Braid Group on n-Strands: B_n

Braid Group on n-Strands: B_n

Some Elements of B_4

Braid Group on n-Strands: B_n

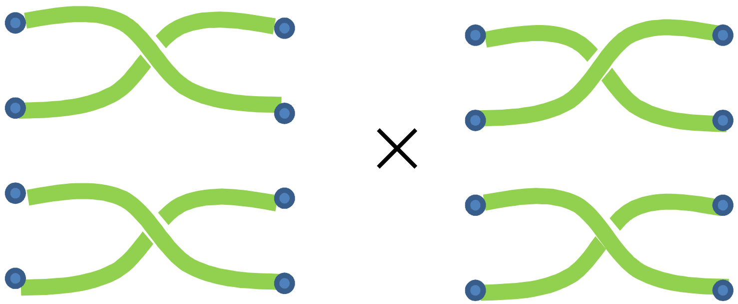
Some Elements of B_4

Not a Braid:

Braid Group on n-Strands: B_n

Some Elements of B_4

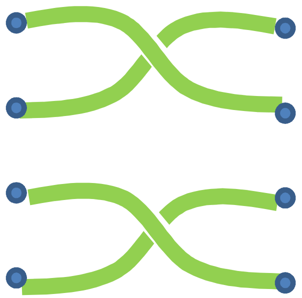
Group Multiplication



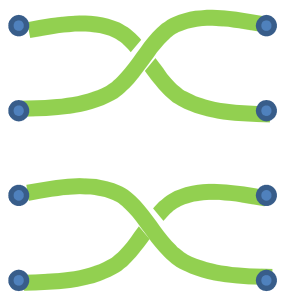
Braid Group on n-Strands: B_n

Some Elements of B_4

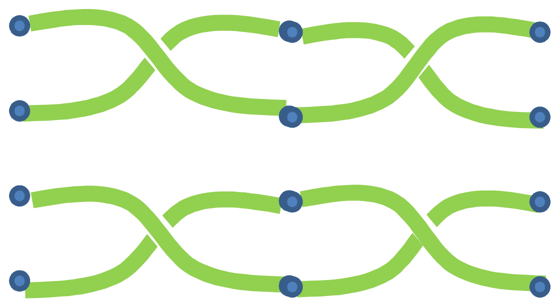
Group Multiplication



$\times$



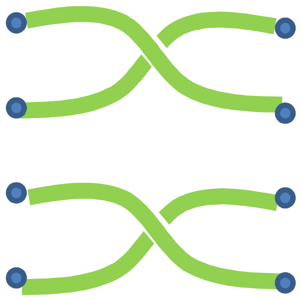
$=$



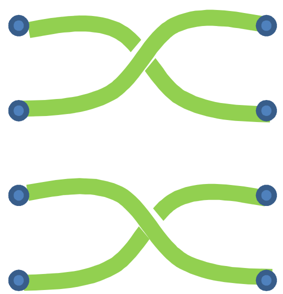
Braid Group on n-Strands: B_n

Some Elements of B_4

Group Multiplication



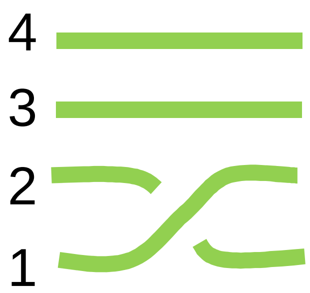
$\times$



$=$

Elementary Braid Operations

σ_i: Braid i[th] strand over i+1[st] strand

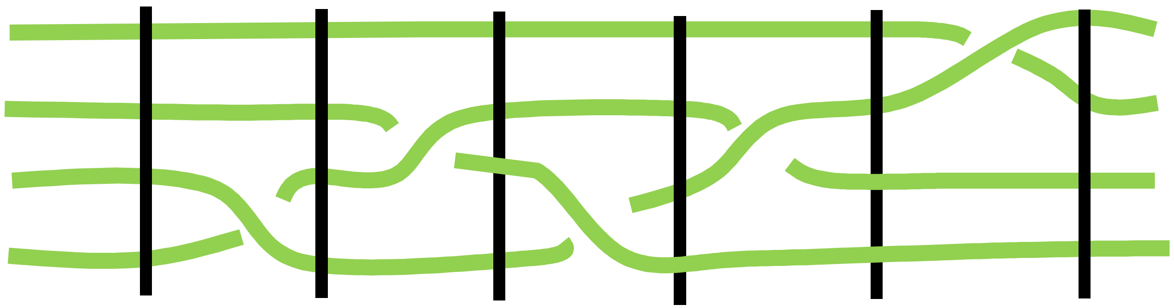


$= \sigma_1$

$= \sigma_2$

$= \sigma_3$

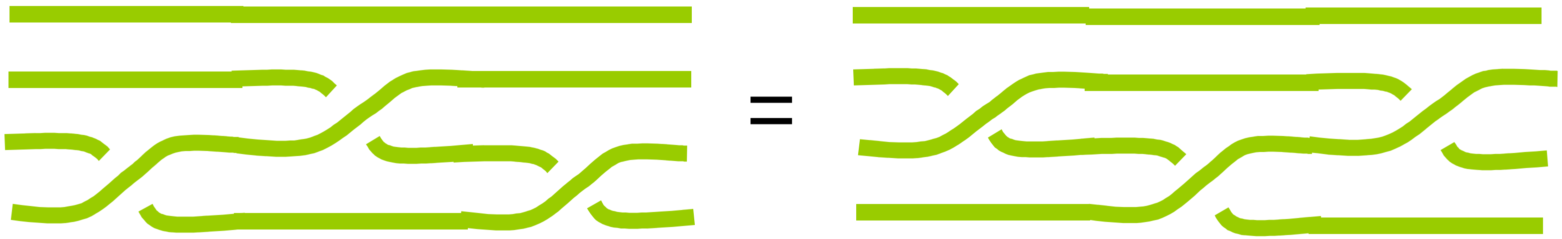
σ_i`s and their inverses generate the braid group



$\sigma_1^{-1} \quad \sigma_2 \quad \sigma_1^{-1} \quad \sigma_2 \quad \sigma_3$

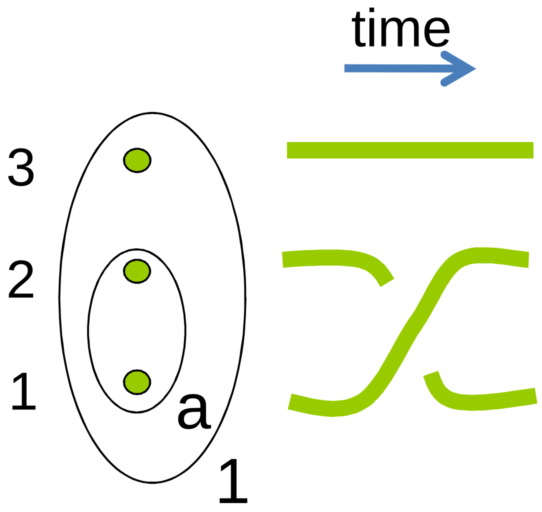
Braid Relations

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



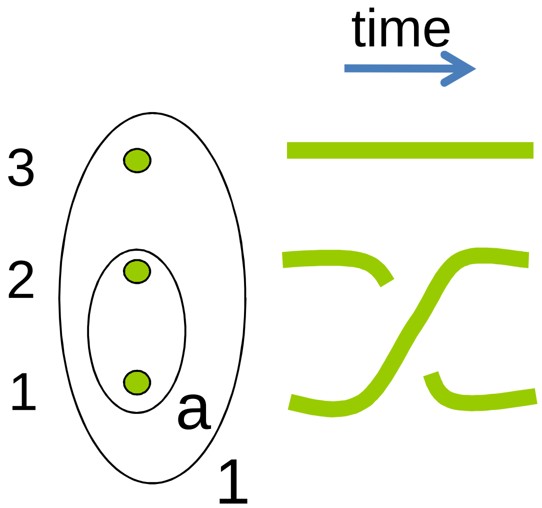
$$\sigma_i \sigma_j = \sigma_j \sigma_i \ , \qquad |i-j| \geq 2$$

Matrix Rep of B_3 from Fib Anyons



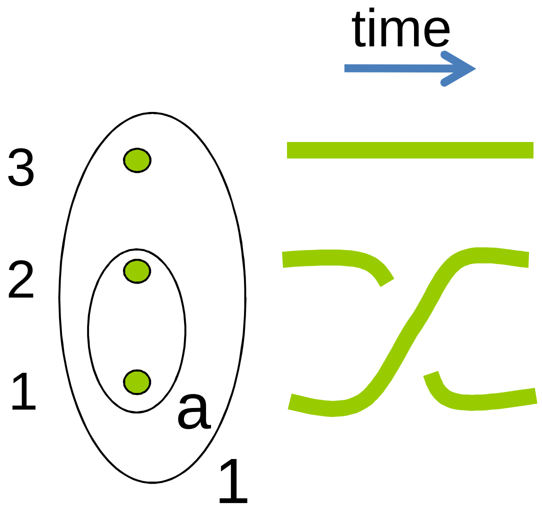
$$\sigma_1 = ?$$

Matrix Rep of B_3 from Fib Anyons

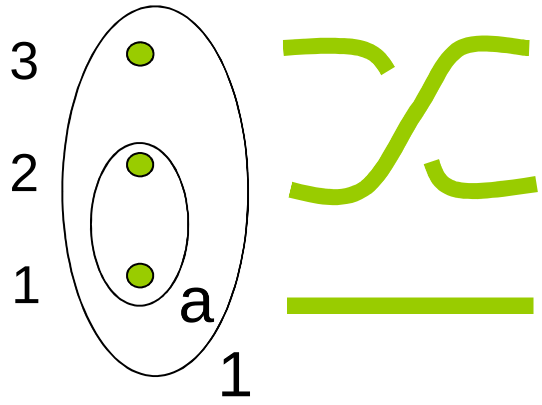


$$\sigma_1 = R = \begin{pmatrix} e^{-i4\pi/5} & 0 \\ 0 & e^{i3\pi/5} \end{pmatrix}$$

Matrix Rep of B_3 from Fib Anyons

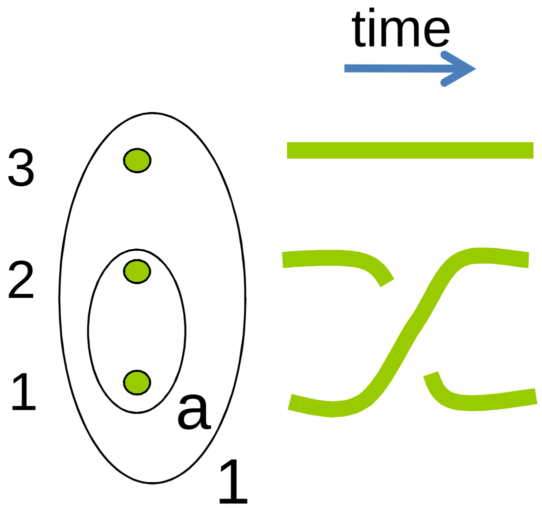


$$\sigma_1 = R = \begin{pmatrix} e^{-i4\pi/5} & 0 \\ 0 & e^{i3\pi/5} \end{pmatrix}$$

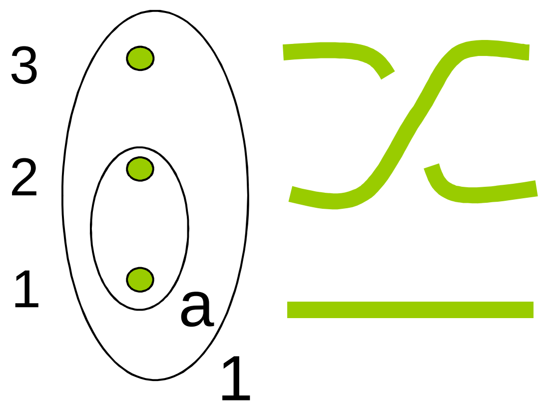


$$\sigma_2 = ?$$

Matrix Rep of B_3 from Fib Anyons

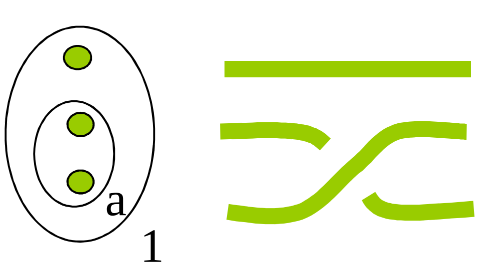


$$\sigma_1 = R = \begin{pmatrix} e^{-i4\pi/5} & 0 \\ 0 & e^{i3\pi/5} \end{pmatrix}$$



$$\sigma_2 = F\,R\,F = \begin{pmatrix} -\tau\, e^{-i\pi/5} & \sqrt{\tau}\, e^{-i3\pi/5} \\ \sqrt{\tau} e^{-i3\pi/5} & -\tau \end{pmatrix}$$

