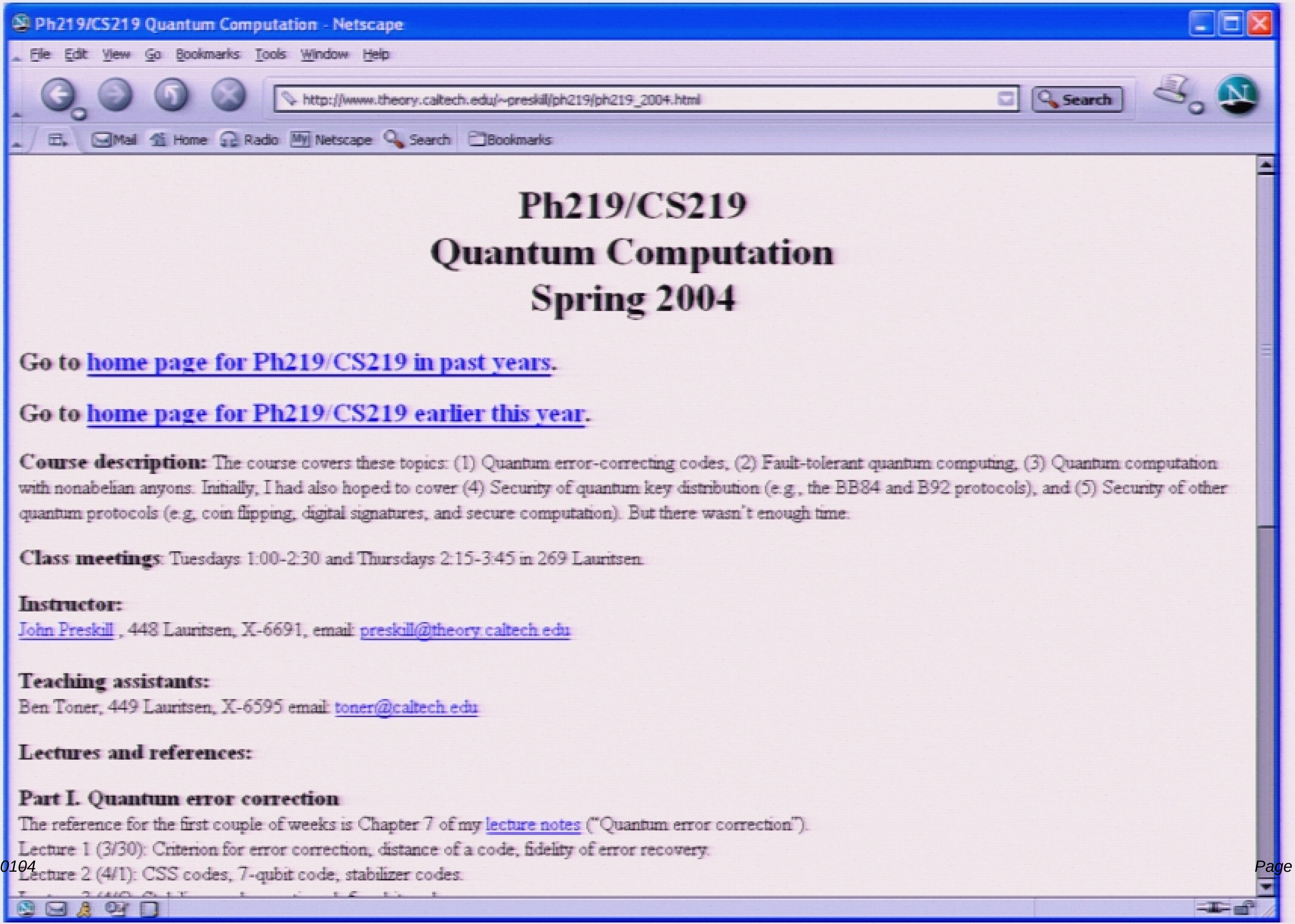
Instructor:
John Preskill , 448 Lauritsen, X-6691, email: preskill@theory.caltech.edu

Teaching assistants:
Ben Toner, 449 Lauritsen, X-6595 email: toner@caltech.edu

Lectures and references:

Part I. Quantum error correction
The reference for the first couple of weeks is Chapter 7 of my lecture notes ("Quantum error correction").
Lecture 1 (3/30): Criterion for error correction, distance of a code, fidelity of error recovery.
Lecture 2 (4/1): CSS codes, 7-qubit code, stabilizer codes.

http://www.theory.caltech.edu/~preskill/ph219/ph219_2004.html


Ph219/CS219 Quantum Computation - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.theory.caltech.edu/~preskill/ph219/ph219_2004.html
Search
Mail Home Radio Netscape Search Bookmarks

Ph219/CS219
Quantum Computation
Spring 2004

Go to home page for Ph219/CS219 in past years.

Go to home page for Ph219/CS219 earlier this year.

Course description: The course covers these topics: (1) Quantum error-correcting codes, (2) Fault-tolerant quantum computing, (3) Quantum computation with nonabelian anyons. Initially, I had also hoped to cover (4) Security of quantum key distribution (e.g., the BB84 and B92 protocols), and (5) Security of other quantum protocols (e.g. coin flipping, digital signatures, and secure computation). But there wasn't enough time.

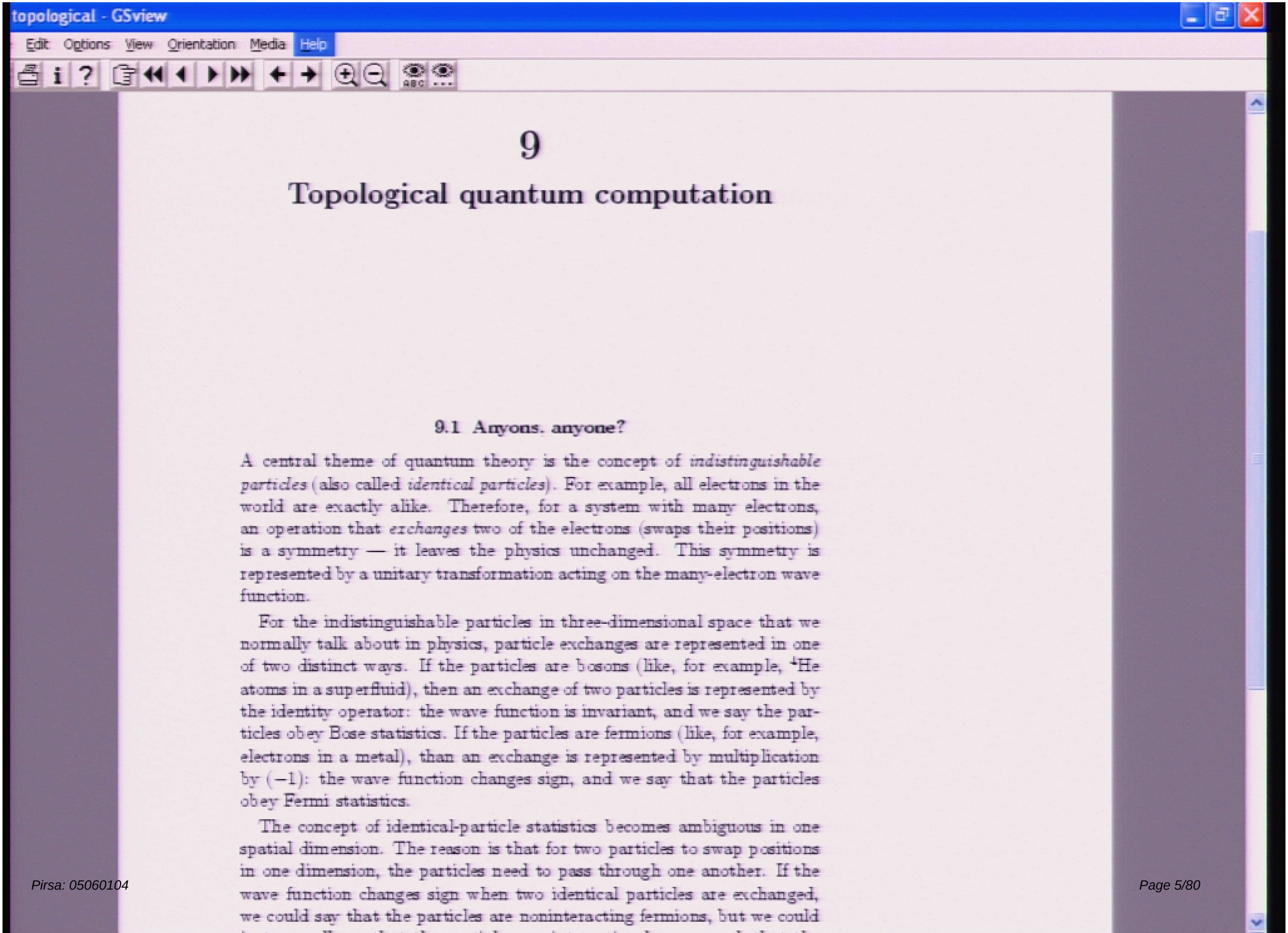
Class meetings: Tuesdays 1:00-2:30 and Thursdays 2:15-3:45 in 269 Lauritsen.

Instructor:
John Preskill , 448 Lauritsen, X-6691, email: preskill@theory.caltech.edu

Teaching assistants:
Ben Toner, 449 Lauritsen, X-6595 email: toner@caltech.edu

Lectures and references:

Part I. Quantum error correction
The reference for the first couple of weeks is Chapter 7 of my lecture notes ("Quantum error correction").
Lecture 1 (3/30): Criterion for error correction, distance of a code, fidelity of error recovery.
Lecture 2 (4/1): CSS codes, 7-qubit code, stabilizer codes.



9
Topological quantum computation

9.1 Anyons, anyone?

A central theme of quantum theory is the concept of *indistinguishable particles* (also called *identical particles*). For example, all electrons in the world are exactly alike. Therefore, for a system with many electrons, an operation that *exchanges* two of the electrons (swaps their positions) is a symmetry — it leaves the physics unchanged. This symmetry is represented by a unitary transformation acting on the many-electron wave function.

For the indistinguishable particles in three-dimensional space that we normally talk about in physics, particle exchanges are represented in one of two distinct ways. If the particles are bosons (like, for example, ^{4}He atoms in a superfluid), then an exchange of two particles is represented by the identity operator: the wave function is invariant, and we say the particles obey Bose statistics. If the particles are fermions (like, for example, electrons in a metal), than an exchange is represented by multiplication by (-1): the wave function changes sign, and we say that the particles obey Fermi statistics.

The concept of identical-particle statistics becomes ambiguous in one spatial dimension. The reason is that for two particles to swap positions in one dimension, the particles need to pass through one another. If the wave function changes sign when two identical particles are exchanged, we could say that the particles are noninteracting fermions, but we could

Kitaev

Freedman

Kitaev

Kitaev, Fault-tolerant quantum computation by anyons (1997).

Preskill and Ogburn, Topological quantum computation (1997).

Preskill, Fault-tolerant quantum computation (1997).

Mochon, Anyons from non-solvable groups are sufficient for universal quantum computation (2003).

Mochon, Anyon computers with smaller groups (2004).

Freedman

Freedman, Larsen, and Wang, A modular functor which is universal for quantum computation (2000).

Freedman, Kitaev, and Wang, Simulation of topological field theories by quantum computers (2000).

Quantum Computation

Feynman ‘81

Deutsch ‘85

Shor ‘94

A computer that operates on quantum states can perform tasks that are beyond the capability of any conceivable classical computer.

Feynman ‘81

Deutsch ‘85

Shor ‘94

Quantum computer: the model

(1) Hilbert space of *n* qubits: $\mathfrak{H} = \left(\mathbb{C}^{2^n}\right)$

spanned by

$$|x\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle, \; x \in \{0,1\}^n$$

Important: the Hilbert space is equipped with a natural tensor-product decomposition into subsystems.

$$\mathbb{C}^{2^n} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}}$$

Physically, this decomposition arises from spatial locality. Elementary operations ("quantum gates") that act on a small number of qubits (independent of *n)* are "easy;" operations that act on many qubits (increasing with *n*) are "hard."

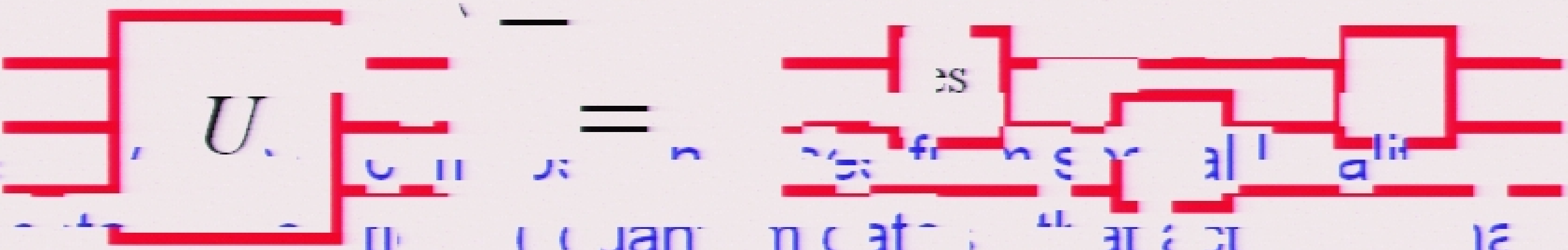
(2) Initial state: $|000\ldots0\rangle = |0\rangle^{\otimes n}$

Quantum computer: the model

(3) A finite set of fundamental quantum gates.

$$\{U_1, U_2, U_3, \ldots U_{n_G}\}$$

Each gate is a unitary transformation acting on a bounded number of qubits. The gates form a universal set: arbitrary unitary transformations can be constructed, to any specified accuracy, as a quantum circuit constructed from the gates.



(Universal gates are generic.)

Important: One universal set of gates can simulate another efficiently, so there is a notion of complexity that is independent of the details of the quantum hardware.

Quantum computer: the model

(4) Classical control:

The construction of a quantum circuit is directed by a classical computer, *i.e.*, a Turing machine. (We're not interested in what a quantum circuit can do unless the circuit can be designed efficiently by a classical machine.)

(5) Readout:

At the end of the quantum computation, we read out the result by measuring σ_z , *i.e.*, projecting onto the basis $\{|0\rangle, |1\rangle\}$

(We don't want to hide computational power in the ability to perform difficult measurements.)

Quantum computer: the model

(1) *n* qubits
(2) initial state
(3) quantum gates
(4) classical control
(5) readout

Clearly, the model can be simulated by a classical computer with access to a random number generator. But there is an exponential slowdown, since the simulation involves matrices of exponential size.

The quantum computer might solve efficiently some problems that can't be solved efficiently by a classical computer. ("Efficiently" means that the number of quantum gates = polynomial of the number of bits of input to the problem.)

Quantum Error Correction

Shor ‘95

Steane ‘95

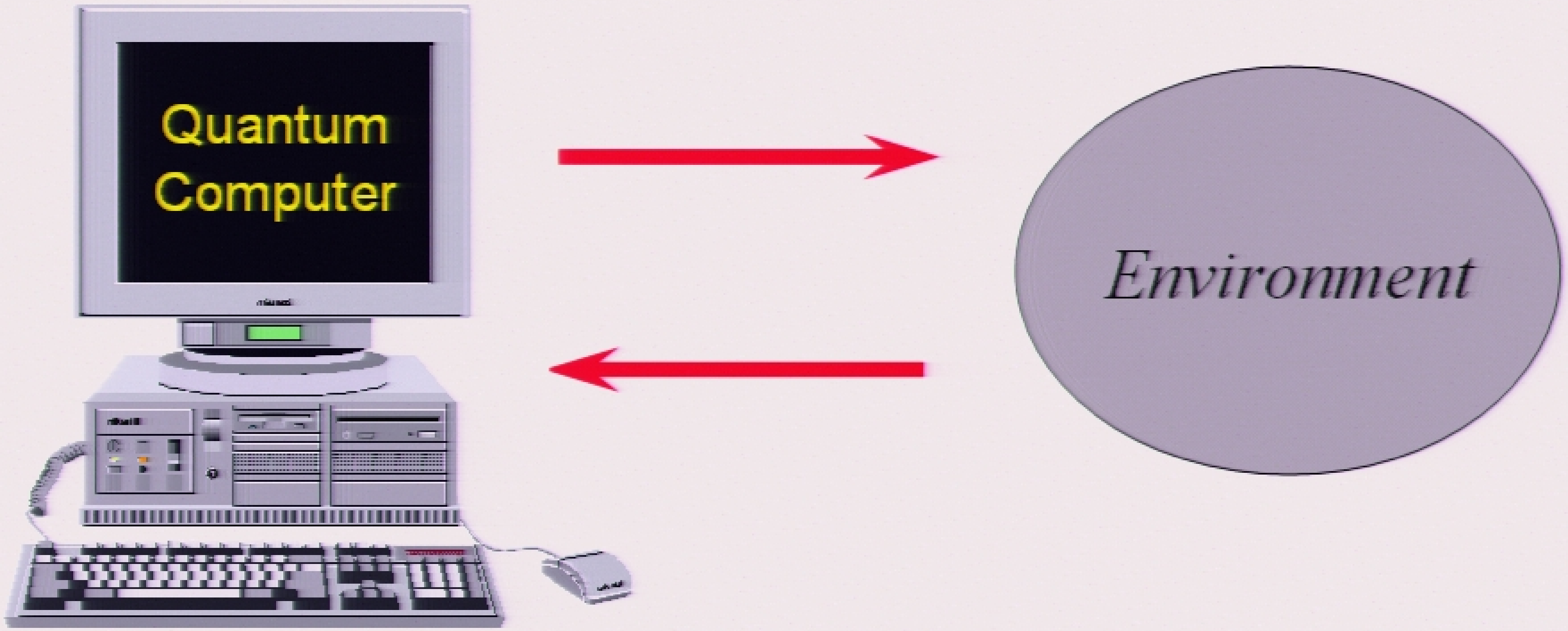
Quantum information can be protected, and processed fault-tolerantly.

Shor ‘95

Steane ‘95

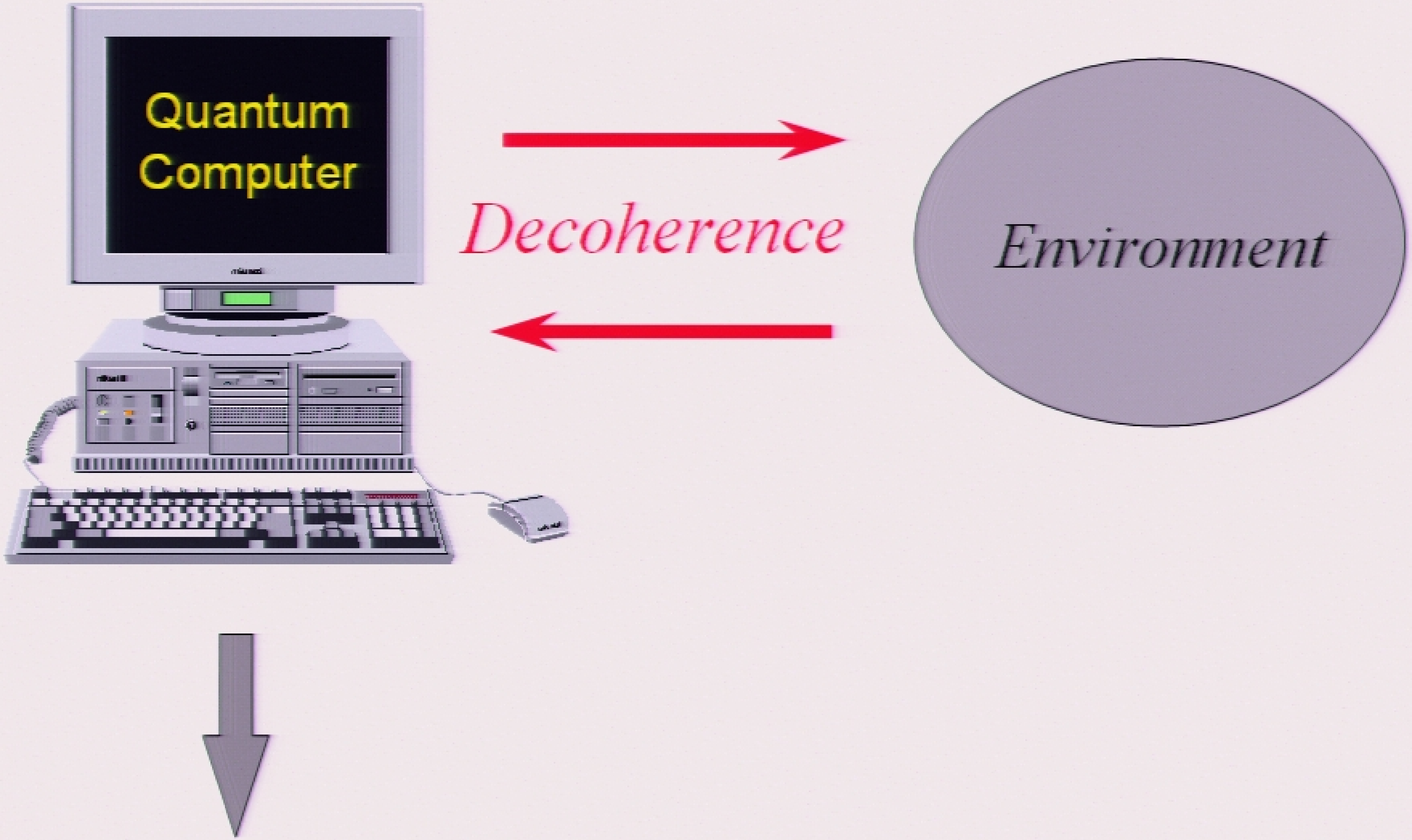
Quantum
Computer

Environment



Quantum Computer

Environment



Quantum Computer

Decoherence

Environment

ERROR!

