Topological Quantum Hashing with Icosahedral Group

Michele Burrello

Sestri Levante, June 2009

Work done with: Haitan Xu, Giuseppe Mussardo, Xin Wan

Contents

'... yet among the better educated Classes it is known that no Circle is really a Circle, but only a Polygon with a very large number of very small sides' E.

A. Abbot, *FlatLand*

Universal Quantum Computation

- **Quantum Computation** is based on the possibility of storing and processing information in Qubits.

Universal Quantum Computation

- **Quantum Computation** is based on the possibility of storing and processing information in Qubits.
- **Quantum Circuits** are unitary operators on a Hilbert space describing n Qubits.

Universal Quantum Computation

- **Quantum Computation** is based on the possibility of storing and processing information in Qubits.
- **Quantum Circuits** are unitary operators on a Hilbert space describing n Qubits.
- In order to develop all the possible circuits we must be able to implement every **unitary operator** in $SU(N)$ (with $N = 2^n$).

Definition

A **Universal Quantum Computer** is a machine able to realize, *at any accuracy*, all the unitary operators in the space $SU(N)$

Universal Quantum Computation

- **Quantum Computation** is based on the possibility of storing and processing information in Qubits.
- **Quantum Circuits** are unitary operators on a Hilbert space describing n Qubits.
- In order to develop all the possible circuits we must be able to implement every **unitary operator** in $SU(N)$ (with $N = 2^n$).

Definition

A **Universal Quantum Computer** is a machine able to realize, *at any accuracy*, all the unitary operators in the space $SU(N)$

- In particular we will focus on **Single - Qubit gates** in $SU(2)$

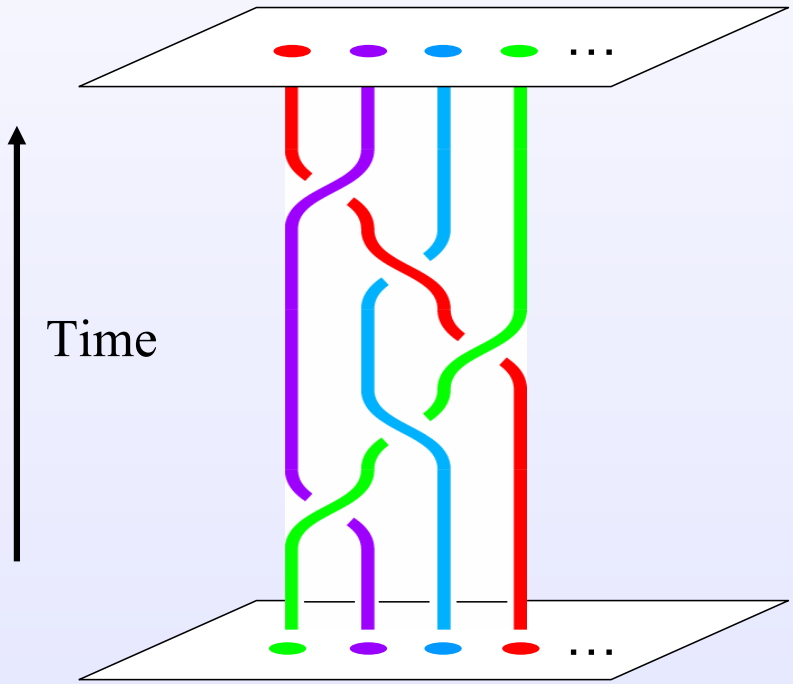
Topological Quantum Computation and Anyons

- Local errors, thermic noise and decoherence are the main problems in realizing a Quantum Computer

Topological Quantum Computation and Anyons

- Local errors, thermic noise and decoherence are the main problems in realizing a Quantum Computer

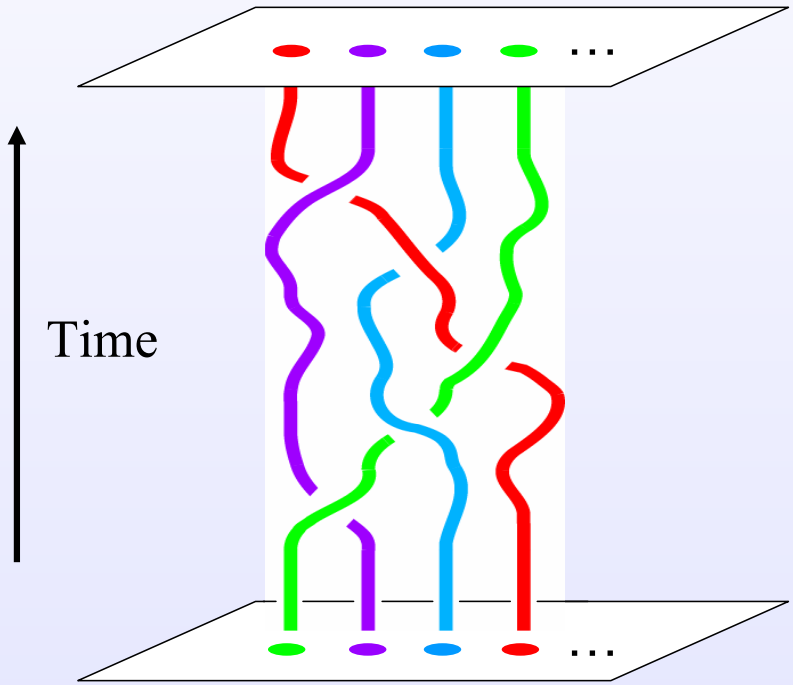
- **Topology**



Topological Quantum Computation and Anyons

- Local errors, thermic noise and decoherence are the main problems in realizing a Quantum Computer

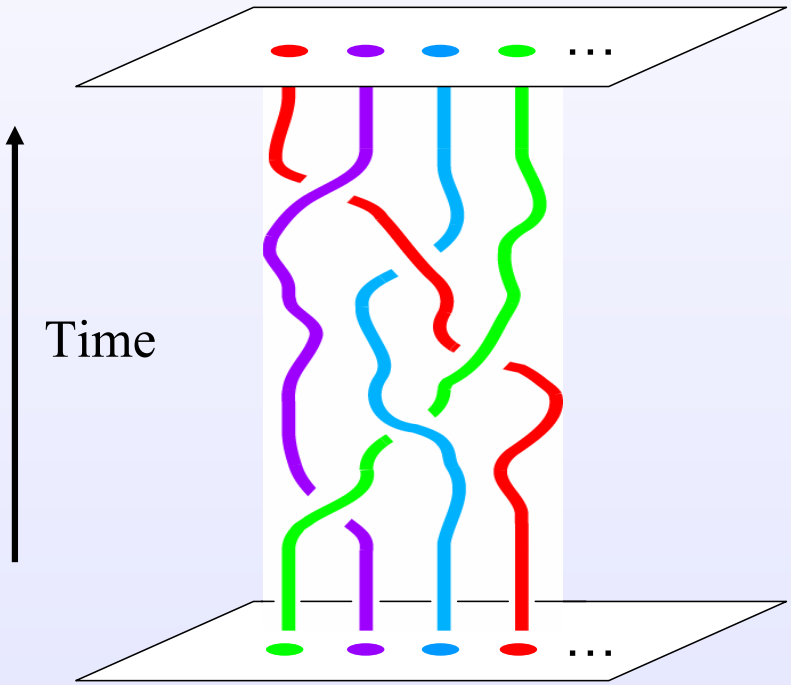
- **Topology**
- Topological properties are insensitive to local perturbations!



Topological Quantum Computation and Anyons

- Local errors, thermic noise and decoherence are the main problems in realizing a Quantum Computer

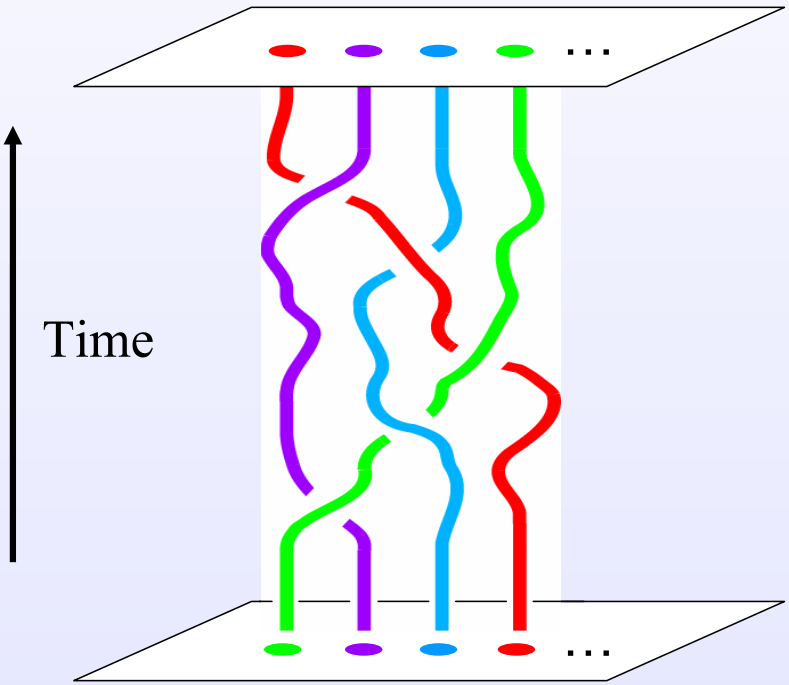
- **Topology**
- Topological properties are insensitive to local perturbations!
- **Anyons** in $2+1$ dimensions



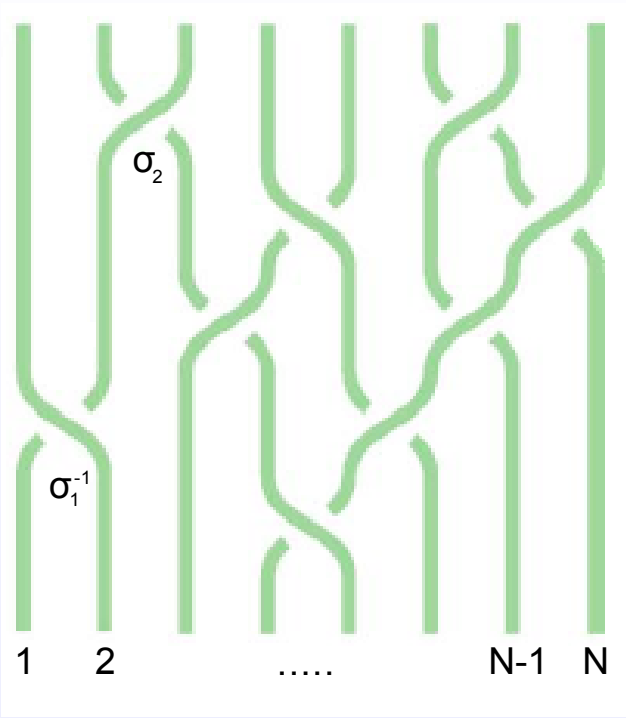
Topological Quantum Computation and Anyons