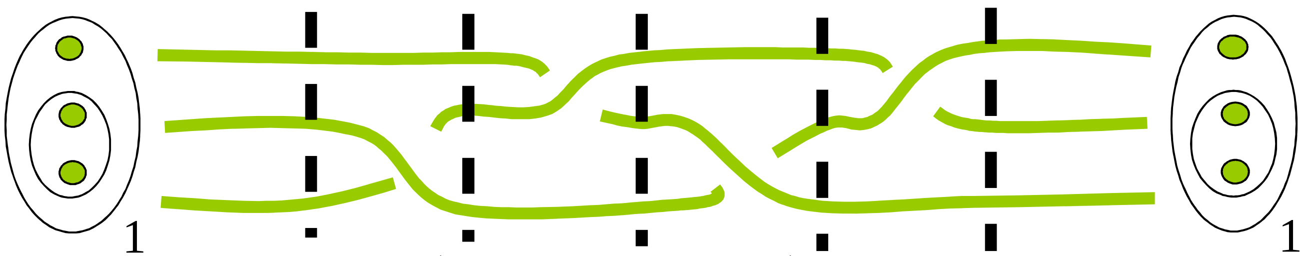
Elementary Braid Matrices



$$\sigma_1 = \begin{pmatrix} e^{-i4\pi/5} & 0 \\ 0 & e^{i3\pi/5} \end{pmatrix}$$

$$\sigma_2 = F\,\sigma_1 F = \begin{pmatrix} -\tau\, e^{-i\pi/5} & \sqrt{\tau}\, e^{-i3\pi/5} \\ \sqrt{\tau} e^{-i3\pi/5} & -\tau \end{pmatrix}$$

$\left|\Psi_i\right\rangle$



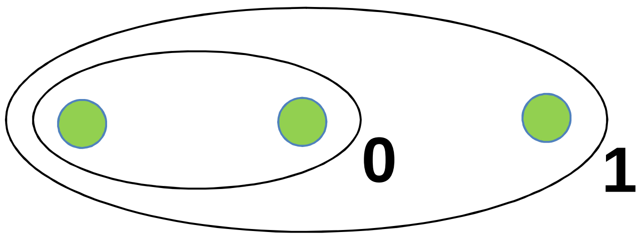
$\left|\Psi_f\right\rangle = M^T \left|\Psi_i\right\rangle$

$\sigma_1^{-1} \quad \sigma_2 \quad \sigma_1^{-1} \quad \sigma_2 \quad = \quad M$

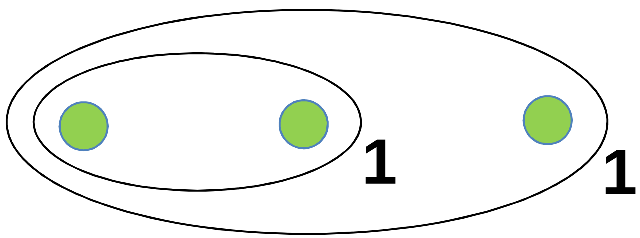
Qubit Encoding

Qubit States

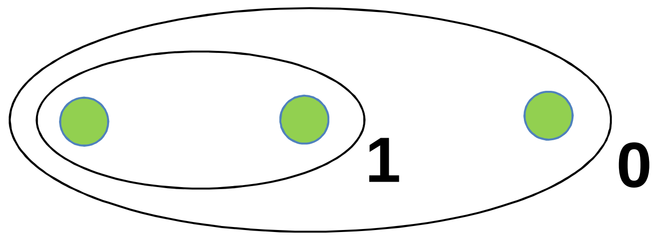
$|0\rangle =$



$|1\rangle =$



Non-Computational State

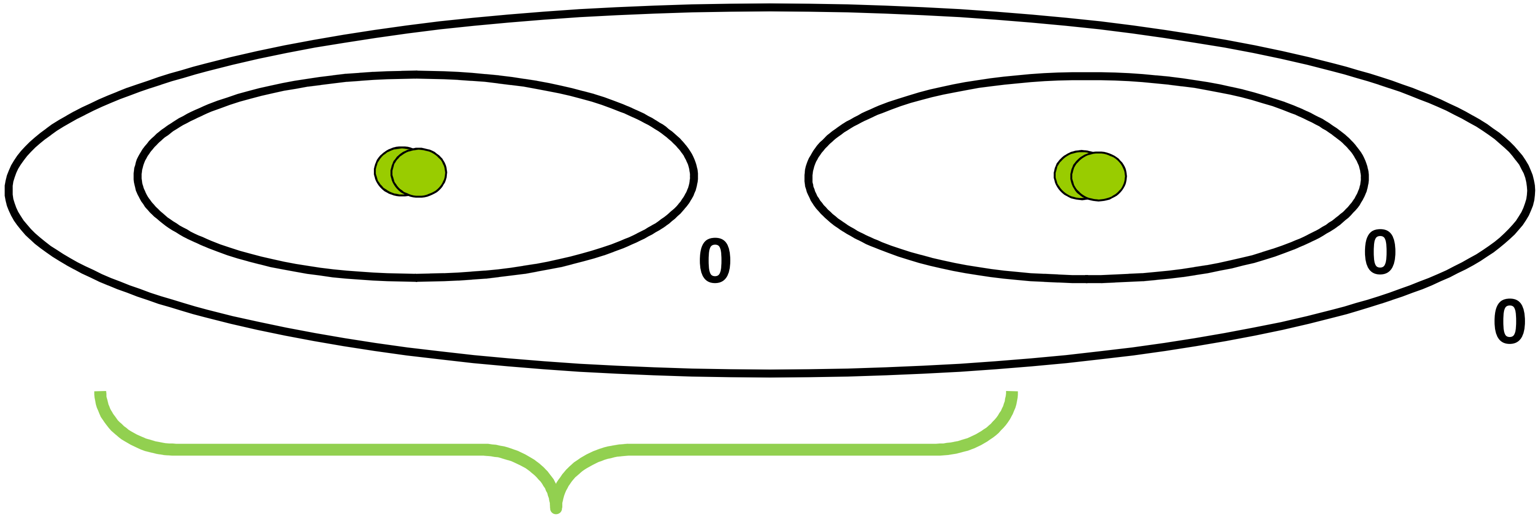


State of qubit is determined by q-spin of two leftmost particles

Transitions to this state are **leakage errors**

Initializing a Qubit

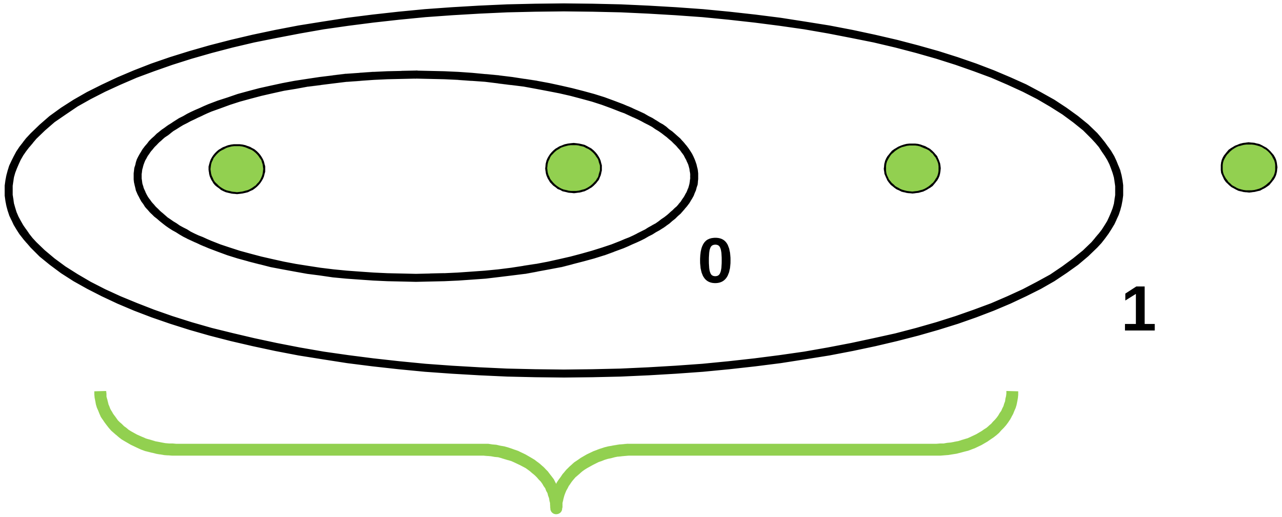
Pull two quasiparticle-quasihole pairs out of the “vacuum”.



These three particles have total q-spin 1

Initializing a Qubit

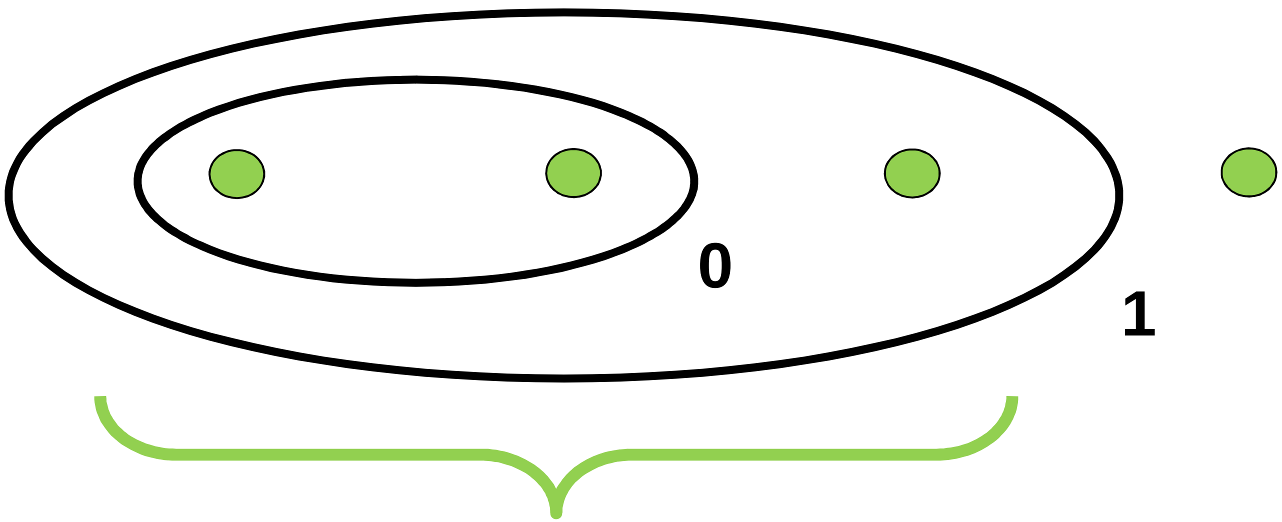
Pull two quasiparticle-quasihole pairs out of the “vacuum”.