Fault-tolerant quantum computing

Threshold Theorem: Suppose that faults occur independently at the locations within a quantum circuit, where the probability of a fault at each location is no larger than ε. Then there exists $\varepsilon_0 > 0$ such that for a fixed $\varepsilon < \varepsilon_0$ and fixed $\delta > 0$, any circuit of size L can be simulated by a circuit of size L^* with fidelity greater than 1-δ, where, for some constant c,

$$L^* = O\left[L(\log L)^c \right]$$

The numerical value of the *accuracy threshold* ε_0 is of practical interest --- we know that $\varepsilon_0 > 2.7 \times 10^{-5}$ ... (and believe that the threshold is much larger, *e.g.*, $\varepsilon_0 > 10^{-2}$.)

Essential asumptions:

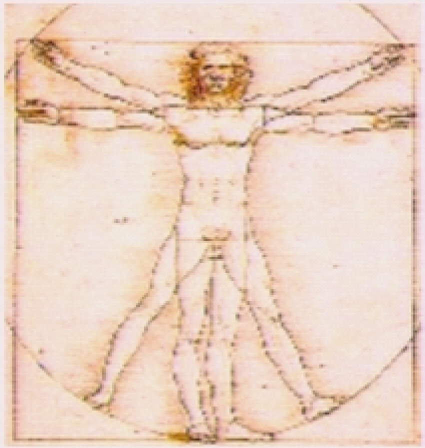
- *Constant fault rate* (independent of number of qubits).
- *Weakly correlated faults* (both in space and in time).
- *Parallelism* (to correct errors in all blocks simultaneously.)
- *Reusable memory* (to refresh ancillas that carry away entropy introduced by errors).

Helpful assumptions (used in threshold estimates):

- *Fast measurements* (to read out error syndromes -- without measurement, threshold is more demanding).
- *Fast classical processing* (to interpret error syndromes).
- *Nonlocal gates* (with local gates, threshold is more demanding).
- *No "leakage"* (e.g., loss of qubits).

Two Physical Systems

What is the difference between:

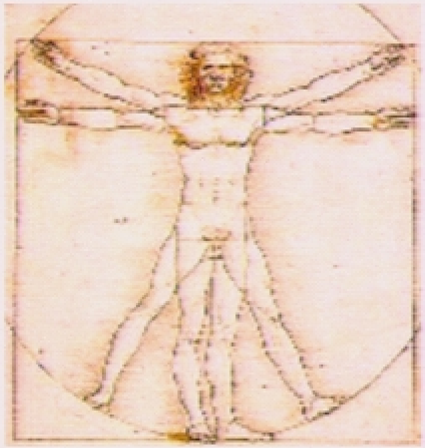


A: Human

B: Chip

Two Physical Systems

What is the difference between:



A: Human

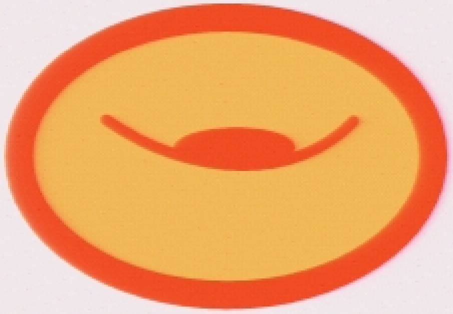
B: Chip

Imperfect hardware.
Hierarchical architecture with
error correction at all scales...

Reliable hardware.

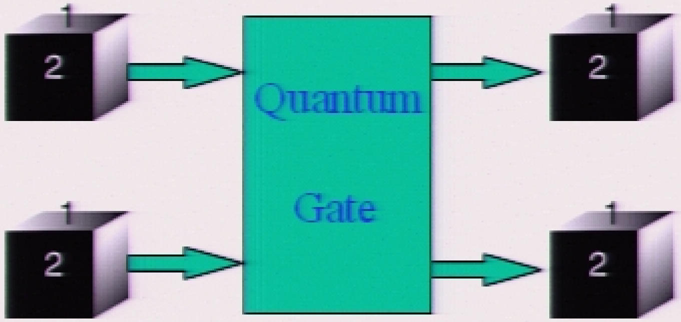
Information *processing* prevents information *loss*.

Topology

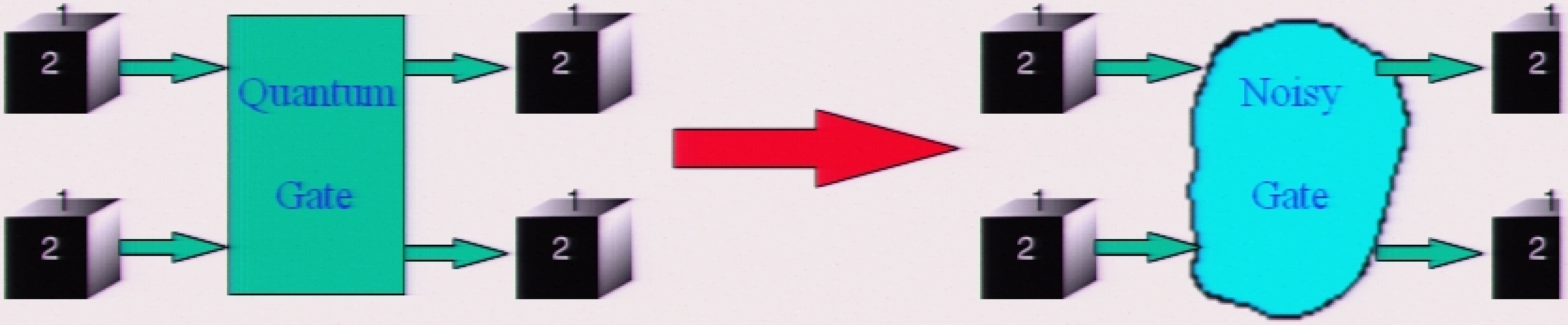


Topology

Topology



Topology

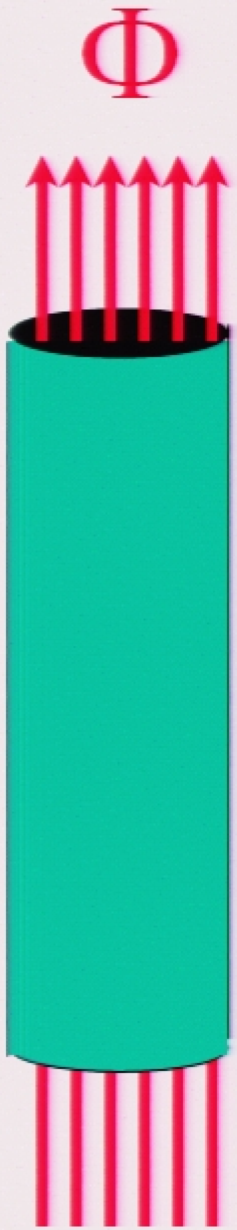


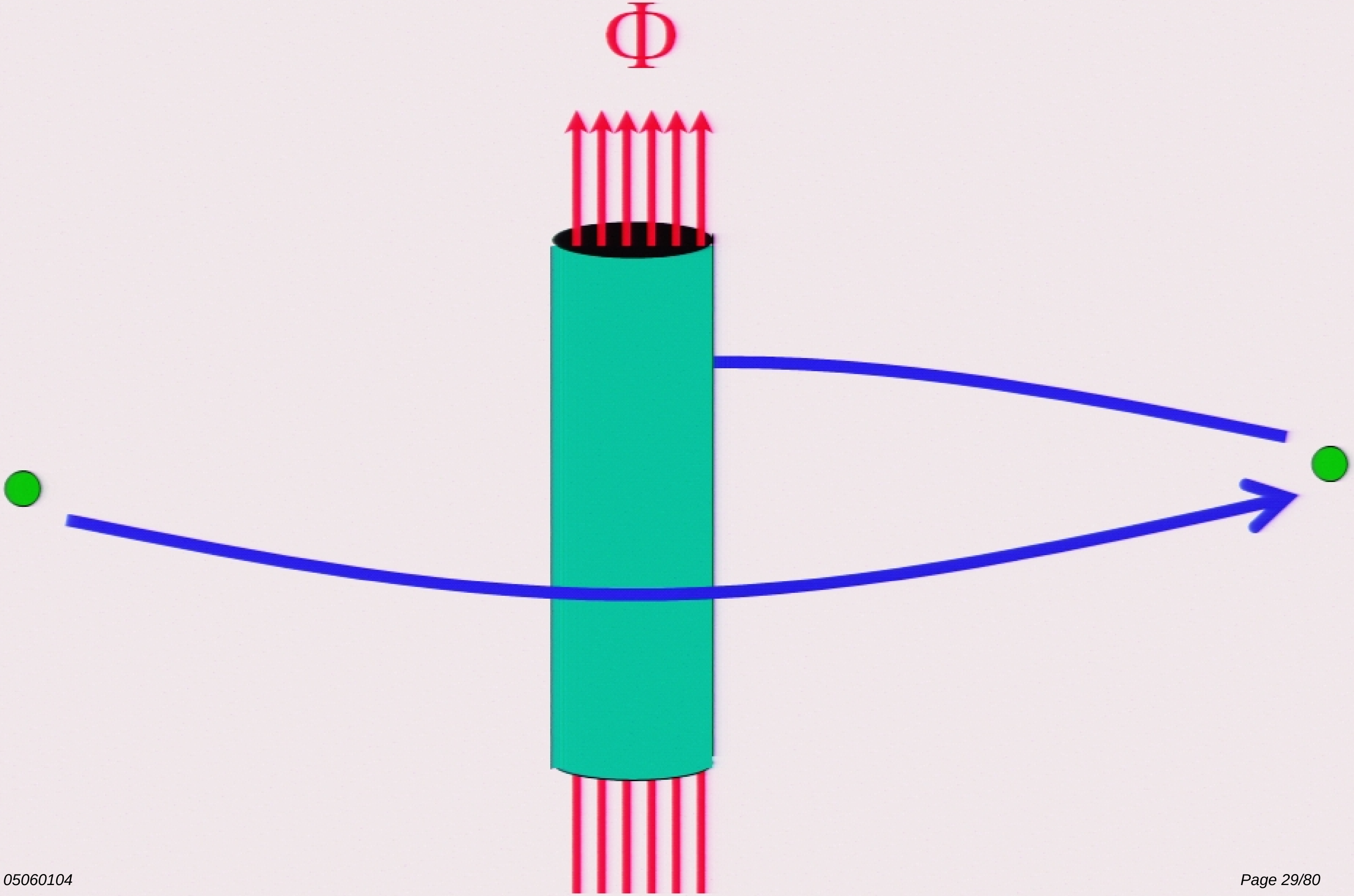
Quantum

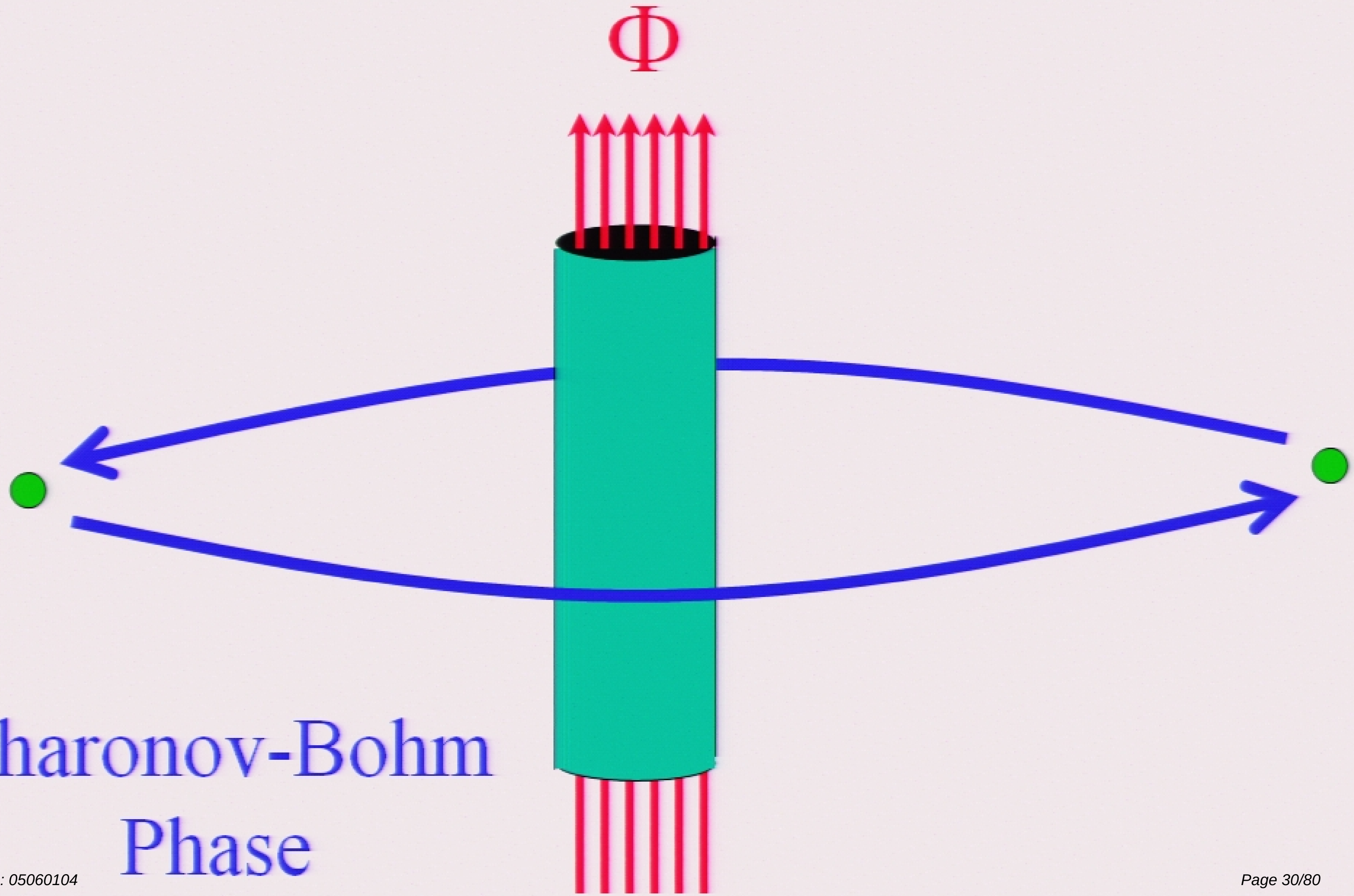
Gate

Noisy

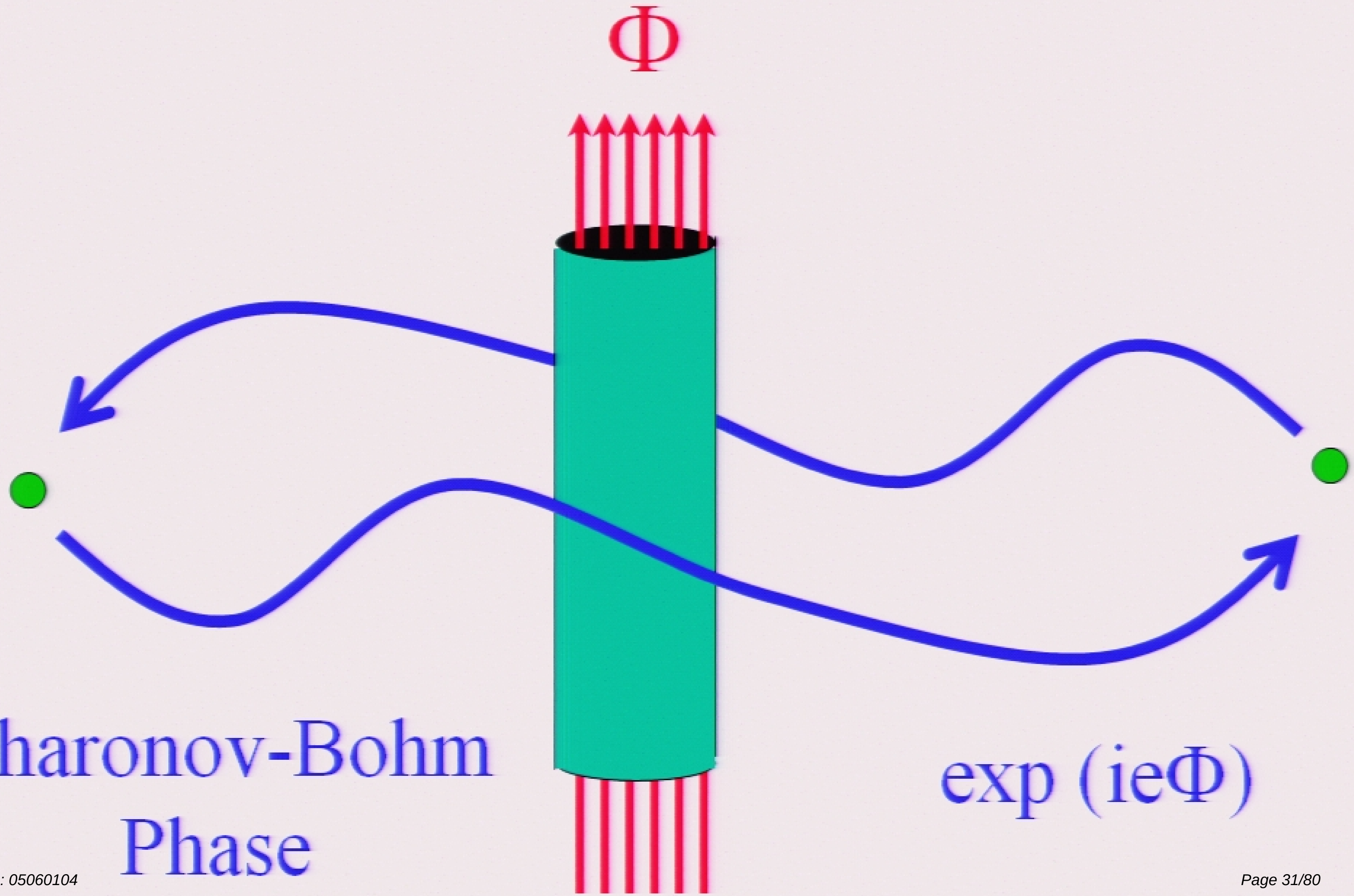
Gate


Φ


Φ



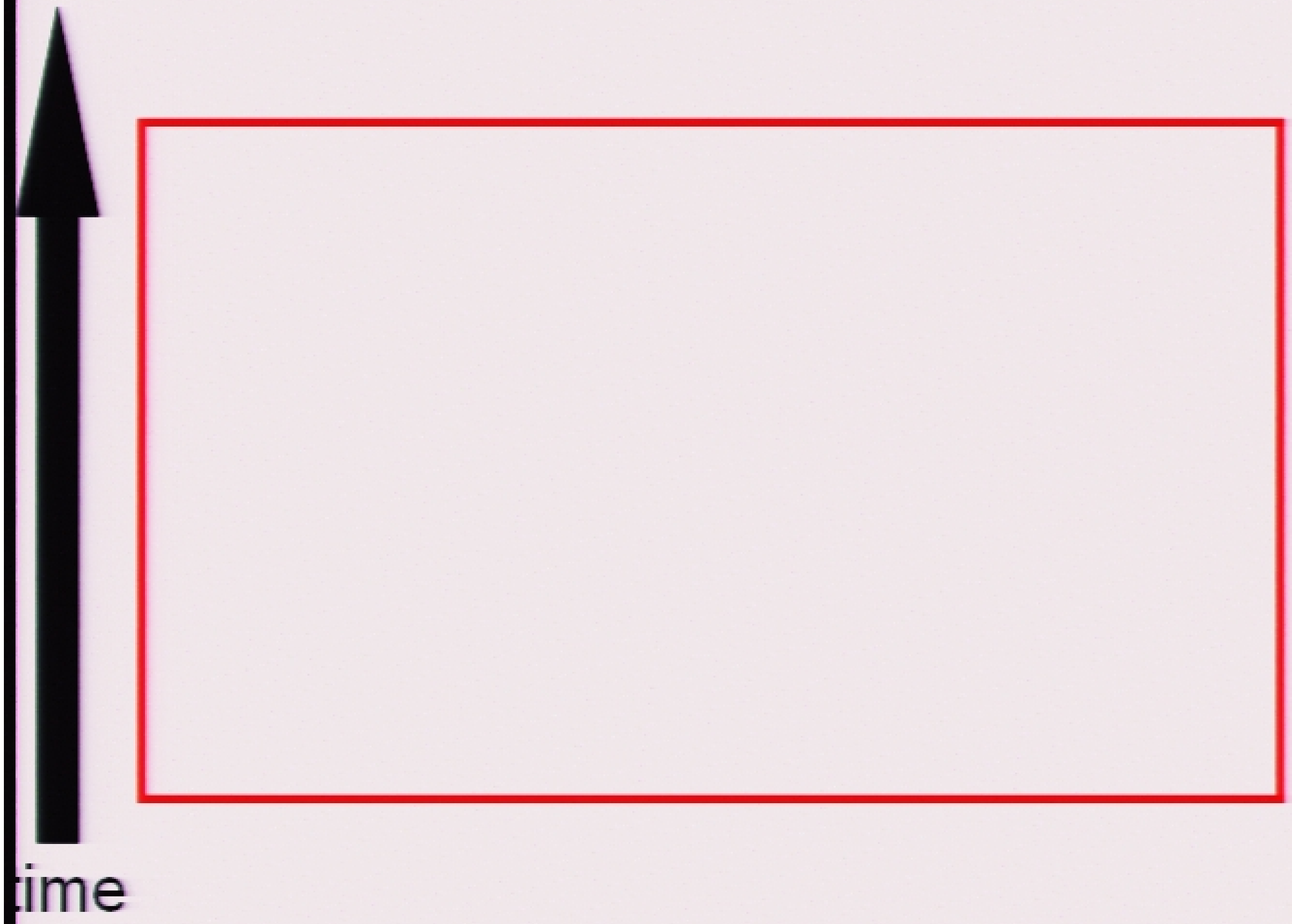
Aharonov-Bohm Phase



Aharonov-Bohm Phase

$\exp(ie\Phi)$

Topological quantum computation (Kitaev '97, FLW '00)