- Local errors, thermic noise and decoherence are the main problems in realizing a Quantum Computer

- **Topology**
- Topological properties are insensitive to local perturbations!
- **Anyons** in $2+1$ dimensions
- **Braid Group**

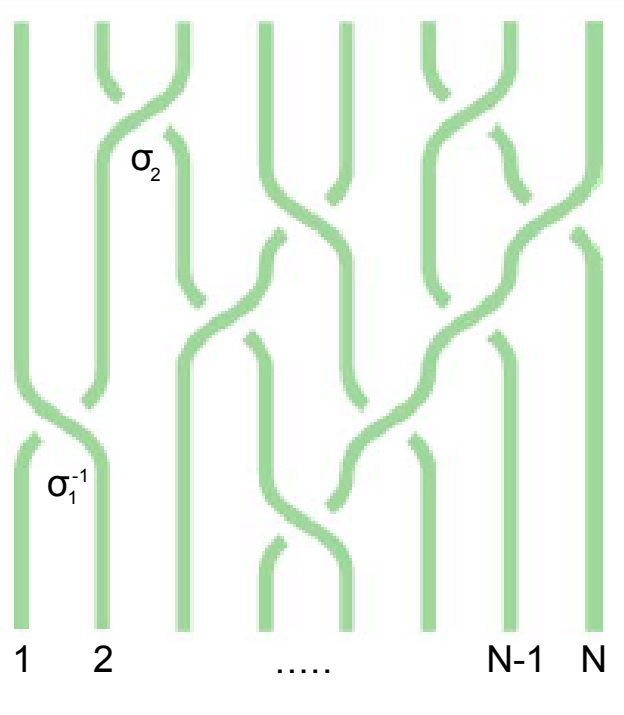


Braid Group



- The World Lines in $2+1$ D of N anyons describe N-strand Braids.
- These trajectories are robust with respect to local perturbations (Topology is preserved).

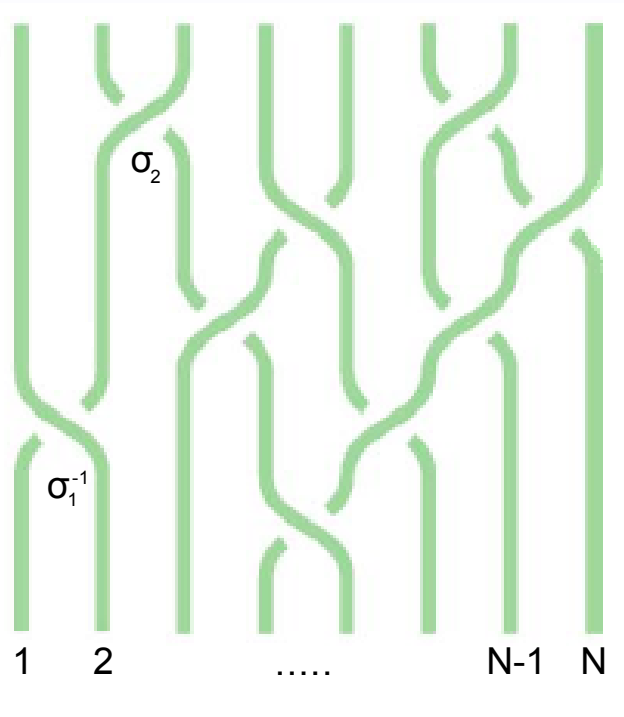
Braid Group



- The World Lines in $2+1$ D of N anyons describe N-strand Braids.
- These trajectories are robust with respect to local perturbations (Topology is preserved).
- Braids of N strands form an infinite group generated by:

$$\left\{\sigma_i, \sigma_i^{-1}\right\} \quad \text{with} \quad i = 1, \ldots, N$$

Braid Group



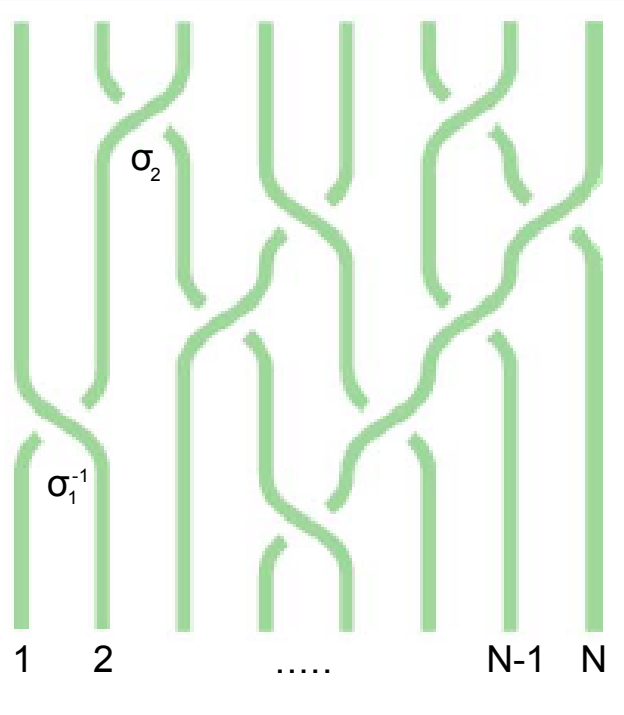
- The World Lines in $2+1$ D of N anyons describe N-strand Braids.
- These trajectories are robust with respect to local perturbations (Topology is preserved).
- Braids of N strands form an infinite group generated by:

$$\left\{\sigma_i, \sigma_i^{-1}\right\} \quad \text{with} \quad i = 1, \ldots, N$$

- For non-adjacent operators:

$$[\sigma_i, \sigma_k] = 0 \quad \text{if} \quad |i-k| \geq 2$$

Braid Group



- The World Lines in $2+1$ D of N anyons describe N-strand Braids.
- These trajectories are robust with respect to local perturbations (Topology is preserved).
- Braids of N strands form an infinite group generated by:

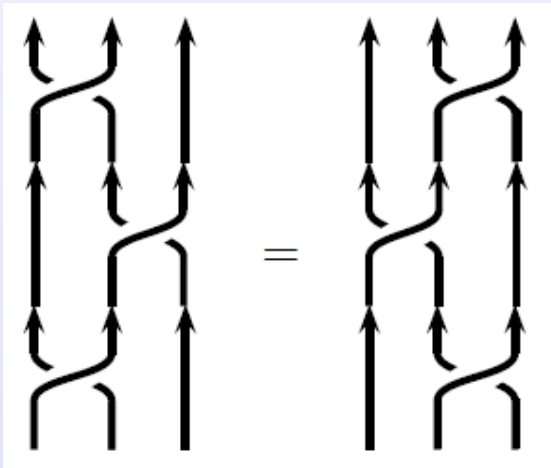
$$\left\{\sigma_i, \sigma_i^{-1}\right\} \quad \text{with} \quad i = 1, \ldots, N$$

- For non-adjacent operators:

$$[\sigma_i, \sigma_k] = 0 \quad \text{if} \quad |i-k| \geq 2$$

- Yang Baxter Relations:

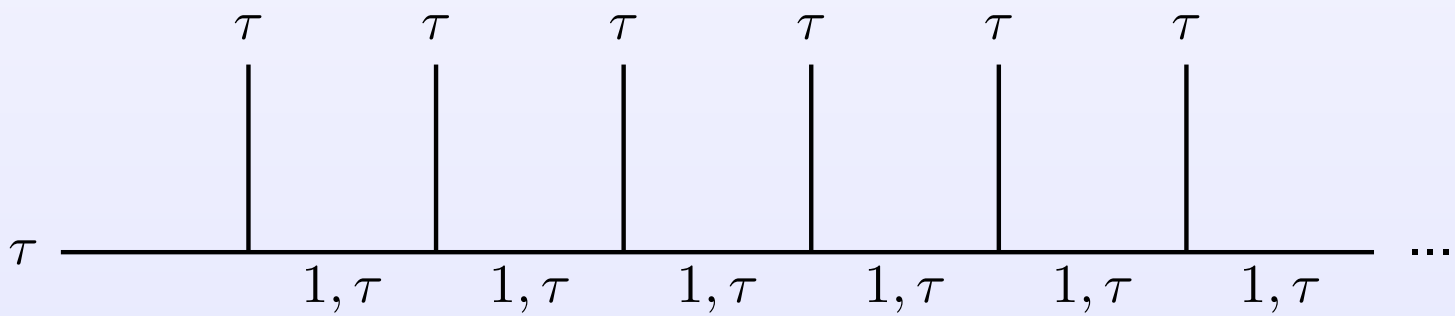
$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$$



- Fibonacci Anyons τ are the simplest Non - Abelian anyons.
- **Fusion Rules**:

$$\tau \times \tau = 1 + \tau \qquad\qquad 1 \times \tau = \tau$$

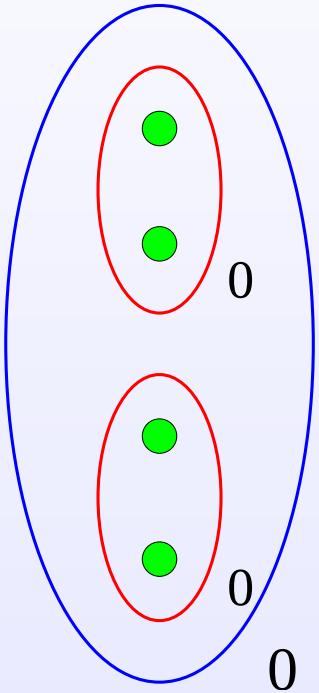
- **Fibonacci chain** of *n* Fibonacci anyons:



- Constraint: there cannot be two consecutive vacua 1.
- *n* anyons can be in F_n states (Fibonacci numbers).

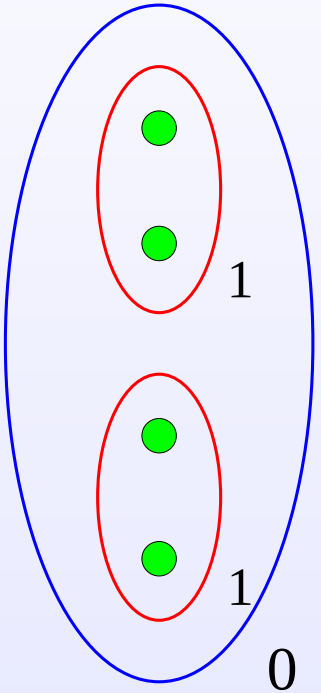
Fibonacci Anyons and Qubits

To encode a single qubit we use a system of 4 Fibonacci anyons with trivial total charge. There are two possible states:



$|0\rangle$

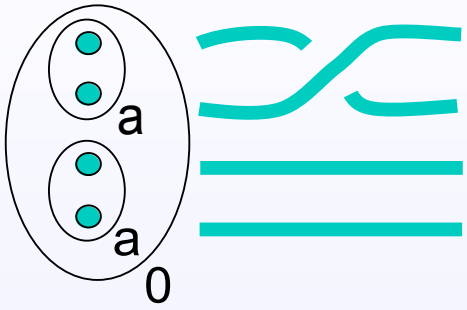
Each pair annihilates.