$$|0\rangle$$

Initializing a Qubit

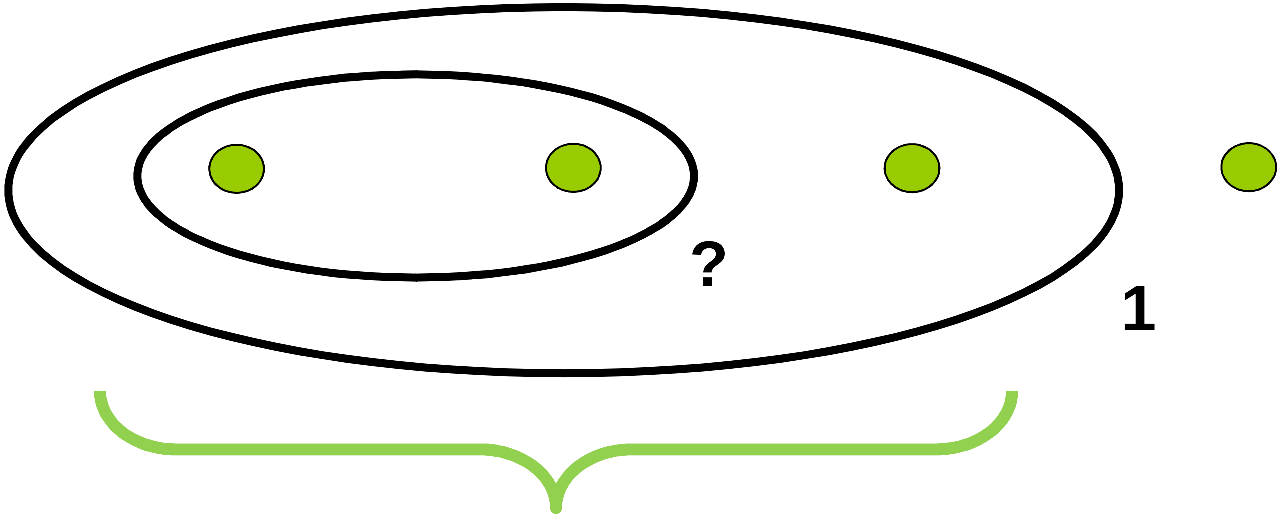
Pull two quasiparticle-quasihole pairs out of the “vacuum”.



$$|0\rangle$$

Measuring a Qubit

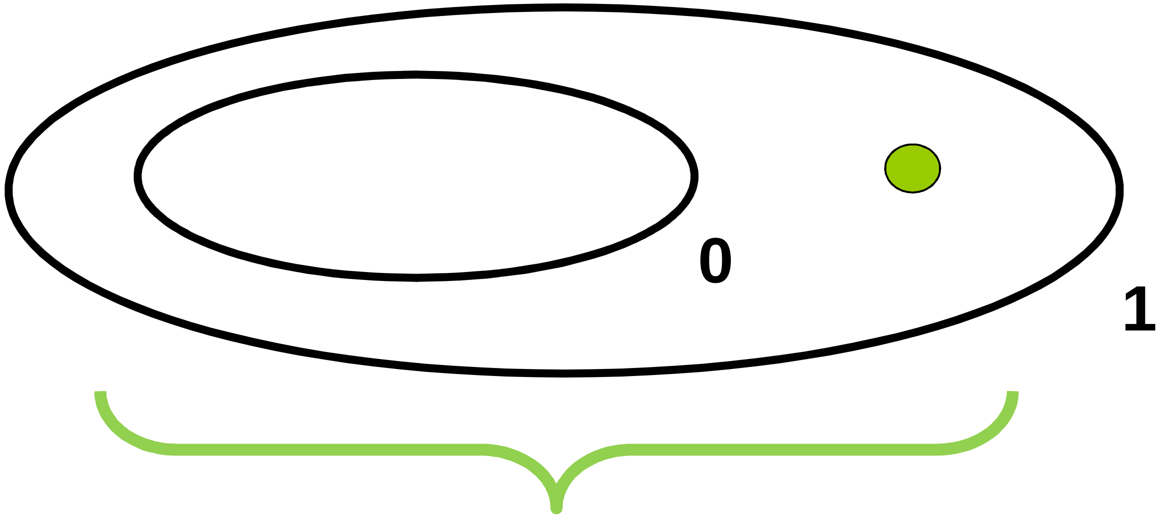
Try to fuse the leftmost quasiparticle-quasihole pair.



$$\alpha|0\rangle + \beta|1\rangle$$

Measuring a Qubit

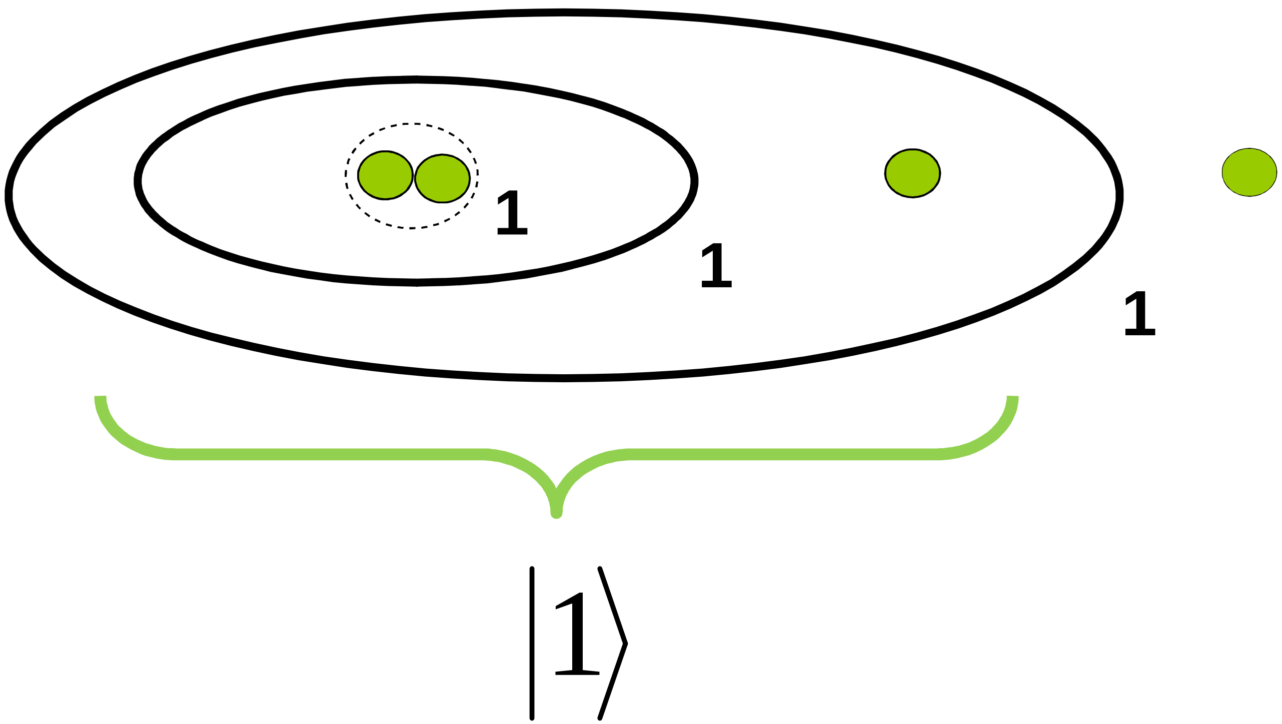
If they fuse back into the “vacuum” the result of the measurement is 0.



