IAS-ICTP School on Quantum Information Processing, Singapore, January 18-29, 2016

FQH-Based Topological Quantum Computer: Materials, Devices & Algorithms

Xin Wan

Zhejiang University

xinwan@zju.edu.cn

http://zimp.zju.edu.cn/~xinwan/Singapore2016/

Model of Anyons

- A model of anyons is a theory of a two-dimensional medium with a mass gap, where the particles carry locally conserved charges. One defines
  - A finite *label set* $\{a,b,c,\ldots\}$;
  - The *fusion rules* $a \times b = \Sigma_c N_{ab}^{\ c}\, c$;
  - The *F-matrix* (expressing associativity of fusion);
  - The *R-matrix* (braiding rules).

F & R satisfy self-consistency equations, known as the pentagon and hexagon equations.

Ising anyon model:

$\{1, \sigma, \psi\}$

$\sigma \times \sigma = 1 + \psi$
$\psi \times \psi = 1$
$\psi \times \sigma = \sigma \times \psi = \sigma$

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

$$R = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{3i\pi/8} \end{pmatrix}$$

Diagrams

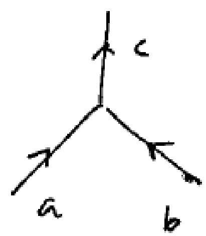
– Anyon a :

– Antiparticle $\bar{a}$:

$=$

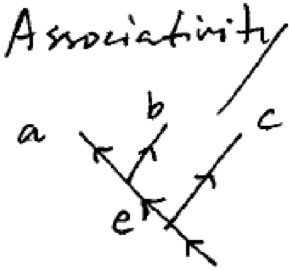
– Fusion $a \times b = c \; (+ \cdots)$

$$\left(\frac{d_c}{d_a d_b}\right)^{1/4}$$

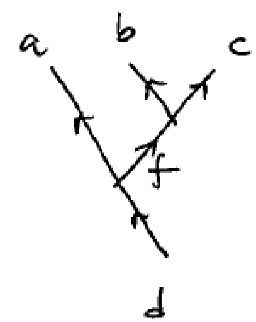


$= \langle ab; c|$

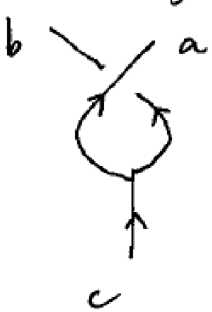
– Associativity



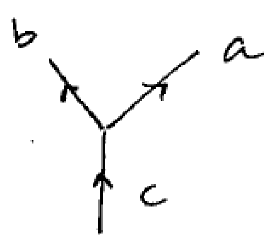
$$= \sum_f \left[F^{abc}_d \right]_{ef}$$



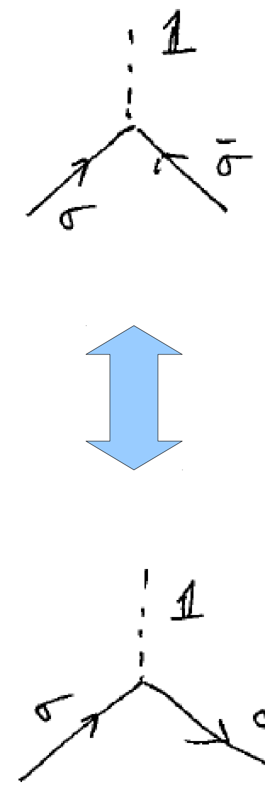
– Braiding



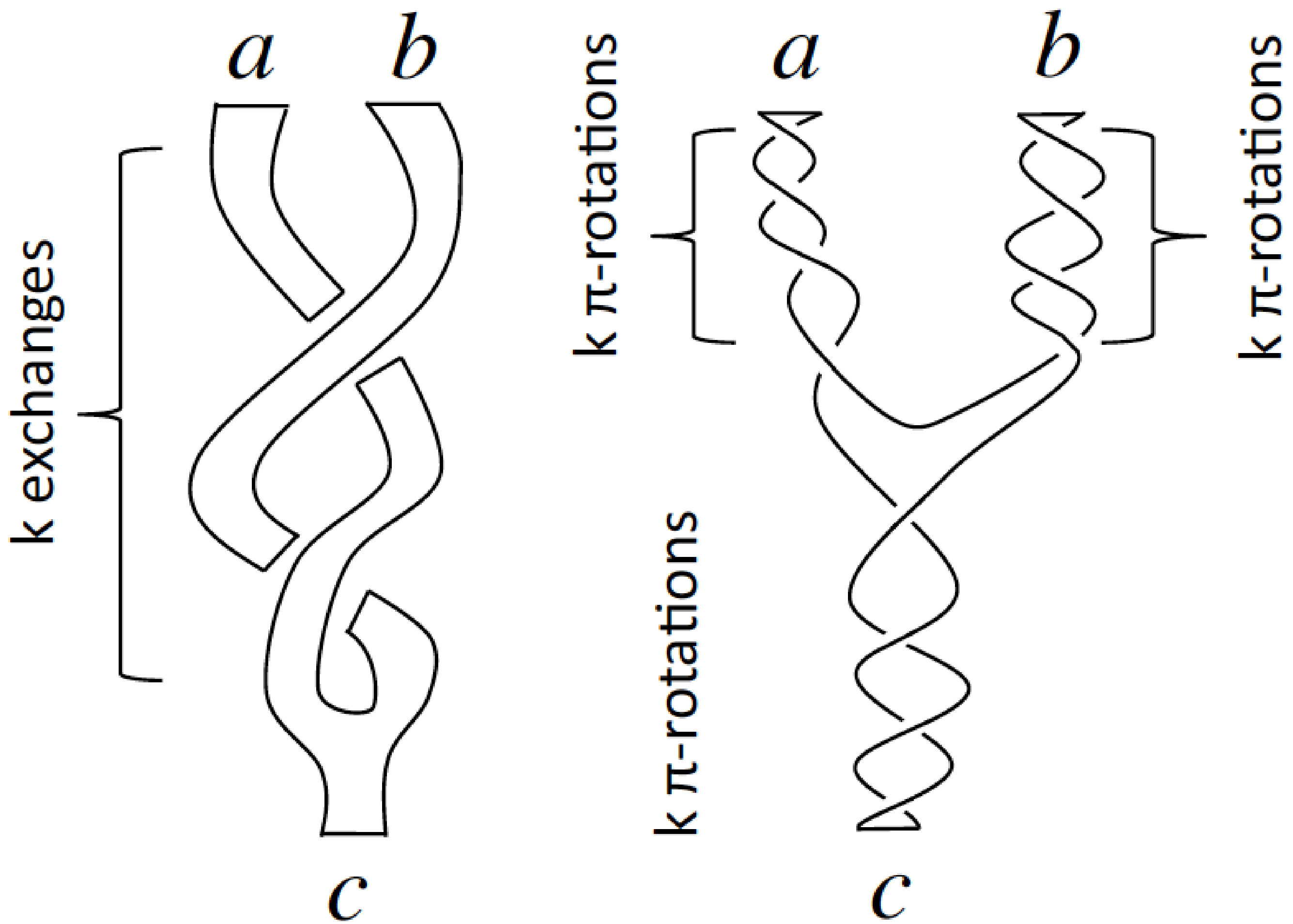
$= R^{ab}_c$



phase

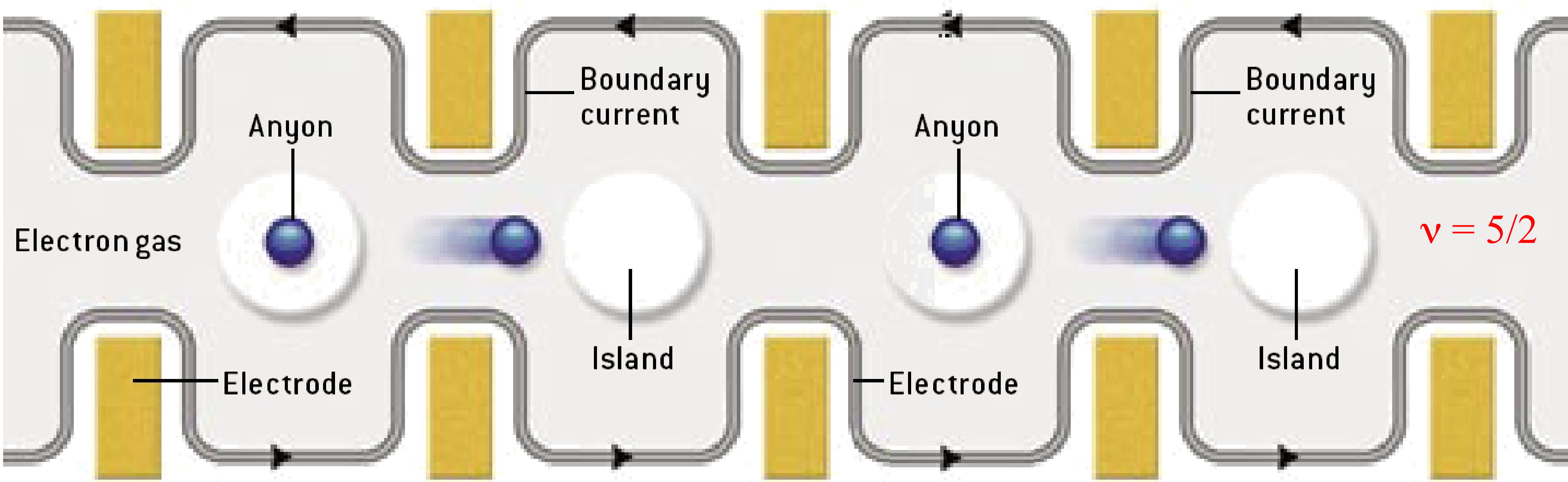


Spin and Statistics



$$(R^c_{ab})^k = e^{-i\pi k s_a} e^{-i\pi k s_b} e^{i\pi k s_c}$$

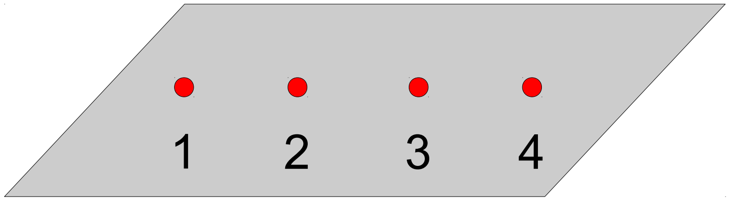
Initialize Anyons



Das Sarma, Freedman & Nayak (2005)

Four Ising Anyons as a Qubit

- Even when one fixes the location of all quasiholes, there are more than one states



$$\Psi_{(12)(34)} = Pf\left(\frac{(z_i-\xi_1)(z_i-\xi_2)(z_j-\xi_3)(z_j-\xi_4)+i\Leftrightarrow j}{z_i-z_j}\right)\prod_{1\leqslant i<j\leqslant N}(z_i-z_j)^2$$

$$\Psi_{(13)(24)} = Pf\left(\frac{(z_i-\xi_1)(z_i-\xi_3)(z_j-\xi_2)(z_j-\xi_4)+i\Leftrightarrow j}{z_i-z_j}\right)\prod_{1\leqslant i<j\leqslant N}(z_i-z_j)^2$$

$$\Psi_{(14)(23)} = Pf\left(\frac{(z_i-\xi_1)(z_i-\xi_4)(z_j-\xi_2)(z_j-\xi_3)+i\Leftrightarrow j}{z_i-z_j}\right)\prod_{1\leqslant i<j\leqslant N}(z_i-z_j)^2$$

- But they are not linearly independent!

$$\Psi_{(12)(34)}-\Psi_{(13)(24)}=(1-x)\left(\Psi_{(12)(34)}-\Psi_{(14)(23)}\right) \qquad x=\frac{(\xi_1-\xi_2)(\xi_3-\xi_4)}{(\xi_1-\xi_3)(\xi_2-\xi_4)}$$

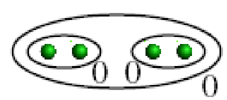
Four Ising Anyons as a Qubit

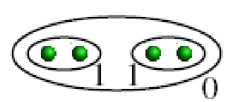
- Ansatz wavefunction (decomposition into two quasihole-paring wavefunctions)

$$\begin{aligned}\Psi^{(0,1)}(\xi_1,\xi_2,\xi_3,\xi_4;z_1,\ldots,z_N) &= A^{(0,1)}(\{\xi\})\,\Psi_{(12)(34)}(\{\xi\},\{z\}) \\ &+ B^{(0,1)}(\{\xi\})\,\Psi_{(13)(24)}(\{\xi\},\{z\})\end{aligned}$$

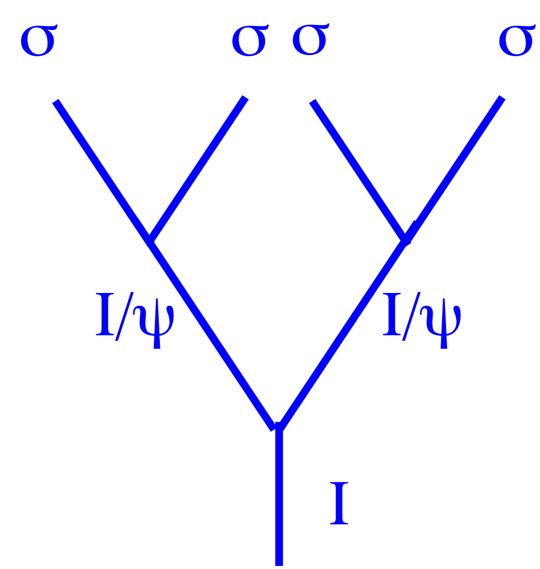
C. Nayak and F. Wilczek, Nucl. Phys. B 479 (1996) 529

E. Ardonne and K. Schoutens, Ann. Phys. 322 (2007) 201

$|0\rangle = |(\cdot\cdot)_0(\cdot\cdot)_0\rangle_0 =$ 

$|1\rangle = |(\cdot\cdot)_1(\cdot\cdot)_1\rangle_0 =$ 

Ising: • = σ, 0 = 1, 1 = ψ

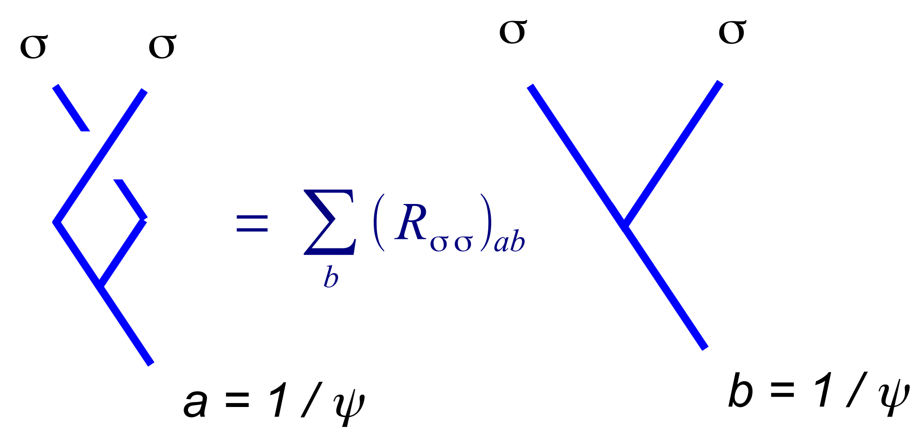


Identify the Two Fusion Channels

- The two linearly independent wave function can be written as

$$\Psi^{\pm} = \frac{[(\xi_1-\xi_3)(\xi_2-\xi_4)]^{1/4}}{\left(1\pm\sqrt{1-x}\right)^{1/2}}\left(\Psi_{(13)(24)}\pm\sqrt{1-x}\,\Psi_{(14)(23)}\right) \qquad \Psi = a^{+}\Psi^{+} + a^{-}\Psi^{-}$$