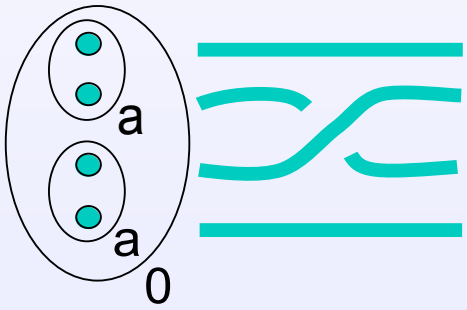
$|1\rangle$

Each pair gives a single τ

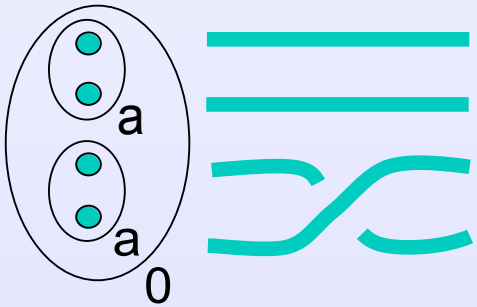
Fibonacci Braidings



$$\sigma_3 = \sigma_1 = R^{-1} = \begin{pmatrix} e^{-\frac{4}{5}\pi i} & 0 \\ 0 & -e^{-\frac{2}{5}\pi i} \end{pmatrix}$$



$$\sigma_2 = F\sigma_1 F = \begin{pmatrix} -\varphi\, e^{-i\frac{\pi}{5}} & -\sqrt{\varphi}\, e^{i\frac{2\pi}{5}} \\ -\sqrt{\varphi}\, e^{i\frac{2\pi}{5}} & -\varphi \end{pmatrix}$$

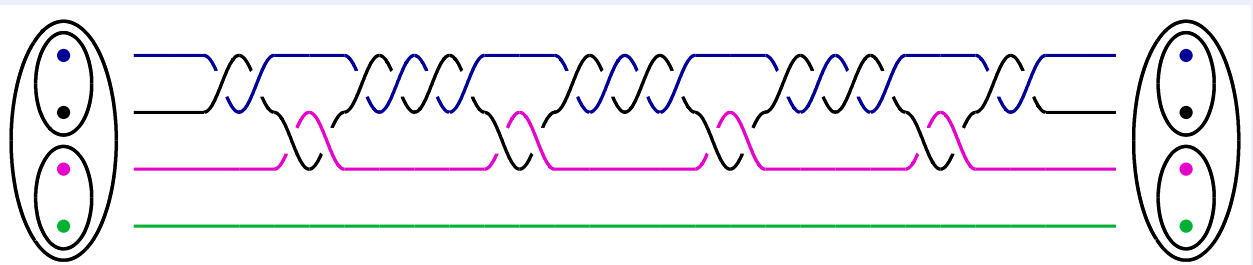


$$\sigma_1 = \sigma_3 = R^{-1} = \begin{pmatrix} e^{-\frac{4}{5}\pi i} & 0 \\ 0 & -e^{-\frac{2}{5}\pi i} \end{pmatrix}$$

Single-Qubit Gate Compiling

Bonesteel et al.

- To the purpose of Universal Quantum Computation we want to approximate, at any give accuracy, any single-qubit gate using as generators the braidings σ_1 and σ_2
- For Fibonacci anyons the elementary braidings generate an **infinite group**, dense in $SU(2)$

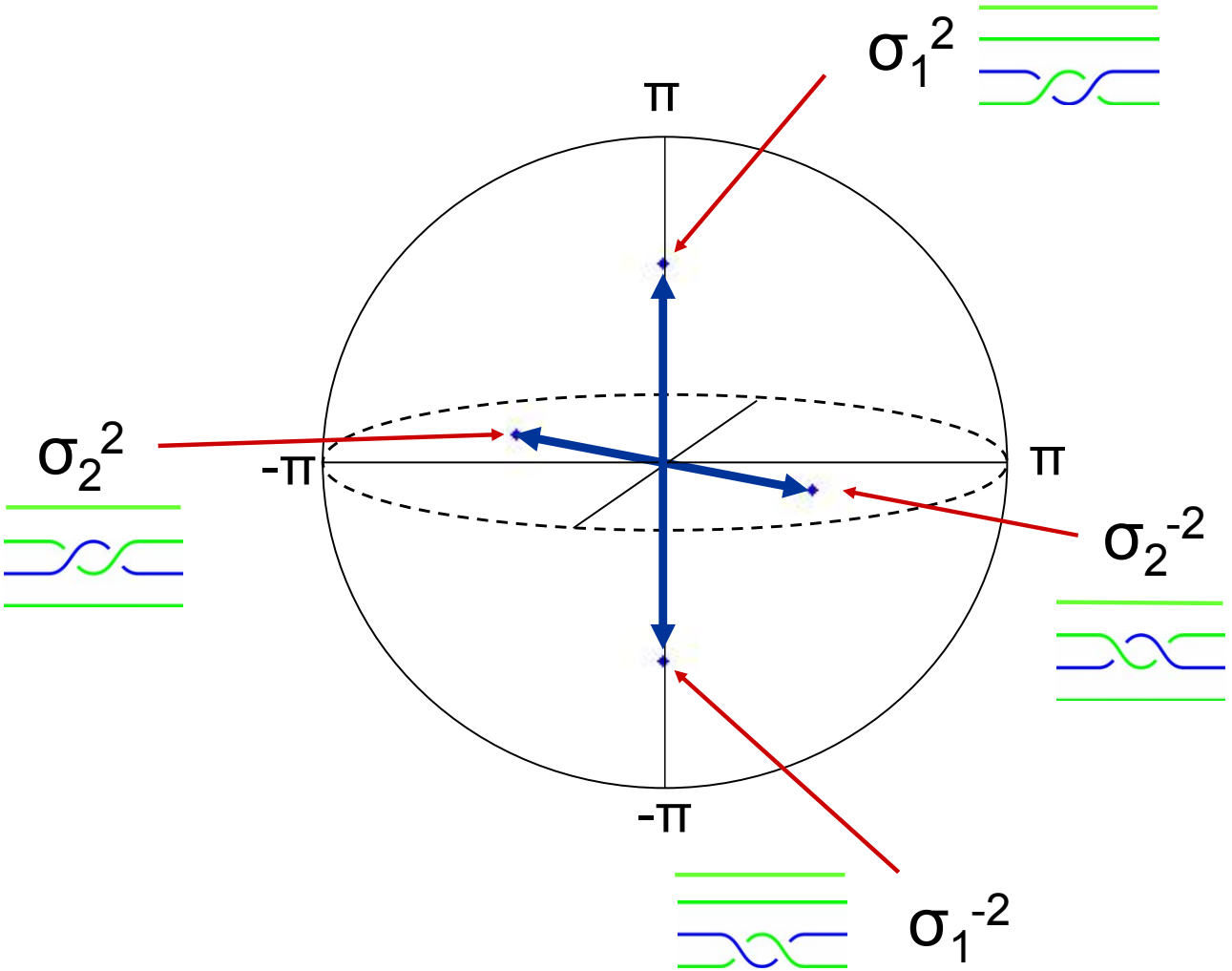


$$\sigma_3^{-2}\sigma_2^2\sigma_3^{-4}\sigma_2^2\sigma_3^{-4}\sigma_2^2\sigma_3^{-4}\sigma_2^2\sigma_3^{-2}$$

$$\cong -iX \pm 0,0031$$

Brute Force search

Bonesteel et al.



Total weaves:

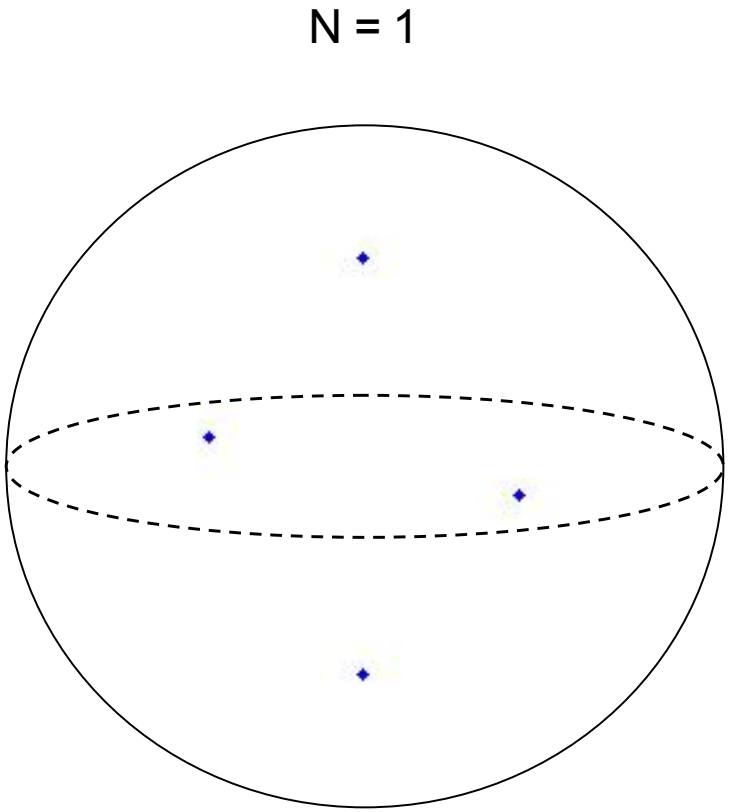
$$B_N \cong 3^N$$

Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.



Total weaves:

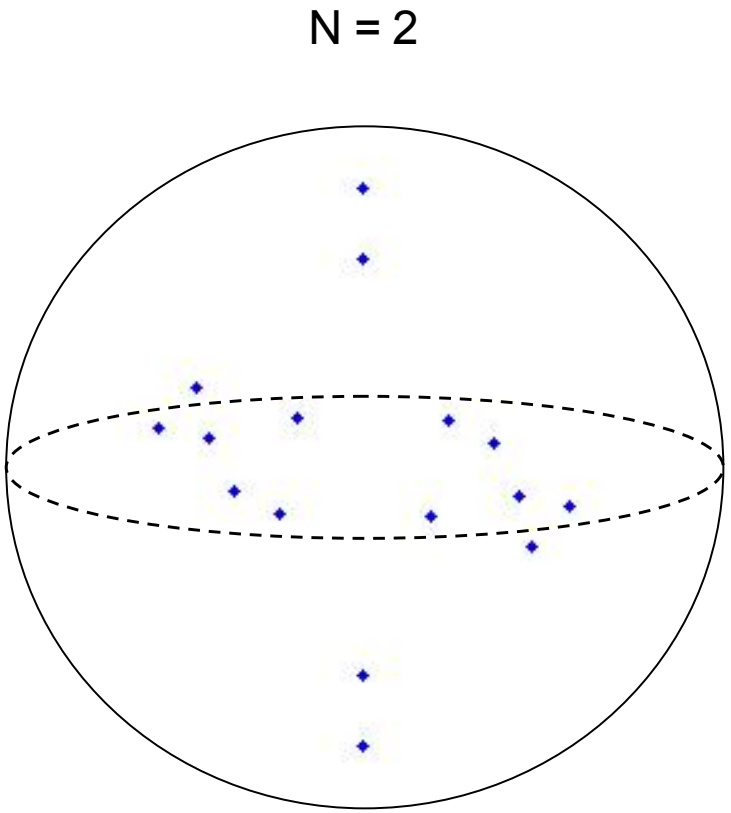
$$B_N \cong 3^N$$

Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.