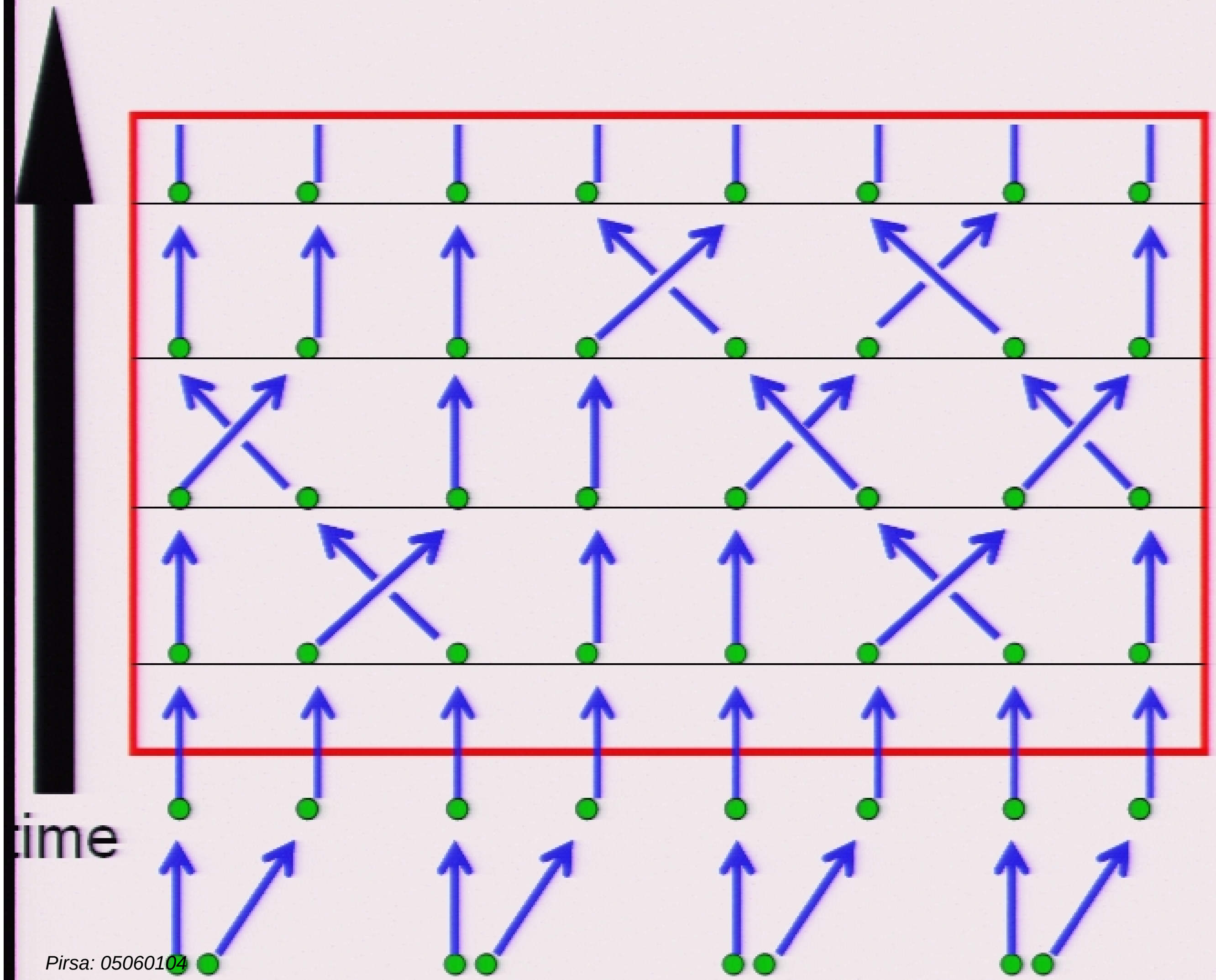


Kitaev

Freedman

Topological quantum computation

(Kitaev '97, FLW '00)



time

braid

braid

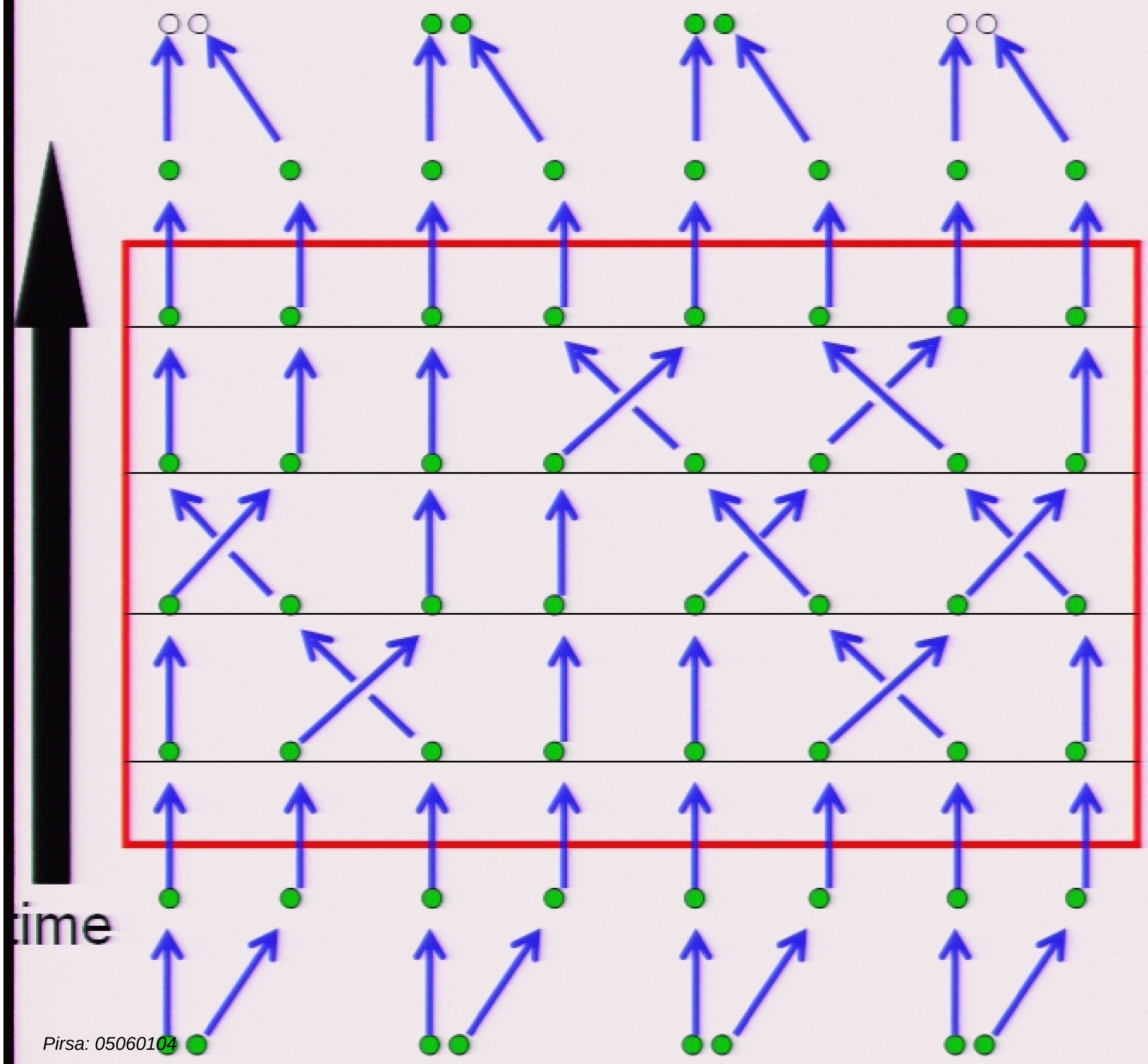
braid

create pairs

Kitaev

Freedman

Topological quantum computation (Kitaev '97, FLW '00)



Physical fault tolerance with nonabelian anyons:

uncontrolled exchange of quantum numbers will be rare if particles are widely separated, and thermal anyons are suppressed...

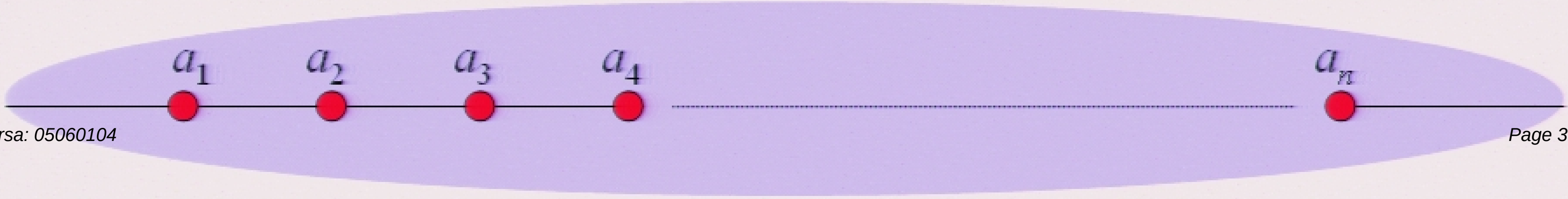
Models of (nonabelian) anyons

A model of anyons is a theory of a two-dimensional medium with a mass gap, where the particles carry locally conserved charges. We define the model by specifying:

1. A finite list of particle *labels* $\{a,b,c,\ldots\}$. These indicate the possible values of the conserved charge that a particle can carry. If a particle is kept isolated from other particles, its label never changes. There is a special label "0" – indicating trivial charge, and a charge conjugation operator C: $a \leftrightarrow \bar{a}$ (where $\bar{0}$=0). (Note: for "particle" you may read "puncture.")

2. Rules for *fusing* (and splitting). These specify the possible values of the charge that can result when two charged particles are combined.

3. Rules for *braiding*. These specify what happens when two neighboring particles are exchanged (or when one is rotated by 2π).

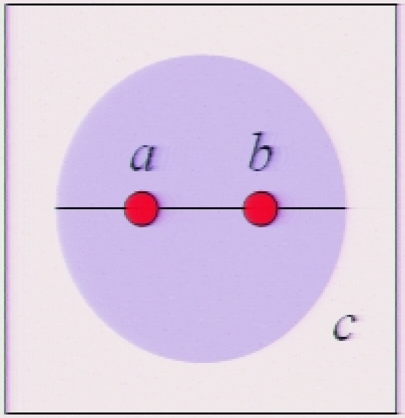


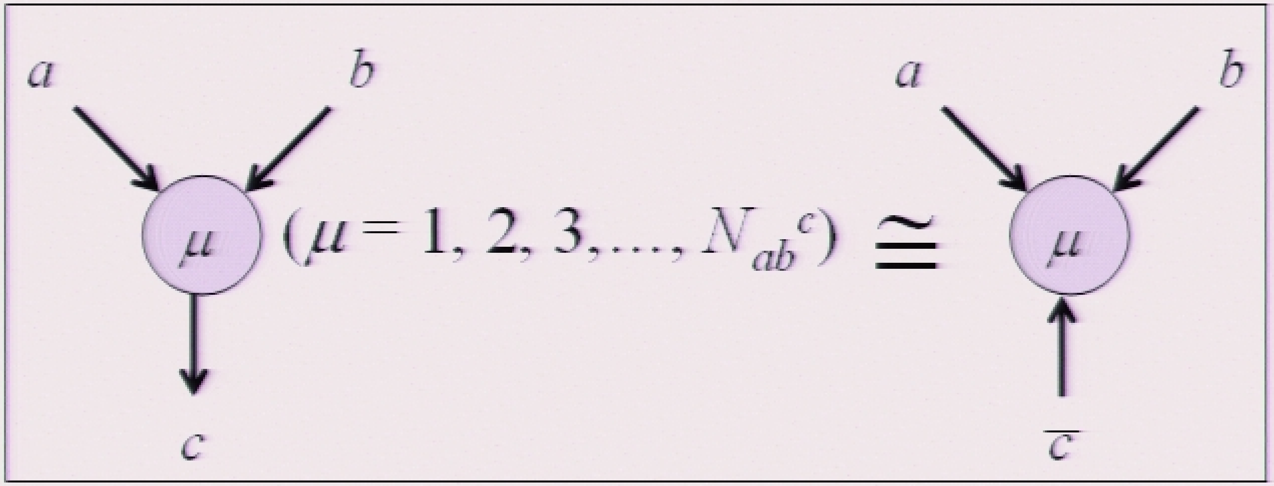
Fusion

Fusion rules: $a \times b = \sum_c N_{ab}^c c = b \times a$

Fusion vector space: $V_{ab}^c \cong V_{ba}^c \cong V_{ab\bar{c}}^0 \cong \cdots$

$$\dim(V_{ab}^c) \cong N_{ab}^c$$





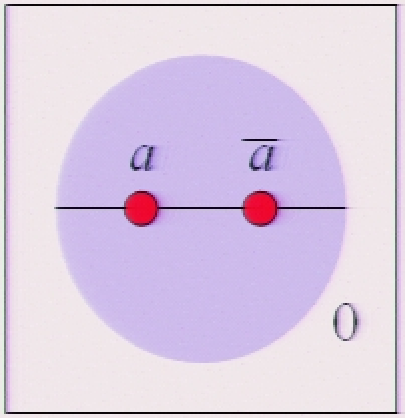
(Cf., *intertwiners*, in group representation theory.)

Fusion

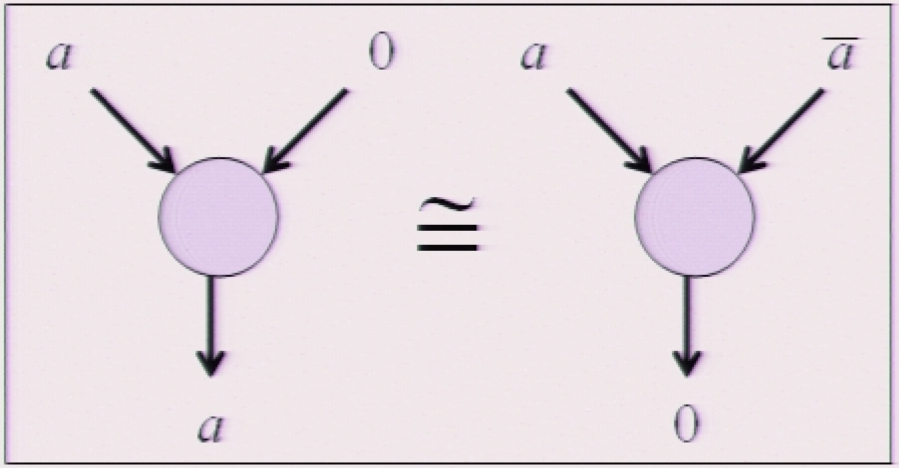
Fusion rules: $$a\times b=\sum_{c}N_{ab}^{c}c=b\times a$$

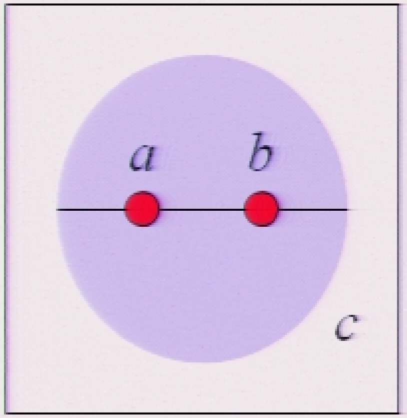
Fusion vector space: $$V_{ab}^{c}\cong V_{ba}^{c}\cong V_{ab\bar{c}}^{0}\cong\cdots$$

$$\dim(V_{ab}^{c})\cong N_{ba}^{c}$$

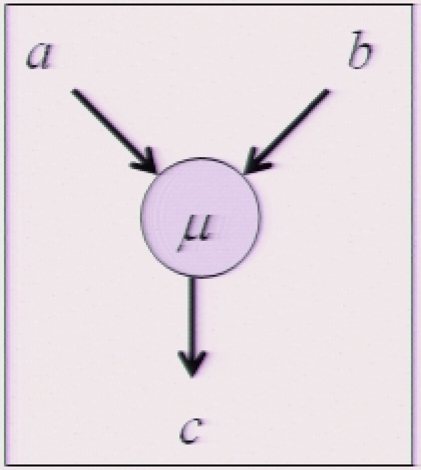


The charge 0 fuses trivially, and $\bar{a}$ is the unique label that can fuse with a to yield charge 0.





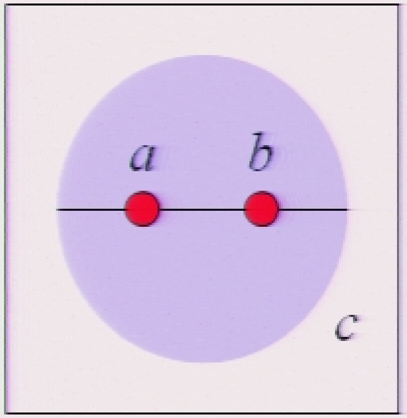
Fusion



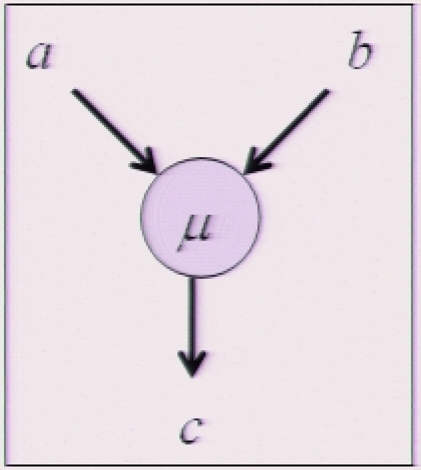
An anyon model is said to be *nonabelian* if for some a, and b,

$$\dim\left(\bigoplus_c V_{ab}^c\right) \cong \sum_c N_{ba}^c \geq 2.$$

Then there is a “topological Hilbert space” that can encode nontrivial quantum information. This encoding is *nonlocal*; the information is a *collective* property of the two anyons, not localized on either particle. When the particles with labels a and b are far apart, different states in the topological Hilbert space look identical to local observers. In particular, the quantum states are invulnerable to *decoherence* due to local interactions with the environment. *That* is why we propose to use this encoding in a quantum computer.



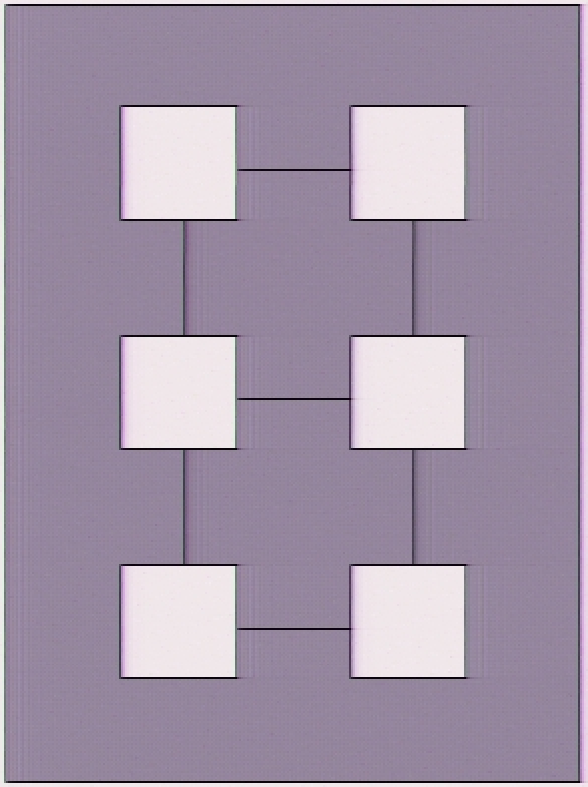
Fusion



When we hide the quantum state from the environment, we hide it from ourselves as well! But, when we are ready to read out the quantum state (for example, at the conclusion of a quantum computation), we can make the information locally visible again by bringing the two particles together, fusing them into a single object. Then we ask, what is this object's label? In fact, it suffices (for universal quantum computation) to be able to distinguish the label $c = 0$ from $c \neq 0$. It is physically reasonable to suppose that we can distinguish annihilation "into the vacuum" ($c = 0$) from a lump that is unable to decay because of its conserved charge ($c \neq 0$).

Abelian vs. nonabelian

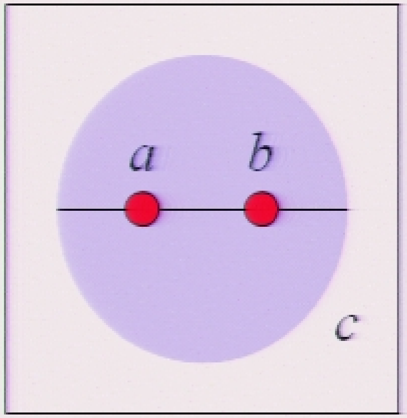
Abelian anyon models can also be used for robust quantum memory, e.g., a model of $\mathbb{Z}_2$ fluxons and their dual $\mathbb{Z}_2$ charges. A qubit is realized because the $\mathbb{Z}_2$ flux in a hole can be either trivial or nontrivial (the information is carried by the labels themselves, not by the *fusion* states). This information is hidden from the environment by making the holes large and keeping them far apart (to prevent flux from tunneling from one hole to another, or to the outside edge, and to prevent the world lines of charges from winding about holes). -- Kitaev (1996)



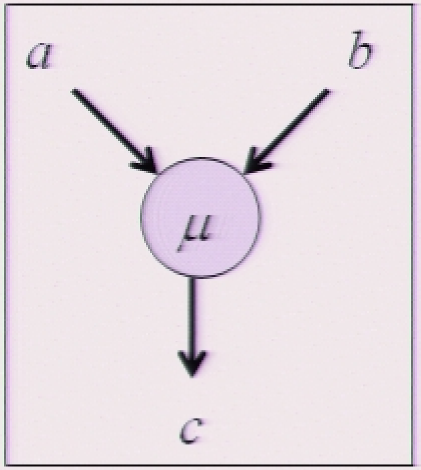
However, this information may not be easy to read out. We'd need to contract a hole to see if a particle appears, or perform a delicate interference experiment to detect the flux, or ...