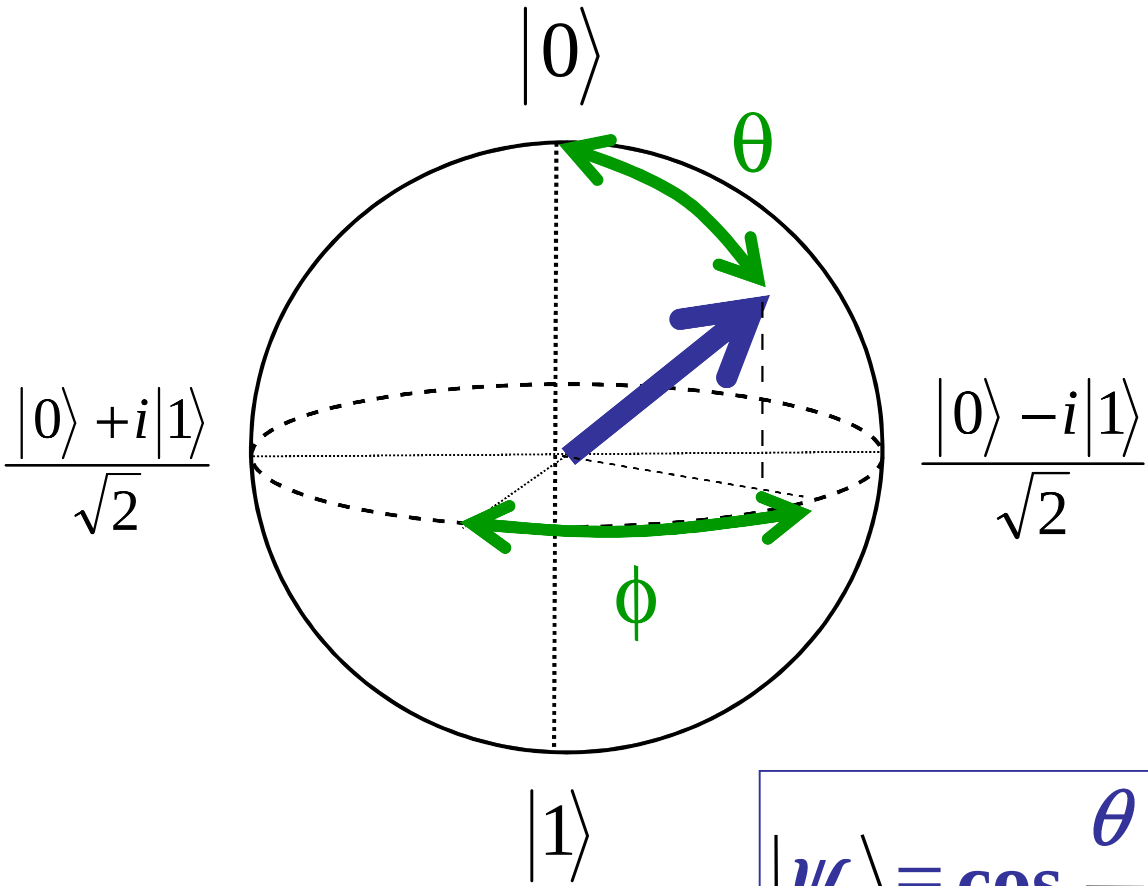
$$|0\rangle$$

Measuring a Qubit

If they cannot fuse back into the “vacuum” the result of the measurement is 1

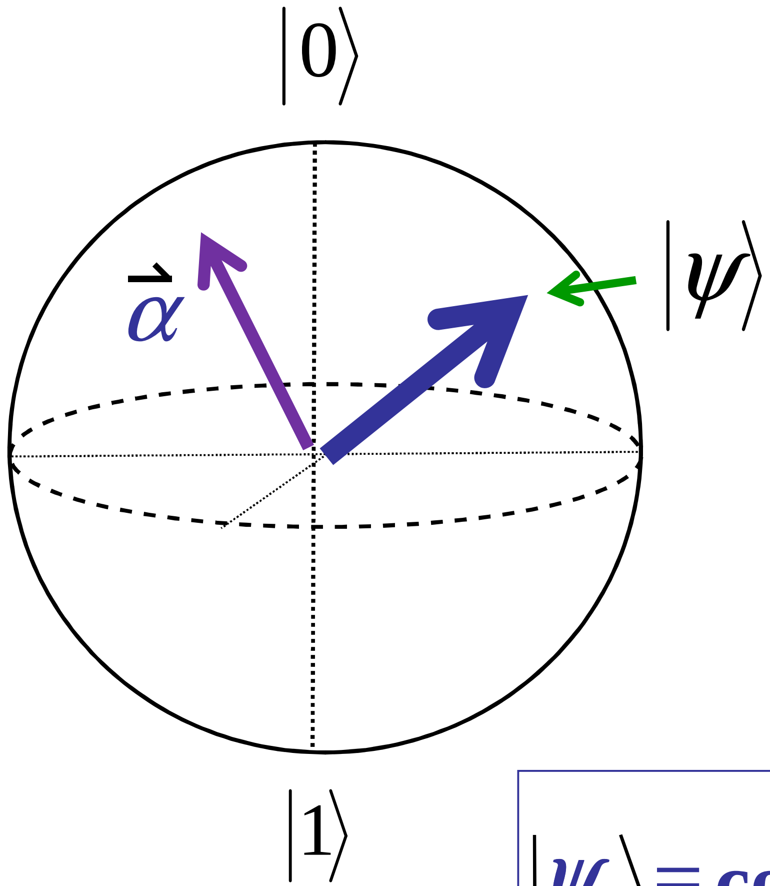


Single Qubit: The Bloch Sphere



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{-i\phi}|1\rangle$$

Single Qubit Operations: Rotations



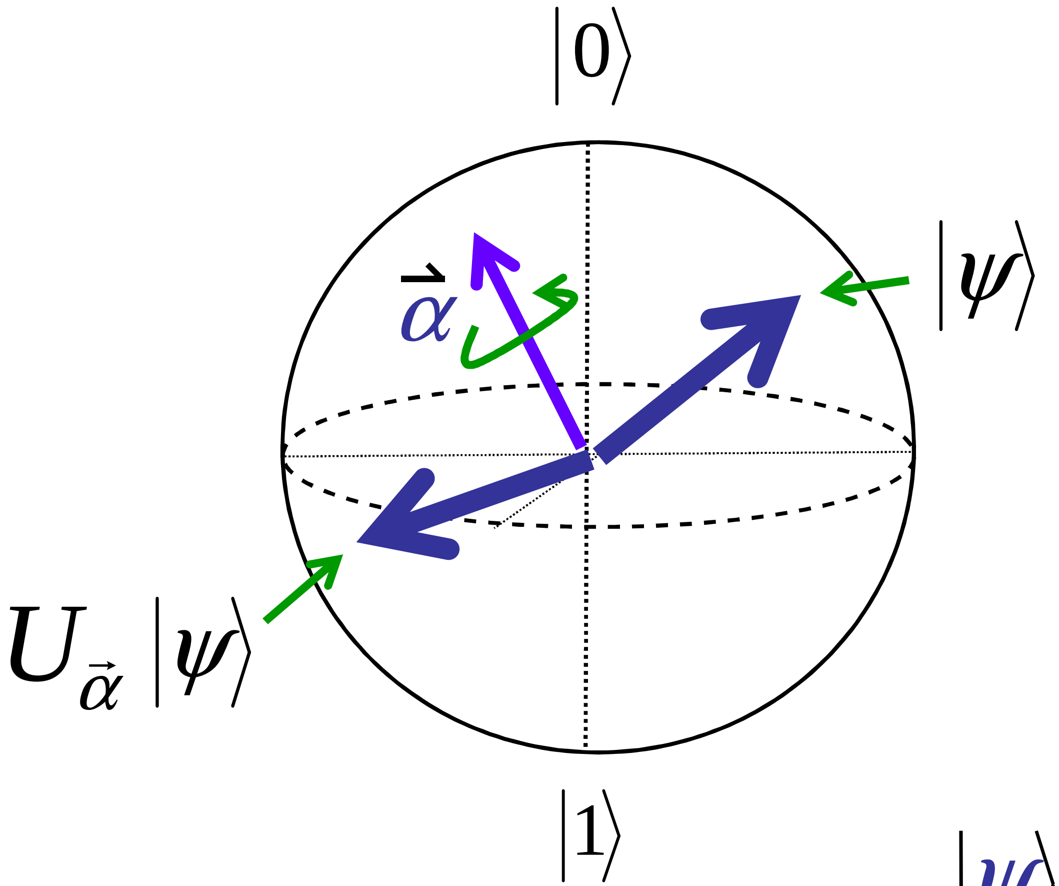
$\vec{\alpha}$ = rotation vector

Direction of $\vec{\alpha}$ is the rotation axis

Magnitude of $\vec{\alpha}$ is the rotation angle

$$\boxed{|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2} e^{-i\phi}|1\rangle}$$

Single Qubit Operations: Rotations

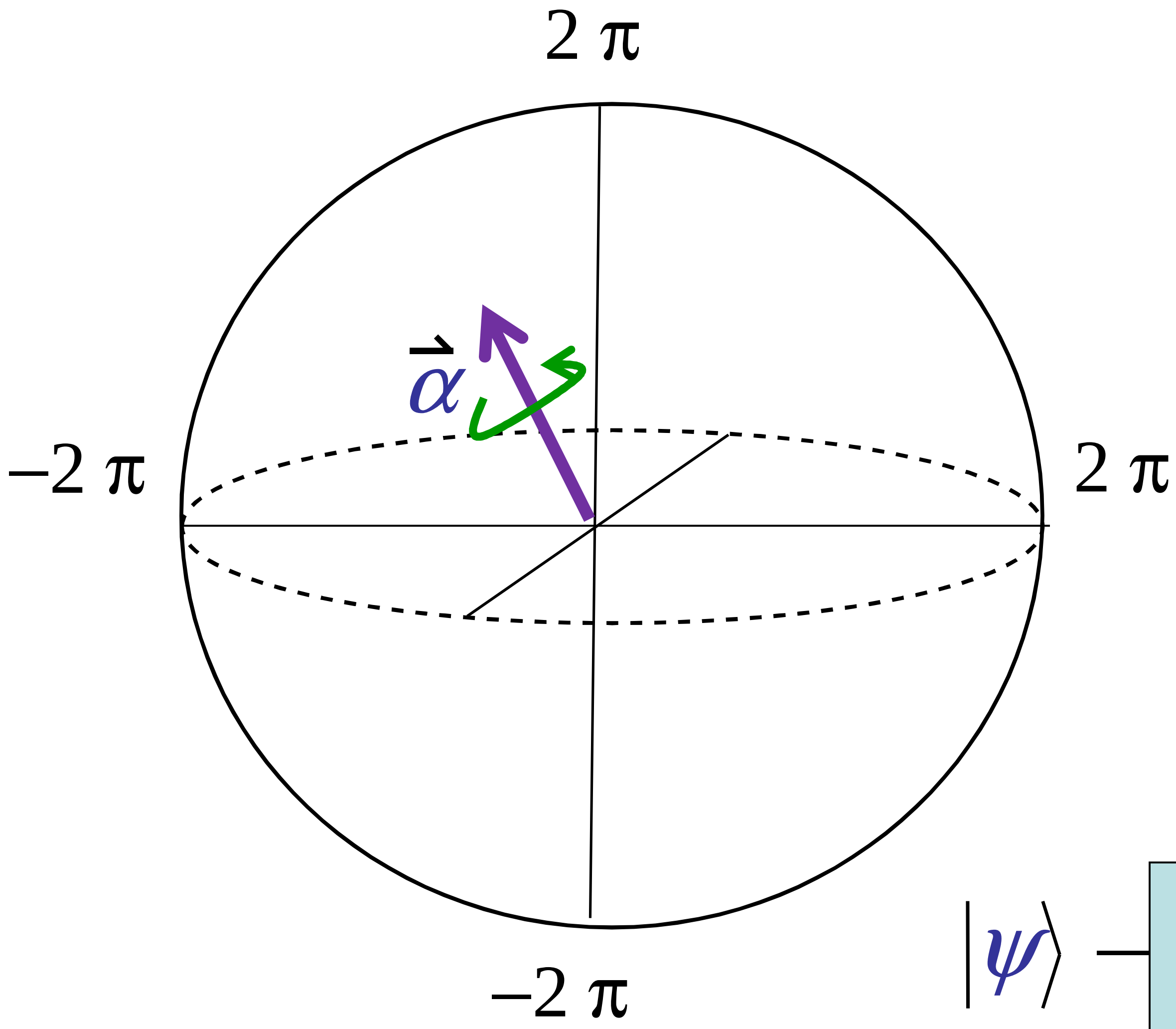


$\vec{\alpha}$ = rotation vector

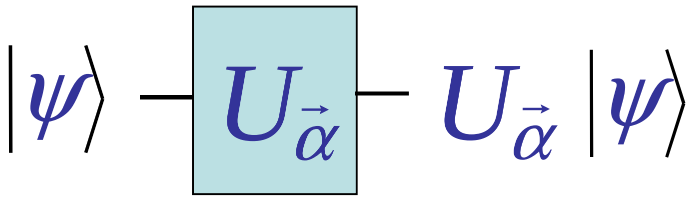
$$U_{\vec{\alpha}} = \exp\frac{i\,\vec{\alpha}\cdot\vec{\sigma}}{2}$$

$$|\psi\rangle \;-\!\boxed{U_{\vec{\alpha}}}\!-\; U_{\vec{\alpha}}|\psi\rangle$$

Single Qubit Operations: Rotations



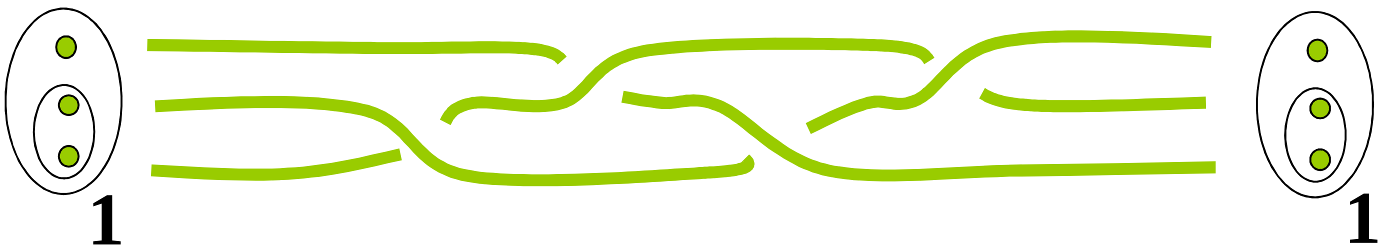
The set of all single qubit rotations lives in a solid sphere of radius 2π.



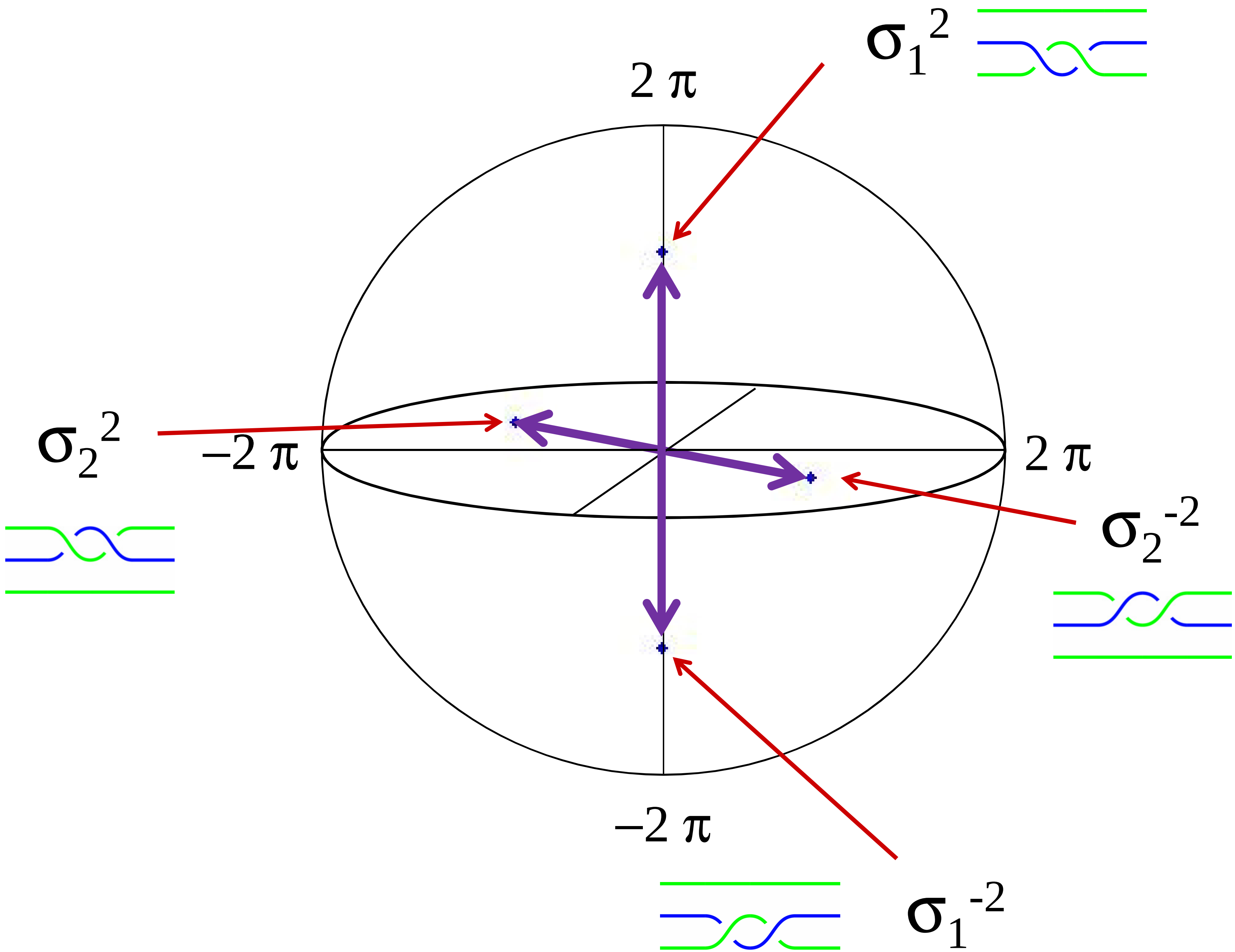
Single Qubit Operations: Rotations

General rule: Braiding inside an oval does not change the total topological charge of the enclosed particles.