Total weaves:

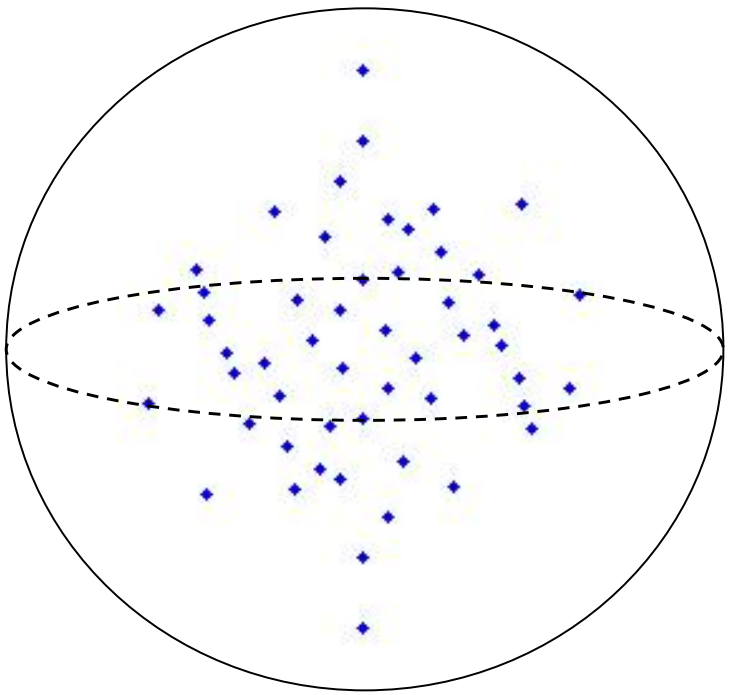
$$B_N \cong 3^N$$

Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.



Total weaves:

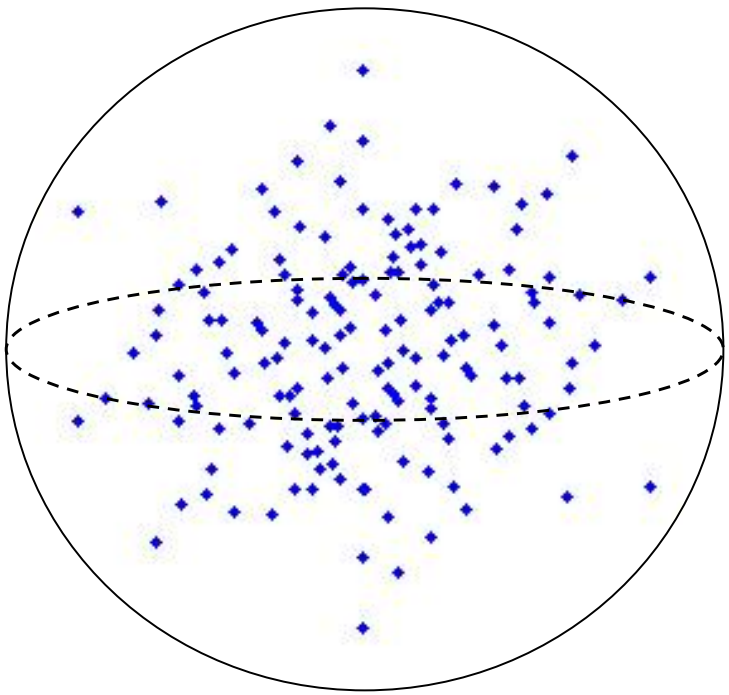
$$B_N \cong 3^N$$

Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.



Total weaves:

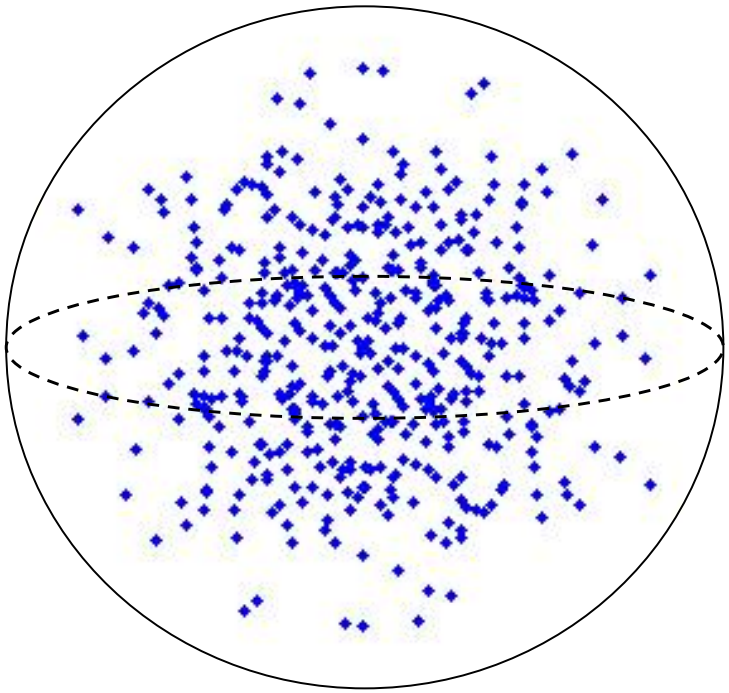
$$B_N \cong 3^N$$

Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.



Total weaves:

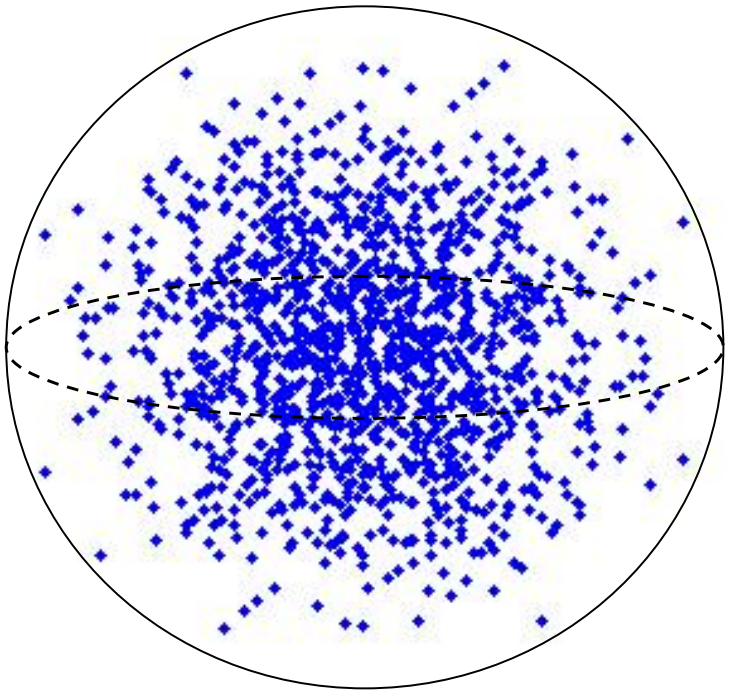
$$B_N \cong 3^N$$

Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.



Total weaves:

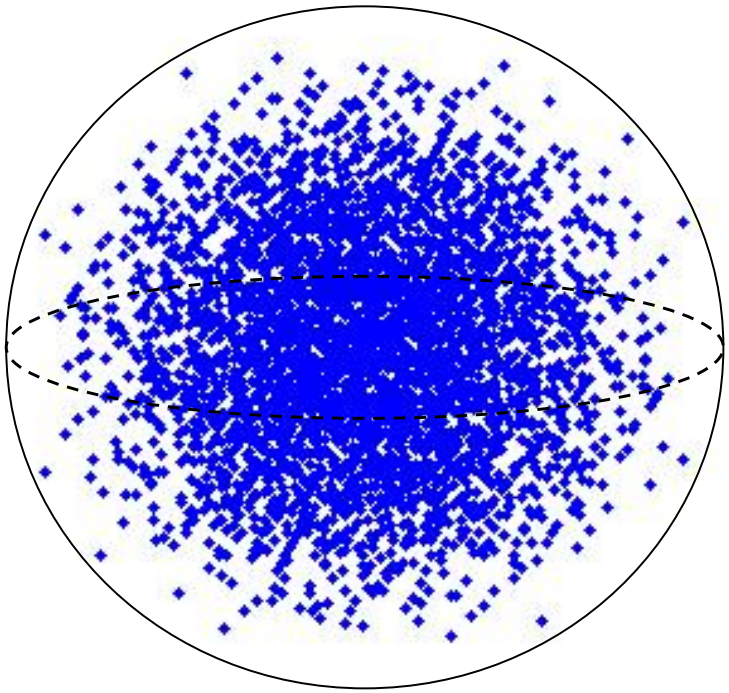
$$B_N \cong 3^N$$

Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.



Total weaves:

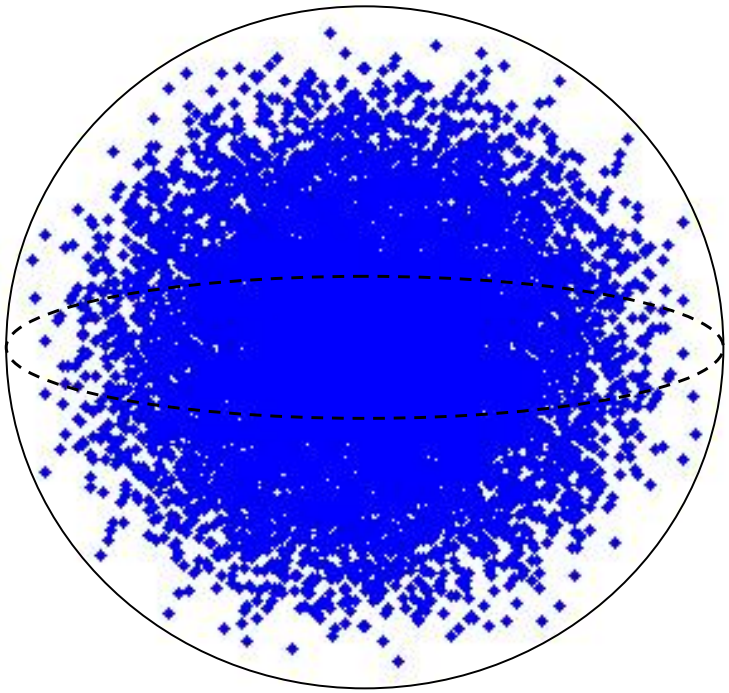
$$B_N \cong 3^N$$

Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.