Alternatively, by mixing the $\mathbb{Z}_2$ with electromagnetic $\mathrm{U}(1)$, we might do the readout via a Senthil-Fisher type experiment (i.e., one that would actually *work*)! -- Ioffe et al. (2002)

Anyway, with nonabelian anyons we can exploit topology not just to store quantum information, but also to process it!

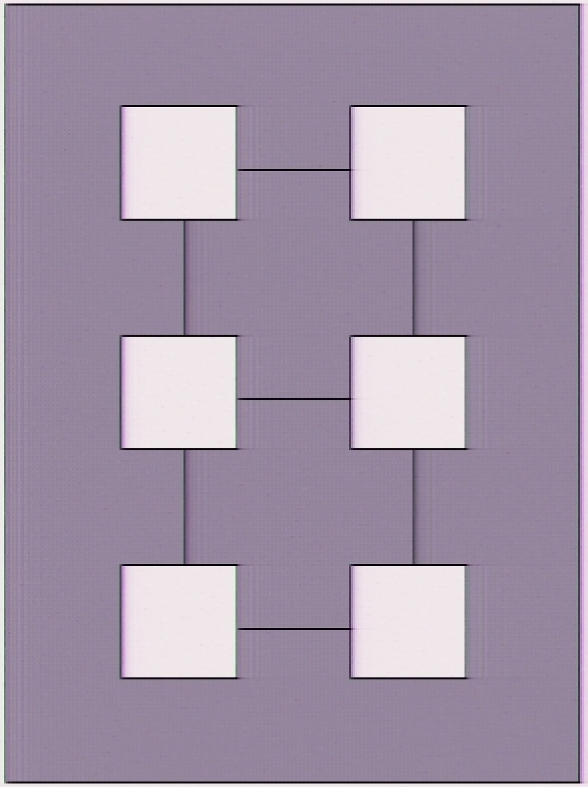


Fusion



When we hide the quantum state from the environment, we hide it from ourselves as well! But, when we are ready to read out the quantum state (for example, at the conclusion of a quantum computation), we can make the information locally visible again by bringing the two particles together, fusing them into a single object. Then we ask, what is this object's label? In fact, it suffices (for universal quantum computation) to be able to distinguish the label $c = 0$ from $c \neq 0$. It is physically reasonable to suppose that we can distinguish annihilation "into the vacuum" ($c = 0$) from a lump that is unable to decay because of its conserved charge ($c \neq 0$).

Abelian vs. nonabelian



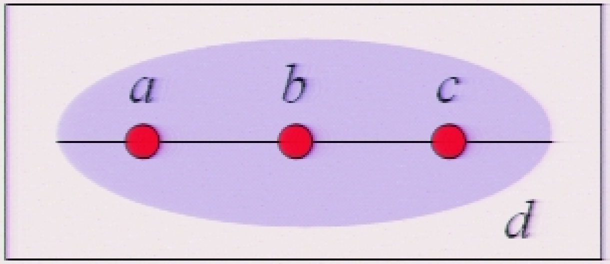
Abelian anyon models can also be used for robust quantum memory, e.g., a model of $\mathbb{Z}_2$ fluxons and their dual $\mathbb{Z}_2$ charges. A qubit is realized because the $\mathbb{Z}_2$ flux in a hole can be either trivial or nontrivial (the information is carried by the labels themselves, not by the *fusion* states). This information is hidden from the environment by making the holes large and keeping them far apart (to prevent flux from tunneling from one hole to another, or to the outside edge, and to prevent the world lines of charges from winding about holes). -- Kitaev (1996)

However, this information may not be easy to read out. We'd need to contract a hole to see if a particle appears, or perform a delicate interference experiment to detect the flux, or ...

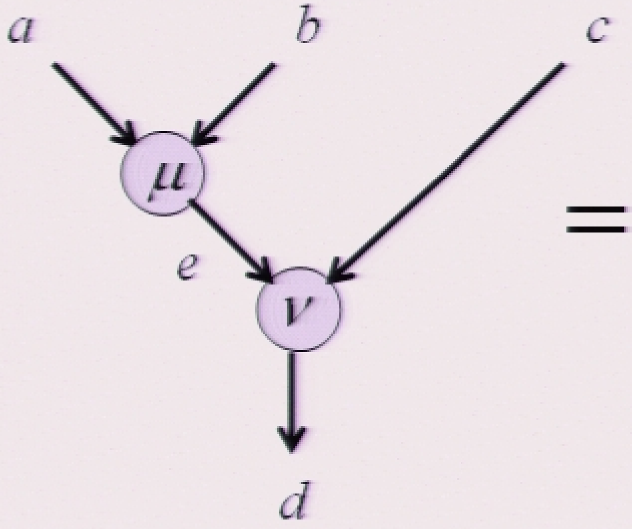
Alternatively, by mixing the $\mathbb{Z}_2$ with electromagnetic $\mathrm{U}(1)$, we might do the readout via a Senthil-Fisher type experiment (i.e., one that would actually *work*)! -- Ioffe et al. (2002)

Anyway, with nonabelian anyons we can exploit topology not just to store quantum information, but also to process it!

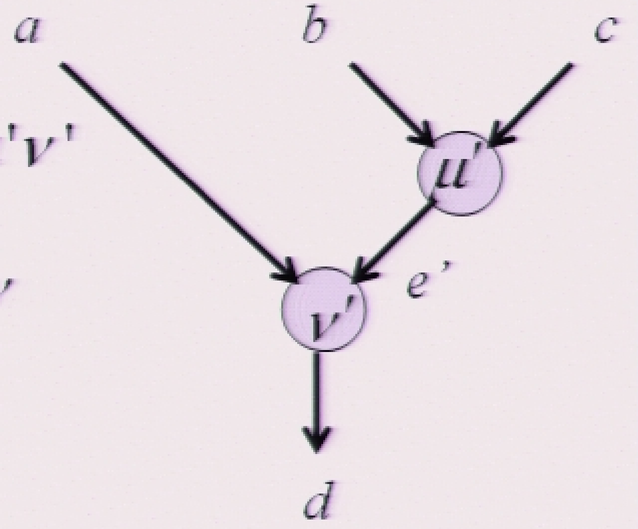
Associativity of fusion: the F-matrix



$$(a\times b)\times c = a\times(b\times c)$$

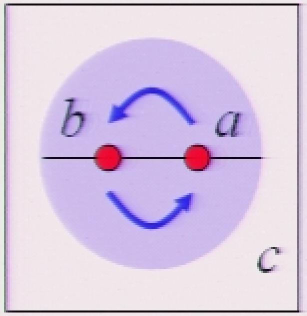


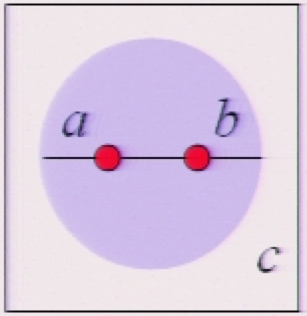
$$= \sum_{e'\mu'\nu'} \left(F^{d}_{abc}\right)^{e'\mu'\nu'}_{e\mu\nu}$$

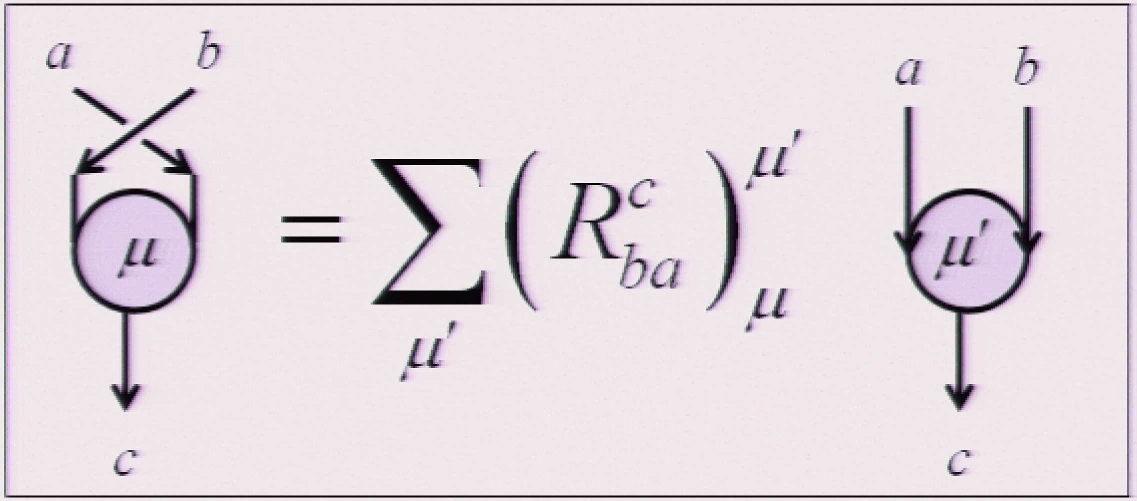


There are two natural ways to decompose the topological Hilbert space V^{d}_{abc} of three anyons in terms of the fusion spaces of pairs of particles. These two orthonormal bases are related by a unitary transformation, the F-*matrix*. (Cf., the 6j-*symbols*, in group representation theory.)

Braiding: the R-matrix $\quad R: \; V^c_{ba} \to V^c_{ab}$:

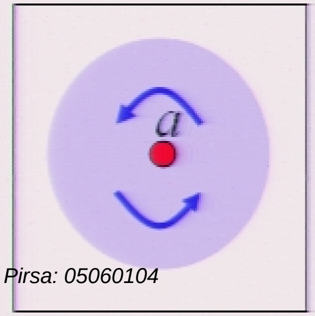




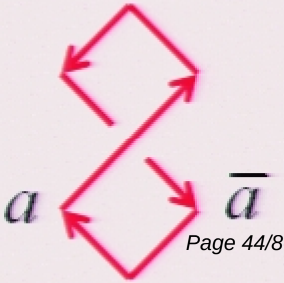


$$= \sum_{\mu'} \left(R^c_{ba} \right)^{\mu'}_{\mu}$$

When two neighboring anyons are exchanged counterclockwise, heir total charge c is unaltered; since the particles swap positions, he fusion space V^c_{ba} changes to the isomorphic space V^c_{ab}. This somorphism is represented by a unitary matrix, the *R-matrix*.



The R-matrix also determines the *topological spin* of the label a, *i.e.*, the phase acquired when the particle is rotated by 2π: $\quad e^{2\pi i J_a} = R^0_{a\bar{a}}$

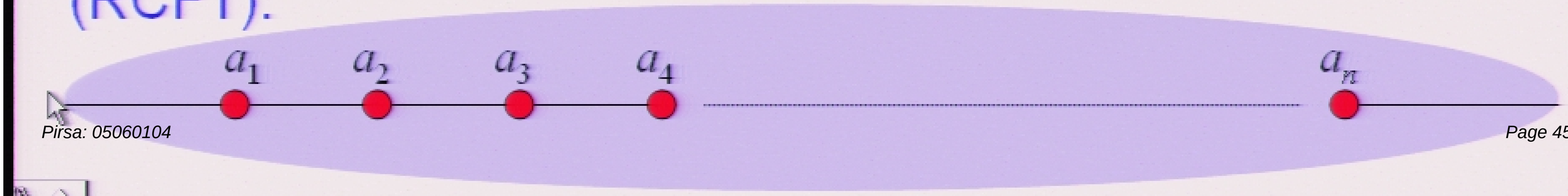


Models of (nonabelian) anyons

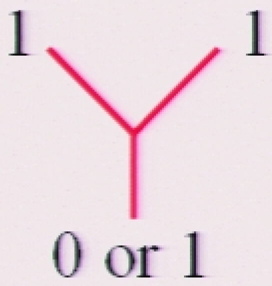
A model of anyons is a theory of a two-dimensional medium with a mass gap, where the particles carry locally conserved charges. We define the model by specifying:

1. A finite label set $\{a,b,c,\ldots\}$.
2. The fusion rules $a \times b = \sum_c N_{ab}^c c$
3. The F-matrix (expressing associativity of fusion).
4. The R-matrix (braiding rules).

These determine a representation of the *mapping class group* (braiding plus 2π rotations), and define a unitary topological modular functor (UTMF), the two-dimensional part of a (2+1)-dimensional topological quantum field theory (TQFT) --- related to a (1+1)-dimensional rational conformal field theory (RCFT).



Example: Yang-Lee (Fibonacci) Model

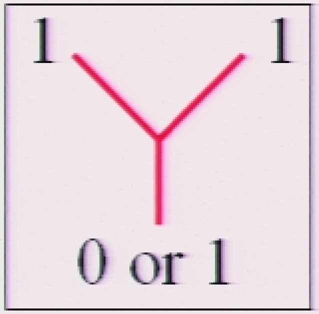


The charge takes two possible values: 0 (trivial) and 1 (nontrivial, and self-conjugate). Anyons have charge 1.Two anyons can "fuse" in either of two ways: $1 \times 1 = 0 + 1$

This is the simplest of all nonabelian anyon models. Yet its deceptively simple fusion rule has profound consequences.

In particular, the fusion rule determines the F-matrix and R-matrix uniquely; the resulting nontrivial braiding properties are adequate for universal quantum computation (pointed out by Kuperberg).

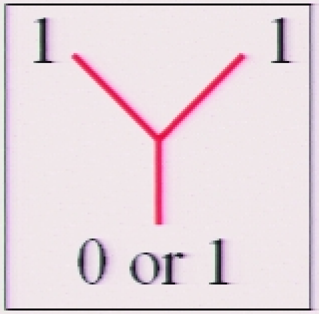
Nonabelian Anyons: Yang-Lee model



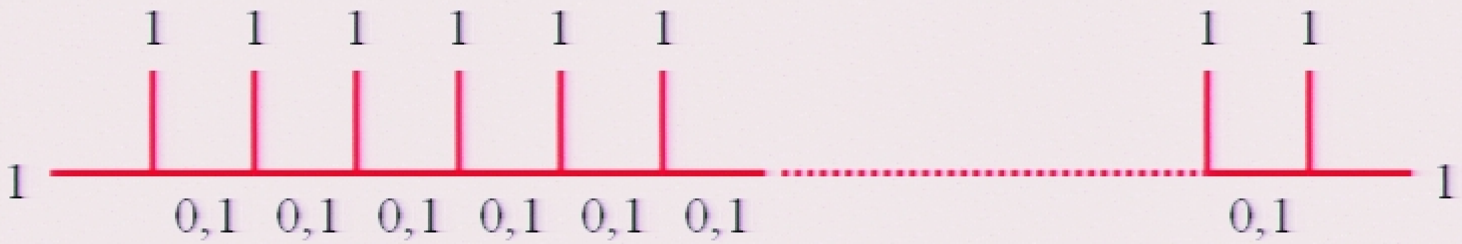
Suppose *n* anyons have a trivial total charge 0.
What is the dimension of the Hilbert space?

The distinguishable states of *n* anyons (a basis for the Hilbert space) are labeled by binary strings of length *n*-3.

Nonabelian Anyons: Yang-Lee model

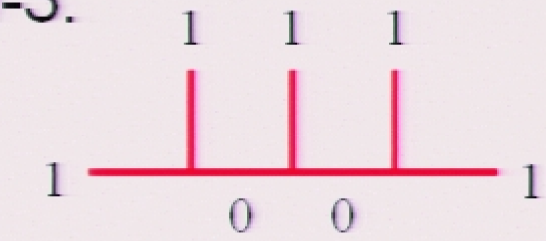


Suppose *n* anyons have a trivial total charge 0.
What is the dimension of the Hilbert space?

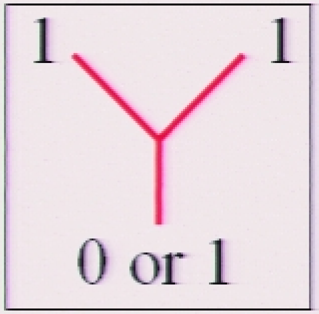


The distinguishable states of *n* anyons (a basis for the Hilbert space) are labeled by binary strings of length *n*-3.

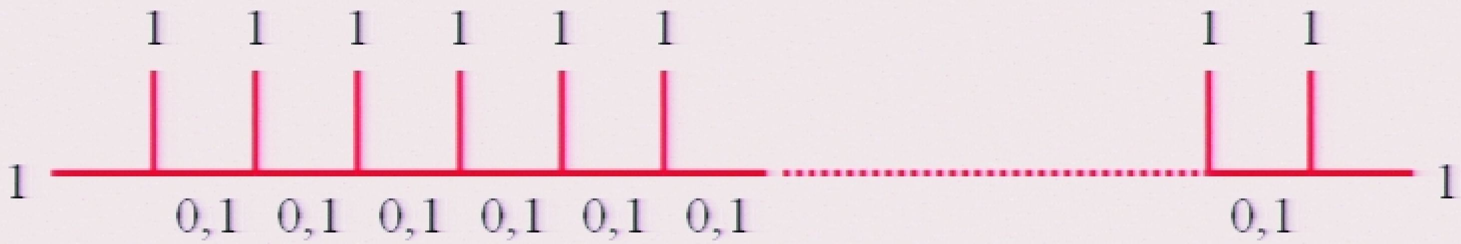
But it is impossible to have two zeros in a row:



Nonabelian Anyons: Yang-Lee model

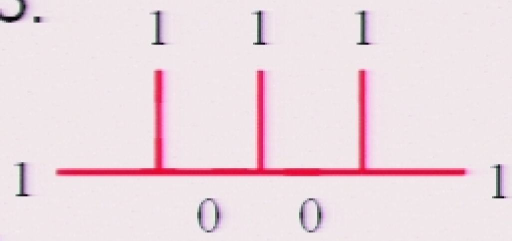


Suppose *n* anyons have a trivial total charge 0.
What is the dimension of the Hilbert space?



The distinguishable states of *n* anyons (a basis for the Hilbert space) are labeled by binary strings of length *n*-3.

But it is impossible to have two zeros in a row:



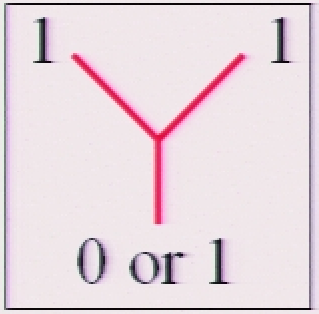
Therefore, the dimension is a Fibonacci number.

$D = 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Asymptotically, the number of qubits encoded by each anyon is:

$\log_2 \phi = \log_2\left[(1+\sqrt{5})/2\right] = \log_2(1.618) = .694$

Nonabelian Anyons: Yang-Lee model



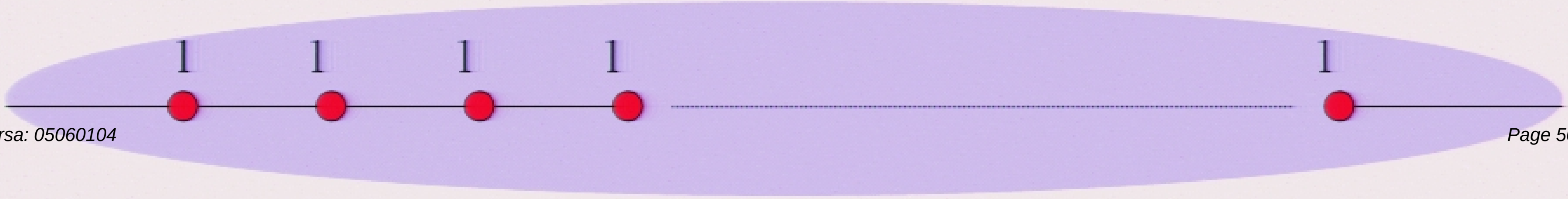
Asymptotically, the number of qubits encoded by each anyon is:

$$\log_2 \phi = \log_2\left[\left(1+\sqrt{5}\right)/2\right] = \log_2(1.618) = .694$$

We say that $d = \phi$ is the (quantum) dimension of the Fibonacci anyon…

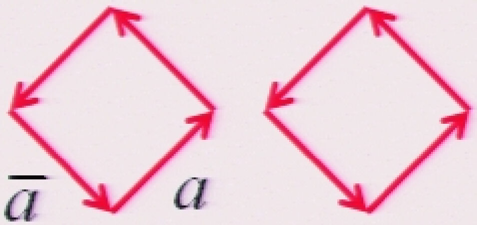
This counting vividly illustrates that the qubits are a nonlocal property of the anyons, and that the topological Hilbert space has no particularly natural decomposition as a tensor product of small subsystems.