Important consequence: As long as we braid *within* a qubit, there is no leakage error.

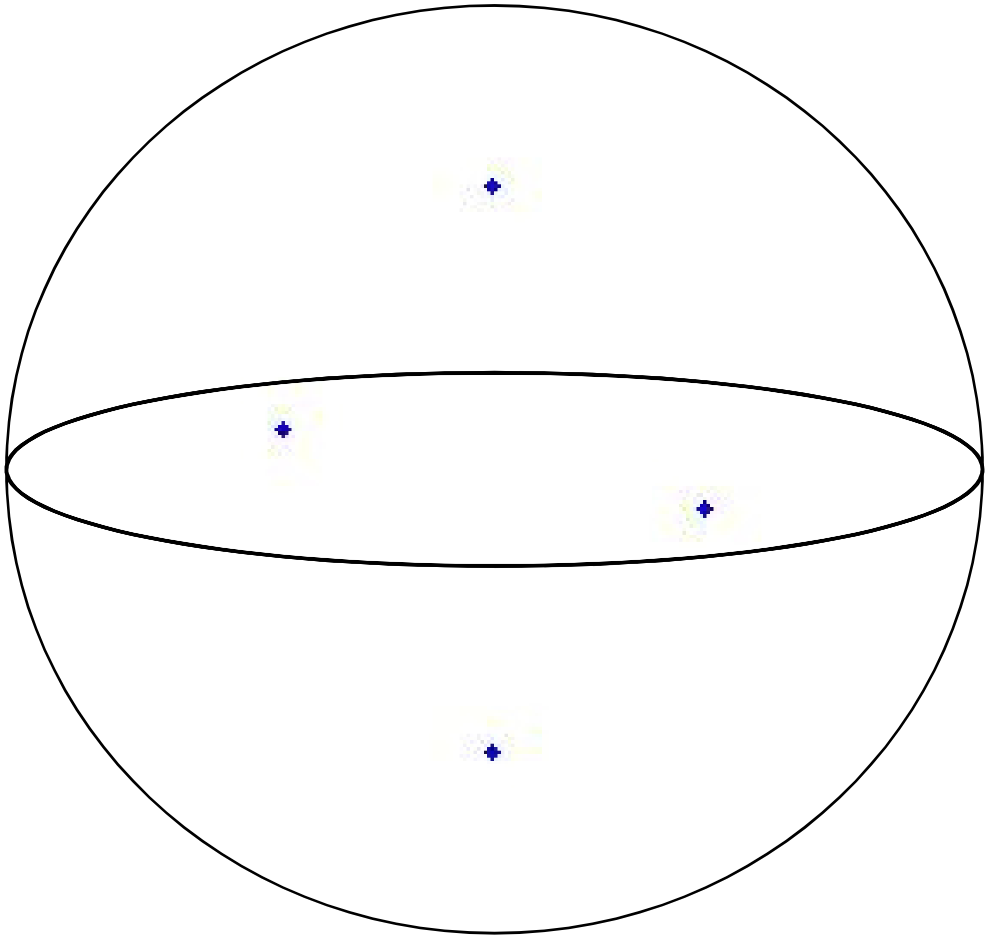


Can we do arbitrary single qubit rotations this way?

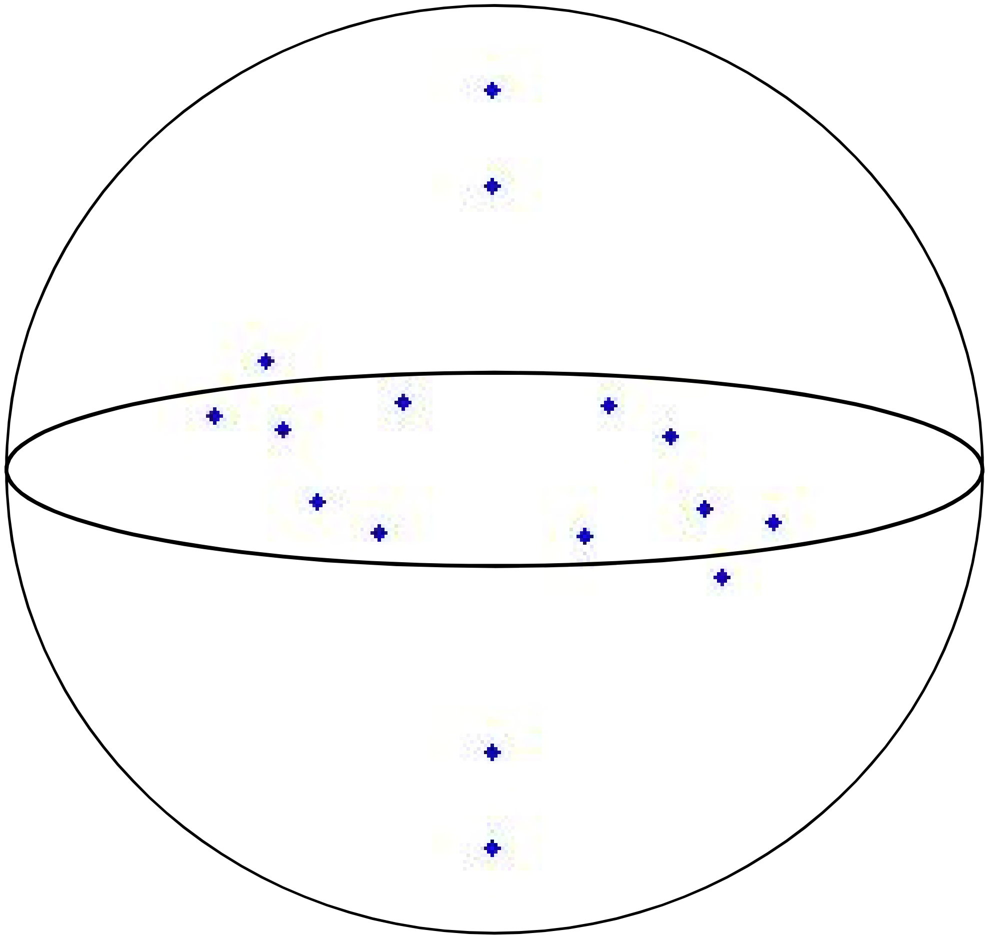


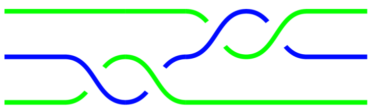
$\sigma_1^{\ 2}$
$2\ \pi$
$\sigma_2^{\ 2}$
$-2\ \pi$
$2\ \pi$
$\sigma_2^{\ -2}$
$-2\ \pi$
$\sigma_1^{\ -2}$