Total weaves:

$$B_N \cong 3^N$$

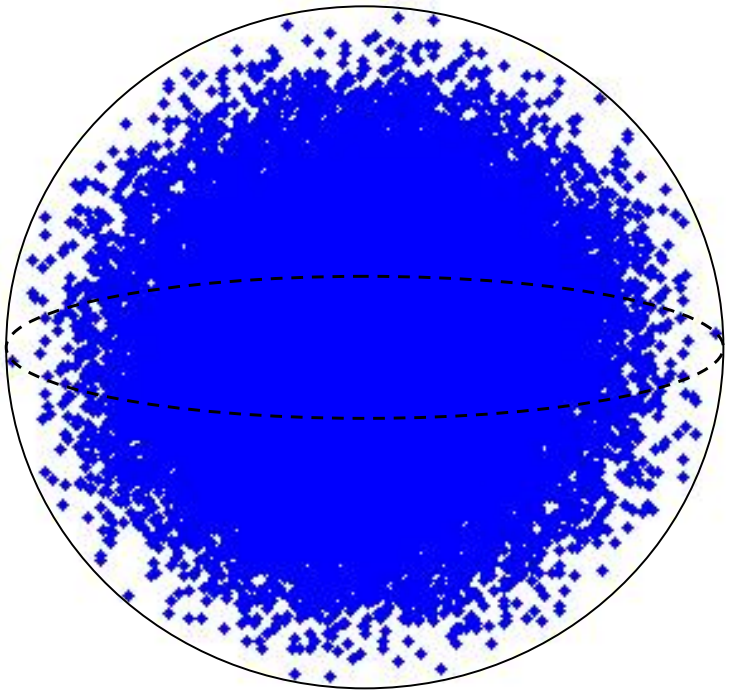
Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.

N = 9



Total weaves:

$$B_N \cong 3^N$$

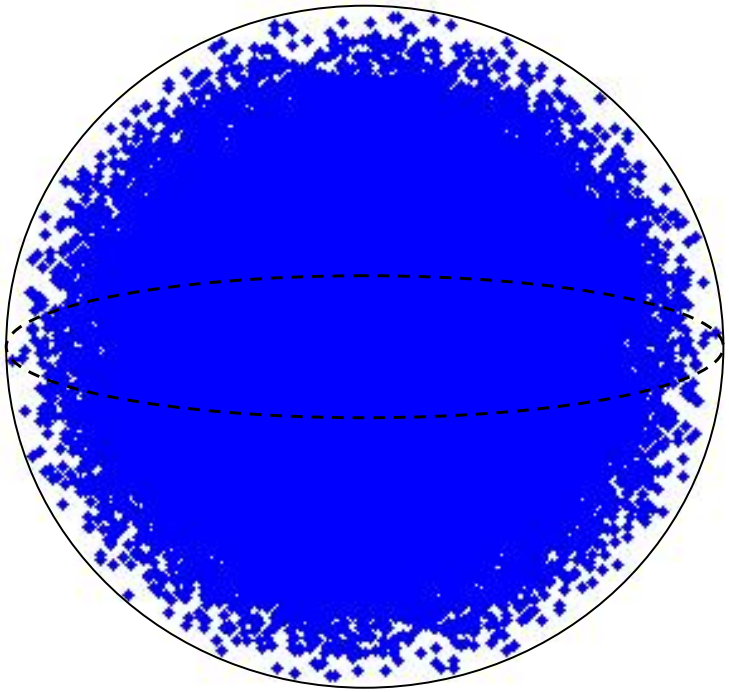
Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.

N = 10



Total weaves:

$$B_N \cong 3^N$$

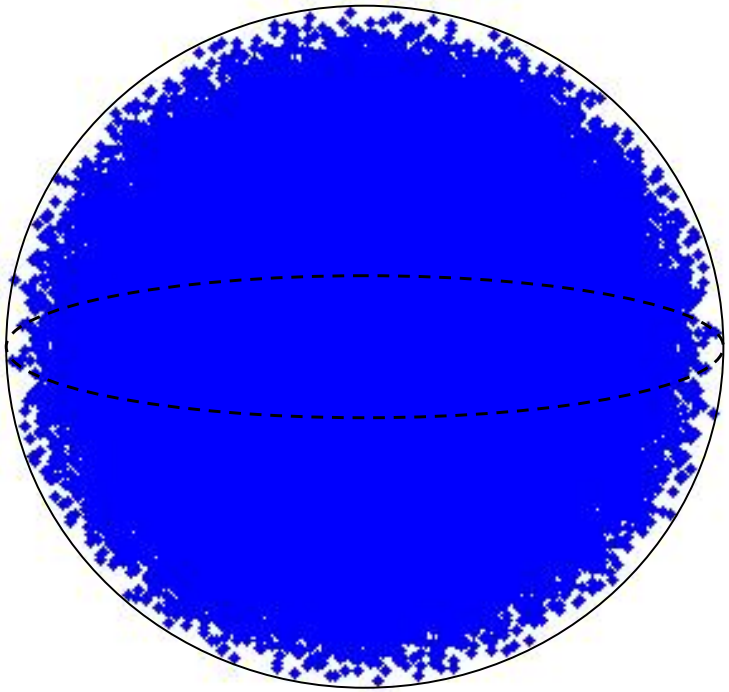
Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force search

Bonesteel et al.

N = 11



Total weaves:

$$B_N \cong 3^N$$

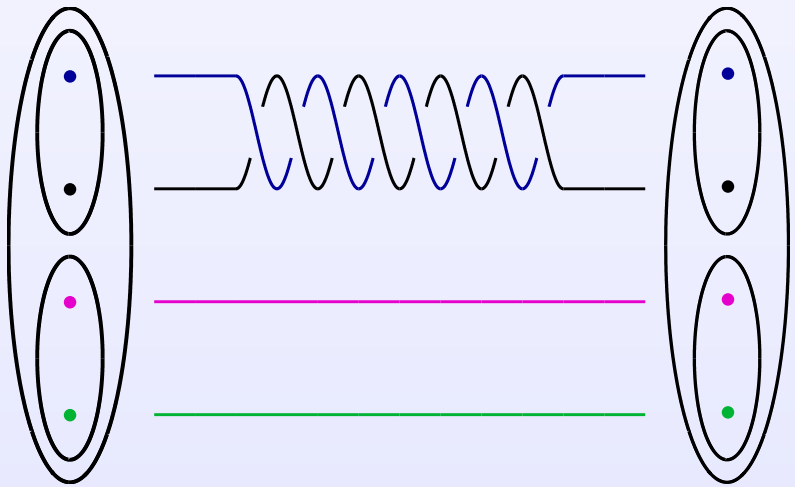
Expected error:

$$\varepsilon_N \cong \frac{1}{3^{N/3}}$$

Brute Force Search with weaves

We can approximate every single-qubit gate choosing the **best** braid among all the $3^{L/2}$ possibilities.
This is a **very slow** process!
Example:

Target Gate: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

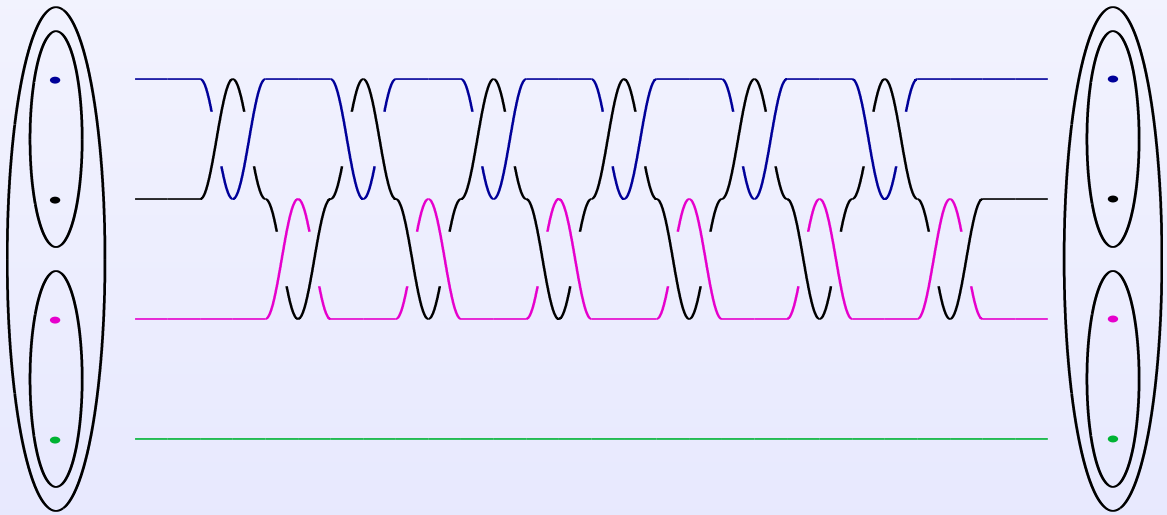


$$L = 8 \qquad \tilde{Z}_8 \cong \begin{pmatrix} 0,31 + 0,95i & 0 \\ 0 & 0,31 - 0,95i \end{pmatrix} \qquad \varepsilon_8 = 0,31$$

Brute Force Search with weaves

We can approximate every single-qubit gate choosing the **best** braid among all the $3^{L/2}$ possibilities.
This is a **very slow** process!
Example:

Target Gate: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

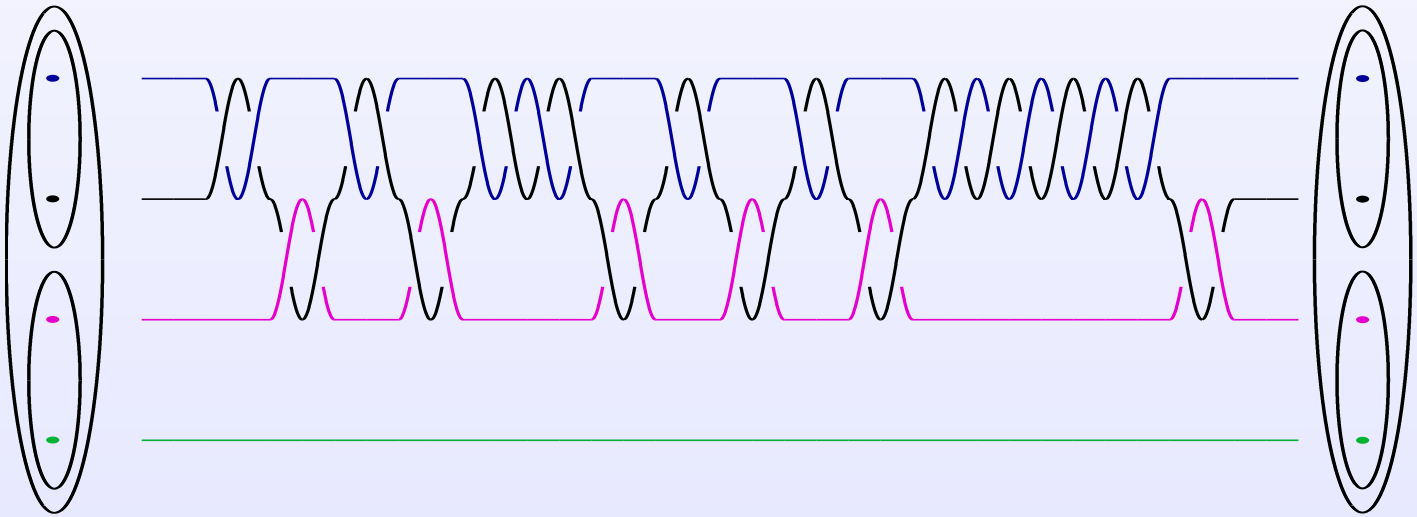


$L = 24$ $\quad \tilde{Z}_{24} \cong \begin{pmatrix} 0,0234 - 0,9997i & 0,006 + 0,002i \\ -0,006 + 0,002i & 0,0234 + 0,9997i \end{pmatrix}$ $\quad \varepsilon_{24} = 0,024$

Brute Force Search with weaves

We can approximate every single-qubit gate choosing the **best** braid among all the $3^{L/2}$ possibilities.
This is a **very slow** process!
Example:

Target Gate: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

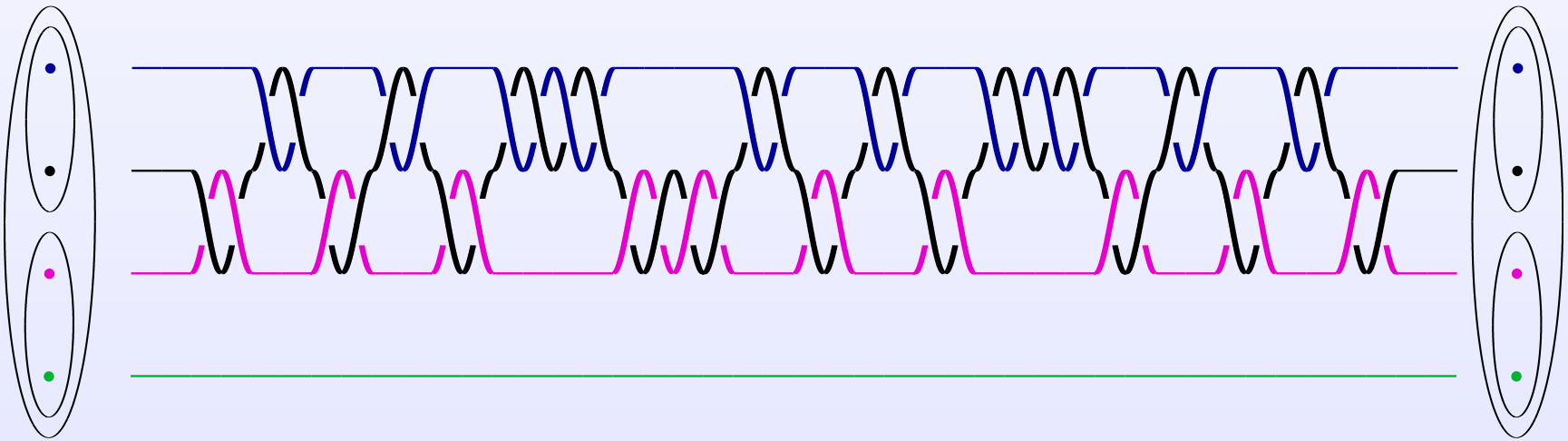


$L = 32$ $\qquad \tilde{Z}_{32} \cong \begin{pmatrix} 0.004 - 0.99997i & 0.004 - 0.003i \\ -0.004 - 0.003i & 0.004 + 0.99997i \end{pmatrix} \qquad \varepsilon_{32} = 0,007$

Brute Force Search with weaves

We can approximate every single-qubit gate choosing the **best** braid among all the $3^{L/2}$ possibilities.
This is a **very slow** process!
Example:

Target Gate: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$



$$L = 44 \qquad \tilde{Z}_{44} \cong \begin{pmatrix} -i & o\left(10^{-3}\right) \\ o\left(10^{-3}\right) & i \end{pmatrix} \qquad \varepsilon_{44} = 0,001$$

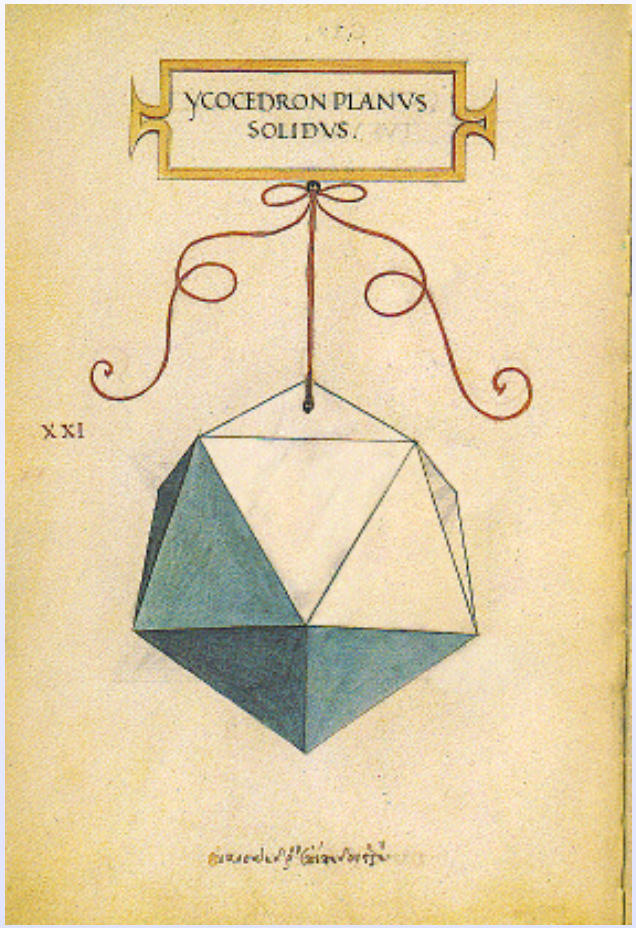
Icosahedral Quantum Hashing

M.B., Haitan Xu, Giuseppe Mussardo, Xin Wan (2009)

'... yet among the better educated Classes it is known that no Circle is really a Circle, but only a Polygon with a very large number of very small sides'

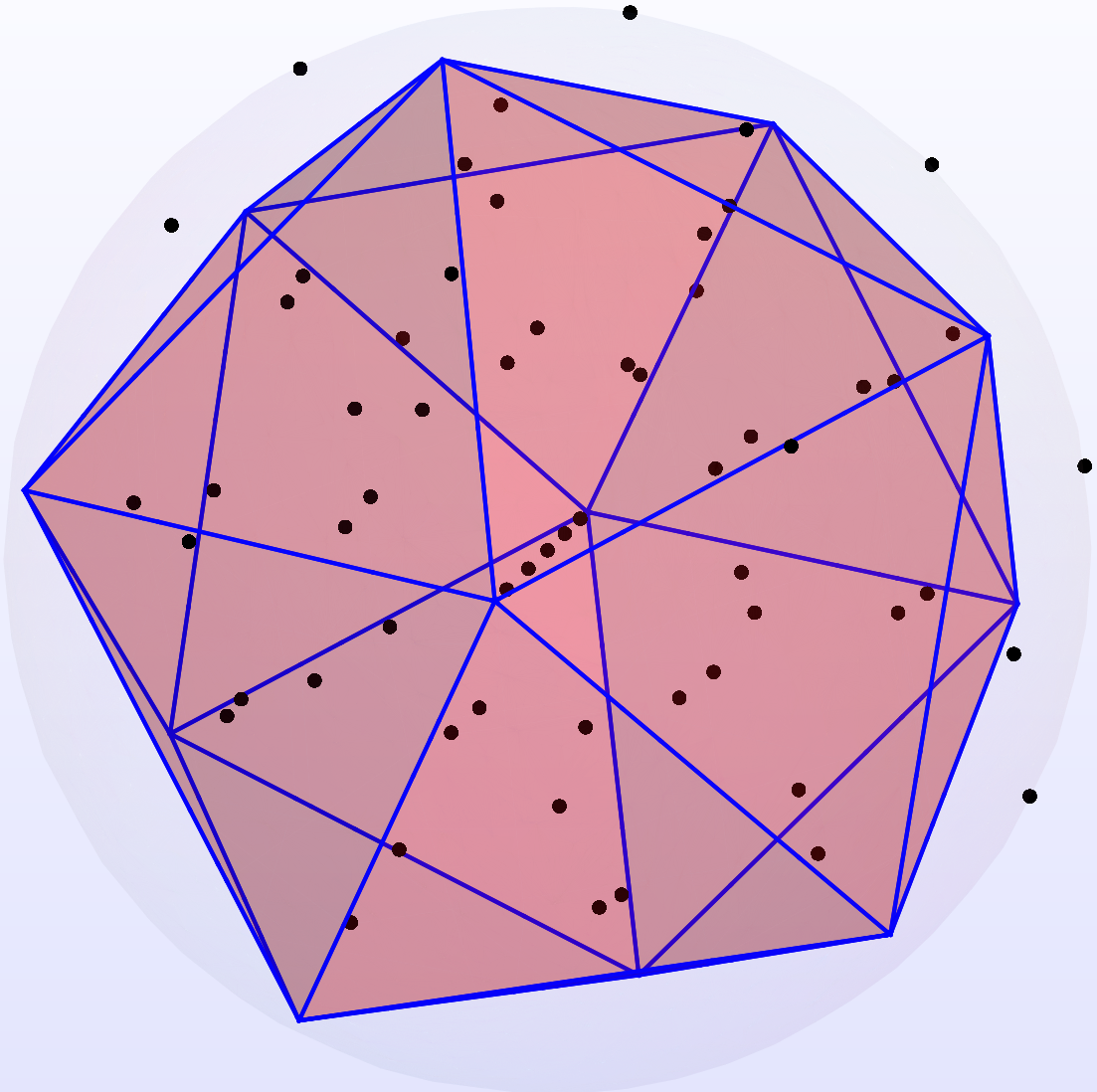
E. A. Abbot, *FlatLand*

- The Brute Force search is optimal but very slow.
- To get a faster algorithm we must **enhance the sampling** near the target gate.
- We study an algorithm which is not optimal as the BF but much faster.
- We will start using the **Icosahedral Group** to cover a sphere.