Anyons have some "nonlocal" features, but they are not so nonlocal as to profoundly alter the computational model (the braiding of anyons can be efficiently simulated by a quantum circuit)…

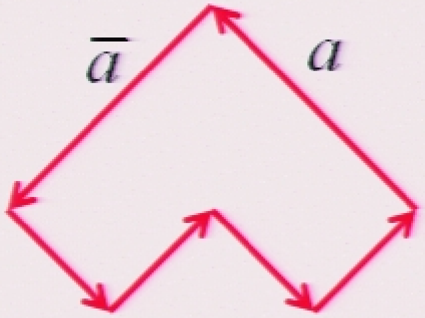


The quantum dimension

Every anyon label a has a *quantum dimension*, which we may define as follows: Imagine creating two particle-antiparticle pairs, and then fusing the particle from one pair with the antiparticle from the other…



$$=1,$$

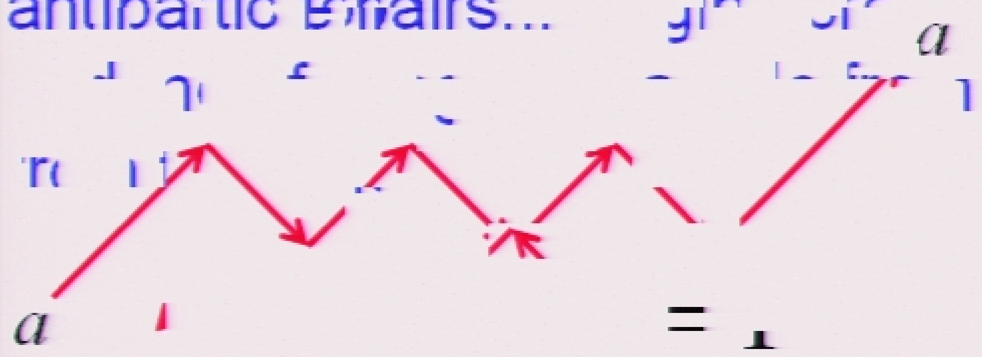


$$=\frac{1}{d_a}$$

Annihilation occurs with probability $1/d_a{}^2$. This is a natural generalization of the case where the charge is an irreducible representation R of a group G, where the “quantum dimension” is just the dimension $|R|$ of the representation (which counts the number of “colors” going around the loop). But there is no logical reason why a dimension defined this way must be can integer, and in general it isn’t an integer.

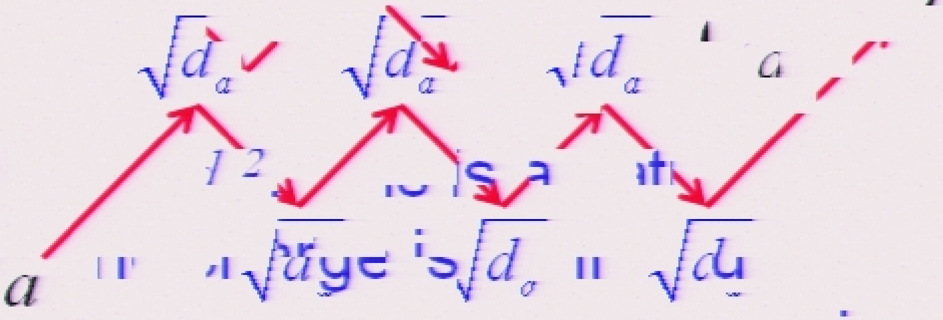
The quantum dimension

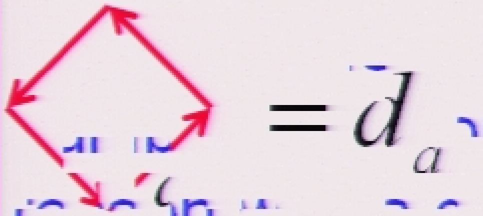
There is a more convenient normalization convention for particle-antiparticle pairs...



Each time we add another tooth to the saw, it costs us another factor of $1/d_a$

We can compensate for that factor by weighting each pair creation or annihilation event by a factor of $\sqrt{d_a}$ ...

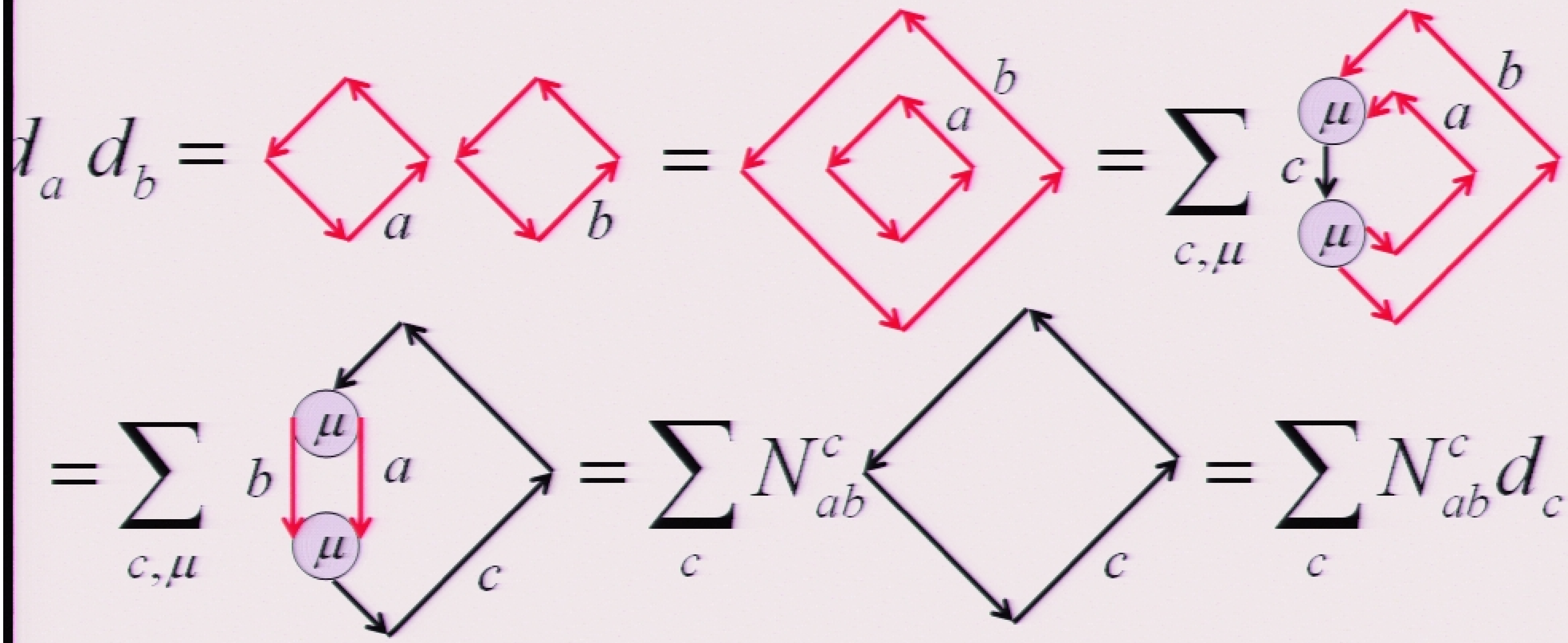




With this convention, a closed loop has weight d_a, as though we were counting colors ...

Now we can deform the world line of a particle (e.g. adding and removing "teeth") without altering the value of a diagram

The quantum dimension

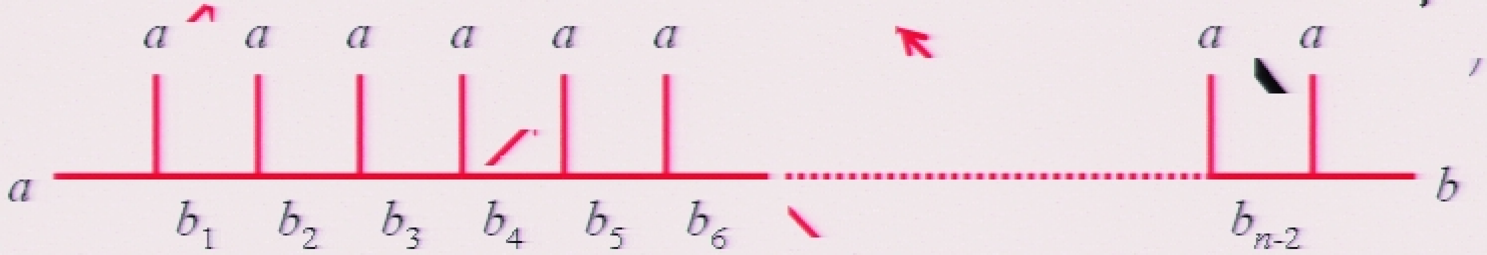


Therefore, the vector of quantum dimensions is the (Perron-Frobenius) eigenvector of each fusion rule matrix, with eigenvalue d_a:

$$\sum_c (N_a)_b^c d_c = d_a d_b \Rightarrow N_a \vec{d} = (d_a)\vec{d}$$

The quantum dimension

$$N_a = |u\rangle d_a \langle u| + \cdots, \quad |u\rangle = \vec{d}\Big/\mathfrak{D}$$



$$N^b_{aaa\ldots a} = \dim(V^b_{aaa\ldots a}) = \sum_{\{b_i\}} N^{b_1}_{aa} N^{b_2}_{ab_1} N^{b_3}_{ab_2} \cdots N^{b}_{ab_{n-2}}$$

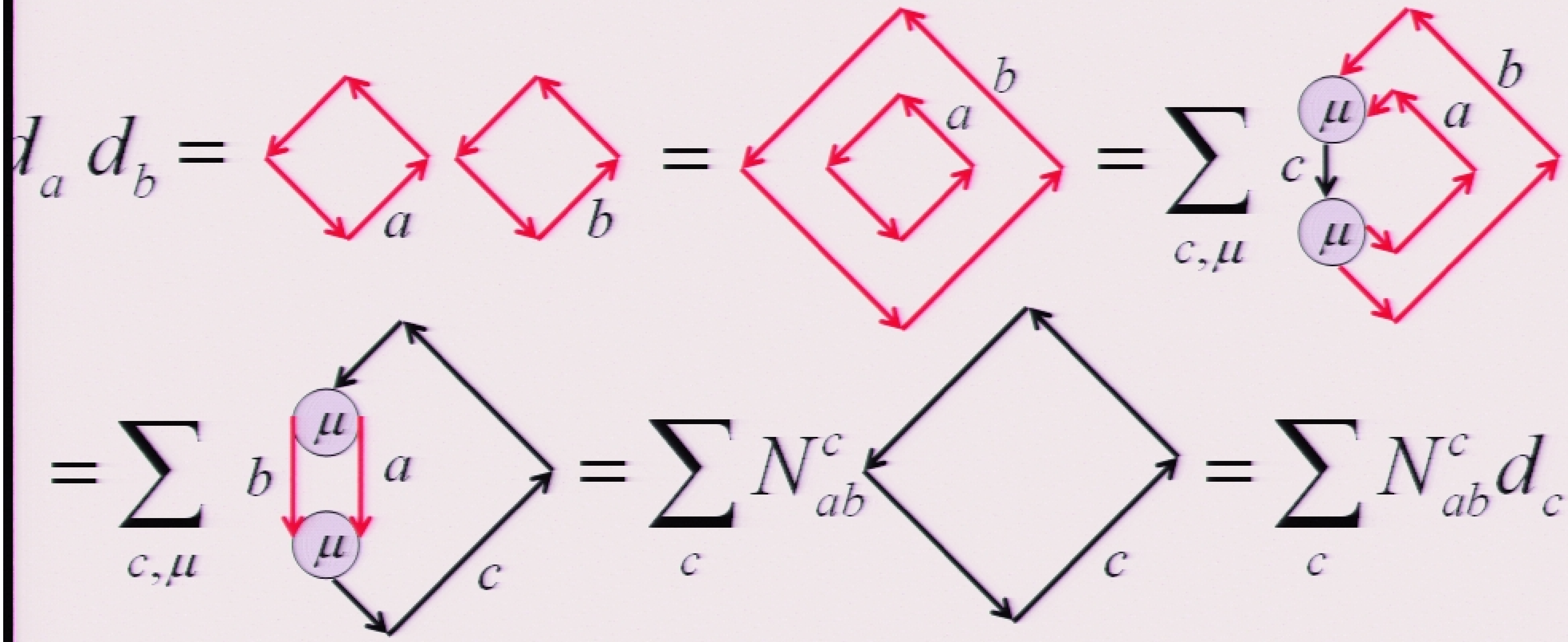
$$= \langle b|\left(N_a\right)^{n-1}|a\rangle = \langle b|u\rangle d_a^{n-1}\langle u|a\rangle + \ldots = d_a^n d_b\Big/\mathfrak{D}^2 + \cdots$$

Thus the quantum dimension controls the rate of growth of the n-particle Hilbert space. The normalization factor

$$\mathfrak{D} = \sqrt{\sum_a d_a^2}$$

is called the *total quantum dimension* of the anyon model.

The quantum dimension

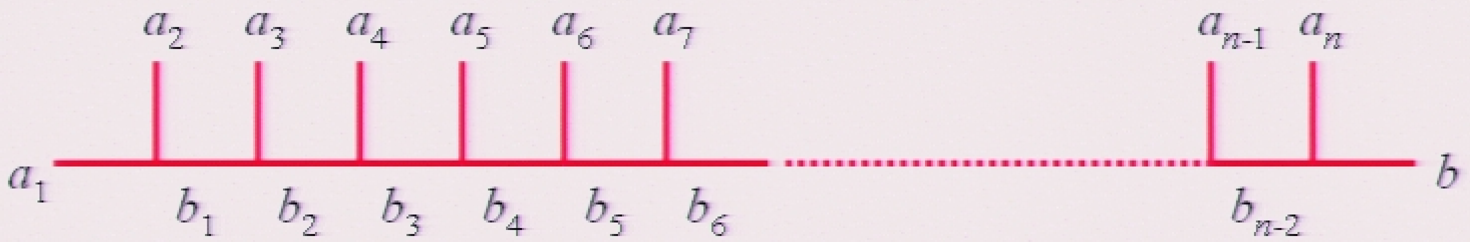


Therefore, the vector of quantum dimensions is the (Perron-Frobenius) eigenvector of each fusion rule matrix, with eigenvalue d_a:

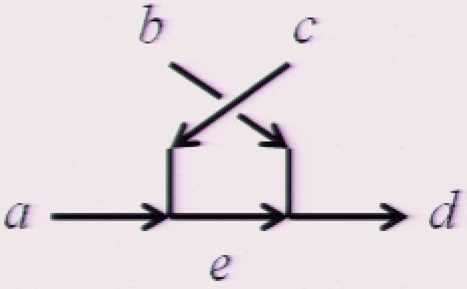
$$\sum_c (N_a)_b^c d_c = d_a d_b \Rightarrow N_a \vec{d} = (d_a)\vec{d}$$

Braiding: the B-matrix $\quad B: \; V^{d}_{acb} \to V^{d}_{abc}$:

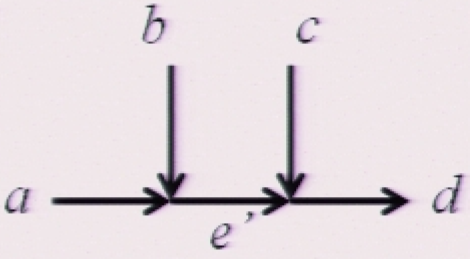
For the n-anyon Hilbert space, we may use the *standard basis*:



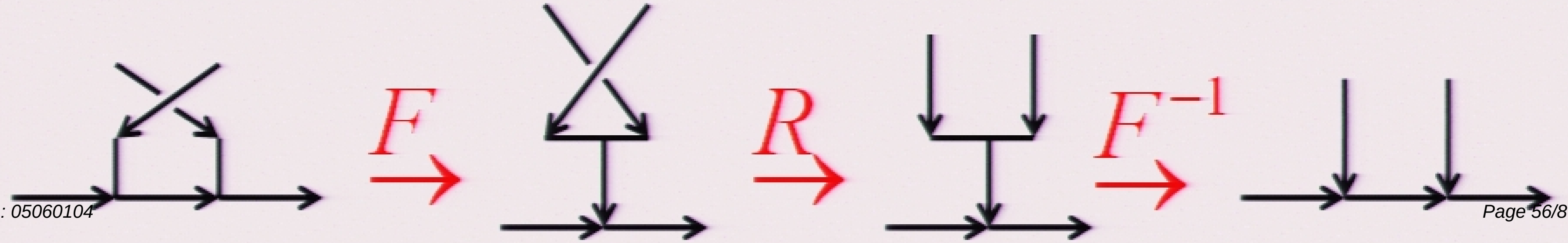
The effect of braiding can be expressed in this basis:



$$= \sum_{e'\mu'\nu'} \left(B^{d}_{abc}\right)^{e'\mu'\nu'}_{e\mu\nu}$$



And … the matrix B is determined by R and F:



$\lambda_{max} - \Sigma \lambda > 0$

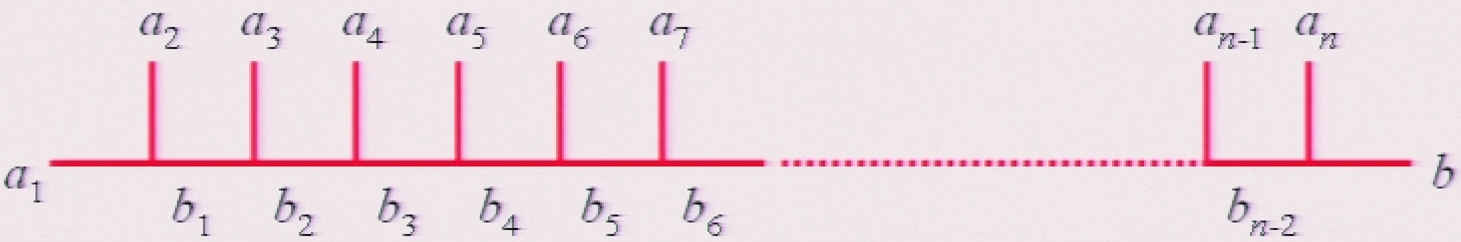
$$\sum_{\alpha=1}^{S} |\eta_\alpha|^2 = 1$$

$\eta_\beta = 1, \quad \eta_{\gamma \neq \beta} = 0$

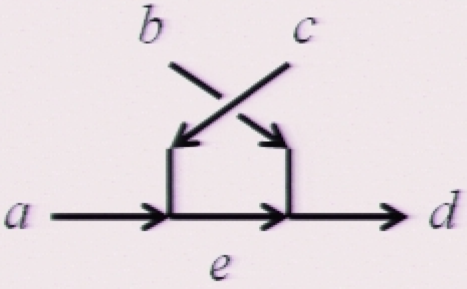
$$1 \times 1 = 1 + \underset{\uparrow \atop 1}{0} \quad \Big| \quad \boxed{d^2 = 1 + d}$$

Braiding: the B-matrix $B: \; V^{d}_{acb} \rightarrow V^{d}_{abc}$:

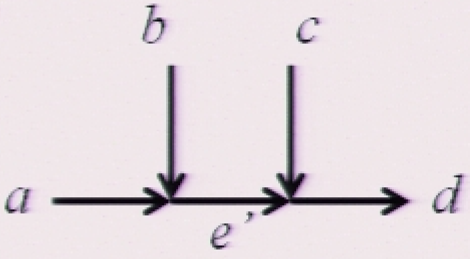
For the n-anyon Hilbert space, we may use the *standard basis*:



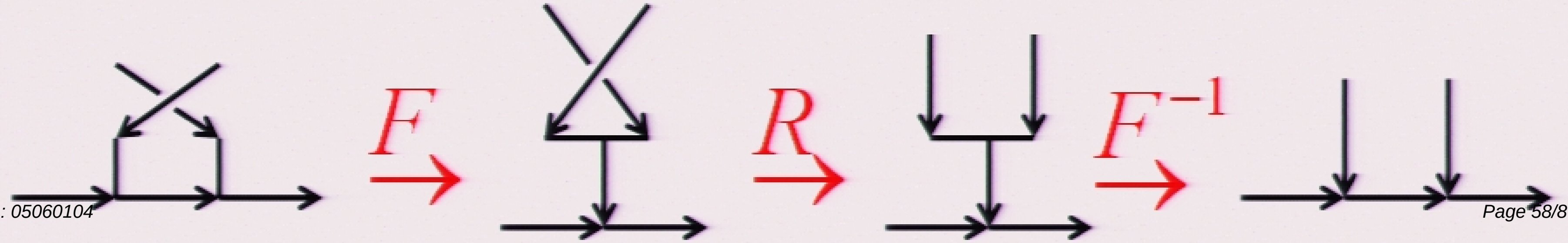
The effect of braiding can be expressed in this basis:



$$= \sum_{e'\mu'\nu'} \left(B^{d}_{abc} \right)^{e'\mu'\nu'}_{e\mu\nu}$$

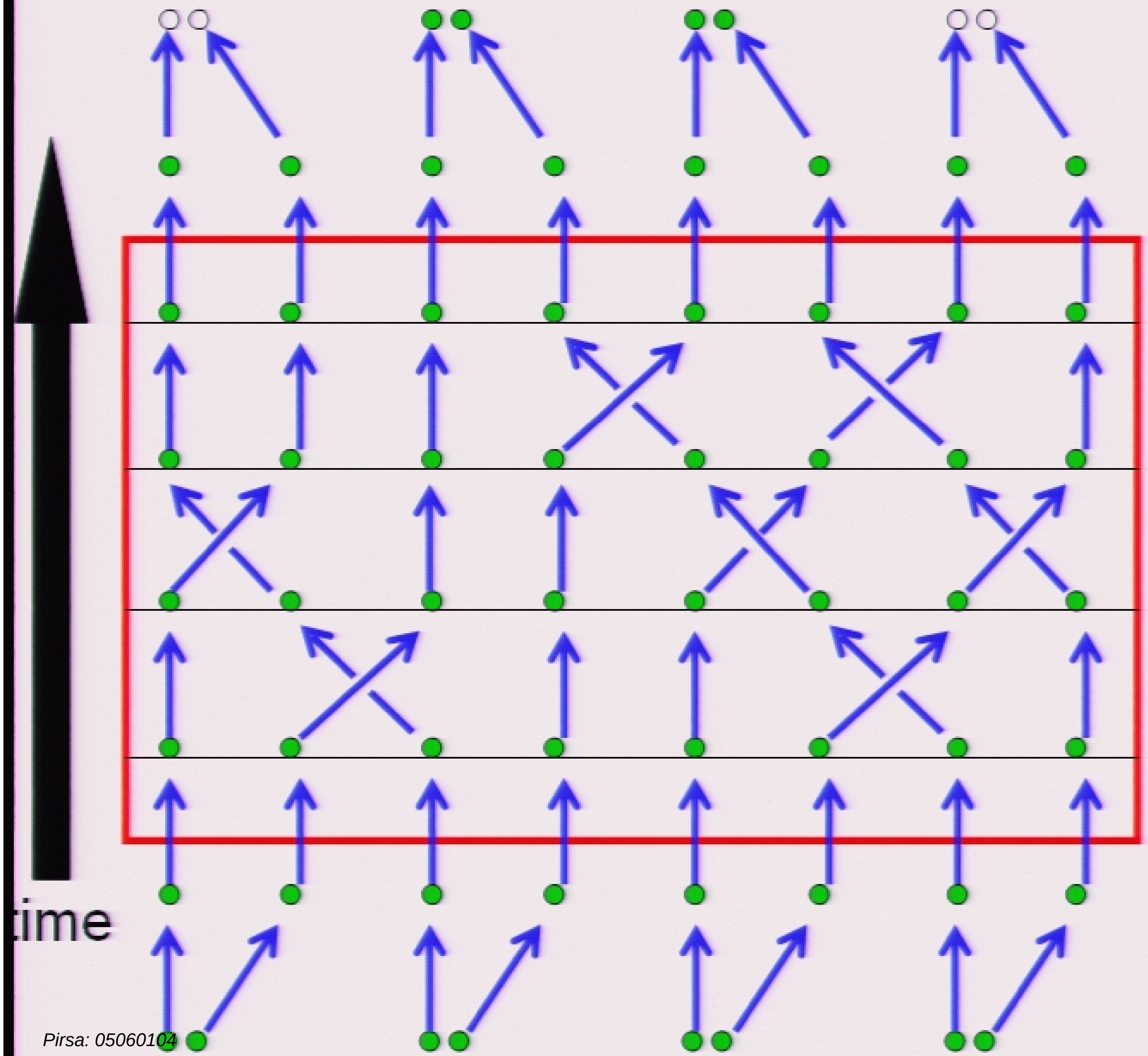


And … the matrix B is determined by R and F:



Topological quantum computation

(Kitaev '97, FLW '00)



annihilate pairs?

braid

braid

braid

create pairs

Kitaev

Freedman

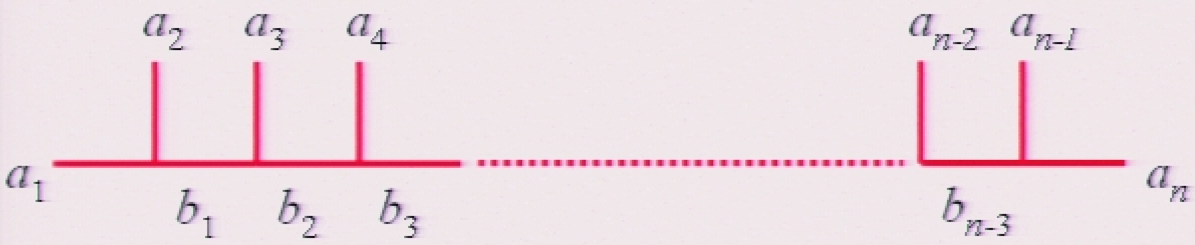
Topological quantum computation

1. Create pairs of particles of specified types.
2. Execute a braid.
3. Fuse neighboring particles, and observe whether they annihilate.