- Exchanging ξ_1 and ξ_2, we have



$$1-x \rightarrow \frac{1}{1-x}$$

$$(\xi_1-\xi_3)(\xi_2-\xi_4) \rightarrow (\xi_2-\xi_3)(\xi_1-\xi_4)$$
$$=(\xi_1-\xi_3)(\xi_2-\xi_4)(1-x)$$

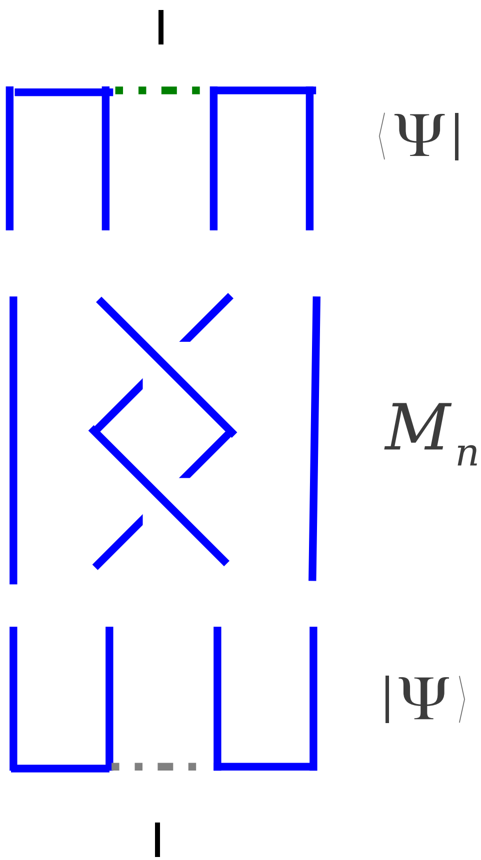
$$1-x = \frac{(\xi_1-\xi_4)(\xi_2-\xi_3)}{(\xi_1-\xi_3)(\xi_2-\xi_4)}$$

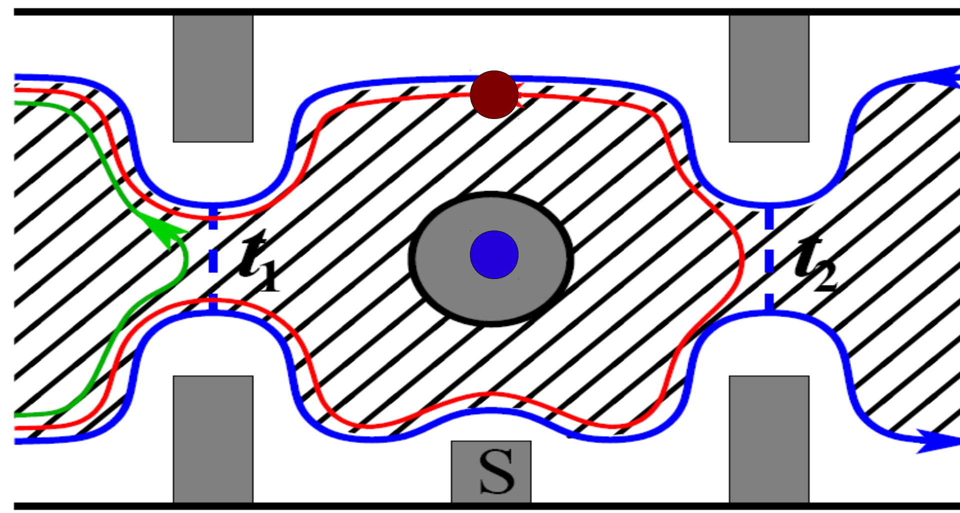
$$\Phi_{(13)(24)}\pm\sqrt{1-x}\,\Phi_{(14)(23)} \rightarrow \Phi_{(23)(14)}\pm\sqrt{\frac{1}{1-x}}\,\Phi_{(24)(13)}$$
$$=\sqrt{\frac{1}{1-x}}\left[\pm\Phi_{(13)(24)}+\sqrt{1-x}\,\Phi_{(14)(23)}\right]$$

$$\boxed{\begin{pmatrix}\Psi^{+}\\ \Psi^{-}\end{pmatrix} \rightarrow \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\Psi^{+}\\ \Psi^{-}\end{pmatrix}}$$

R-matrix (Ising x U(1))

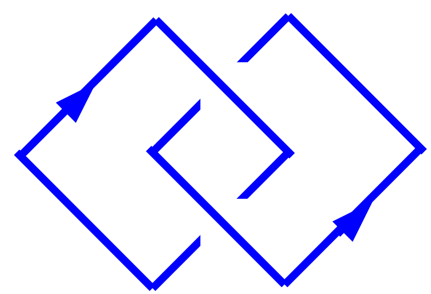
A Simple Quantum Computation



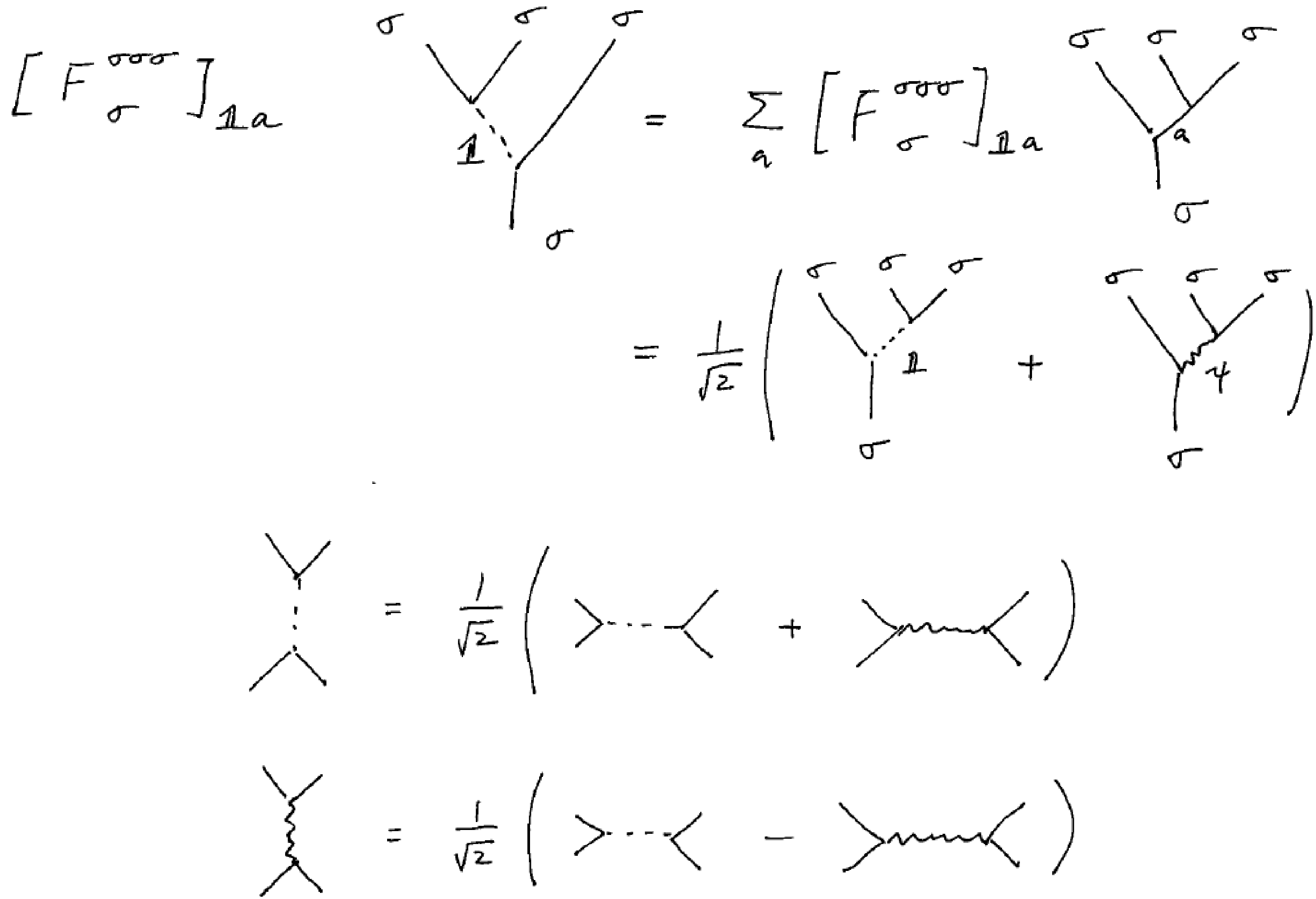


$$G \propto \left| t_1 U_1 + t_2 U_2 |\Psi\rangle \right|^2 = |t_1|^2 + |t_2|^2 + 2\,\Re\left\{ t_1^* t_2 e^{i\phi} \langle \Psi | M_n | \Psi \rangle \right\}$$

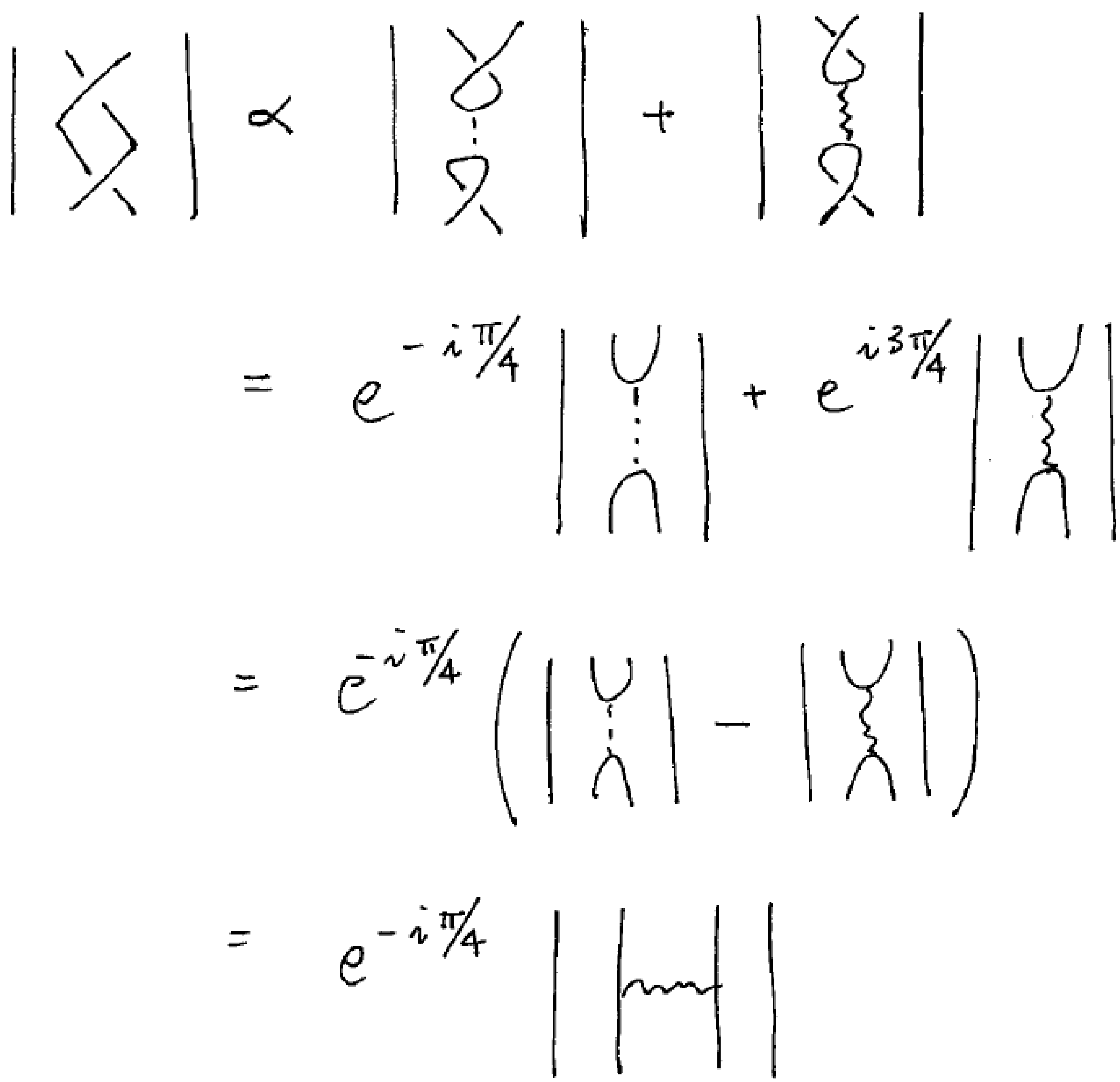
$$\langle \Psi | M_n | \Psi \rangle$$



Calculating with F-Matrix

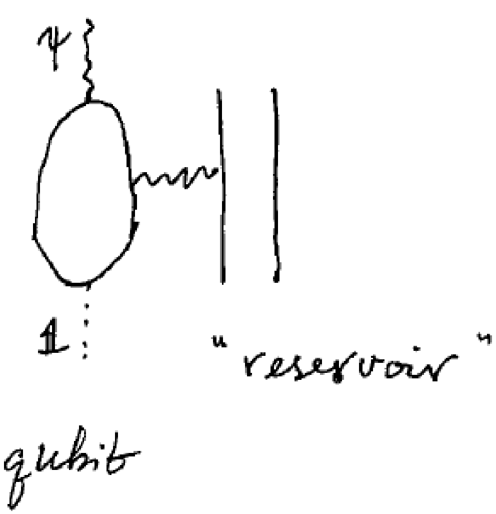


NOT Gate



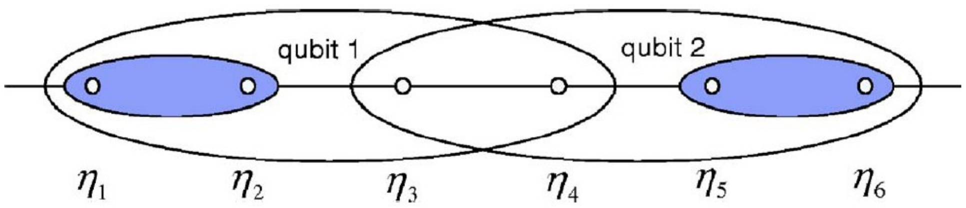
$$R_{\mathbb{1}}^{\sigma\sigma} = e^{-i\pi/8}$$

$$R_{\psi}^{\sigma\sigma} = e^{i3\pi/8}$$



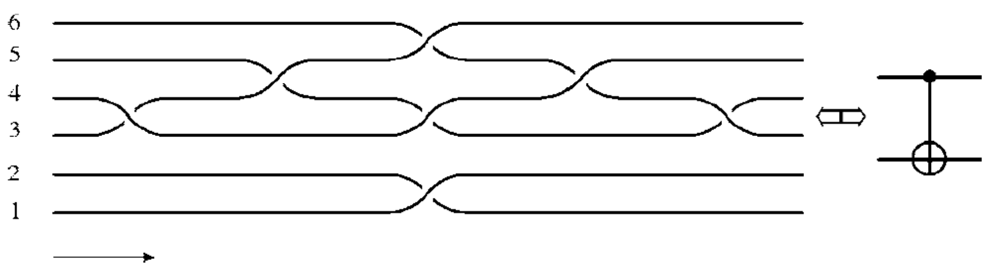
Braiding Example: CNOT Gate

$$R_{12}^{(6)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \end{pmatrix}, \quad R_{23}^{(6)} = \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} \begin{pmatrix} 1 & 0 & -i & 0 \\ 0 & 1 & 0 & -i \\ -i & 0 & 1 & 0 \\ 0 & -i & 0 & 1 \end{pmatrix}$$