Icosahedral Group

$\mathcal{I} = \{g_1, ..., g_{60}\}$

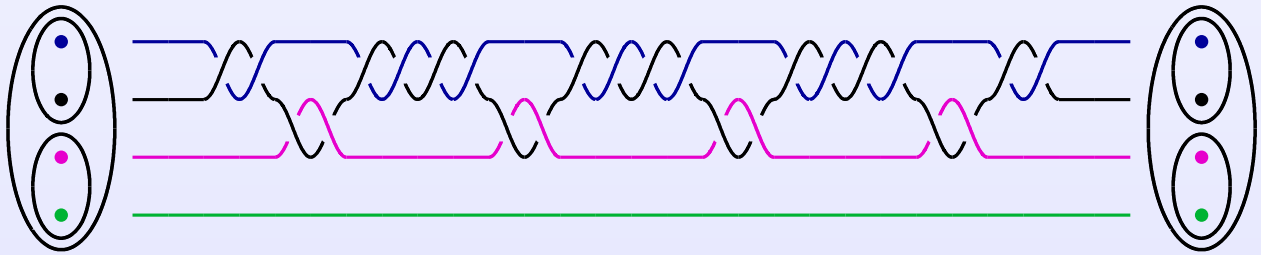


Icosahedral Pseudo Group

- $\mathcal{I}$ is a subgroup of $SO(3)$ and can be mapped in a subgroup of $SU(2)$
- Every rotation in this subgroup can be compiled with a Brute force algorithm in braids of length $L = 8, 24, 44$: we obtain the pseudogroup $\tilde{\mathcal{I}}(L)$:

$$X = e^{-i\sigma_x \pi/2} \in \mathcal{I} \longrightarrow BF_{L=24} \longrightarrow \tilde{X} \in \tilde{\mathcal{I}}(24)$$

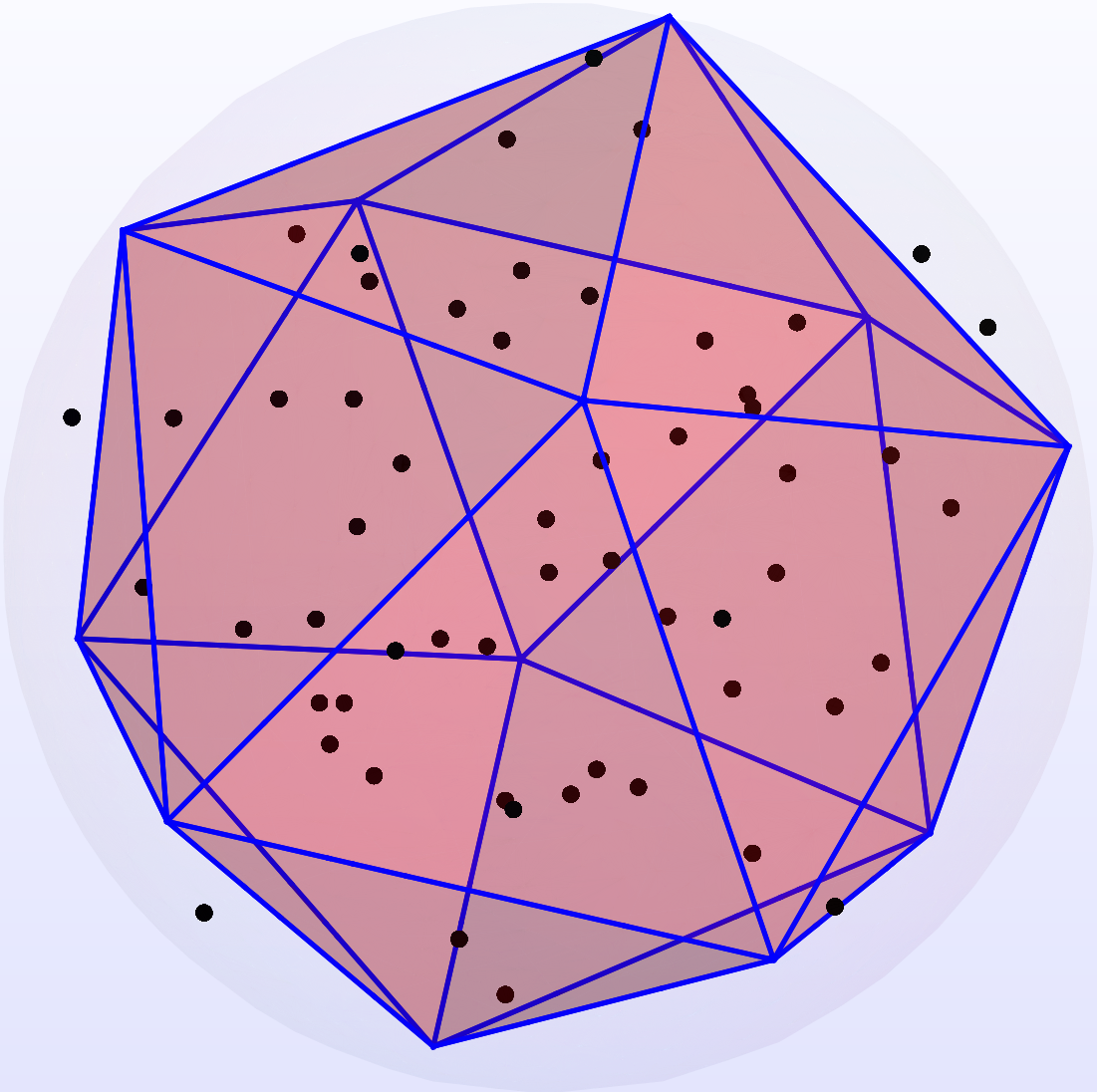
$\tilde{X} =$



- $\tilde{\mathcal{I}}(L)$ is a **Pseudogroup** characterized by errors: $\tilde{g}_i = g_i e^{i\Delta_i}$

Icosahedral Pseudo Group

$\tilde{\mathcal{I}} = \{\tilde{g}_1, ..., \tilde{g}_{60}\}$



Fine Rotations out of the Pseudogroup

The errors in the pseudogroup allow us to create in a simple way a set of **fine rotations around the identity to correct small errors**.

GROUP

$$g_i g_j = g_k$$

Identity is given by the right choice of rotations:

$$g_{i_1} g_{i_2} \dots g_{i_n} g_{i_{n+1}} = 1$$

PSEUDOGROUP

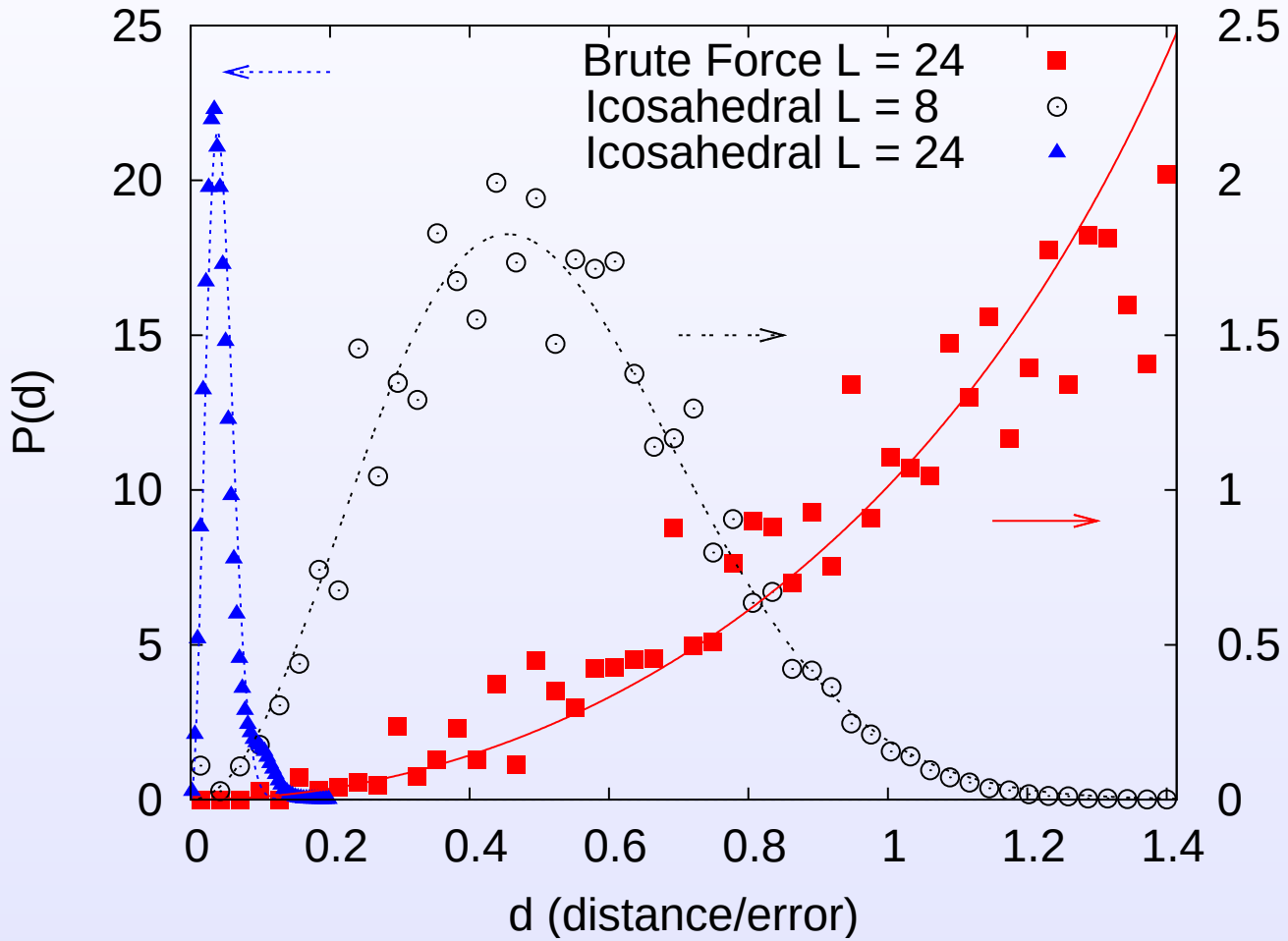
$$\tilde{g}_i \tilde{g}_j \neq \tilde{g}_k$$

We can span the **vicinity of the identity**:

$$\tilde{g}_{i_1} \tilde{g}_{i_2} \dots \tilde{g}_{i_n} \tilde{g}_{i_{n+1}} = e^{iH_n} \approx 1$$