Claim: This process can be simulated efficiently by a quantum circuit.

Need to explain:

1. Encoding of topological Hilbert space.
2. Simulation of braiding (B-matrix as a two-qudit gate).
3. Simulation of fusion (F-matrix plus a one-qudit projective measurement).



$$\subseteq \left(\bigoplus_{a,b,c} V_{abc}^{0} \right)^{\otimes(n-2)}$$

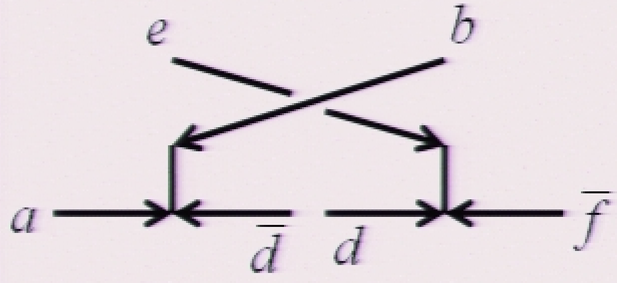
$$\mathfrak{H}_d \hookrightarrow$$

Although the topological vector spaces are not themselves tensor products of subsystems, they all fit into a tensor product of d-dimensional systems, where this qudit is the "total fusion space" of three anyons...

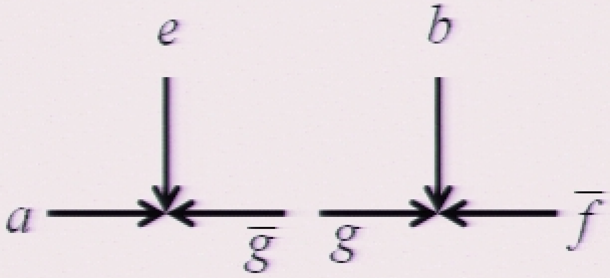
$$d = \sum_{a,b,c} N_{abc}^{0}$$

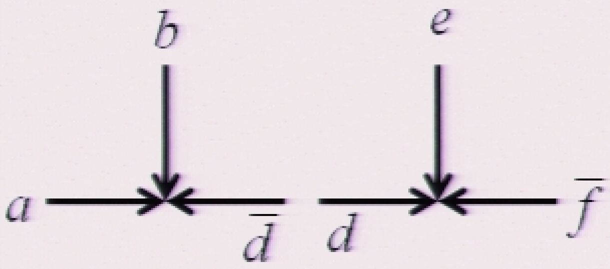
Simulating topological quantum computation

The B-matrix and the F-matrix are two-qudit unitary gates:

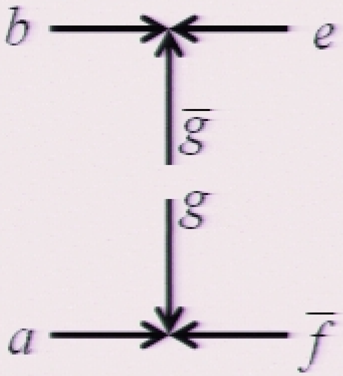


$$= \sum_g \left(B^f_{aeb}\right)^g_d$$



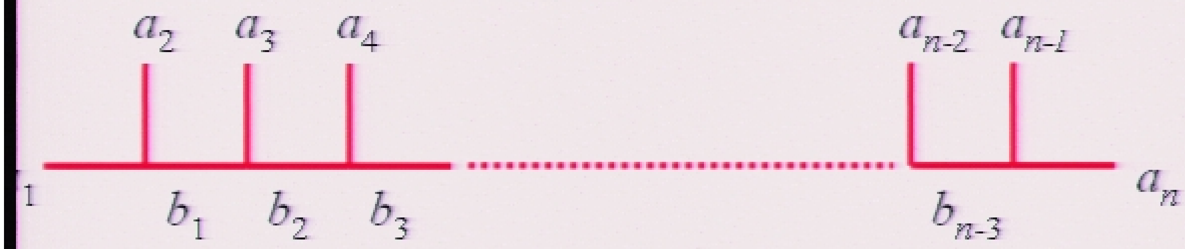


$$= \sum_g \left(F^f_{abe}\right)^g_d$$



To determine whether b and e will annihilate, perform an F-move and then measure the qudit to find out whether g=0.

Topological quantum computation



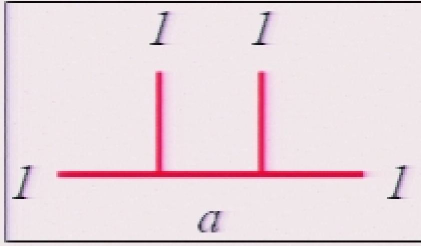
$$\subseteq \left(\mathfrak{H}_d \right)^{\otimes(n-2)}$$

Therefore, the topological model is *no more powerful* than the quantum circuit model. But is it *as powerful*? The answer depends on the model of anyons, and in particular on the properties of the R-matrix and F-matrix.

To simulate a quantum circuit, we encode qubits in the topological vector space, and use braiding to realize a set of *universal quantum gates* acting on the qubits.

That is, the image of our representation of the braid group B_n on n strands should be dense in $SU(2^r)$, for some r linear in n.

Example: in the Fibonacci model, we can encode a qubit in the two-dimensional Hilbert space V^0_{1111} of four anyons with trivial total charge.



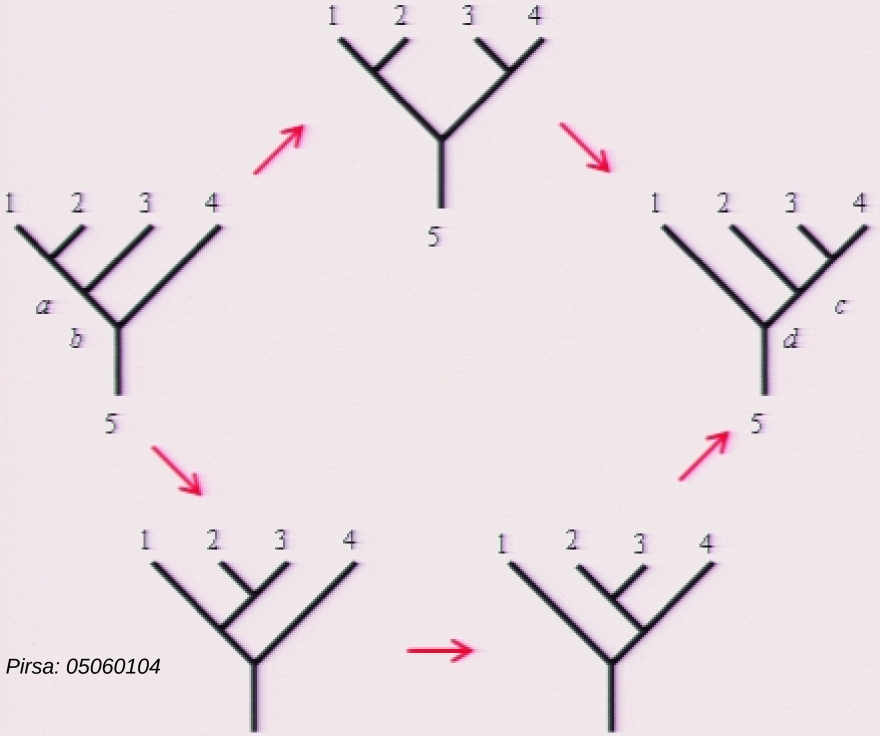
$$a \in \{0,1\}$$

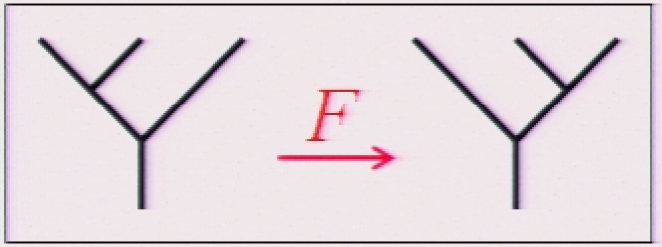
But what are R and F in this model?

Consistency of braiding and fusing

The R-matrix (braiding), and the F-matrix (associativity of fusing) are highly constrained by algebraic consistency requirements (the *Moore-Seiberg polynomial equations*). In the case of the Fibonacci model, these equations allow us to completely determine R and F from the fusion rules.

By a sequence of "F-moves" and "R-moves," we obtain an isomorphism between two opological Hilbert spaces, that is, a relation between two different canonical bases. This relation must not depend on the particular sequence of moves, only on the basis we start with and the basis we end up with. For example, there are 5 different ways (without any exchanges) to fuse five particles, related by F-moves:

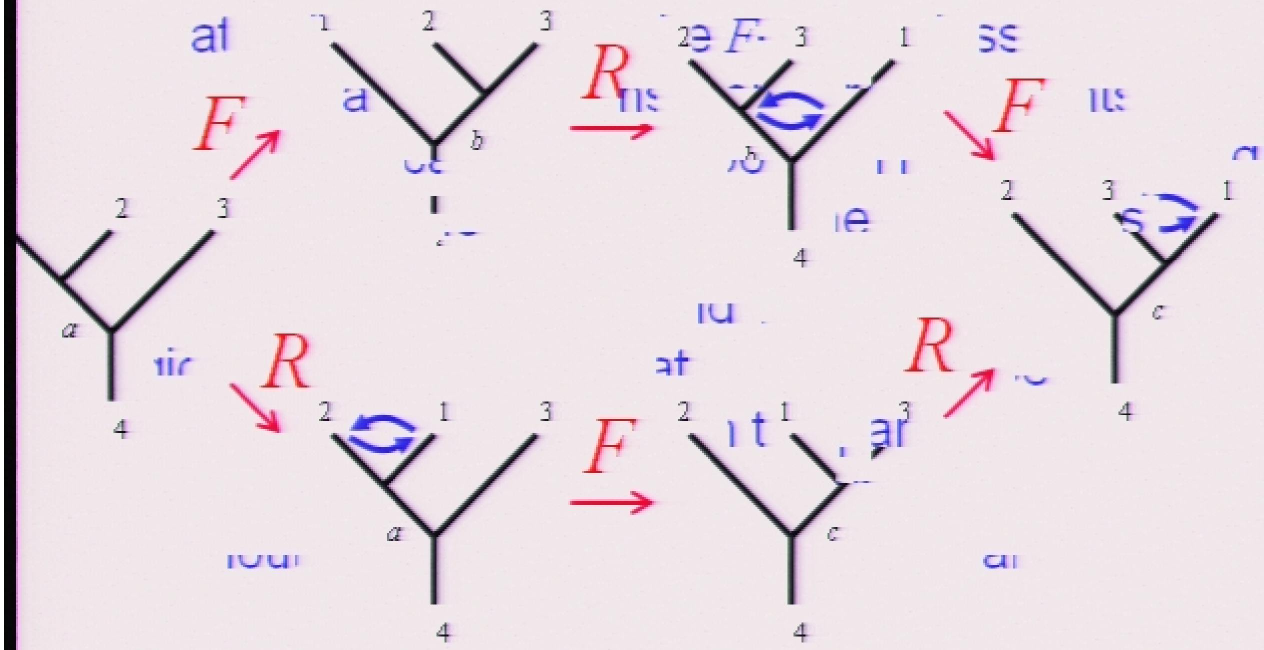


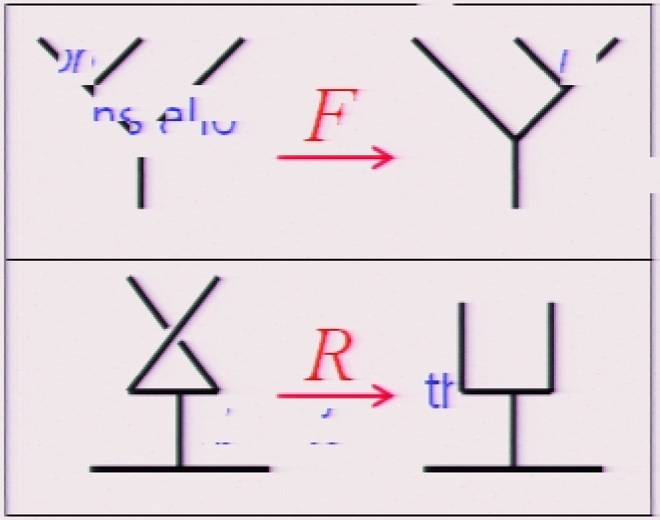


Pentagon equation:

$$\left(F^{5}_{a34}\right)^{c}_{b}\left(F^{5}_{12c}\right)^{d}_{a} = \sum\left(F^{b}_{123}\right)^{e}_{a}\left(F^{5}_{1e4}\right)^{d}_{b}\left(F^{5}_{234}\right)^{c}_{e}$$

Consistency of braiding and fusing





Hexagon equation: $$\sum_b \left(F^4_{123}\right)^b_a R^4_{1b} \left(F^4_{231}\right)^c_b = R^a_{12} \left(F^4_{213}\right)^c_a R^c_{13}$$

Furthermore, if the pentagon and hexagon equations are satisfied, then *all* sequences of F- and R-moves from an initial basis to a final basis yield the same isomorphism!

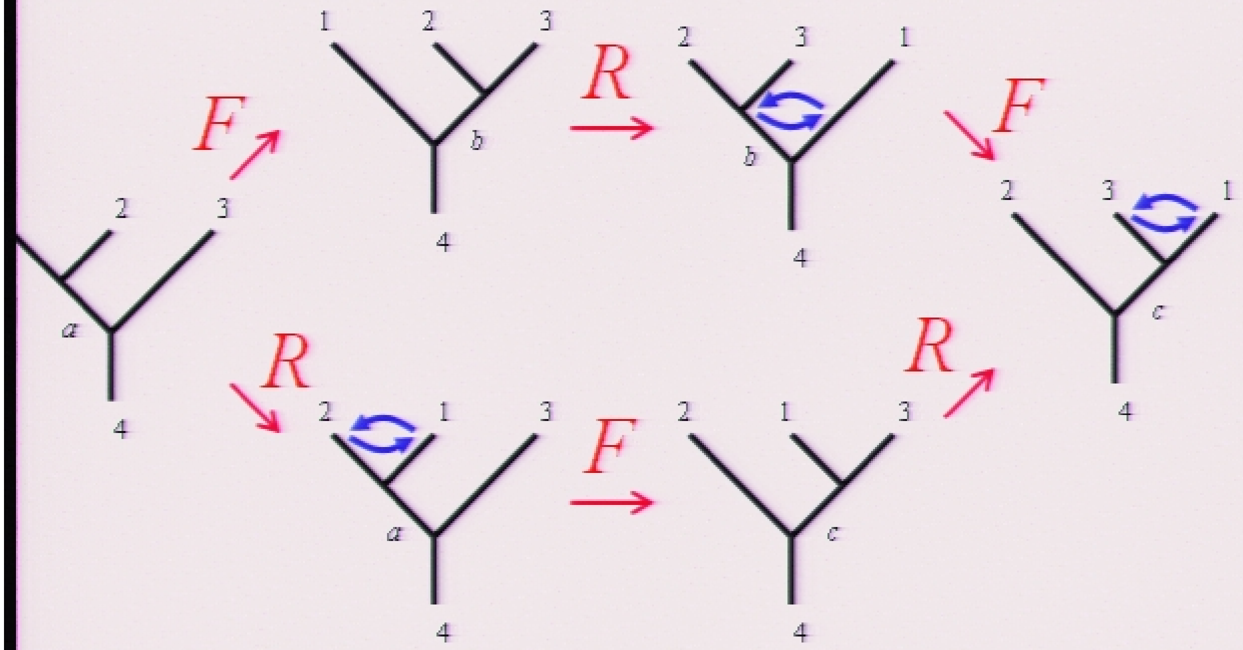
A systematic (in principle) procedure for constructing anyon models:

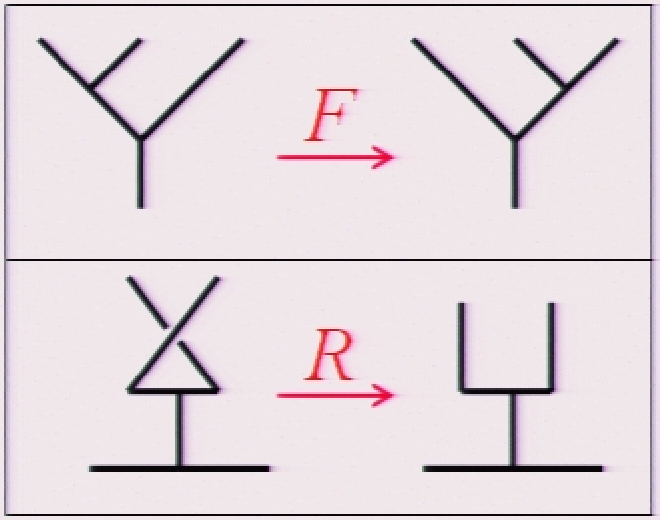
1. Assume a fusion rule.
2. Solve pentagon and hexagon equations for R and F.

-- If no solutions, the fusion rules are incompatible with local quantum physics.

-- If multiple solutions, each is a valid model.

Consistency of braiding and fusing





Hexagon equation:

$$\sum_b \left(F^4_{123}\right)^b_a R^4_{1b} \left(F^4_{231}\right)^c_b = R^a_{12} \left(F^4_{213}\right)^c_a R^c_{13}$$

Furthermore, if the pentagon and hexagon equations are satisfied, then *all* sequences of F- and R-moves from an initial basis to a final basis yield the same isomorphism!