N = 1

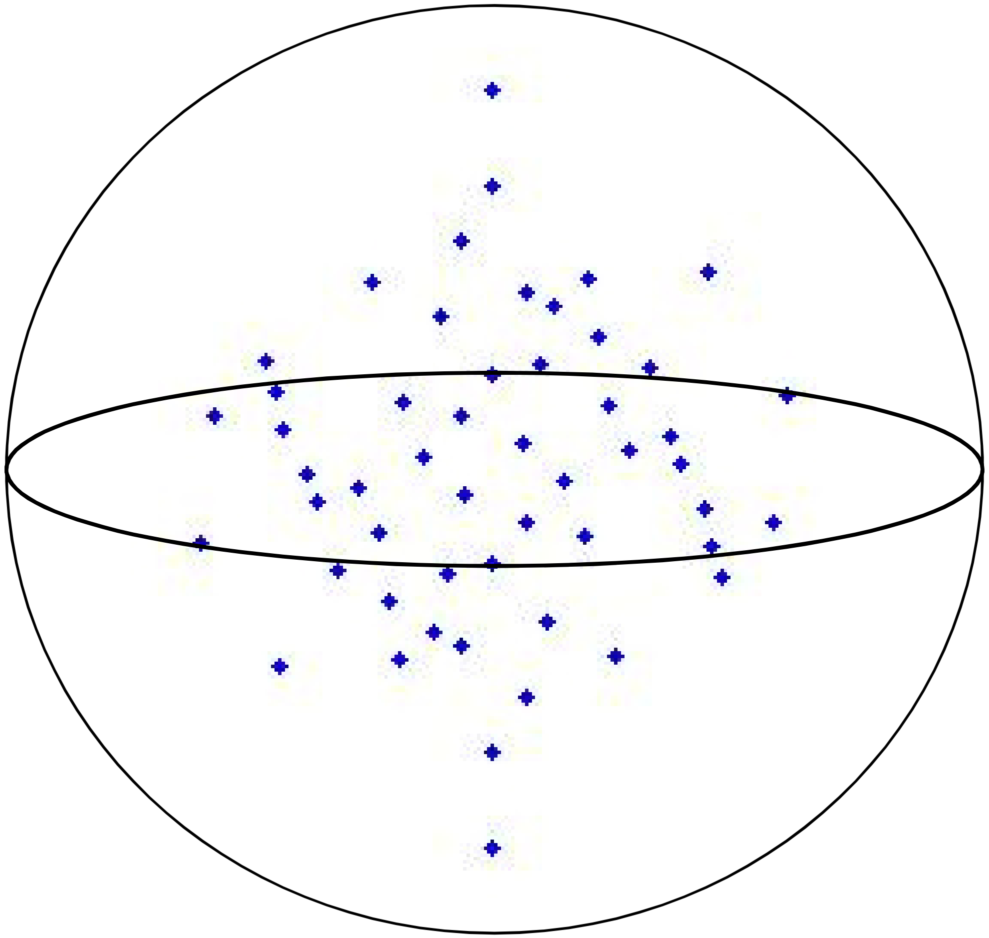


N = 2

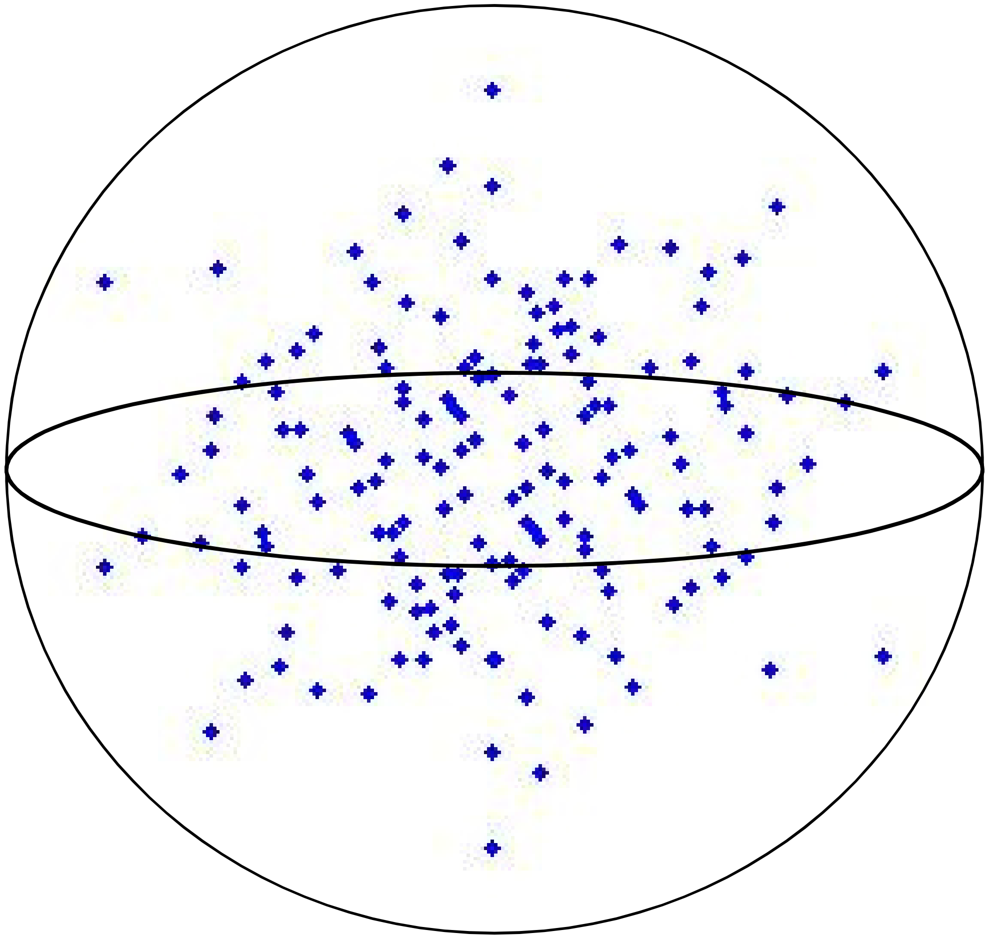




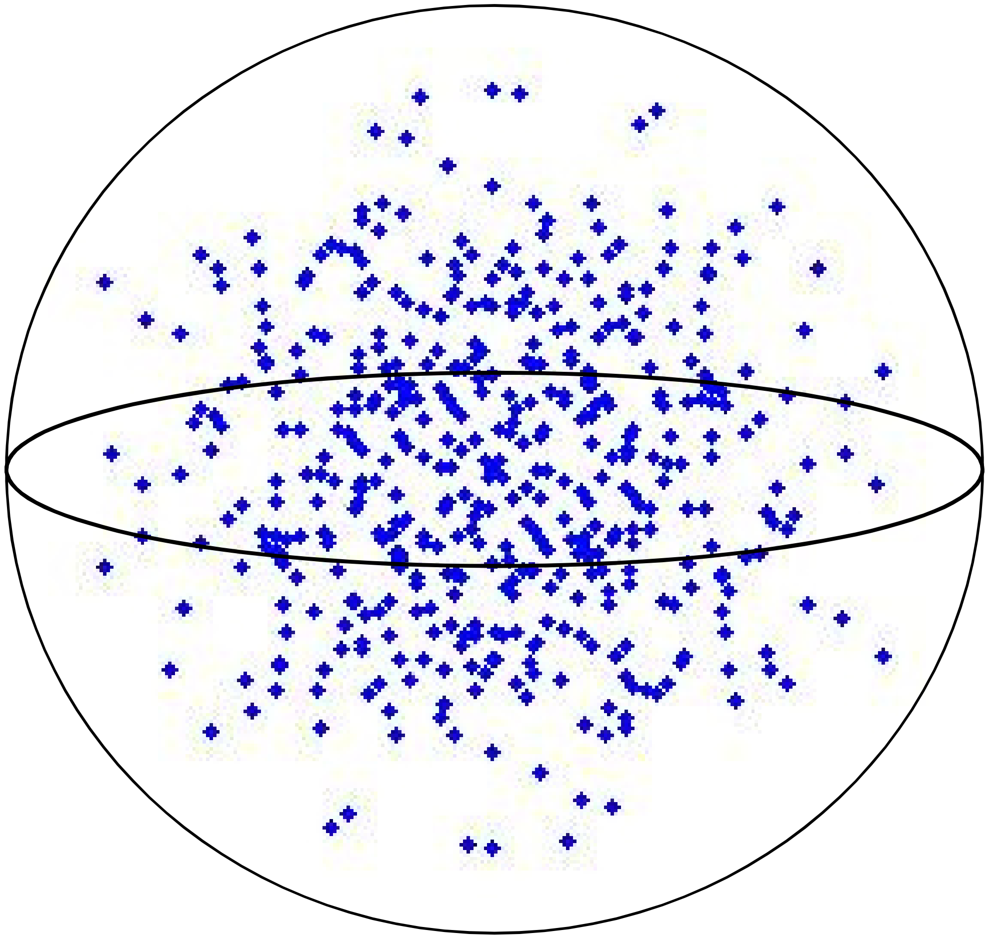
N = 3



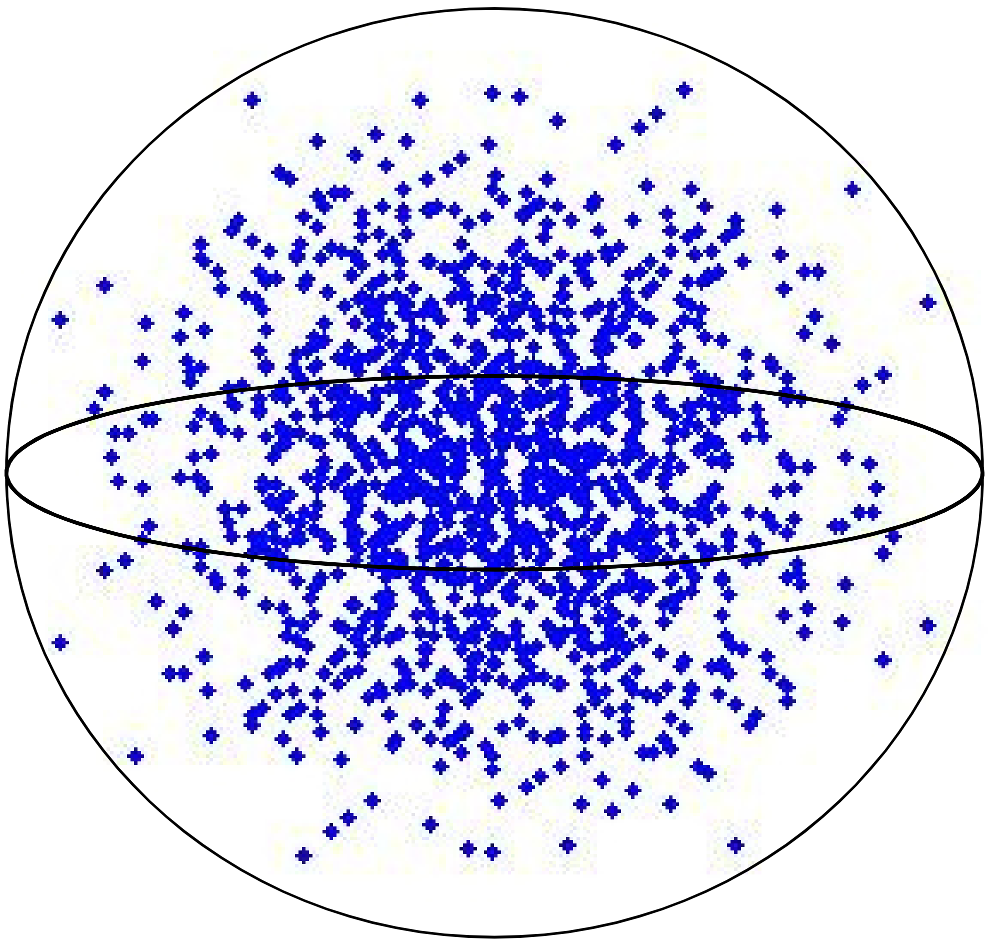
N = 4



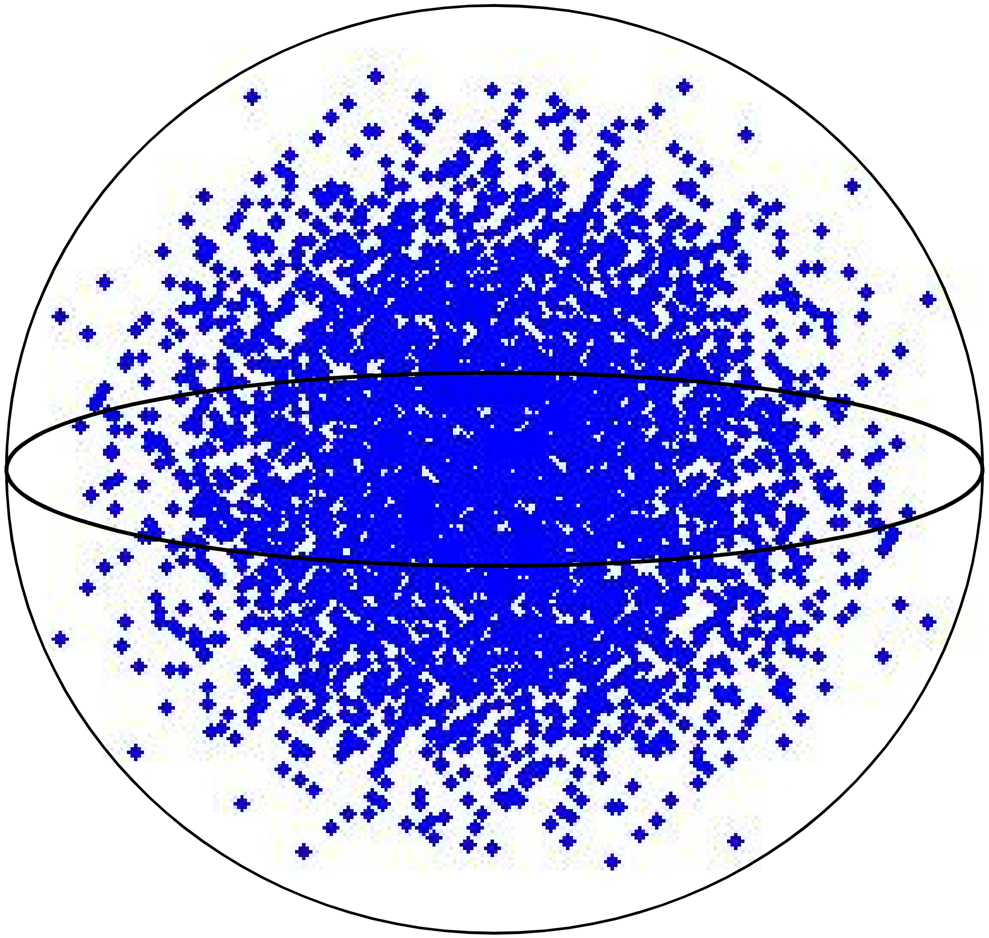
N = 5



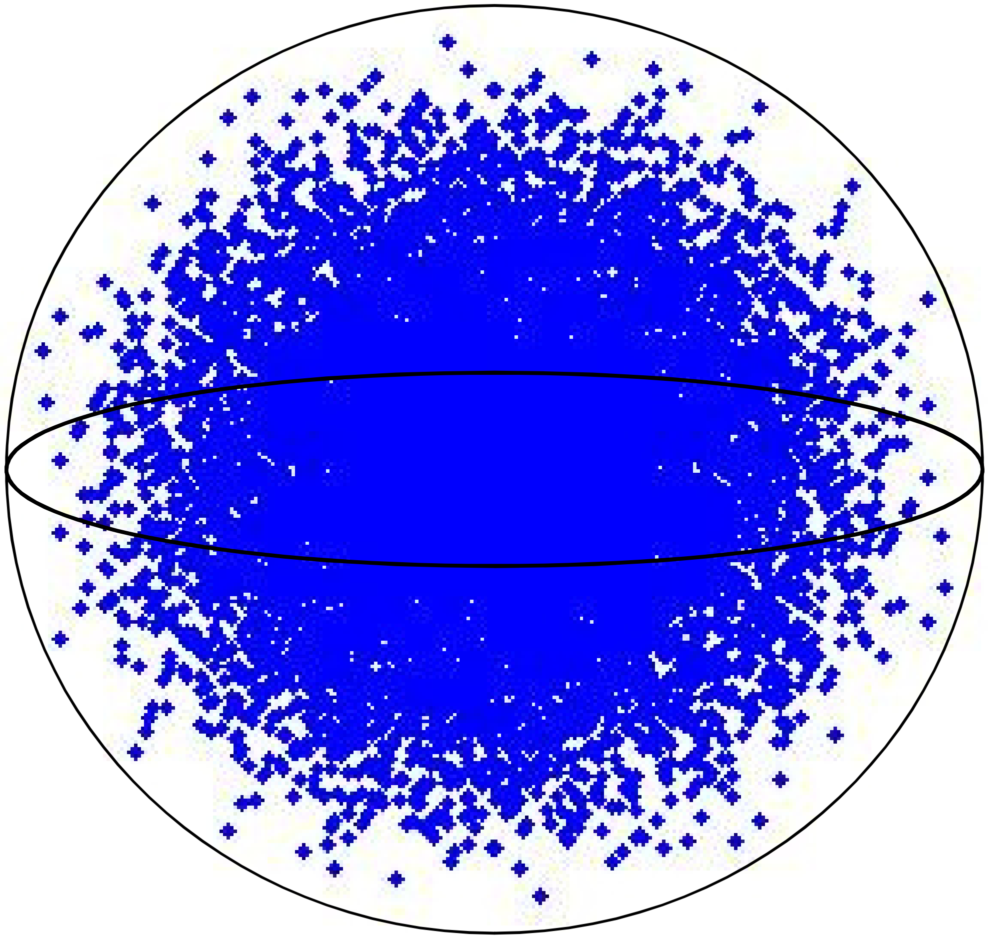
$N = 6$



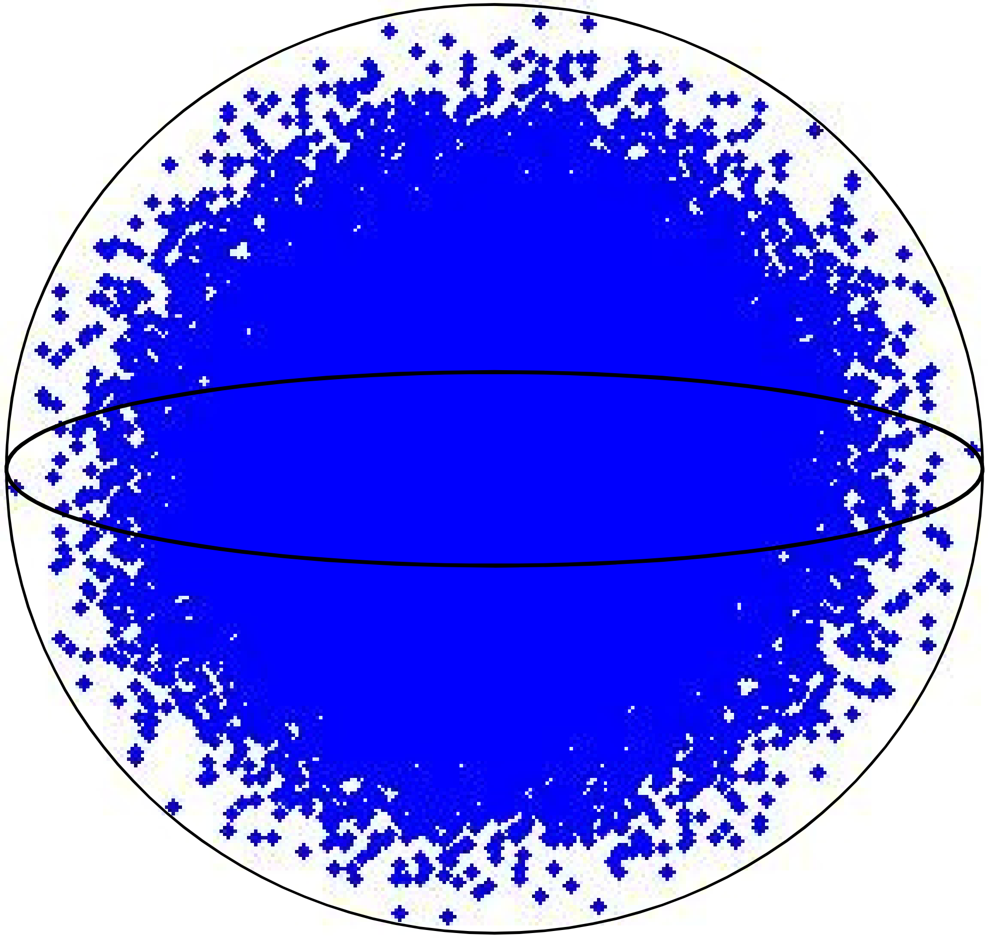
N = 7

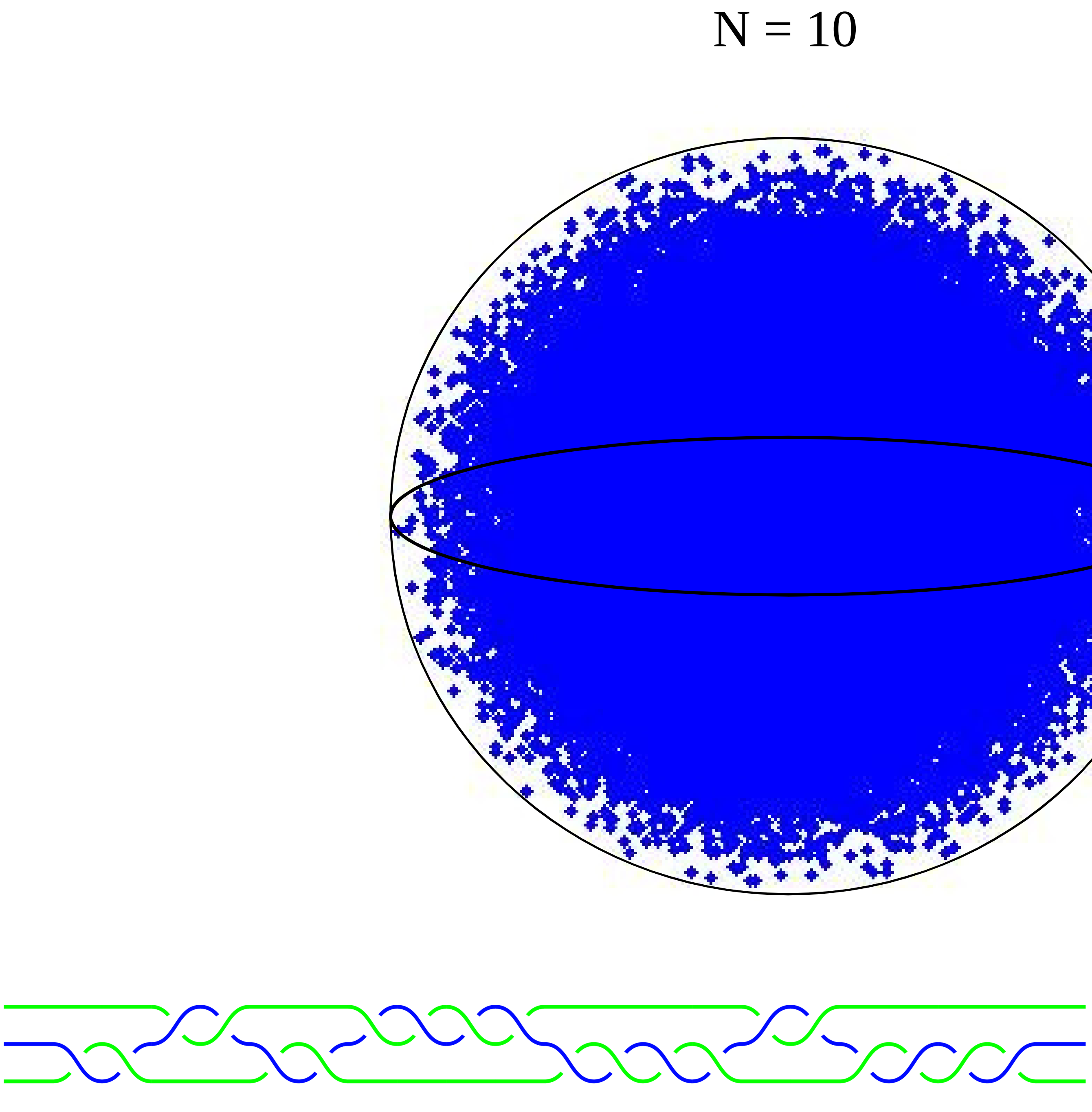


N = 8

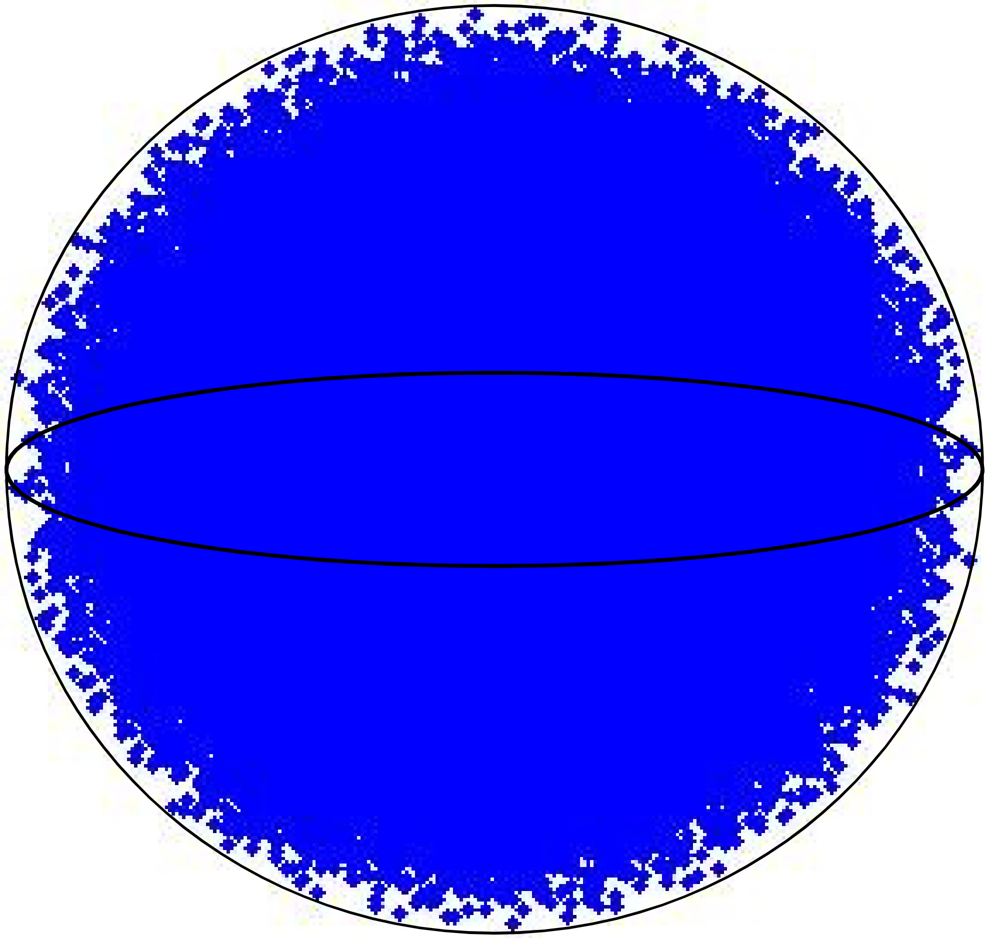


N = 9




N = 10

N = 11



Brute Force Search

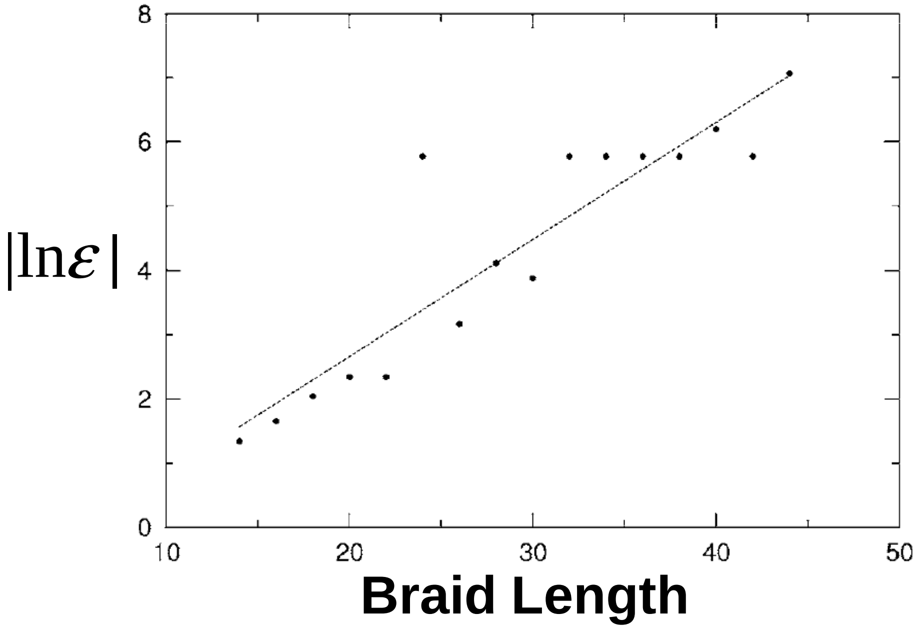
$$\sigma_1^{-2}\sigma_2^{-4}\sigma_1^{4}\sigma_2^{-2}\sigma_1^{2}\sigma_2^{2}\sigma_1^{-2}\sigma_2^{4}\sigma_1^{-2}\sigma_2^{4}\sigma_1^{2}\sigma_2^{-4}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{-2} = \begin{pmatrix} 0 & i & 0 \\ i & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} + O(10^{-3})$$

Brute Force Search