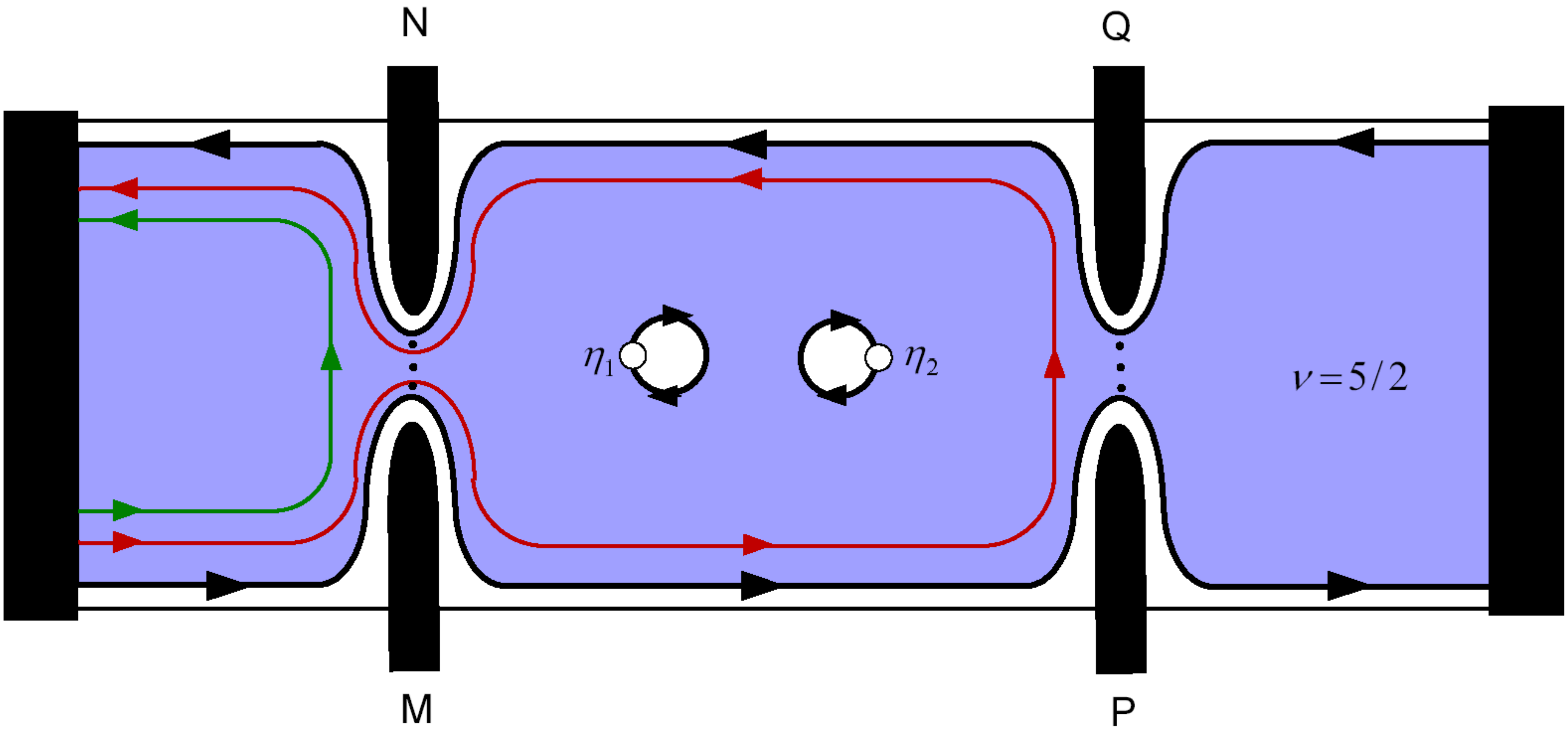
$$R_{34}^{(6)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad R_{45}^{(6)} = \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} \begin{pmatrix} 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & -i & 1 \end{pmatrix} \quad R_{56}^{(6)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$$

Generates representation of the braid group B_6



$$\text{CNOT} = R_{34}^{-1} R_{45} R_{34} R_{12} R_{56} R_{45} R_{34}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

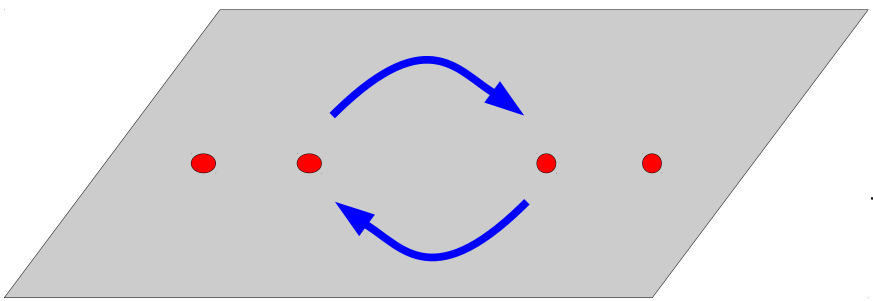
Measuring Anyons



$$\sigma_{xx}^{|0\rangle} \propto |t_{MN} + i t_{PQ}|^2. \qquad \sigma_{xx}^{|1\rangle} \propto |t_{MN} - i t_{PQ}|^2.$$

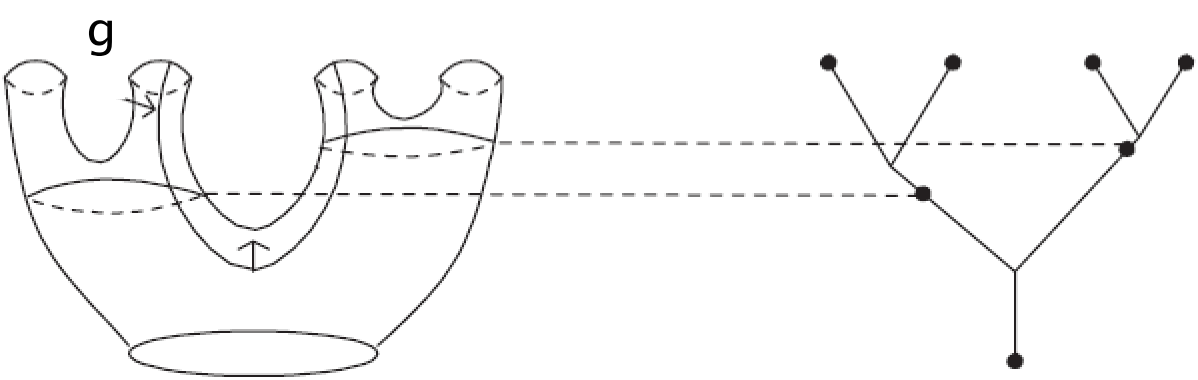
Das Sarma, Freedman & Nayak, PRL 94, 166802 (2005)

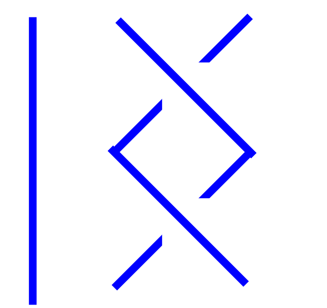
#4: Pictorial Messages



$$\Psi_a \rightarrow M_{ab} \Psi_b$$

Planer graph with punctures <==> Condensate with quasiparticles





initialization/
measurement (inverse process)

braiding = computing

Advantages: GS degeneracy and braiding operation robust against local perturbation

Universal Quantum Gate Set

- A set of universal quantum gates is any set of gates to which any operation possible on a quantum computer can be reduced, that is, any other unitary operation can be expressed as a finite sequence of gates from the set. We only require that any quantum operation can be approximated by a sequence of gates from this finite set. Moreover, for the specific case of single qubit gates, the Solovay-Kitaev theorem guarantees that this can be done efficiently.
- From a more mathematical point of view, the Solovay-Kitaev theorem is a remarkable general statement about how quickly the group SU(d) is "filled in" by a universal set of gates.
- One simple set of universal quantum gates is the Hadamard gate H, the π/8-gate R(π/4), and the controlled-NOT gate.

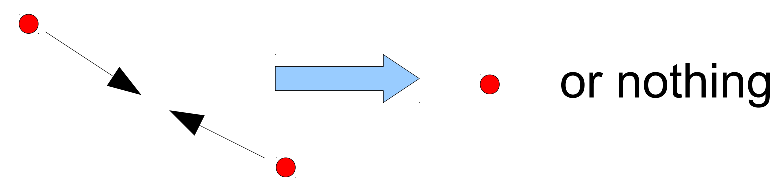
$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

Fibonacci Anyons

- Suppose we have <u>only</u> two types of anyons
  - A trivial anyon I (or 0): representing the ground state of the system (vacuum)
  - A non-trivial anyon τ (or 1) – must be the antiparticle of itself

- Anyons can be fused to a new one

Two possibilities: non-Abelian! → $\tau \times \tau = I + \tau$



Ising: $\sigma \times \sigma = I + \psi$

$$F = \begin{pmatrix} \phi^{-1} & \phi^{-1/2} \\ \phi^{-1/2} & -\phi^{-1} \end{pmatrix} \qquad R = \begin{pmatrix} e^{-i4\pi/5} & 0 \\ 0 & e^{i3\pi/5} \end{pmatrix}$$

$$\phi = \frac{\sqrt{5}+1}{2} \qquad (\phi^2 = 1+\phi)$$

k = 3 Read-Rezayi state; non-Abelian spin-singlet state (Ardonne & Schoutens)

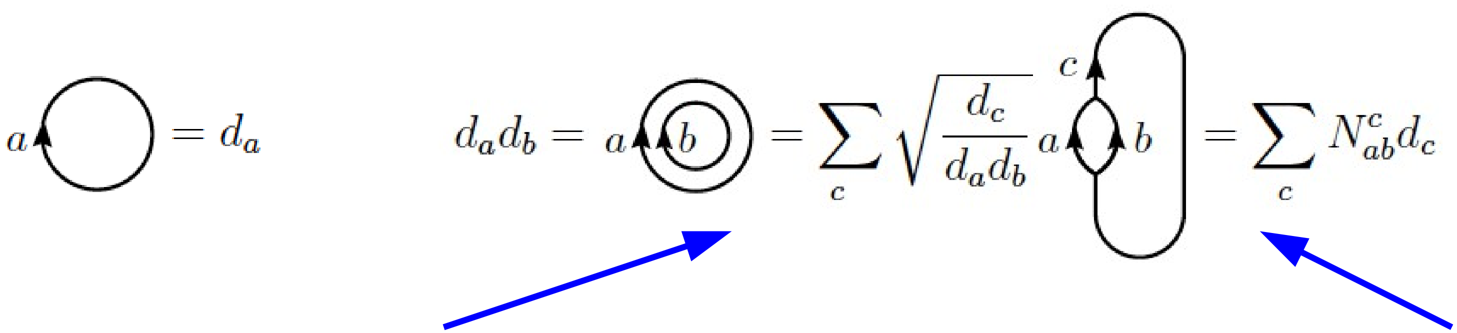
Quantum Dimension

$$\tau\times\tau\times\tau\times\tau=(I+\tau)\times\tau\times\tau=(\tau\times\tau)+(\tau\times\tau\times\tau)=(I+\tau)+(I+\tau+\tau)$$

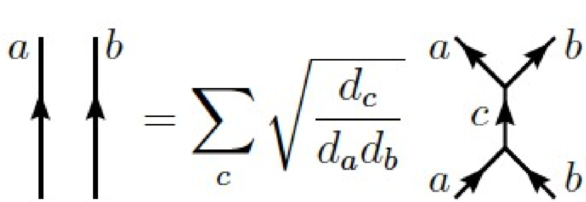
$$V_{n+1}=V_{n-1}+V_n$$

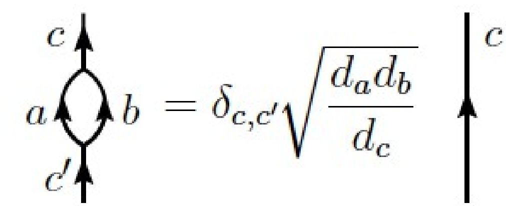
$$Dim(V_n)\sim\phi^n,\quad \phi=(\sqrt{5}+1)/2$$

Dimension of V_n: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...



$\phi^2 = 1 + \phi$



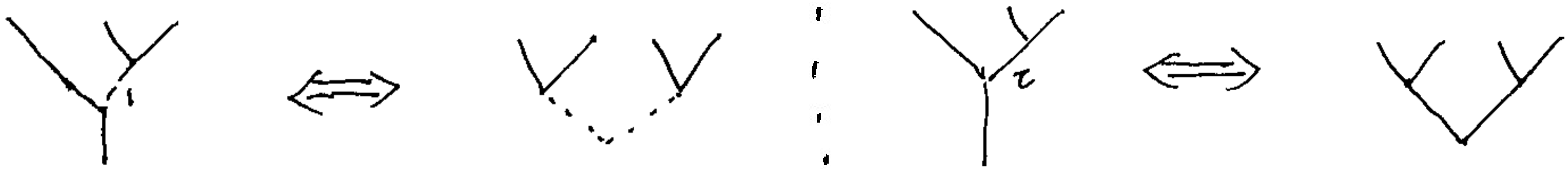


$$\mathbb{I}_{ab}=\sum_c |a,b;c\rangle\langle a,b;c|$$

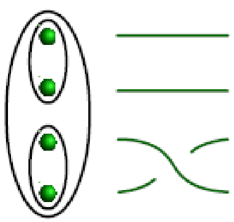
$$\langle a,b;c|a,b;c'\rangle=\delta_{c,c'}$$

Single Qubit and Elementary Braids

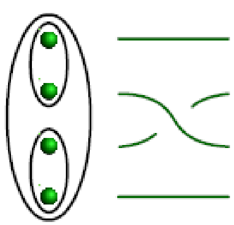
- Either three or four anyons can encode one qubit of information.