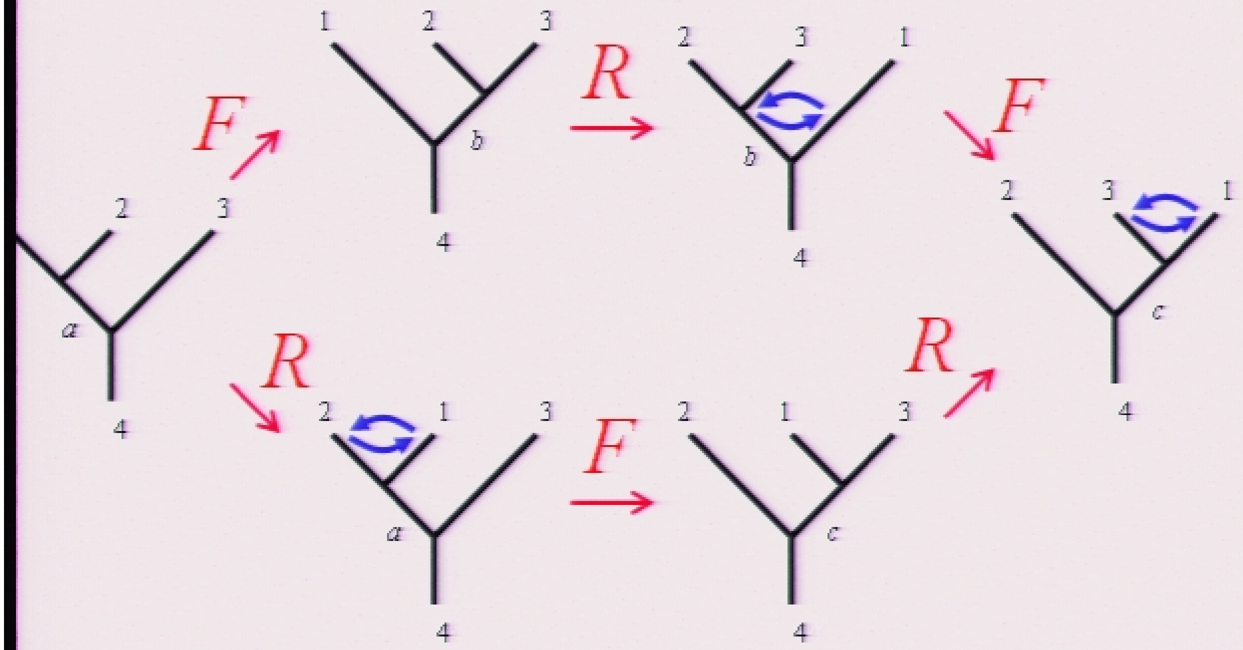
A systematic (in principle) procedure for constructing anyon models:

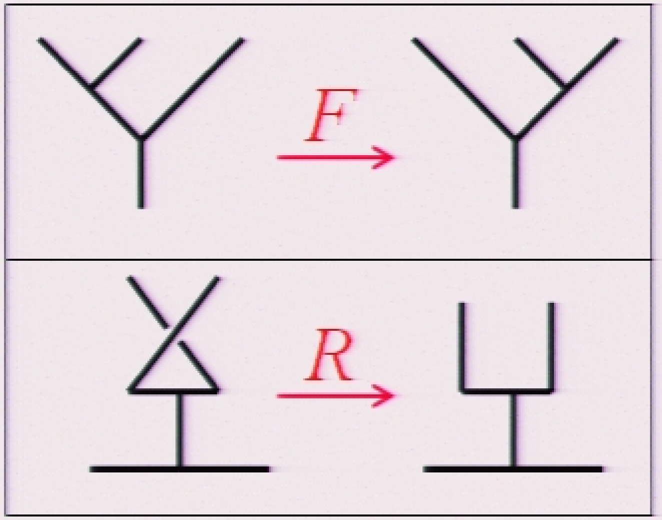
1. Assume a fusion rule.
2. Solve pentagon and hexagon equations for R and F.

-- If no solutions, the fusion rules are incompatible with local quantum physics.

-- If multiple solutions, each is a valid model.

Consistency of braiding and fusing





Hexagon equation:

$$\sum_b \left(F^4_{123}\right)^b_a R^4_{1b} \left(F^4_{231}\right)^c_b = R^a_{12} \left(F^4_{213}\right)^c_a R^c_{13}$$

Furthermore, if the pentagon and hexagon equations are satisfied, then *all* sequences of F- and R-moves from an initial basis to a final basis yield the same isomorphism!

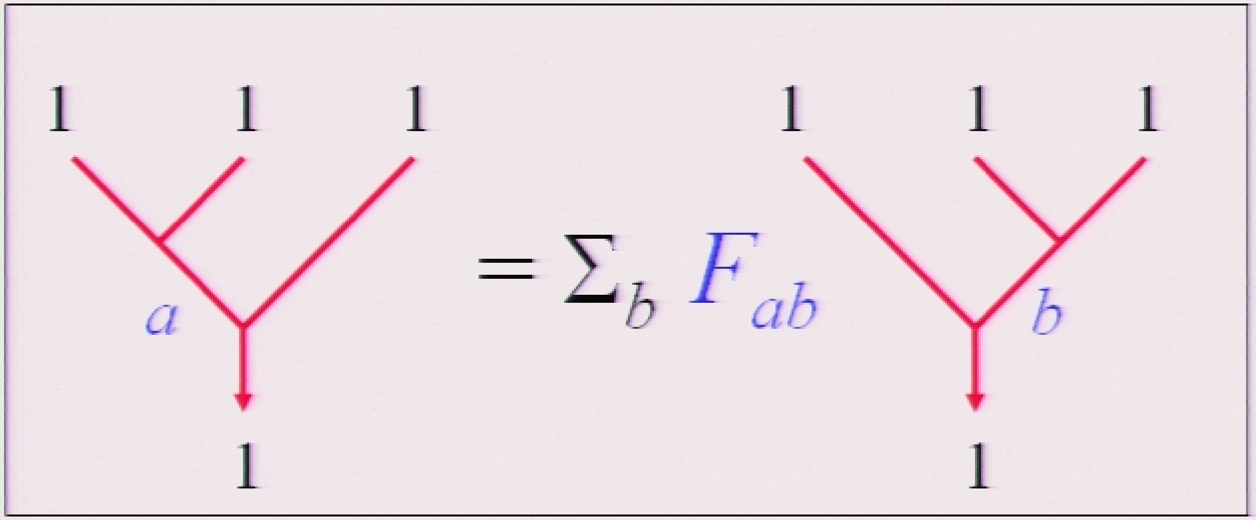
A systematic (in principle) procedure for constructing anyon models:

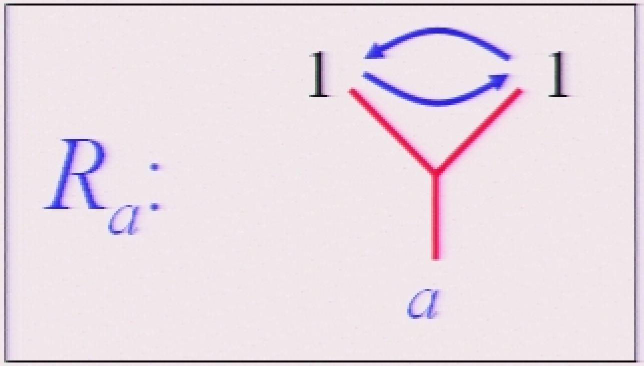
1. Assume a fusion rule.
2. Solve pentagon and hexagon equations for R and F.

-- If no solutions, the fusion rules are incompatible with local quantum physics.

-- If multiple solutions, each is a valid model.

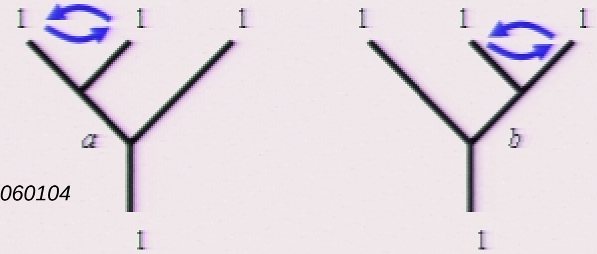
Example: Fibonacci model



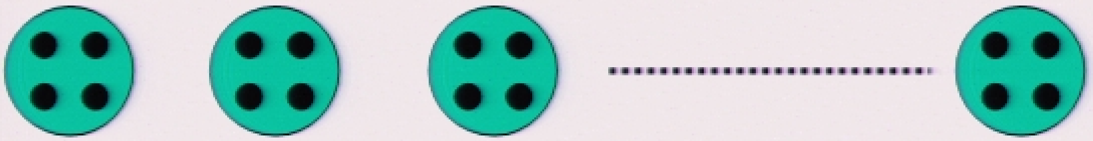


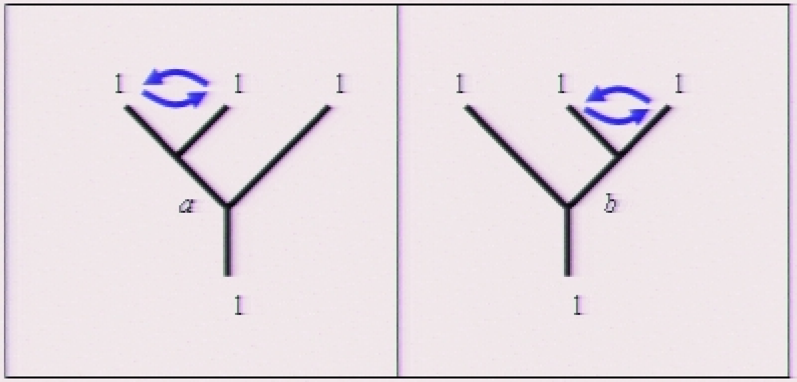
$$F = \begin{pmatrix} \tau & \sqrt{\tau} \\ \sqrt{\tau} & -\tau \end{pmatrix}, \quad R = \begin{pmatrix} e^{4\pi i/5} & 0 \\ 0 & -e^{2\pi i/5} \end{pmatrix}, \quad \tau = \left(\sqrt{5}-1\right)/2 = \phi - 1$$

This solution is *unique* (aside from freedom to redefine phases and take the parity conjugate). Furthermore, products of the noncommuting matrices R and FRF^{-1} (representing the generators of the braid group B_3) are dense in $\mathrm{SU}(2)$.

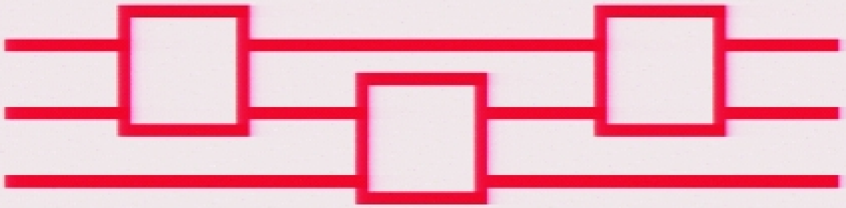


Example: Fibonacci model





We encode a qubit in four anyons. To simulate a quantum circuit, we need to do (universal) two-qubit gates.

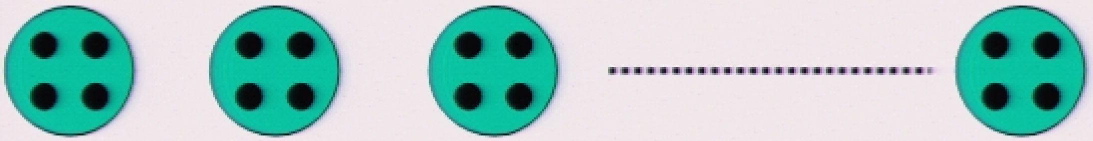


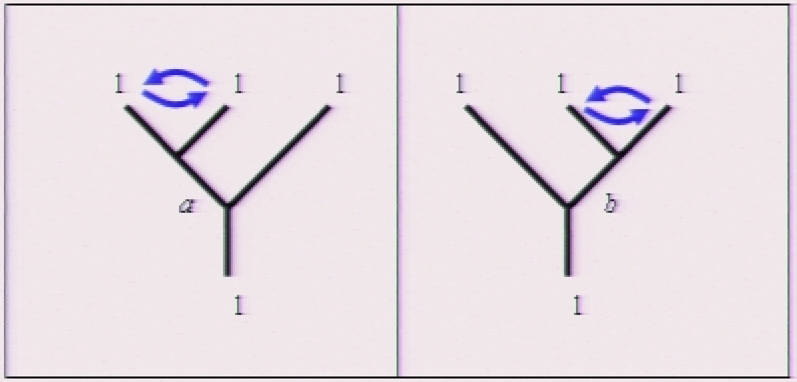
The two-qubits are embedded in the 13-dimensional Hilbert space of *eight* anyons.

The representation of B_8 determined by our R and F matrices is universal – i.e., dense in $SU(13)$, so in particular we can approximate any $SU(4)$ gate arbitrarily well with some finite number of exchanges. If we fix accuracy of the approximation to the gate, we can use quantum error- correcting codes and fault-tolerant simulation to perform an efficient and reliable quantum computation.

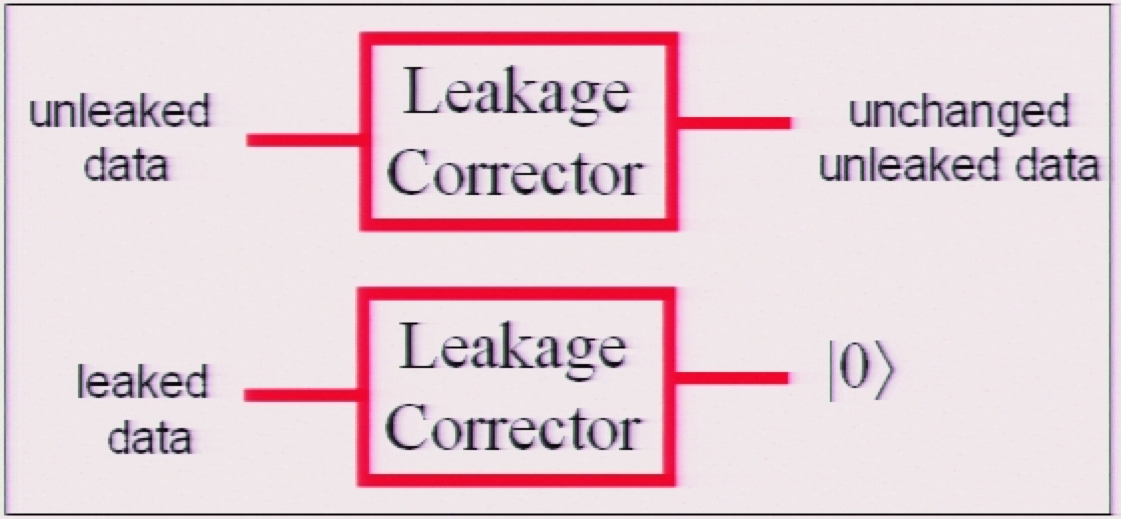
Here quantum-error correction might be needed to correct for the (small) flaws in the gates, but not to correct for storage errors.

“Leakage”





The computation takes place in the r-qubit subspace of a system of $4r$ anyons. As errors accumulate, the state of the computer might drift our of this subspace (the “leakage” problem).



But we can include leakage corrector gates in our simulation. This gate is the identity acting on data in the computational space, but replaces a leaked qubit by the standard state $|0\rangle$ in the computational space.

For example, we can use a quantum teleportation protocol for leakage correction (in effect, this turns quantum leakage into classical leakage, which is easier to detect and correct).

Topological quantum computation

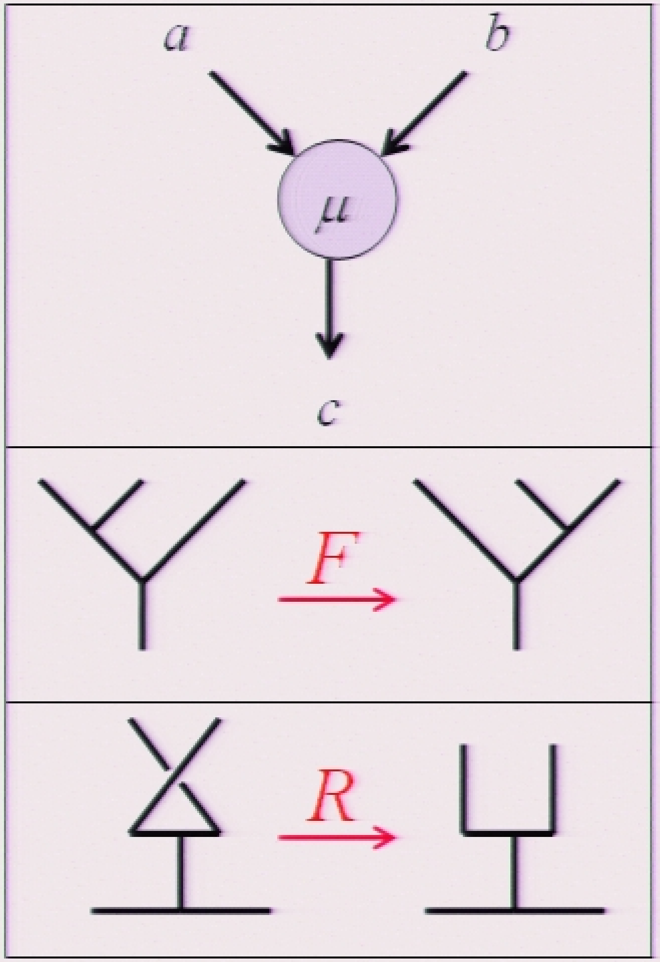
To summarize, we can simulate a universal quantum computer using (for example) Fibonacci anyons, if we have these capabilities:

1. We can create pairs of particles.
2. We can guide the particles along a specified braid.
3. We can fuse particles, and distinguish complete annihilation from incomplete annihilation.

-- The temperature must be small compared to the energy gap, so that stray anyons are unlikely to be excited thermally.

-- The anyons must be kept far apart from one another compared to the correlation length, to suppress charge-exchanging virtual processes, except during the initial pair creation and the final pair annihilation.

(Nonabelian) anyons



An anyon model is characterized by its label set, fusion rules, F-matrix, and R-matrix.

Classifying the models (finding all solutions to the pentagon and hexagon equations) is an important (hard) unsolved mathematical problem. We know how to find some examples (e.g., Chern-Simons theories), but we don't know how rich the possibilities are.

Such a classification would be an important step toward classifying topological order in two dimensions.

There would still be more to do, though ... For example, this would be a classification of gapped two-dimensional *bulk* theories, and one bulk theory can correspond to more than one (1+1)-dimensional theory describing *edge* excitations. And of course, we would like to know, both for practical and theoretical reasons, *whether* the model can be realized robustly with some local Hamiltonian (and *how* to realize it).

Chern-Simons theory

$$a \times b = \sum_c N_{ab}^c c$$

The fusion rules of a Chern-Simons theory are a truncated version of the fusion rules of a compact Lie group. For example, in the theory denoted $\mathrm{SU}(2)_k$, the labels are half integers analogous to angular momenta, where $j \leq k/2$ and j is contained in $j_1 \times j_2$ only if $j_1 + j_2 + j \leq k$.

Example: $\mathrm{SU}(2)_2$

$$\frac{1}{2} \times \frac{1}{2} = 0 + 1$$

$$\frac{1}{2} \times 1 = \frac{1}{2}$$

$$1 \times 1 = 0$$

Therefore:

$$d_0 = d_1 = 1$$

$$d_{1/2} = \sqrt{2}$$

The polynomial equations for these fusion rules have several similar solutions (only one of which describes the braiding properties of the $\mathrm{SU}(2)_2$ model), but no solution has computationally universal braiding rules. Rather, braiding simulates *Clifford group computation*, which can be efficiently simulated classically.

Chern-Simons theory

$$a \times b = \sum_c N_{ab}^c c$$

But the $\mathrm{SU}(2)_k$ models for $k \geq 3$ *are* computationally universal:

Example: $\mathrm{SU}(2)_3$

$$\frac{1}{2} \times \frac{1}{2} = 0+1 \qquad 1 \times 1 = 0+1$$

$$\frac{1}{2} \times 1 = \frac{1}{2} + \frac{3}{2} \qquad 1 \times \frac{3}{2} = 0$$

$$\frac{1}{2} \times \frac{3}{2} = 1 \qquad \frac{3}{2} \times \frac{3}{2} = 0$$

The Fibonacci (Yang-Lee) model is obtained by a further truncation to $\mathrm{SO}(3)_3$ (with the noninteger labels eliminated).

All anyon models with no more than four labels have been classified by Wang, and all are closely related to the models found in Chern-Simons theory.

Models of nonabelian topological order

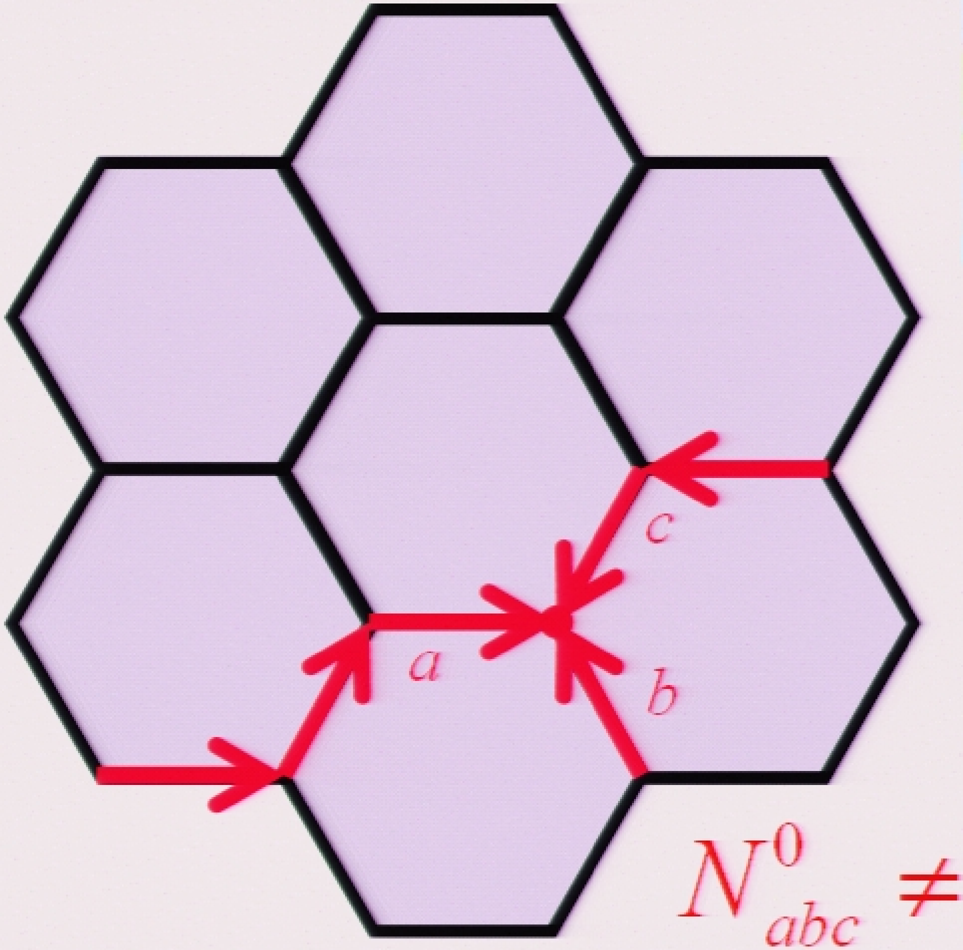
Kitaev (quant-ph/9707021 and unpublished), Freedman, Nayak, Shtengel, Walker, and Wang (cond-mat/0307511), Levin and Wen (cond-mat/0404617), and Fendley and Fradkin (cond-mat/0502071 have constructed nonabelian anyon models that arise from a two-dimensional lattice Hamiltonian with local interactions.