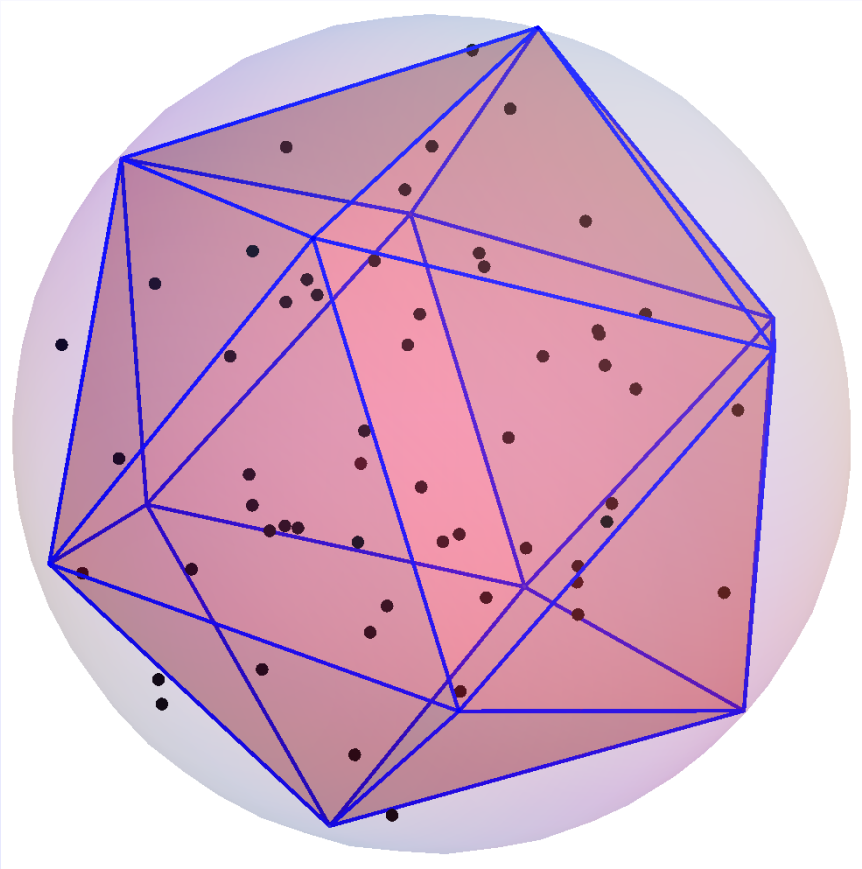
We have 60^n fine rotations!

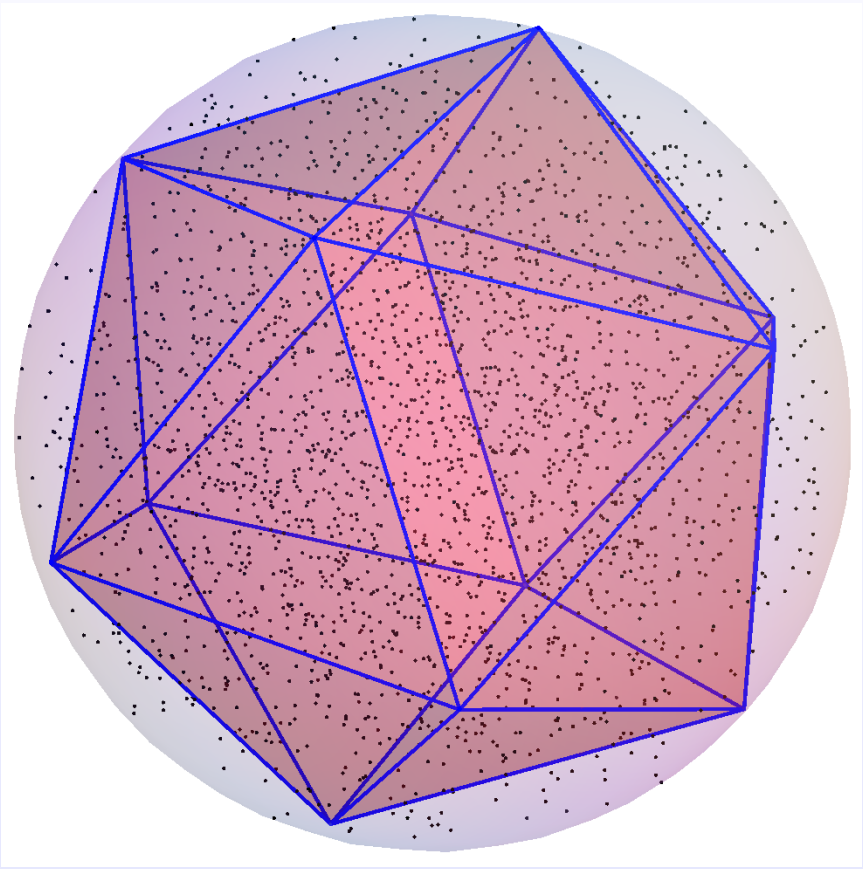
Distance distribution and random matrices



Preprocessor: $L = 8$

With the Pseudogroup with $L = 8$ we can span the whole $SU(2)$ sphere to obtain a first fast approximation:

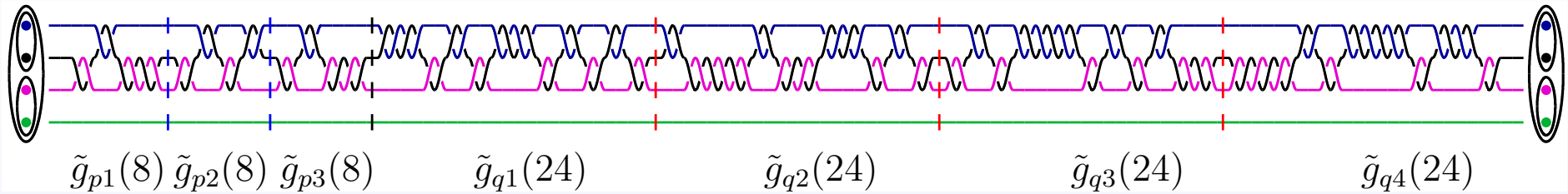


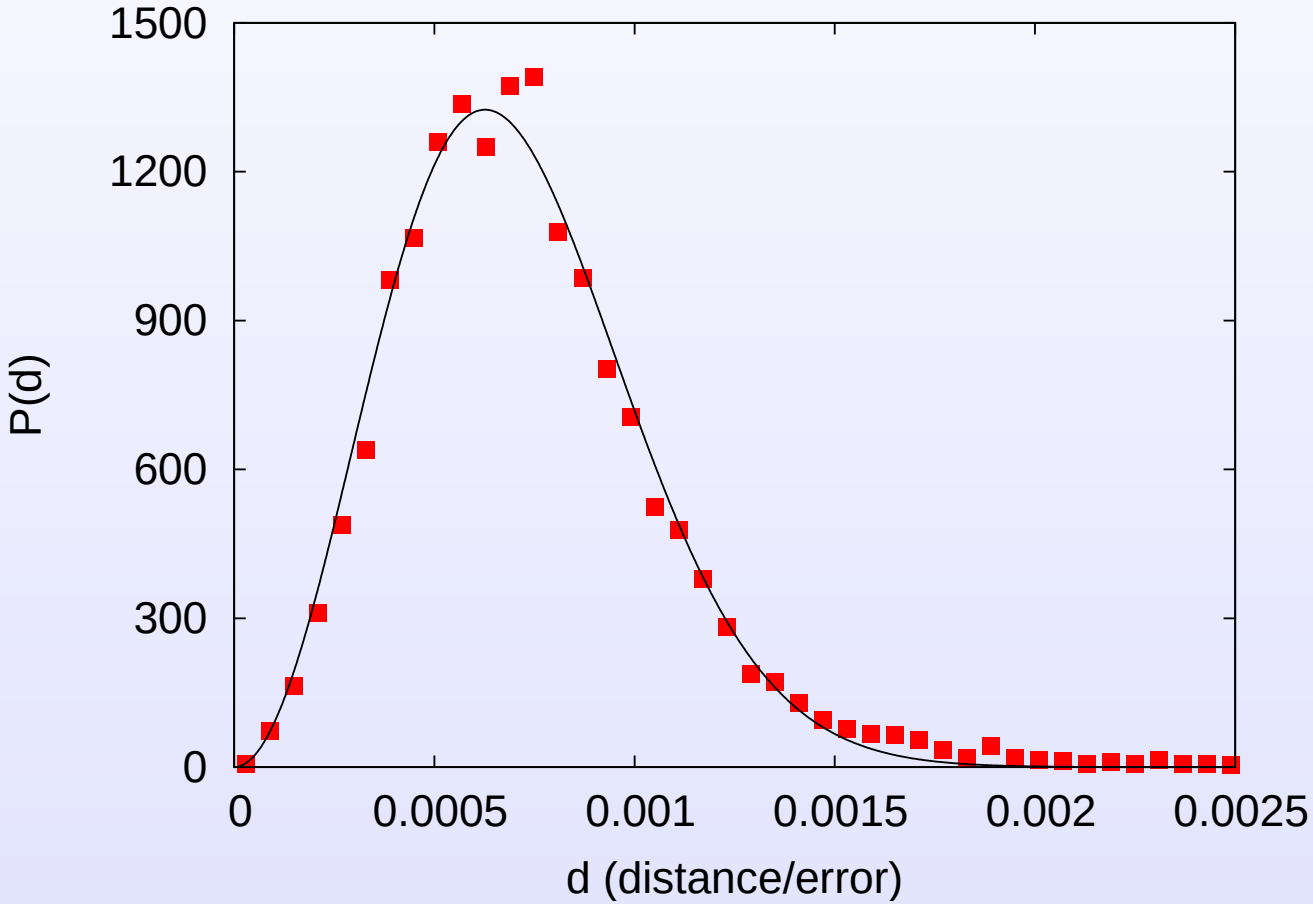


Then we can correct the error with 60^3 fine rotations.

Results

Maximal Length = 120





Average error:

$$7,1 \cdot 10^{-4}$$

Time required:

less than a second!

Results

- Topological quantum computation allows to avoid local error
- We need a technique to compile single qubit gates
- Brute force search gives the optimal solution but is very slow
- Icosahedral hashing gives a good solution in a very short time

BF SEARCH:	ICOSAHEDRAL:	ICOSAHEDRAL:
$L = 44$	$L = 120$	$L = 296$
$\varepsilon \approx 10^{-3}$	$\varepsilon \approx 7,1 \cdot 10^{-4}$	$\varepsilon \approx 2 \cdot 10^{-5}$
$t > 2$ hours	$t < 1s$	$t \approx 1s$

References

- J. Preskill, *Lecture notes on topological quantum computation*
- S. Trebst, A. W. Ludwig et al., *A short introduction to Fibonacci anyon models*, arXiv:0902.3275 (2009)
- N. E. Bonesteel et al., *Topological quantum compiling*, Phys. Rev B **75** (2007)
- G. Mussardo, X. Wan et al., T*opological quantum hashing with icosahedral group*, arXiv:0903.1497 (2009)