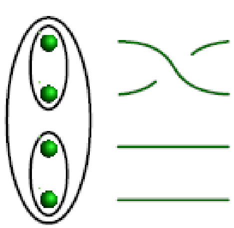
- A braid represents the worldline of anyons in the (2+1)-dim spacetime.



$$\sigma_1 = \begin{bmatrix} e^{-i4\pi/5} & 0 \\ 0 & -e^{-i2\pi/5} \end{bmatrix}$$



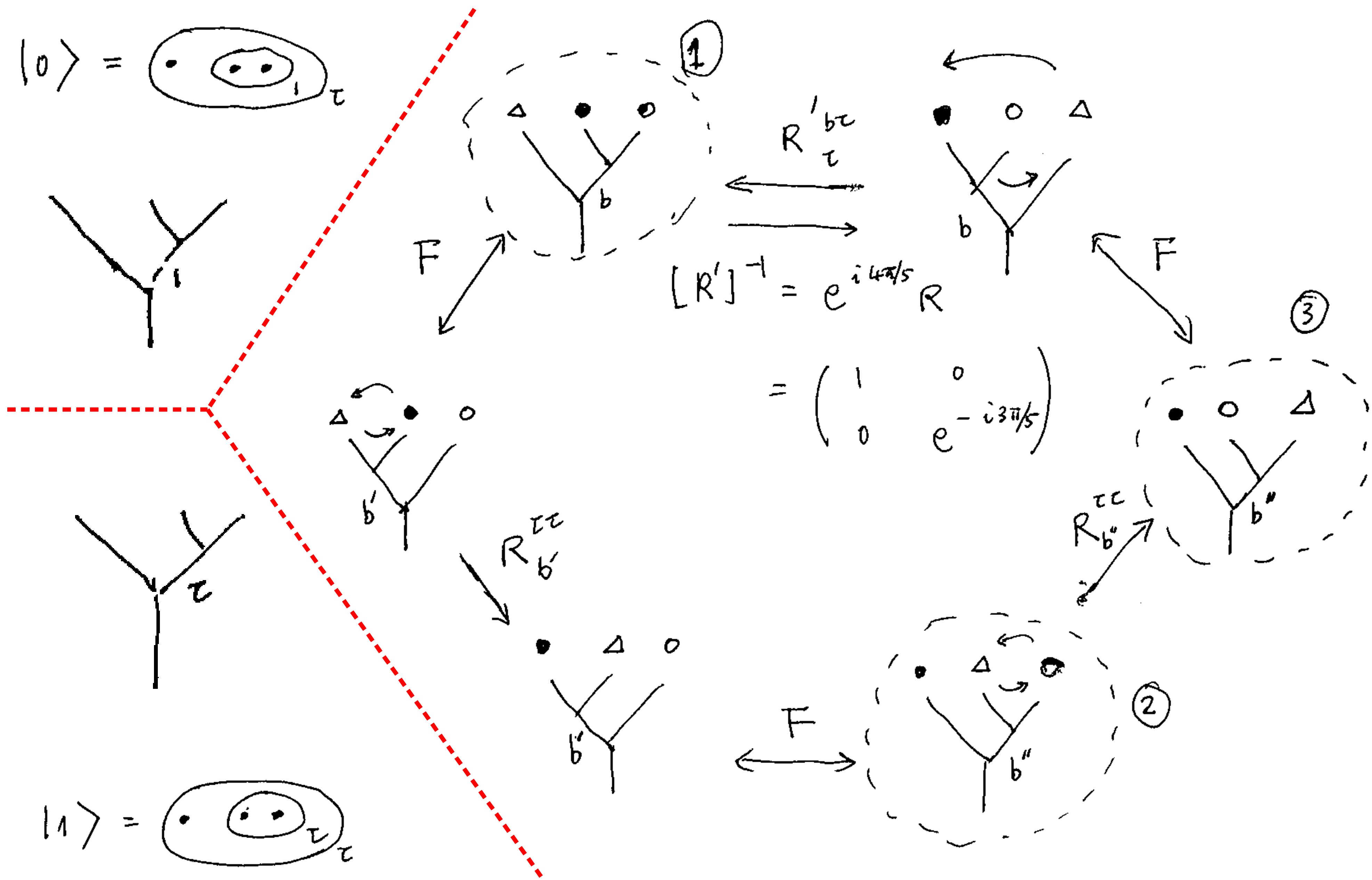
$$\sigma_2 = \begin{bmatrix} -\tau e^{-i\pi/5} & -\sqrt{\tau} e^{i2\pi/5} \\ -\sqrt{\tau} e^{i2\pi/5} & -\tau \end{bmatrix} \qquad \tau = \frac{\sqrt{5}-1}{2}$$



$$\sigma_3 = \begin{bmatrix} e^{-i4\pi/5} & 0 \\ 0 & -e^{-i2\pi/5} \end{bmatrix}$$

Identical to σ_1

Braiding Matrices from the Hexagon Equation

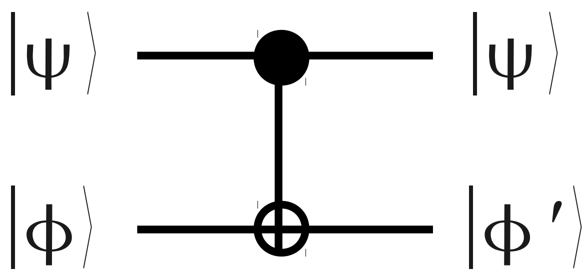


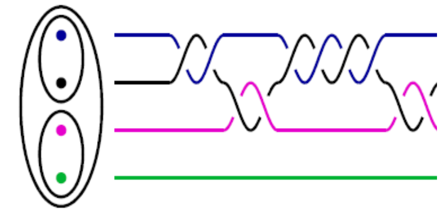
Universal Quantum Gates

- Single-qubit gates (rotation)

$$|\psi\rangle \; — \boxed{U} — \; U|\psi\rangle$$

- At least a two-qubit gate, such as CNOT





$$U^{-1} = \sigma_1^{-2}\sigma_2^{2}\sigma_1^{4}\cdots$$

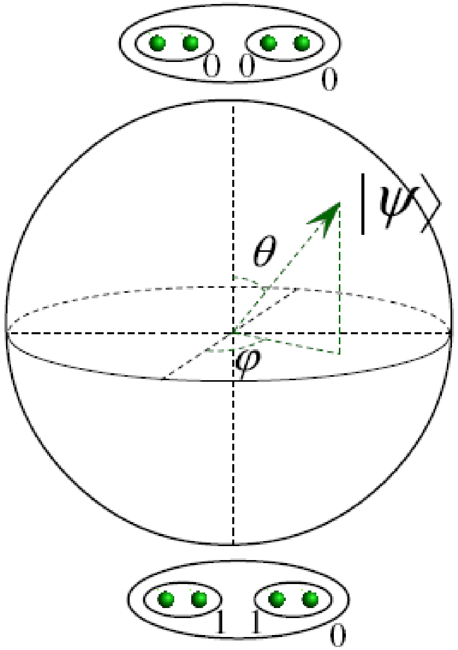
Goal: Efficiently find a sequence that approximates the target gate within a given error ε.

- Any N-qubit gates can be realized by the set of universal gates
- Freedman et al. proved TQC is as powerful as conventional QC; implemented by Bonesteel and co-workers using Fibonacci anyons.

Importance of Algorithm

- In a classical computer, one can build up a circuit, e.g., to add two numbers using OR and NOT gates.
- In a quantum computer, the set of possible quantum gates forms a continuum, and it's not necessarily possible to use one gate set to simulate another exactly. Instead, some approximation may be necessary.
- We explore an algorithm that guarantees the efficient construction of any quantum gate, to a very good approximation.
  - From a practical point of view, this is important in compiling quantum algorithms (like Shor's) into a form that can be implemented fault-tolerantly.
  - From a more mathematical point of view, we give a general statement about how quickly the group SU(d) is "filled in" by a universal set of gates.
- This is also the importance of the textbook example – the Solovay-Kitaev algorithm (c.f. Nielsen & Chung).

Single-Qubit Gates: Brute-Force Search



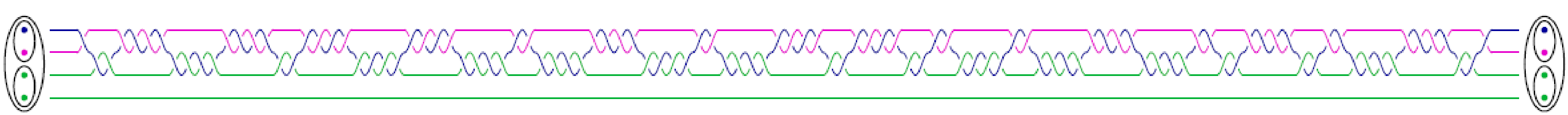
$$|\psi\rangle = \cos\theta|\,0\,\rangle + \sin\theta\, e^{i\varphi}|\,1\,\rangle$$

$$|\psi\rangle = e^{i\alpha}\left(\cos\theta\ |((11)_0(11)_0)_0\rangle + \sin\theta\ e^{i\varphi}|((11)_1(11)_1)_0\rangle\right)$$

- We have σ_1 (or σ_3), σ_2, and inverses σ_1^{-1}, σ_2^{-1}
- Each exchange has 3 possibilities (no return)
- Finding the best braid in ~3^N possibilities
- Exhaustive search: non-polynomial time

$$\sigma_i^{10} = 1$$

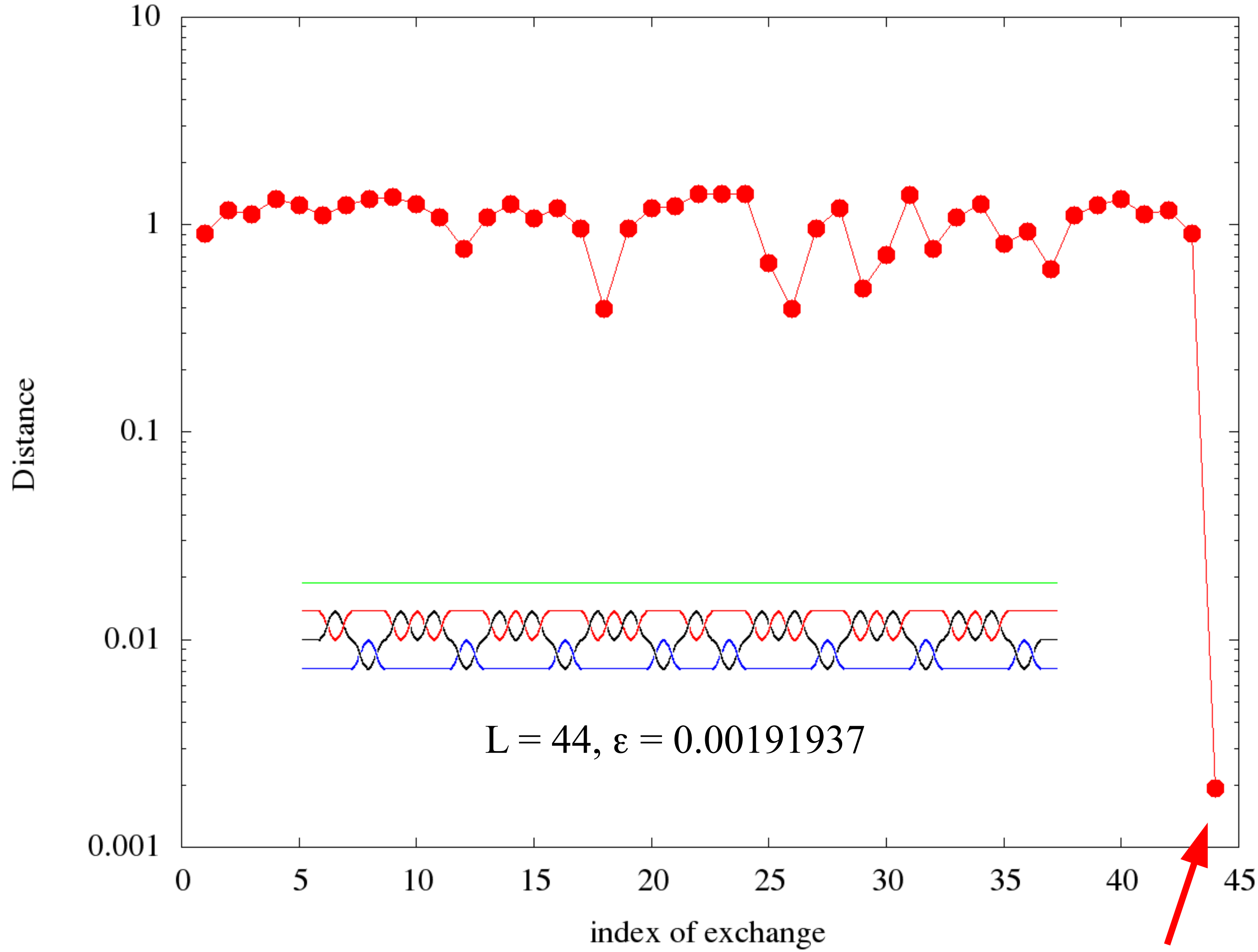
$$\sigma_1\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1 = 1$$



$$\approx \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

$$\sigma_3\sigma_2^2\sigma_3^4\sigma_2^4\sigma_3^4\sigma_2^{-2}\sigma_3^{-4}\sigma_2^{-4}\sigma_3^{-4}\sigma_2^4\sigma_3^{-2}\sigma_2^4\sigma_3^4\sigma_2^{-4}\sigma_3^{-2}\sigma_2^4\sigma_3^{-4}\sigma_2^{-2}\sigma_3^{-4}\sigma_2^{-2}\sigma_3^{-4}\sigma_2^{-2}\sigma_3^{-2}\sigma_2^{-4}\sigma_3^{-2}\sigma_2^4\sigma_3^4\sigma_2^4\sigma_3^2\sigma_2^{-2}\sigma_3^4\sigma_2^{-2}\sigma_3^2\sigma_2^4\sigma_3^4\sigma_2^{-2}\sigma_3^{-1}$$

Exchange-by-Exchange Distance

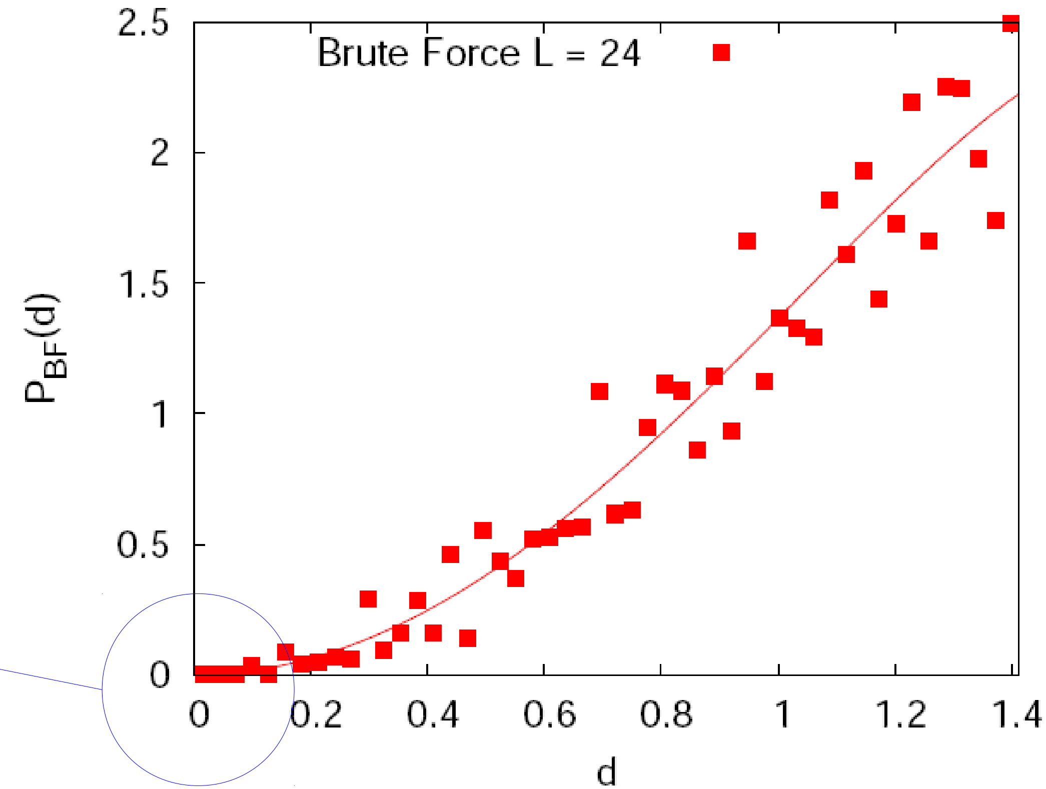


Distance between matrices U and V is defined as the square root of the highest eigenvalues of (U-V)*(U-V)

rare fluctuation!