$$\sigma_1^{-2}\sigma_2^{-4}\sigma_1^{4}\sigma_2^{-2}\sigma_1^{2}\sigma_2^{2}\sigma_1^{-2}\sigma_2^{4}\sigma_1^{-2}\sigma_2^{4}\sigma_1^{2}\sigma_2^{-4}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{-2} = \begin{pmatrix} \boxed{\begin{matrix} 0 & i \\ i & 0 \end{matrix}} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & 1 \end{pmatrix} + \underbrace{O(10^{-3})}_{\text{“error” } \varepsilon}$$

For brute force search:

Braid Length $\sim \; |\ln \varepsilon|$



L. Hormozi, G. Zikos, NEB, S.H. Simon, PRB ‘07

Brute Force Search

$$\sigma_1^{-2}\sigma_2^{-4}\sigma_1^{4}\sigma_2^{-2}\sigma_1^{2}\sigma_2^{2}\sigma_1^{-2}\sigma_2^{4}\sigma_1^{-2}\sigma_2^{4}\sigma_1^{2}\sigma_2^{-4}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{-2} = \begin{pmatrix} \boxed{\begin{matrix} 0 & i \\ i & 0 \end{matrix}} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & 1 \end{pmatrix} + \underset{\uparrow}{O(10^{-3})}$$