Kitaev

Freedman

Wen

Variables on oriented links of a honeycomb lattice are the anyon labels. The Hamiltonian imposes an energetic penalty the labels meeting at a site disobey the fusion rules.
Low energy configurations are branching string networks that respect the fusion rule. Quasiparticles appear at the ends of "broken strings.



$$N_{abc}^{0} \neq 0$$

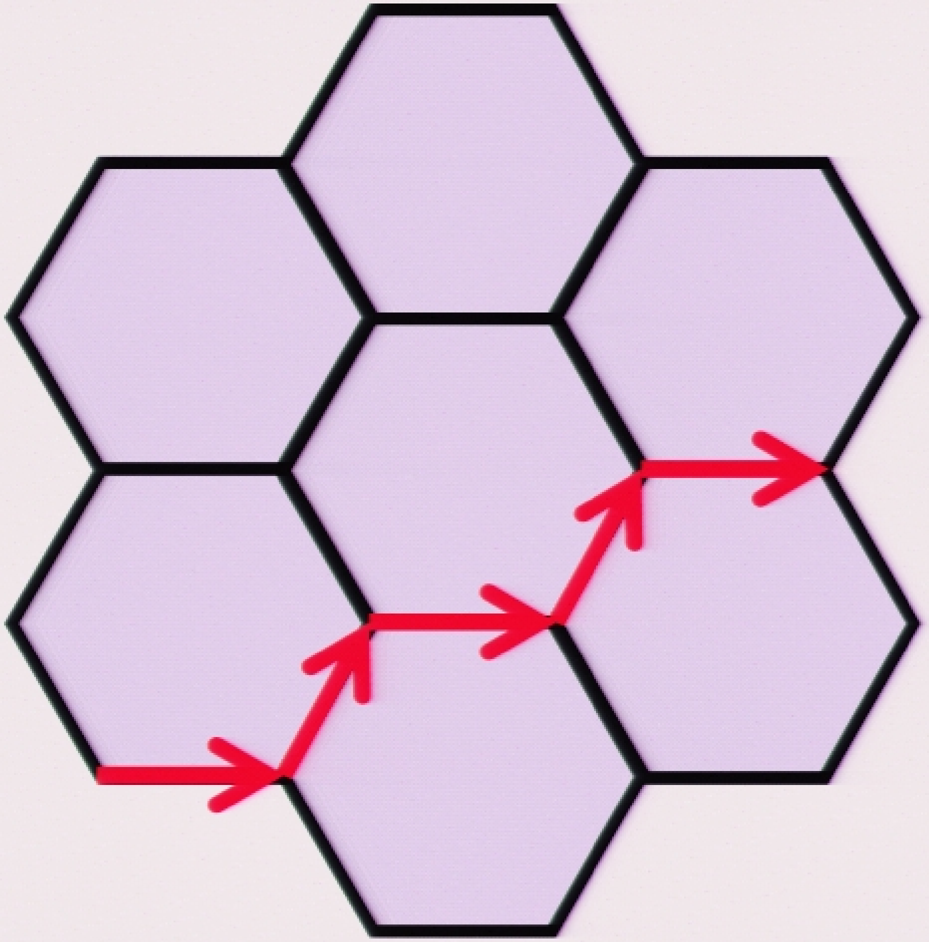
Models of nonabelian topological order

Kitaev (quant-ph/9707021 and unpublished), Freedman, Nayak, Shtengel, Walker, and Wang (cond-mat/0307511), and Levin and Wen (cond-mat/0404617) have constructed nonabelian anyon models that arise from a two-dimensional lattice Hamiltonian with local interactions.

Kitaev

Freedman

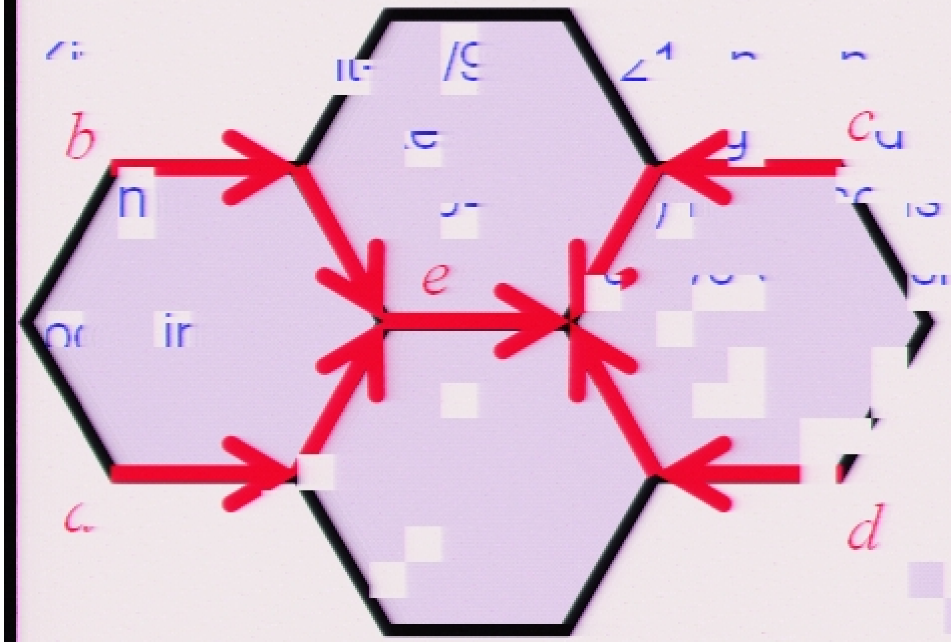
The Hamiltonian also enforces that the ground state is invariant under a deformation of a string that moves it across a plaquette.



Wen

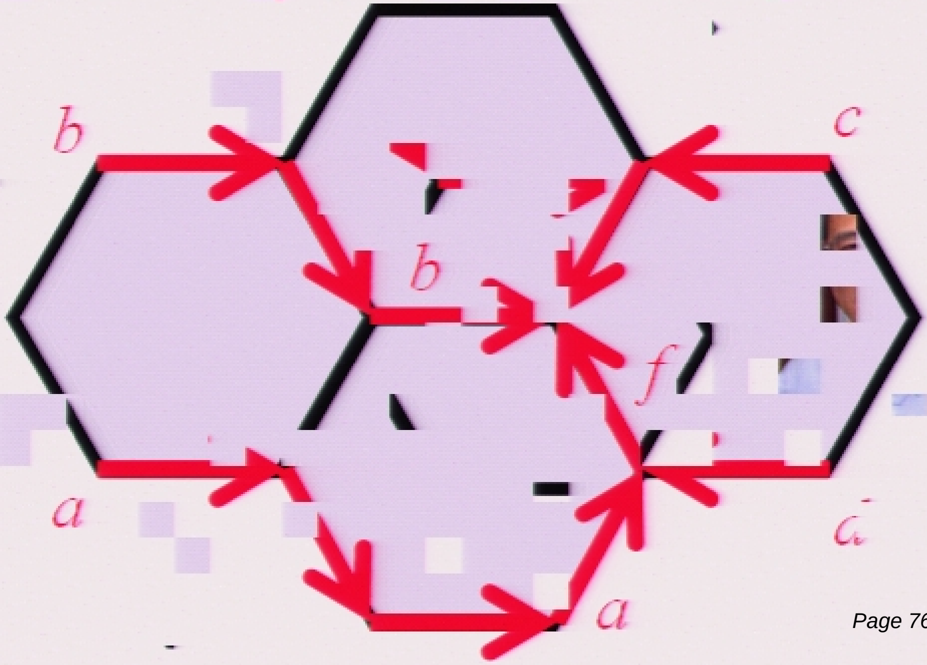
Forward

Models of nonabelian topological order



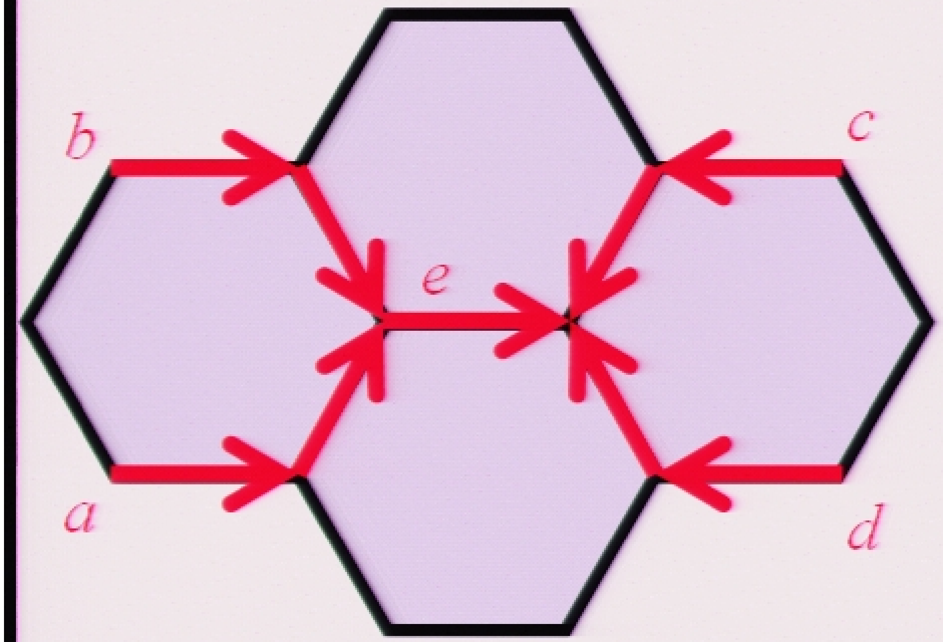
Furthermore, the Hamiltonian enforces that the ground state is invariant under an F-move. The quasiparticles are persuaded to behave just like the particles in the anyon model (except that the model is “parity doubled”).

$$= \left(F_{abcd}\right)^{f}_{e}$$



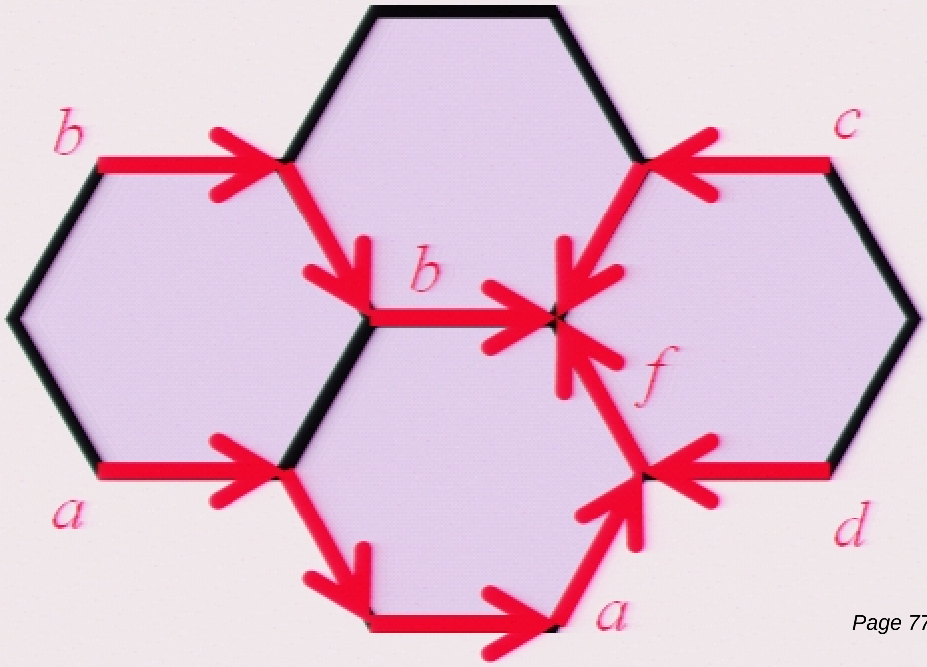
The topological order is expected to survive when the Hamiltonian is slightly perturbed

Models of nonabelian topological order



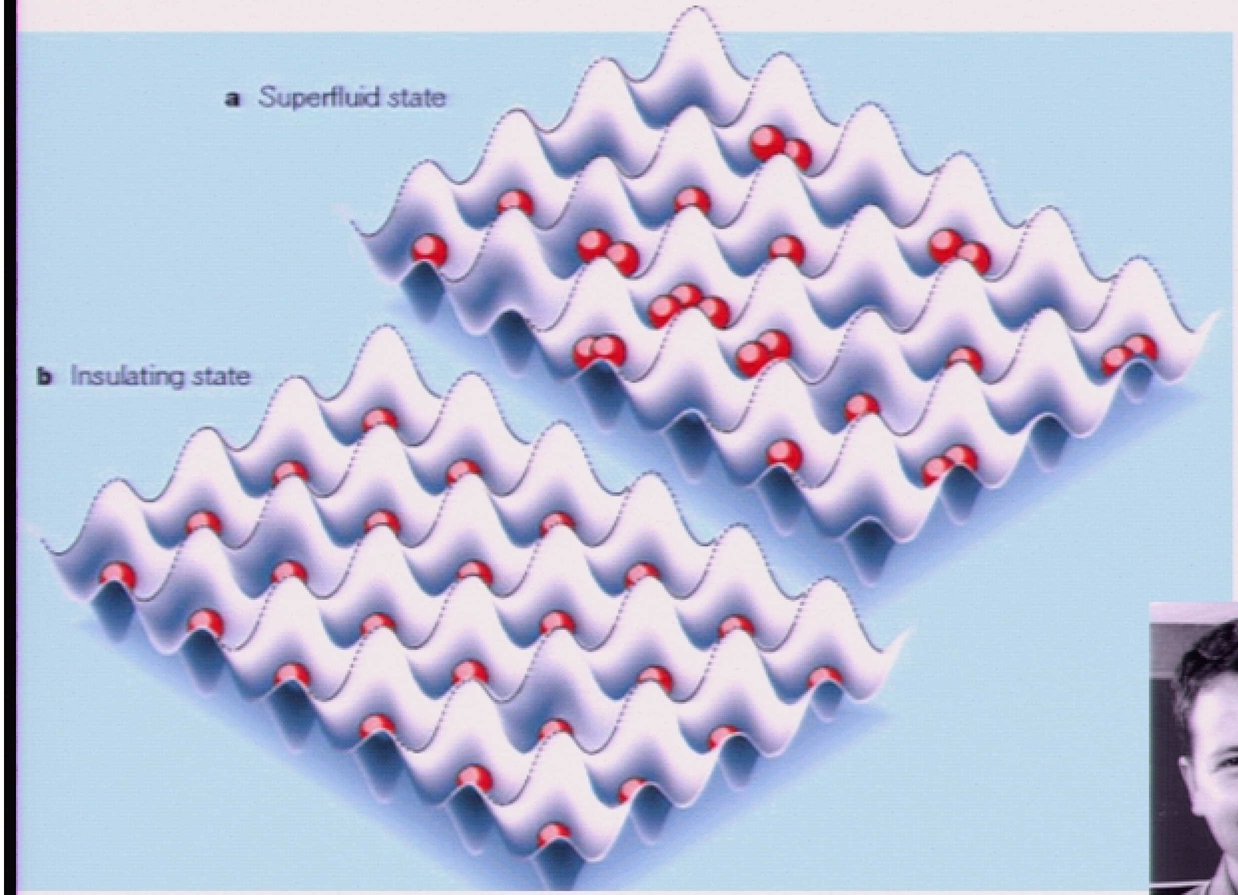
Furthermore, the Hamiltonian enforces that the ground state is invariant under an F-move. The quasiparticles are persuaded to behave just like the particles in the anyon model (except that the model is “parity doubled”).

$$= \left(F_{abcd}\right)_e^f$$



The topological order is expected to survive when the Hamiltonian is slightly perturbed.

Quantum many-body physics: Exotic phases in optical lattices



Atoms can be trapped in an optical lattice. The lattice geometry and interactions between neighbors can be chosen by the "material designer" (direction-dependent and spin dependent tunneling between sites).

n particular, Duan, Lukin, and Demler (cond-mat/0210564) have lescribed how Kitaev's honeycomb lattice model, which supports ionabelian anyons, can be simulated using an optical lattice.

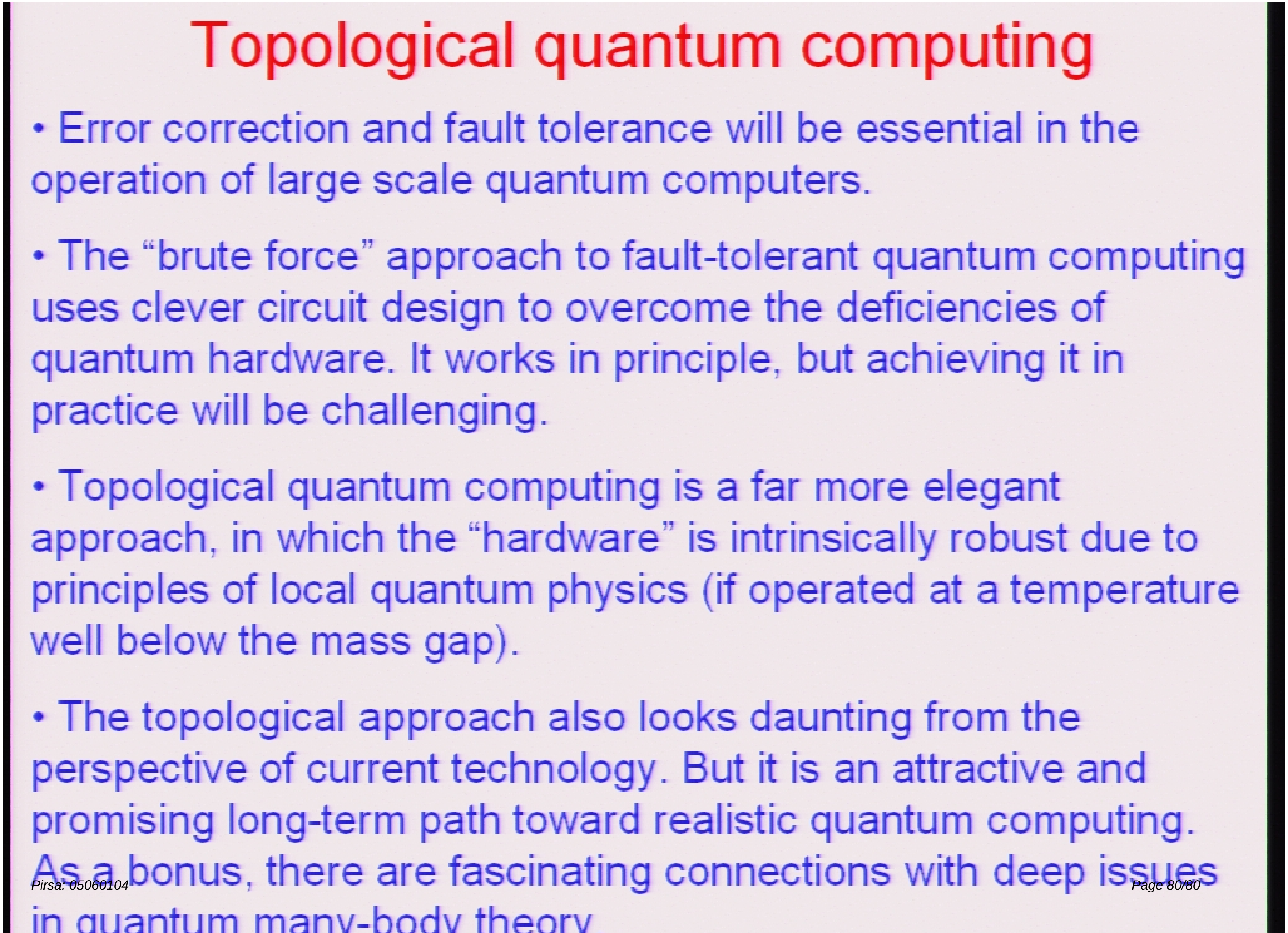
Topological quantum computing

- Error correction and fault tolerance will be essential in the operation of large scale quantum computers.

- The “brute force” approach to fault-tolerant quantum computing uses clever circuit design to overcome the deficiencies of quantum hardware. It works in principle, but achieving it in practice will be challenging.

- Topological quantum computing is a far more elegant approach, in which the “hardware” is intrinsically robust due to principles of local quantum physics (if operated at a temperature well below the mass gap).

- The topological approach also looks daunting from the perspective of current technology. But it is an attractive and promising long-term path toward realistic quantum computing. As a bonus, there are fascinating connections with deep issues in quantum many-body theory



Topological quantum computing

- Error correction and fault tolerance will be essential in the operation of large scale quantum computers.
- The “brute force” approach to fault-tolerant quantum computing uses clever circuit design to overcome the deficiencies of quantum hardware. It works in principle, but achieving it in practice will be challenging.
- Topological quantum computing is a far more elegant approach, in which the “hardware” is intrinsically robust due to principles of local quantum physics (if operated at a temperature well below the mass gap).
- The topological approach also looks daunting from the perspective of current technology. But it is an attractive and promising long-term path toward realistic quantum computing. As a bonus, there are fascinating connections with deep issues in quantum many-body theory