Distance Distribution for a Fixed Length

Distribution of distance to the identity for all weaves (a subset of braids in which only one anyon moves) with a length 24:



How to enhanced the sampling at small *d*?

$$g = e^{i\hat{m}\cdot\vec{\sigma}(\phi/2)} = \begin{bmatrix} \cos(\phi/2) + i m_z \sin(\phi/2) & m_y \sin(\phi/2) + i m_x \sin(\phi/2) \\ -m_y \sin(\phi/2) + i m_x \sin(\phi/2) & \cos(\phi/2) - i m_z \sin(\phi/2) \end{bmatrix}$$

$$d = 2\sin(\phi/4) \qquad P_{BF}(d) = \frac{4}{\pi} d^2 \sqrt{1 - d^2/4}$$

assuming that the braids distributed uniformly in the space of unitary matrices

Randomly Uniform Approximation

- Assumption: The matrix representations of long enough braids distribute randomly in the space of unitary matrices (3-sphere). There is no local correlation.

$$g = e^{i\hat{m}\cdot\vec{\sigma}(\phi/2)}$$

  - Total number of weaves for a fixed braid length L:

$$N(L) \sim \alpha^{L/2}, \quad \alpha \approx 2.732 < 3$$

$$\sigma_i^{10} = 1 \qquad \sigma_1\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1 = 1$$

  - Average volume per weave on the 3-sphere:

$$[\epsilon(L)]^3 \sim 1/N(L) \sim \alpha^{-L/2}$$

  - Average error: $\epsilon(L) \sim \alpha^{-L/6}$

or $L \sim \ln(1/\epsilon)$

$$T \sim (1/\epsilon)^3 \sim e^{\gamma L}$$

inefficient!

$$\sigma_1^{n_1}\sigma_2^{n_2}\sigma_1^{n_3}\sigma_2^{n_4}\cdots\sigma_1^{n_{m-1}}\sigma_2^{n_m}$$

$$n_i = \pm 2, \pm 4$$

$$L = \sum_i |n_i|$$

$$N(L) \sim \left(1 + \sqrt{3}\right)^{L/2}$$

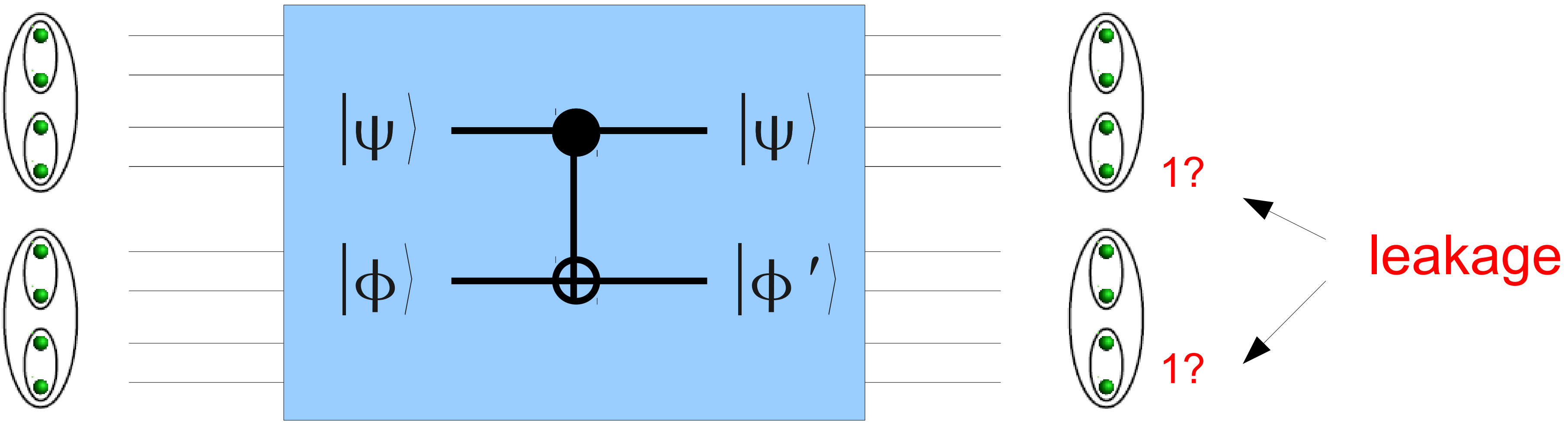
Burrello et al., 2011

Two-Qubit Gates

- Single-qubit gate: 3 free parameters [SU(2)]

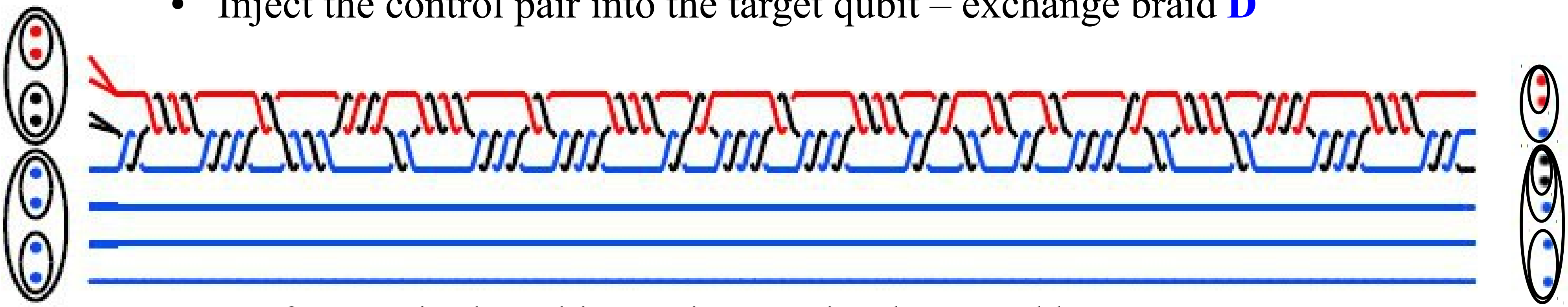
$$e^{i\alpha}\begin{bmatrix} \sqrt{1-b^2}e^{-i\beta} & be^{i\gamma} \\ -be^{-i\gamma} & \sqrt{1-b^2}e^{i\beta} \end{bmatrix}$$

- Two-qubit gate: too many parameters

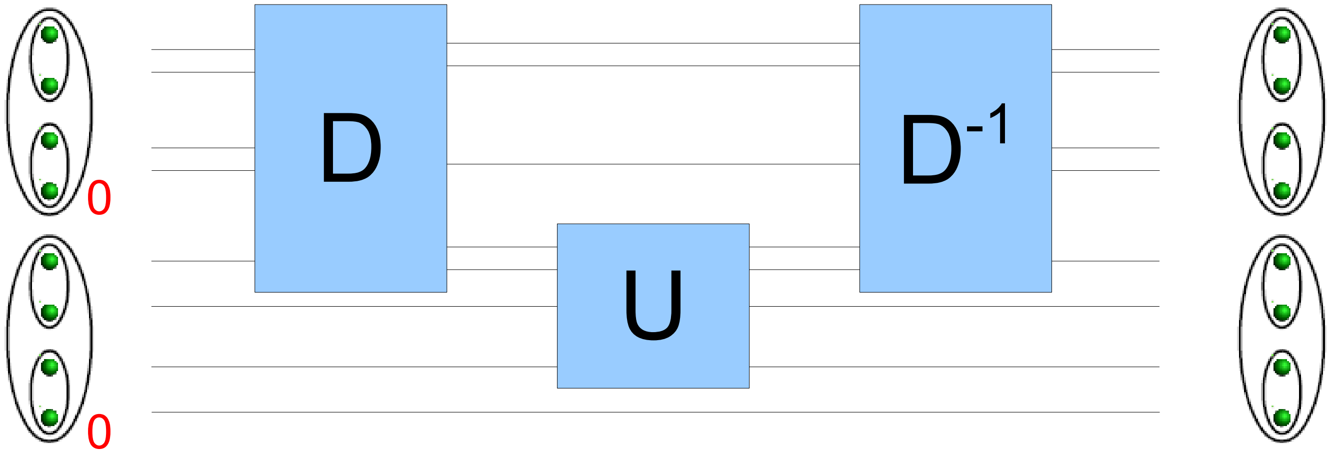


Decomposing Two-Qubit Gates

- Idea proposed by Bonesteel et al. (2005) – leakage error ~10^{-3}
- [Xu & Wan, 08] Reduces leakage error significantly, ~10^{-9}
  - Inject the control pair into the target qubit – exchange braid **D**



  - Perform a single-qubit rotation **U** – implemented by a weave
  - Extract the control pair use the inverse of the inverse of the exchange braid **D^{-1}**

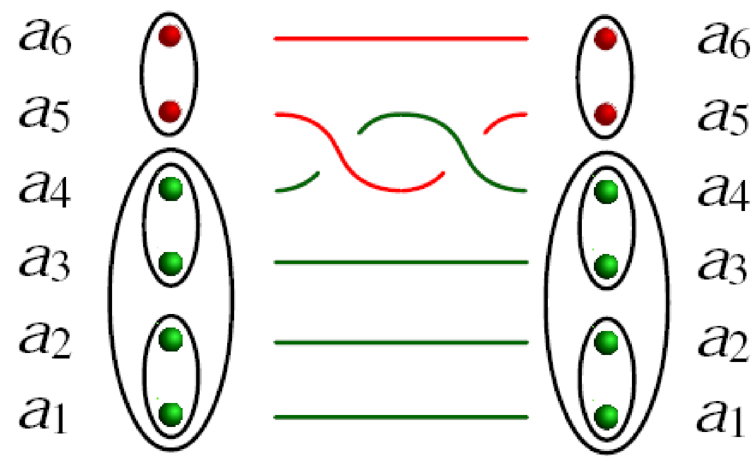


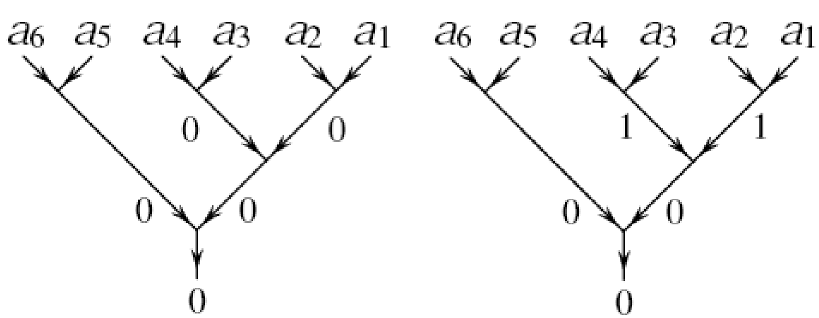
Generic controlled-gates with leakage error ~10^{-9}.

Leakage Error

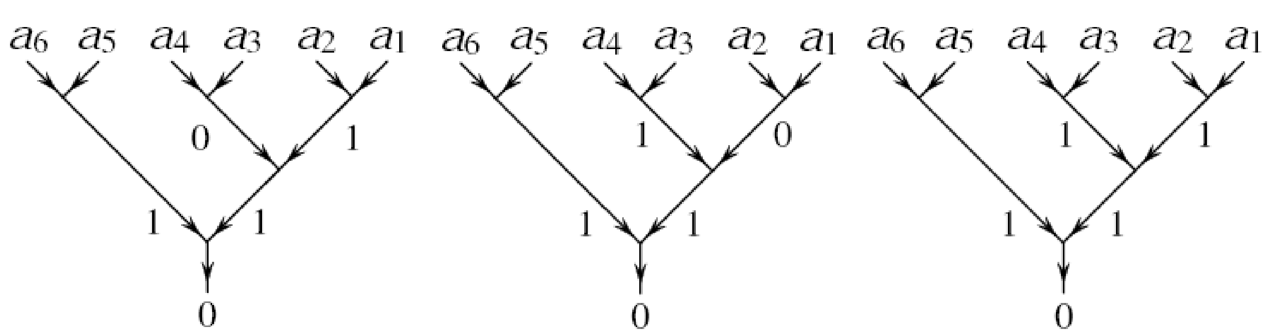
Create a pair of anyons out of vacuum (so fuse to 0).

Note they could also be stray anyons thermally excited.



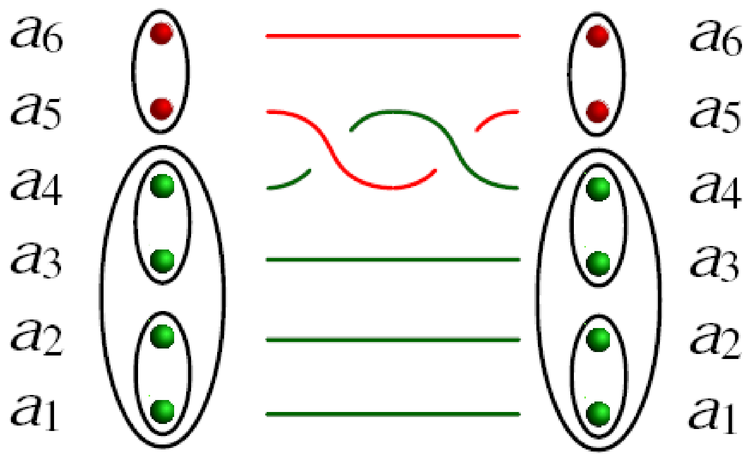


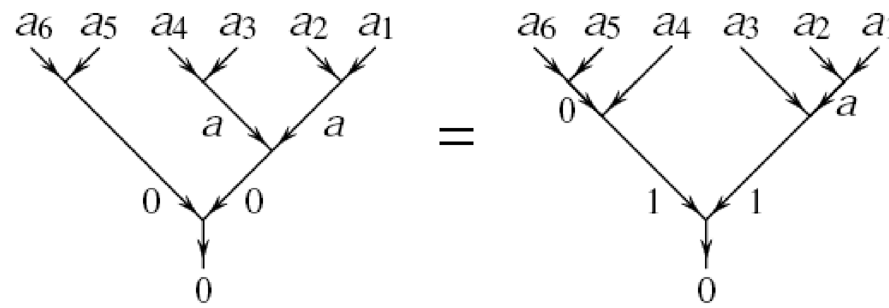
Computing basis



Non-computing basis

Leakage-Error Analysis

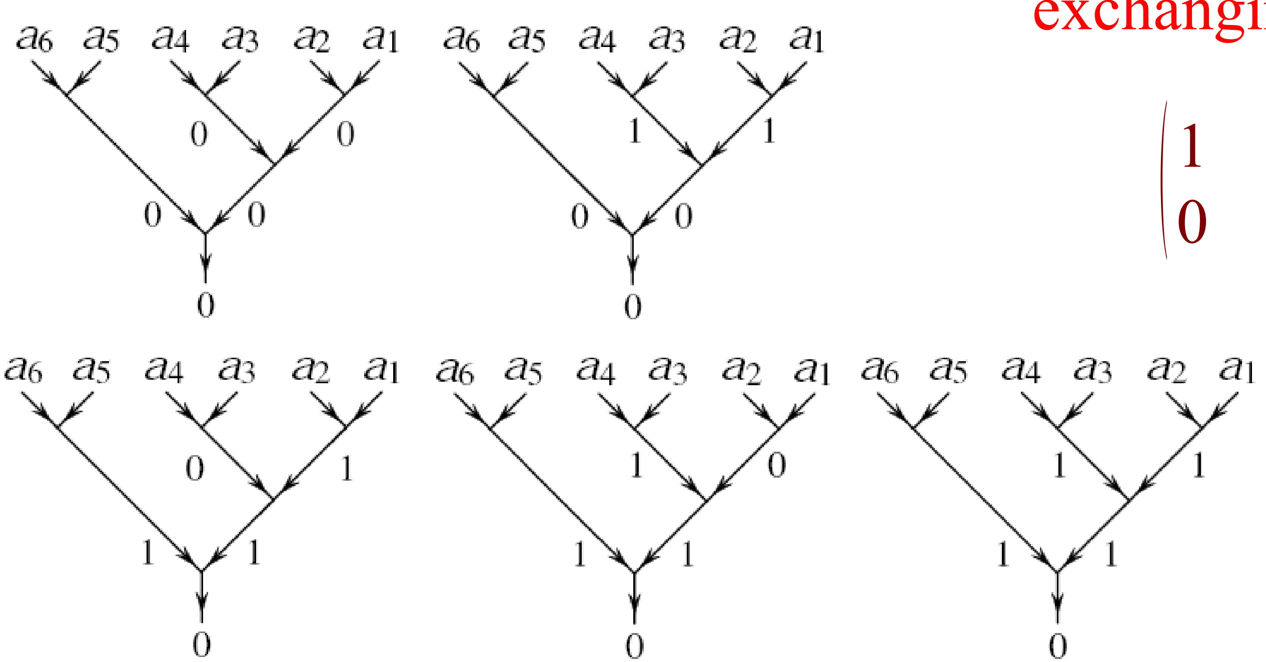




What kind of braids (of a_4, a_5, a_6) leave the left qubit in state 0, after exchanging a_4 and a_5?

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

$$\begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\beta} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = e^{i\alpha}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

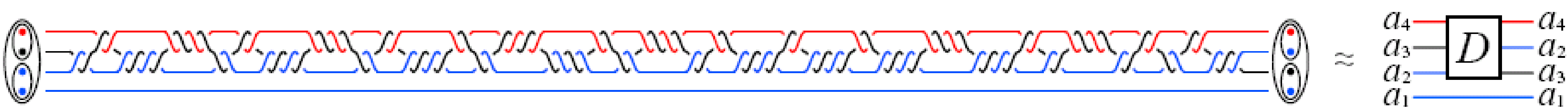


Phase Gates

- Let us look for diagonal matrices, rather than the identity matrix; this means we introduce a phase error.

$$e^{i\alpha}\begin{bmatrix} \sqrt{1-b^2}e^{-i\beta} & be^{i\gamma} \\ -be^{-i\gamma} & \sqrt{1-b^2}e^{i\beta} \end{bmatrix}$$

- For small b, γ is irrelavent. Targeting less parameter – higher accuracy!



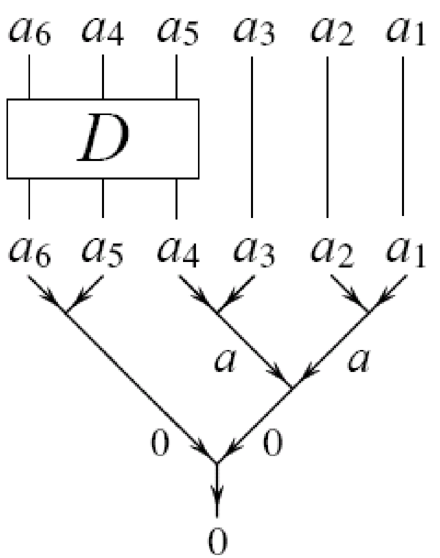
$$\sigma_2^{-2}\sigma_3^{-2}\sigma_2^{-4}\sigma_3^{4}\sigma_2^{2}\sigma_3^{-2}\sigma_2^{-4}\sigma_3^{4}\sigma_2^{2}\sigma_3^{-2}\sigma_2^{-4}\sigma_3^{2}\sigma_2^{2}\sigma_3^{-4}\sigma_2^{4}\sigma_3^{2}\sigma_2^{2}\sigma_3^{4}\sigma_2^{-2}\sigma_3^{2}\sigma_2^{-4}\sigma_3^{-2}\sigma_2^{-4}\sigma_3^{2}\sigma_2^{-4}\sigma_3^{4}\sigma_2^{-4}\sigma_3^{-2}\sigma_2^{-2}\sigma_3^{4}\sigma_2^{-2}\sigma_3^{-2}\sigma_2^{2}\sigma_3^{-2}\sigma_2^{-3} = e^{i\vartheta}\begin{bmatrix} r & \delta_1 \\ \delta_2 & re^{i\varphi} \end{bmatrix}$$

$$|\delta_1| = |\delta_2| = \sqrt{1-r^2} = 1.56\times 10^{-10}$$

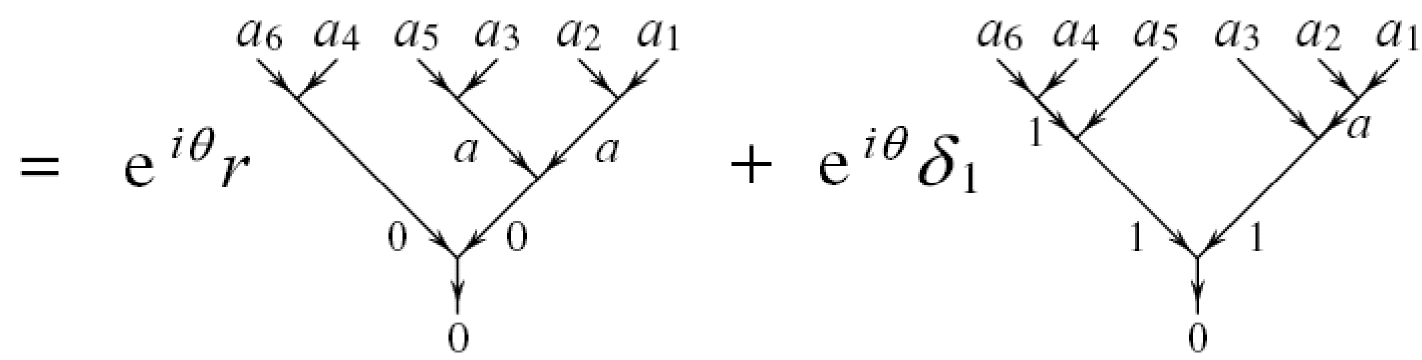
- But how do we use it? What about the phase?

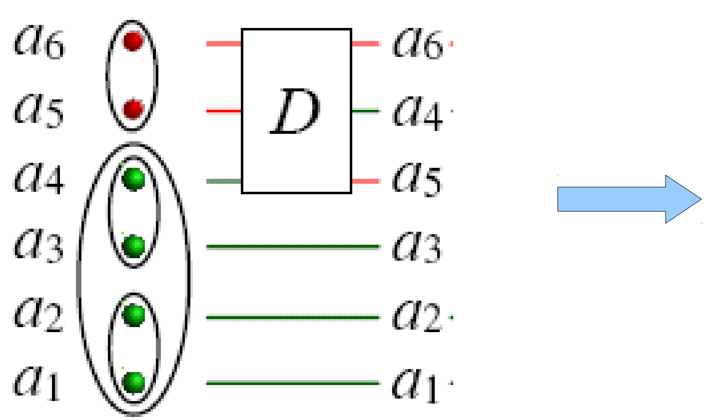
Exchange Braid

- Apply the diagonal gate (with the irrelevant phase) to the leakage model



Low leakage! $|\delta_1| = 1.56 \times 10^{-10}$



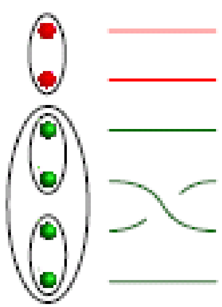


$$e^{i\theta} \left[\begin{array}{cc|ccc} r & 0 & 0 & \epsilon_1 & 0 \\ 0 & r & \epsilon_2 & 0 & \epsilon_3 \\ \hline 0 & \epsilon_5 & & & \\ \epsilon_4 & 0 & & A & \\ 0 & \epsilon_6 & & & \end{array} \right]$$

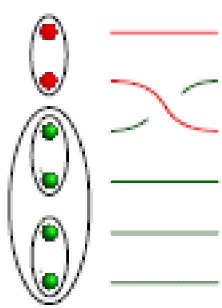
$$|\epsilon_1| = \sqrt{|\epsilon_2|^2 + |\epsilon_3|^2} = |\epsilon_4| = \sqrt{|\epsilon_5|^2 + |\epsilon_6|^2} = |\delta_1| = \sqrt{1 - r^2} \approx 1.56 \times 10^{-10}$$

5-Dimensional Representation

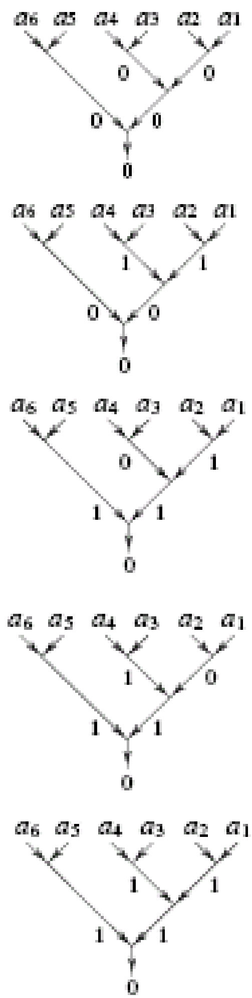
- One calculate the braiding matrix in an enlarged space, including non-computing bases.



$$\sigma_2 = \begin{bmatrix} -\tau e^{-i\pi/5} & -\sqrt{\tau}e^{i2\pi/5} & 0 & 0 & 0 \\ -\sqrt{\tau}e^{i2\pi/5} & -\tau & 0 & 0 & 0 \\ 0 & 0 & -\tau e^{-i\pi/5} & -\tau e^{i2\pi/5} & \tau^{3/2}e^{i2\pi/5} \\ 0 & 0 & -\tau e^{i2\pi/5} & -\tau e^{-i\pi/5} & \tau^{3/2}e^{i2\pi/5} \\ 0 & 0 & \tau^{3/2}e^{i2\pi/5} & \tau^{3/2}e^{i2\pi/5} & \nu \end{bmatrix}$$

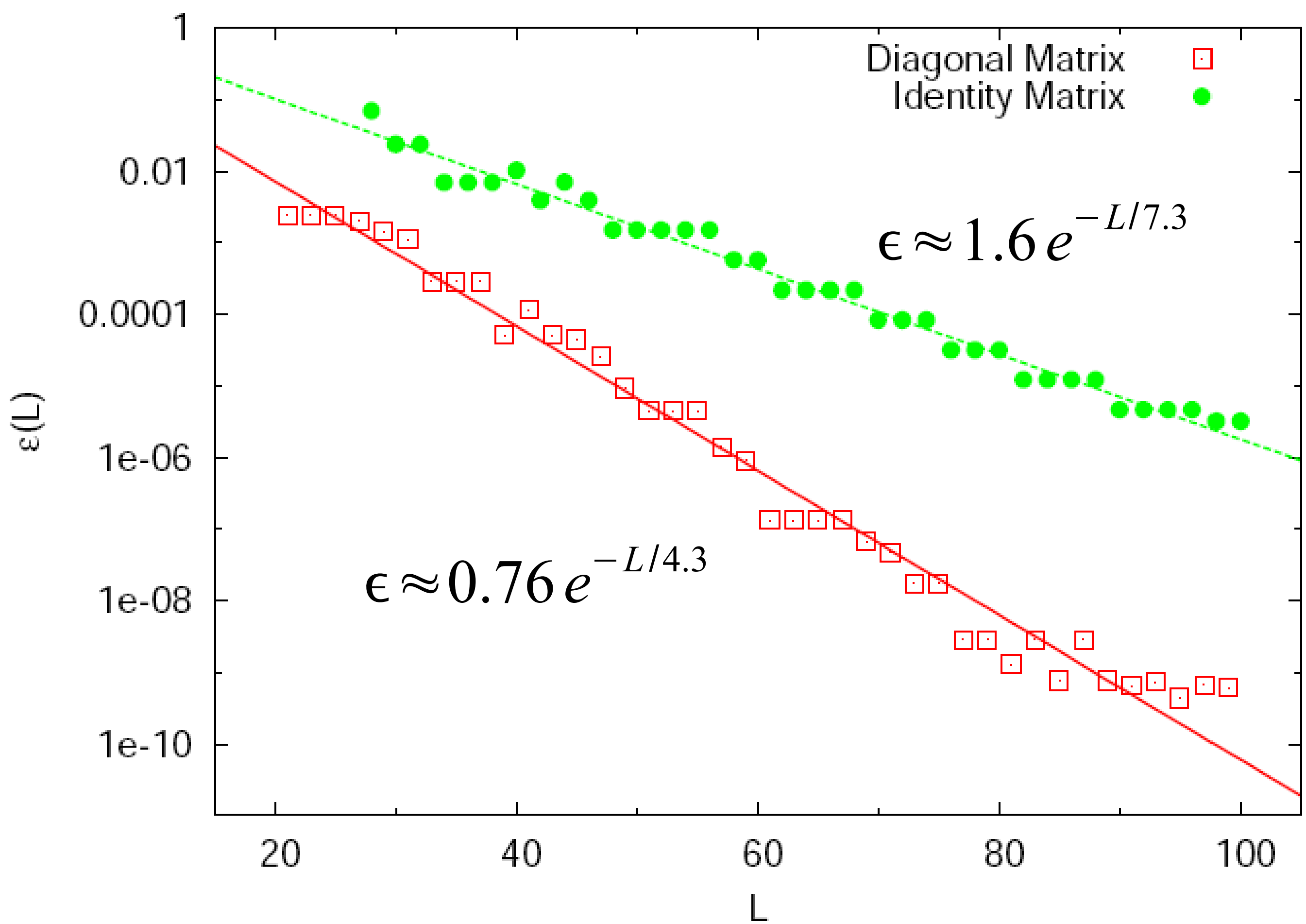


$$\sigma_4 = \begin{bmatrix} -\tau e^{-i\pi/5} & 0 & 0 & -\sqrt{\tau}e^{i2\pi/5} & 0 \\ 0 & -\tau e^{-i\pi/5} & -\tau e^{i2\pi/5} & 0 & \tau^{3/2}e^{i2\pi/5} \\ 0 & -\tau e^{i2\pi/5} & -\tau e^{-i\pi/5} & 0 & \tau^{3/2}e^{i2\pi/5} \\ -\sqrt{\tau}e^{i2\pi/5} & 0 & 0 & -\tau & 0 \\ 0 & \tau^{3/2}e^{i2\pi/5} & \tau^{3/2}e^{i2\pi/5} & 0 & \nu \end{bmatrix}$$



$$\nu = -\tau(1+\tau^3)e^{-i2\pi/5} + \tau^3 e^{-i4\pi/5}.$$

Improvement in the Brute-Force Performance



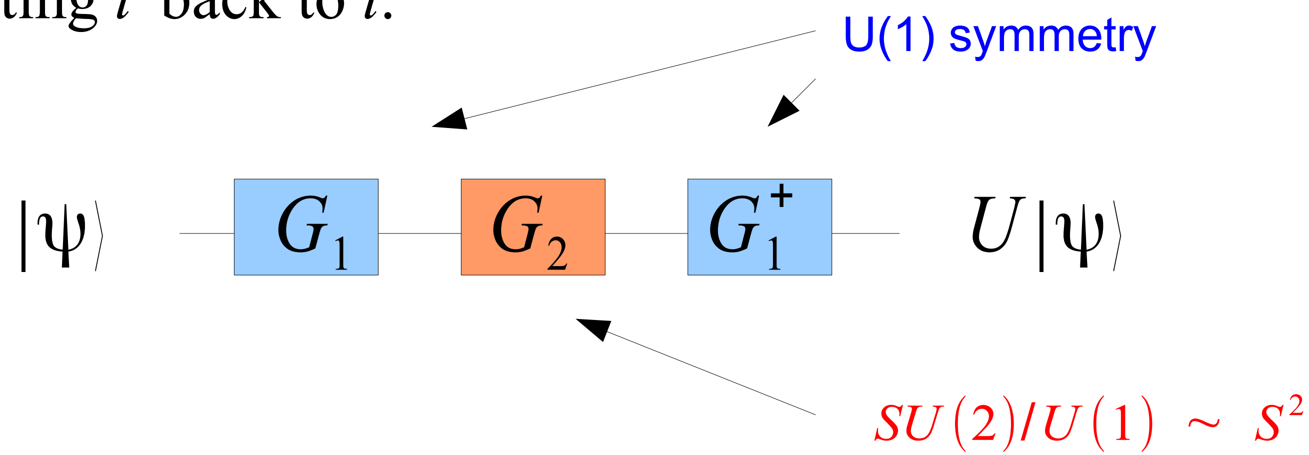
Search for one point on the bloch sphere

Search for any point on a circle on the Bloch sphere

Leakage error reduction by several orders of magnitude

Single-Qubit Construction Again

- Single-qubit construction hides an SU(2) symmetry. A rotation around an arbitrary axis l by an angle θ on a Bloch sphere can be carried out by first rotating l to another direction l', then rotating around l' by an angle θ, and finally rotating l' back to l.



- Implementation: Instead of search for a gate G, we search a pair of gates G_1 and G_2, such that $G \approx G_1 G_2 G_1^+$

$$G_{1,2} = e^{i\alpha_{1,2}} \begin{bmatrix} \sqrt{1-b_{1,2}^2}\, e^{-i\beta_{1,2}} & b_{1,2} e^{i\gamma_{1,2}} \\ -b_{1,2} e^{-i\gamma_{1,2}} & \sqrt{1-b_{1,2}^2}\, e^{i\beta_{1,2}} \end{bmatrix}$$

Geometric Redundancy for Single-qubit Gates

- We first rotate the axis of rotation, then rotate around the axis, and finally rotate the axis back – physically, this means that we have a geometric redundancy in search, due to the SU(2) rotation symmetry.
  - We can search G_1 and G_2 separately
  - Both searches are achievable in lower (than 3) dimensions
  - i.e., we can fix

  G_1 up to a U(1) rotation, and
  G_2 up to SU(2) / U(1) ~ S^2

$$P = \begin{bmatrix} e^{-i\beta} & 0 \\ 0 & e^{i\beta} \end{bmatrix}$$

$$(1 - b_2^2)^{1/2} \cos \beta_2 = \cos \beta,$$

$$b_1 = \frac{b_2}{\sqrt{2 \sin^2 \beta + 2(1 - b_2^2)^{1/2} \sin \beta_2 \sin \beta}},$$

$$\beta_1 + \gamma_1 = \gamma_2 + (k + 1/2)\pi,$$

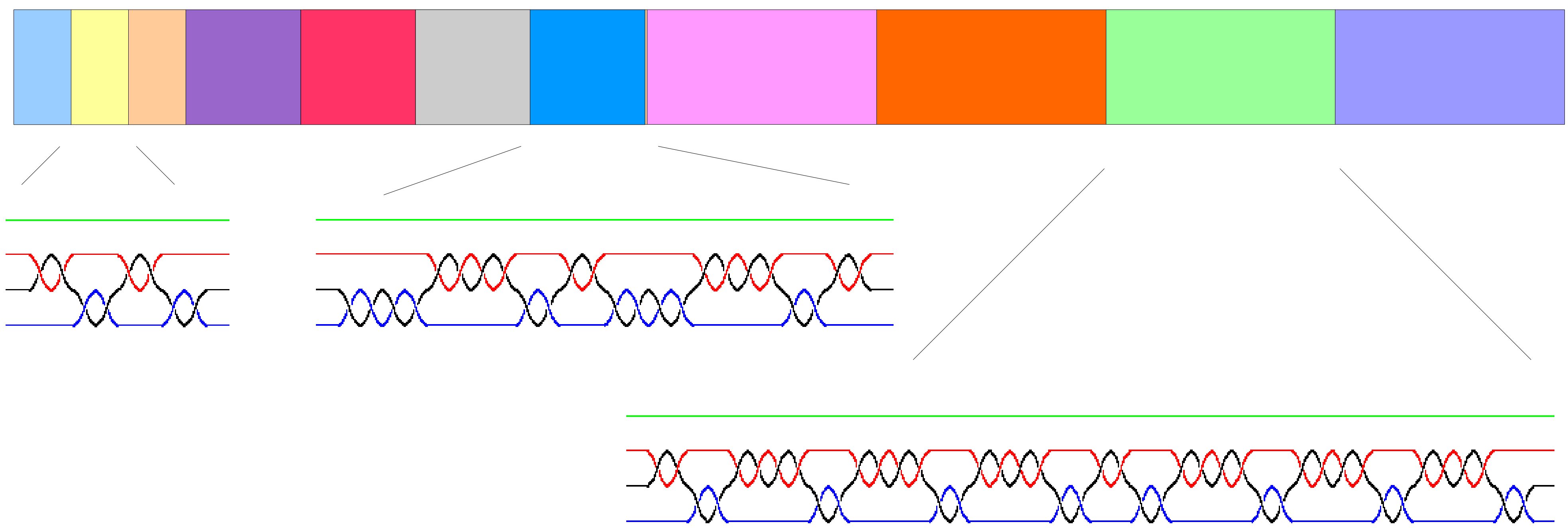
- Outcome: Generic single-qubit gates with error (distance) ~10^{-10} with braids of ~300 exchanges (length) – Xu & XW (2009).
  - Hormozi et al. (07): 4 ×10^{-5} for a braid of length 220 with Solovay-Kitaev algorithm

#5: Messages on Topological Quantum Gates

- Three or four Fibonacci anyons can encode one qubit of information.
- Quantum gates can be achieved by braiding anyons; in particular, moving one or one pair of anyons is enough to generate all quantum gates.
- Braids for quantum gates can be compiled into sequences of two elementary exchanges and their inverses.
- The construction of two-qubit gates can be mapped to that of single-qubit gates. But at least one high-precision phase gate is needed to eliminate leakage errors.
- In the brute-force search for braids geometrical redundancy can be explored to boost the efficiency.

Renormalization Group Like Scheme

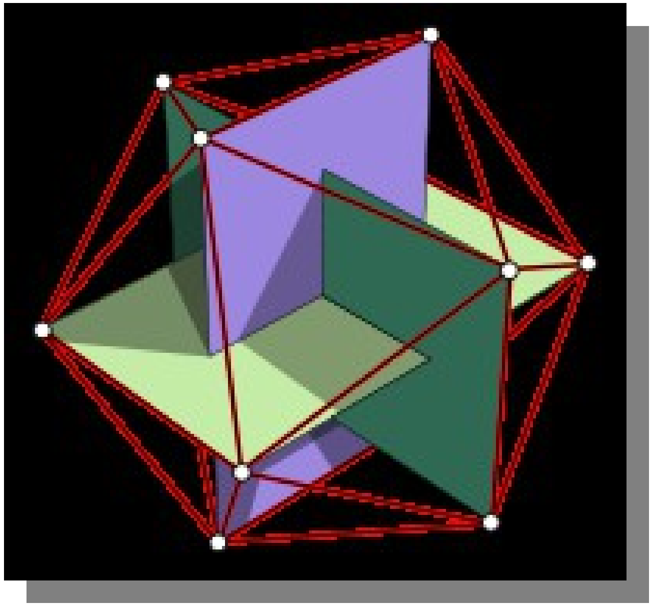
1. Start from a collection of braids of certain length
2. Find the cluster of braids that approximates the target best
3. Moving on to a collection of longer braids (finer in distance) matching the residual error
4. Repeat 2-3, and stop when the desired error scale is reached



Icosahedral Group

- The following Cartesian coordinates define the vertices of an icosahedron with edge-length 2, centered at the origin:

$$(0,\pm 1,\pm\phi),(\pm 1,\pm\phi,0),(\pm\phi,0,\pm 1)$$



$$\phi=\frac{1+\sqrt{5}}{2}$$

- The icosahedral group is the largest finite subgroup of SU(2). It is composed by the 60 rotations around the axes of symmetry of the icosahedron.

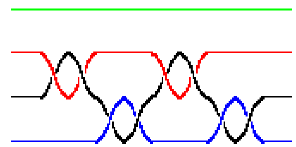
- There are 6 axes of the 5th order, 10 of the 3rd, and 15 of the 2nd.

$$I_{60}=\{g_{0,}g_{1,}g_{2,}\cdots,g_{59}\} \qquad g_0=e$$

- We approximate all group elements by braids of various length.

Braid Representations for the Identity e

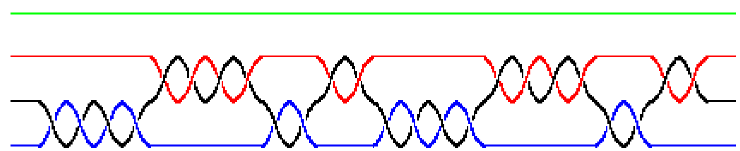
- L = 8, ε = 0.236068



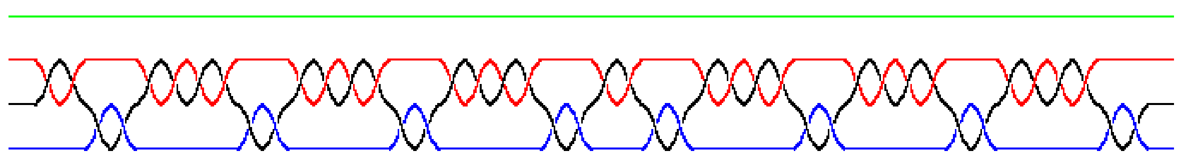
$$\tilde{g}_0(8)=\sigma_2^{-2}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{2}=g_0\, e^{i\Delta_0^{(8)}}$$

$\Delta_0^{(8)}$: a Hermitian matrix characterizing error

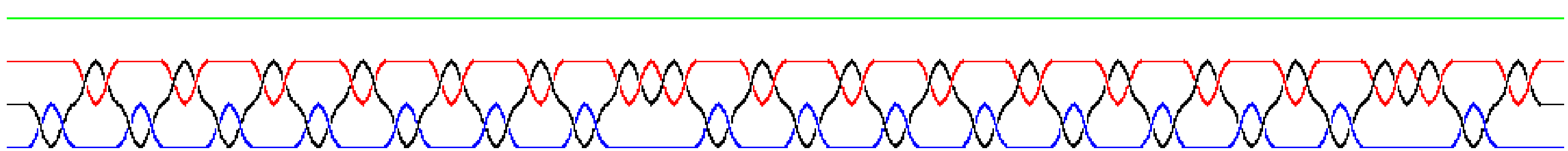
- L = 24, ε = 0.0344419



- L = 44, ε = 0.00191937



- L = 68, ε = 0.000304193



The braid representations can be computed and stored once for all. Hence no additional cost to the search later.

Connection to Random Matrix Theory

- Pseudogroup of braids (for small Δ_i)

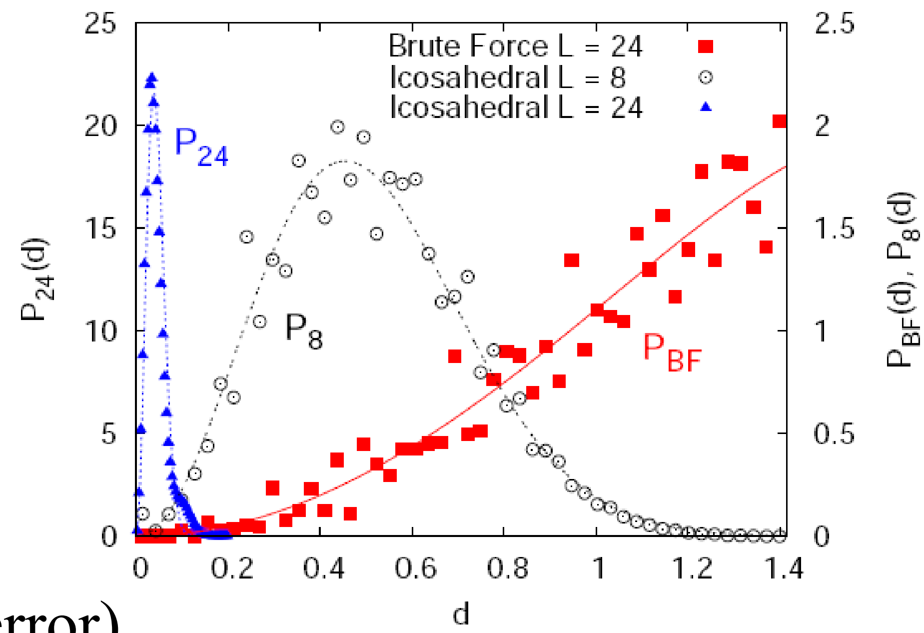
$$g_i g_j = g_k, \qquad \tilde{g}_i \tilde{g}_j = g_i e^{i\Delta_i} g_j e^{i\Delta_j} \approx g_k e^{i(g_j^{-1}\Delta_i g_j + \Delta_j)} \neq \tilde{g}_k = g_k e^{i\Delta_k}$$

- To approximate $g_i g_j \cdots g_{n+1} = e$

$$\tilde{g}_i \tilde{g}_j \cdots \tilde{g}_{n+1} = g_i e^{i\Delta_i} g_j e^{i\Delta_j} \cdots g_{n+1} e^{i\Delta_{n+1}} \equiv e^{iH_n}$$

$$\begin{aligned} H_n = {} & g_i \Delta_i g_i^{-1} + g_i g_j \Delta_j g_j^{-1} g_i^{-1} + \cdots \\ & + g_i g_j \cdots g_n \Delta_n g_n^{-1} \cdots g_j^{-1} g_i^{-1} \\ & + \Delta_{n+1} + O(\Delta^2) \end{aligned}$$

- We conjecture H_n is a random matrix in the Wigner-Dyson Gaussian Unitary Ensemble (s for eigenvalue/error)



$$P(s) = \frac{32}{\pi^2 s_0} \left(\frac{s}{s_0} \right)^2 e^{-(4/\pi)(s/s_0)^2}$$

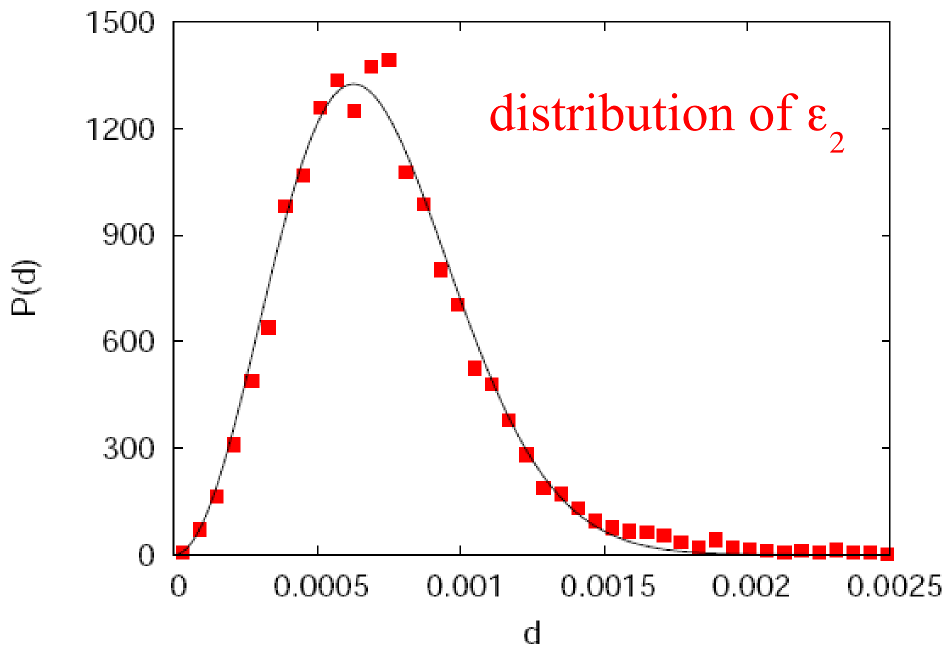
n = 3 is large enough

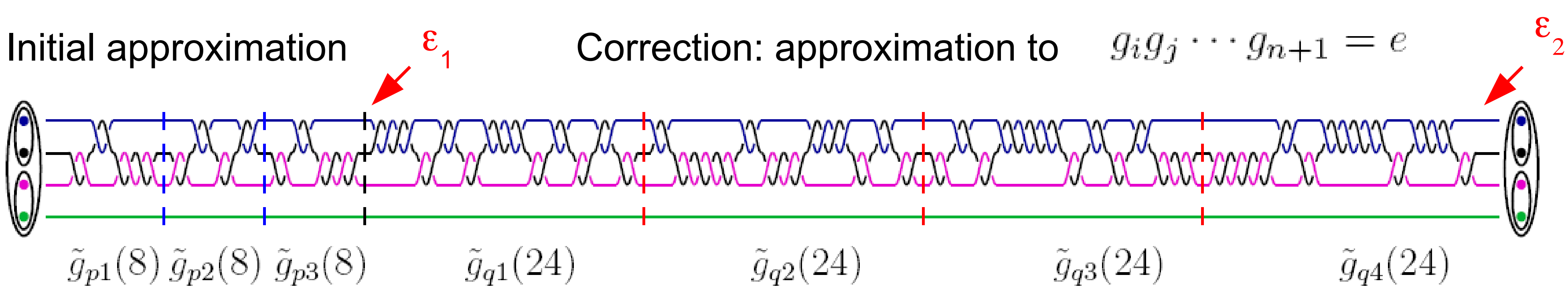
A single parameter s_0 controls the flow of the (distribution of) error.

Understanding Error Renormalization

- First approximate by gluing 3 short (L = 8) segments (1 out of 60^3).
- Reduce the error (ε_1) by gluing 4 (= n + 1) longer (L = 24) segments (1 out of 60^3).
- The resulting error (ε_2) follows the Wigner-Dyson distribution.
- Average error reduction:

$$<\varepsilon_1> / <\varepsilon_2> \sim \quad f = \frac{60^{n/3}}{\sqrt{n+1}}$$

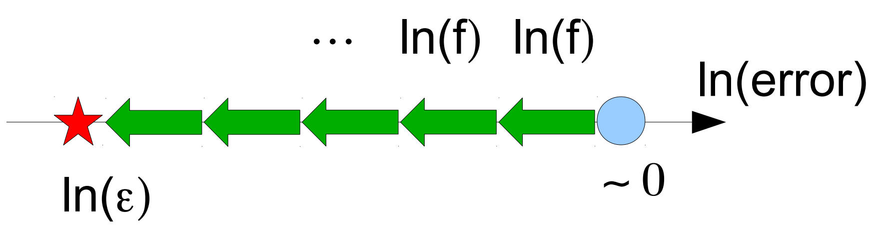




Scaling Analysis

- The number of iteration for a given final error $\epsilon \ll 1$

$$\sim \frac{\ln(1/\varepsilon)}{\ln f} \qquad \ln(1/\varepsilon_i) \sim i \ln f$$



- Choose suitable braid segment length to match the residual error

$$l_i \sim L_0 \ln\left(1/\varepsilon_{i-1}\right)$$

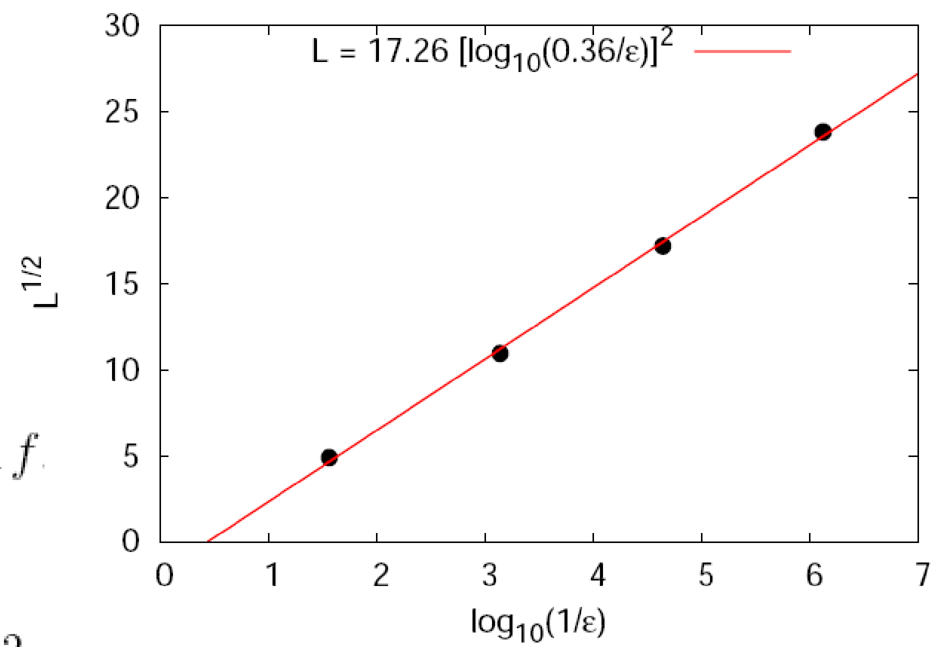
- Each iteration increases the length by 4 (= n + 1) segments

$$L_i - L_{i-1} = 4L_0 \ln\left(1/\varepsilon_{i-1}\right) \sim 4L_0(i-1)\ln f$$

- Length of braid after *q* iterations

$$L_q \sim \sum_{i=1}^{q} 4L_0(i-1)\ln f \sim q^2 \sim \left(\ln\left(1/\varepsilon\right)\right)^2$$

- Time $\sim \ln\left(1/\varepsilon\right)$



Comparison with Other Algorithms

- Compiling with the RG-like algorithm

$$L_{\mathrm{qh}} \sim (\ln(1/\varepsilon))^2$$
$$T_{\mathrm{qh}} \sim N \sim \ln(1/\varepsilon)$$

- Brute-force search

$$L_{\mathrm{bf}} \approx L_0 \ln(1/\varepsilon),$$
$$T_{\mathrm{bf}} \sim (1/\varepsilon)^3.$$

- Solovay-Kitaev

$$L \sim (\ln(1/\varepsilon))^c \quad \text{with} \quad c = \frac{\ln 5}{\ln(3/2)} \approx 3.97$$
$$T \sim (\ln(1/\varepsilon))^d \quad \text{with} \quad d = \frac{\ln 3}{\ln(3/2)} \approx 2.71$$

$$U_{i+1} = A_i B_i A_i^{-1} B_i^{-1} U_i$$

Hormozi *et al.*

$$L \sim (\ln(1/\varepsilon))^2 \ln(\ln(1/\varepsilon))$$
$$T \sim (\ln(1/\varepsilon))^2 \ln(\ln(1/\varepsilon))$$

Dawson and Nielsen

It takes less than a second on a 3 GHz Intel E6850 processor to reach an average precision of 7×10^{-4} for an arbitrary gate.

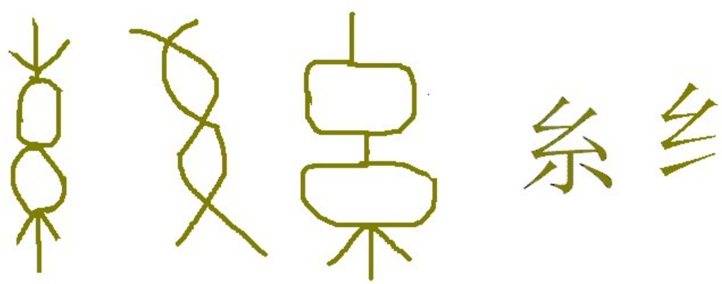
Thanks to randomness in the building blocks, we save time in search exponentially.

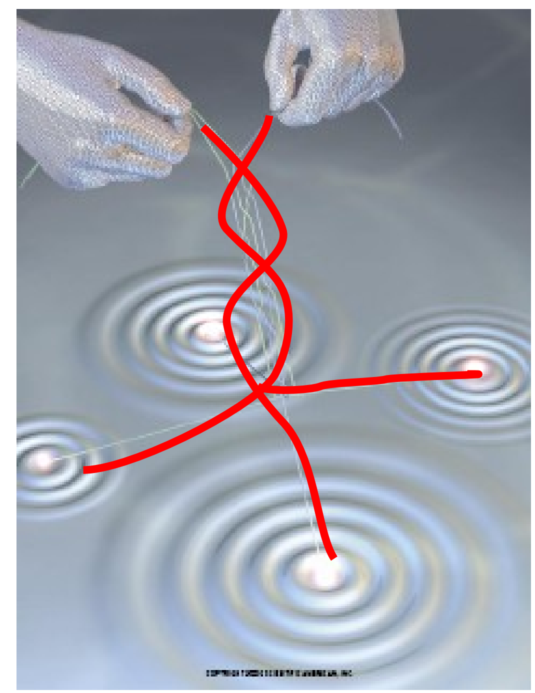
#6: Importance of Algorithm

- In a classical computer, one can build up a circuit, e.g., to add two numbers using OR and NOT gates.
- In a quantum computer, the set of possible quantum gates forms a continuum, and it's not necessarily possible to use one gate set to simulate another exactly. Instead, some approximation may be necessary.
- We explore an algorithm that guarantees the efficient construction of any quantum gate, to a very good approximation.
  - From a practical point of view, this is important in compiling quantum algorithms (like Shor's) into a form that can be implemented fault-tolerantly.
  - From a more mathematical point of view, we give a general statement about how quickly the group SU(d) is "filled in" by a universal set of gates.
- This is also the importance of the textbook example – the Solovay-Kitaev algorithm.

I Ching of Knots

- *I Ching* (~1100 BC): Ancient people tied knots on cords to keep record, while people during later periods replaced with writing
- 《易 · 系辞》载：“上古结绳而治，后世圣人易之以书契”

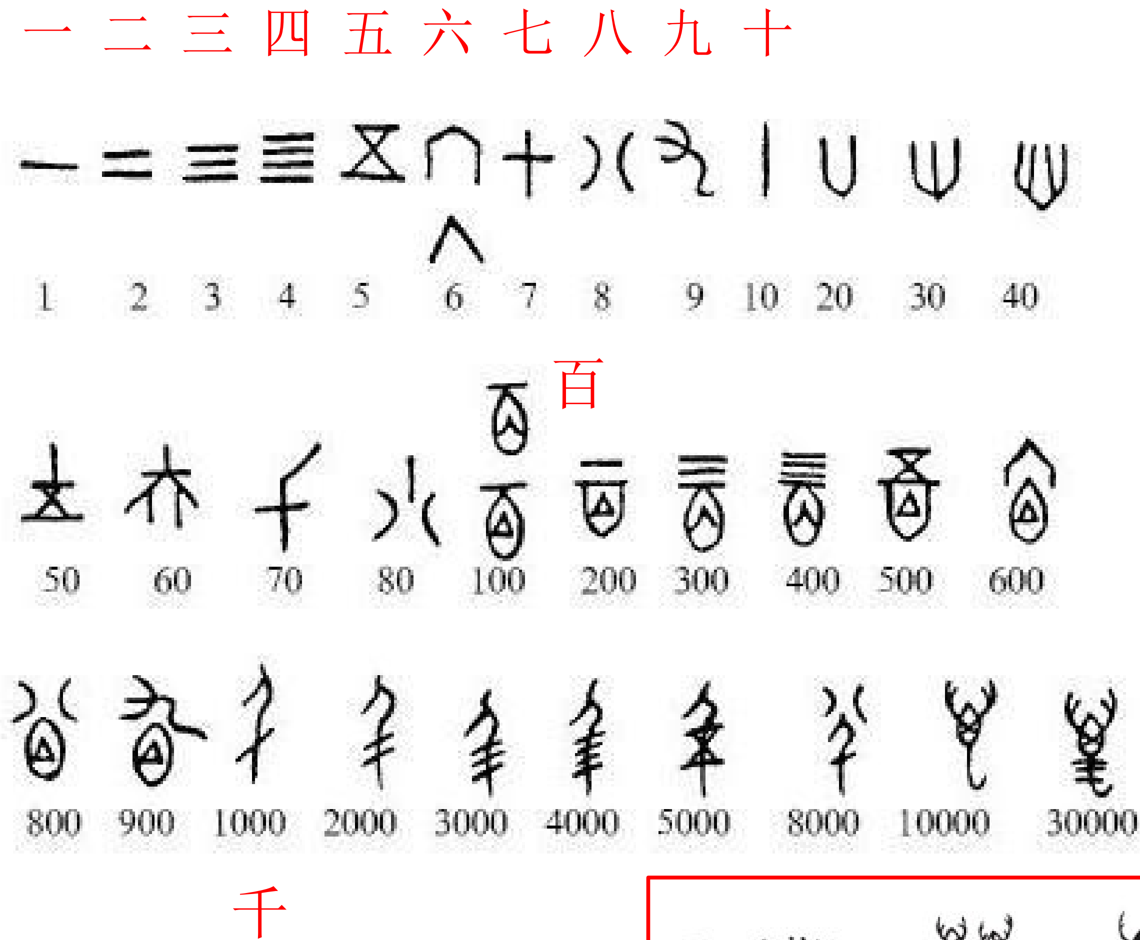




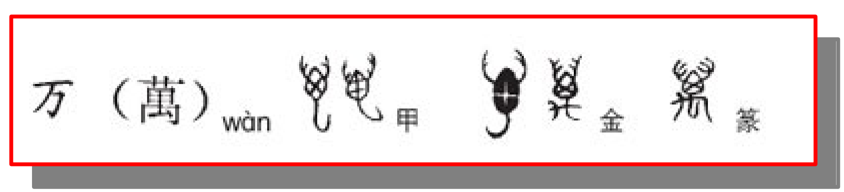
纠缠 ↔ entanglement

Stability in Chinese Characters

- Decimal system in China (over 3000 years ago)



Chinese characters encode information, in some sense, in the topology of the strokes.

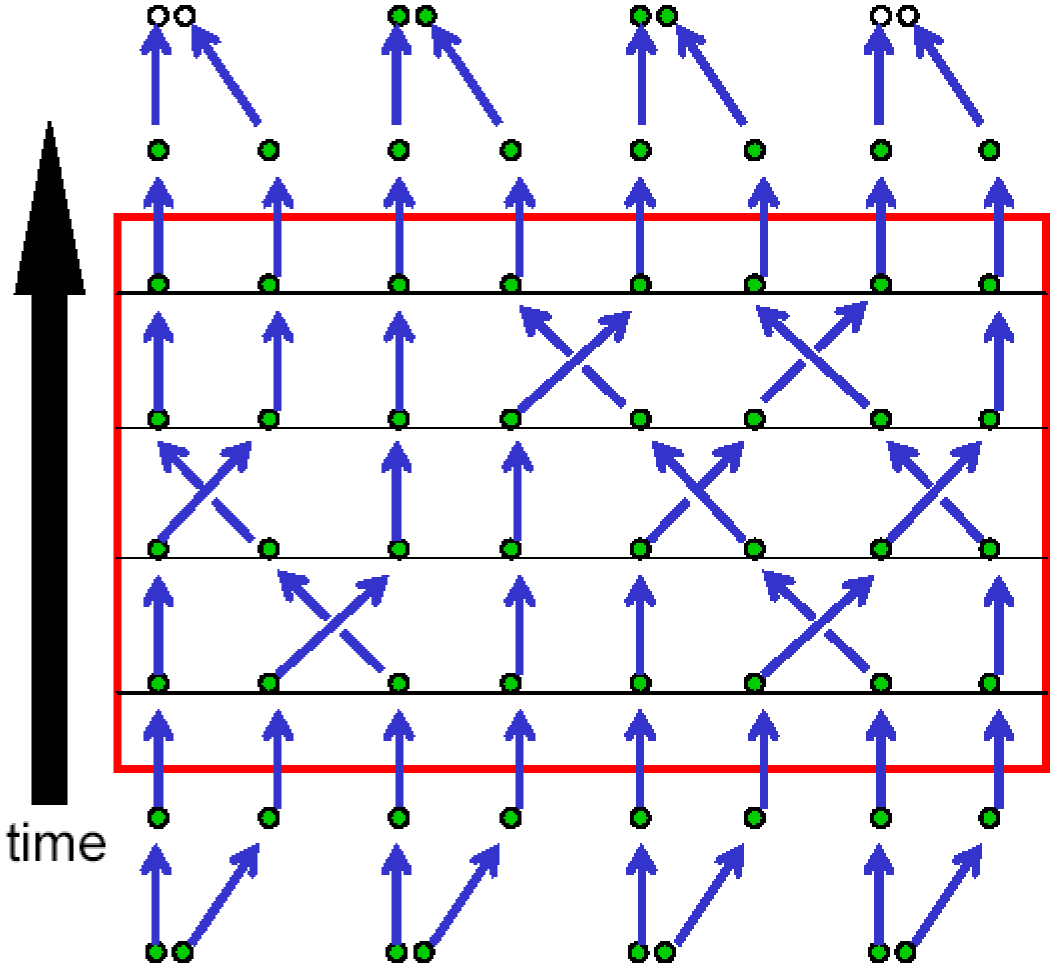


Topological Quantum Computation

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

Kitaev

Freedman



Next: compute with Fibonacci anyons