"error" ε

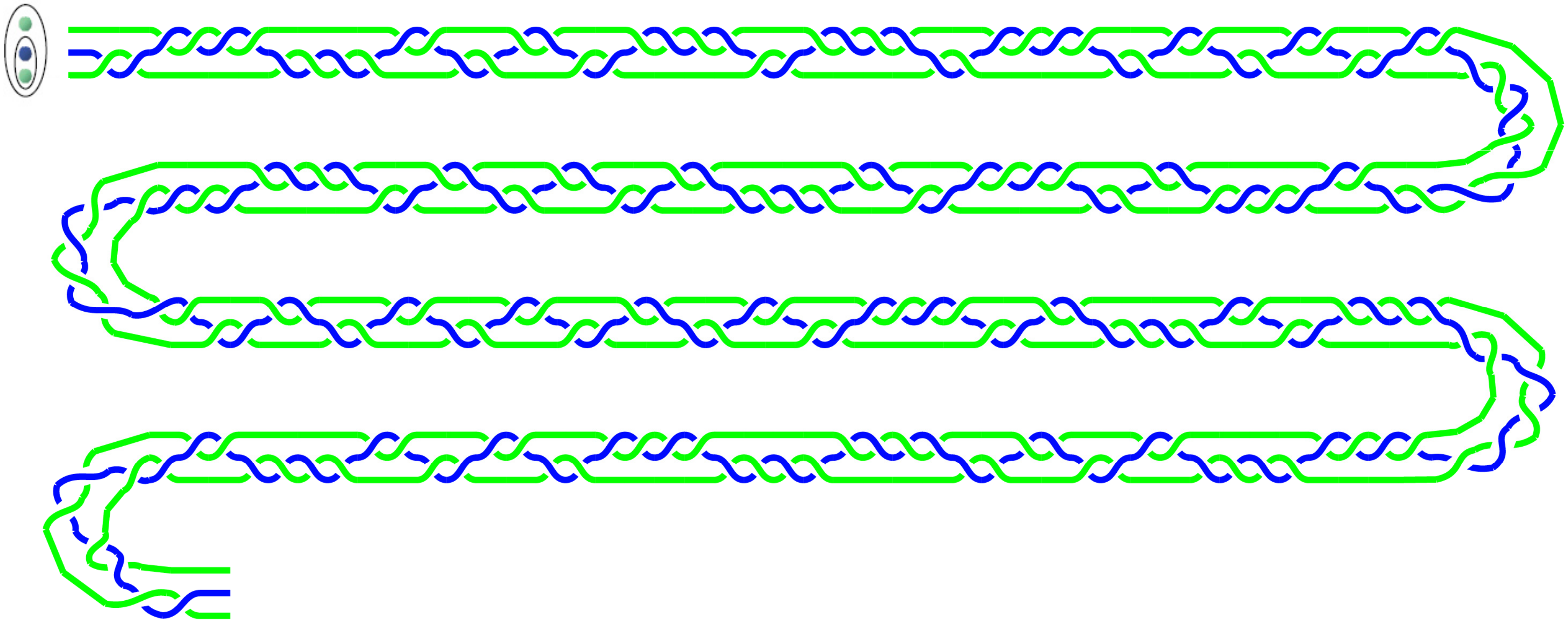
Brute force searching rapidly becomes infeasible as braids get longer.

Fortunately, a clever algorithm due to Solovay and Kitaev allows for systematic improvement of the braid given a sufficiently dense covering of *SU(2)*.

Solovay-Kitaev Construction

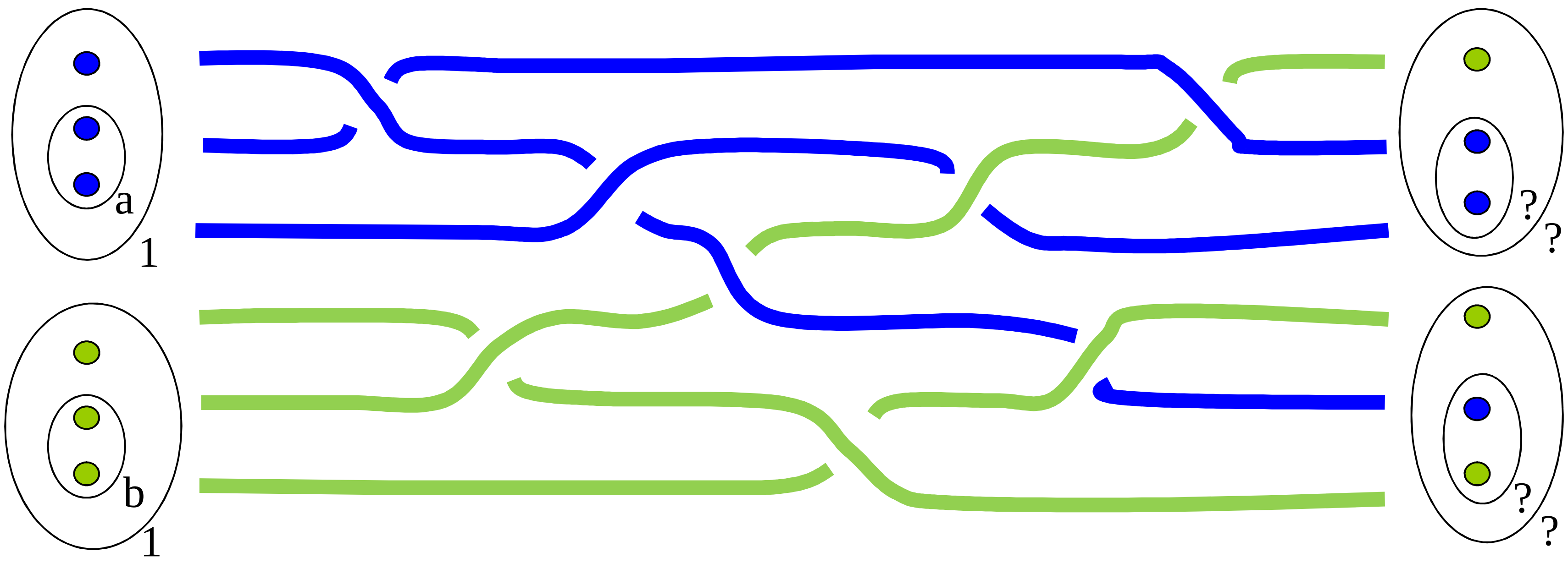
$$\left(\begin{array}{cc|c} 0 & i & 0 \\ i & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right) + O(10^{-4})$$

“error” ε



$$\text{Braid Length} \sim |\ln \varepsilon|^{c}, \quad c \approx 4$$

What About Two Qubit Gates?

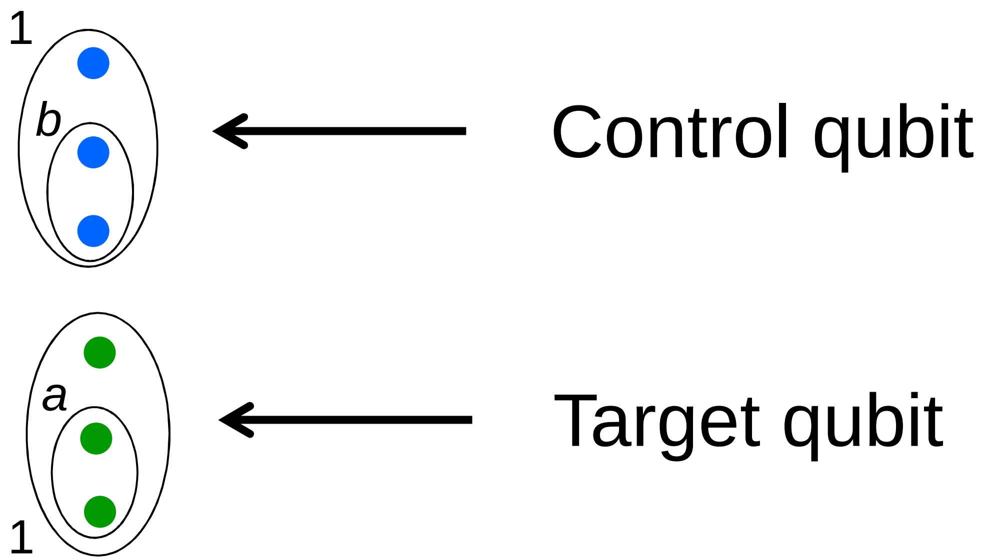


Problems:

1. We are pulling quasiparticles out of qubits: Leakage error!

2. 87 dimensional search space (as opposed to 3 for three-particle braids). Straightforward “brute force” search is problematic.

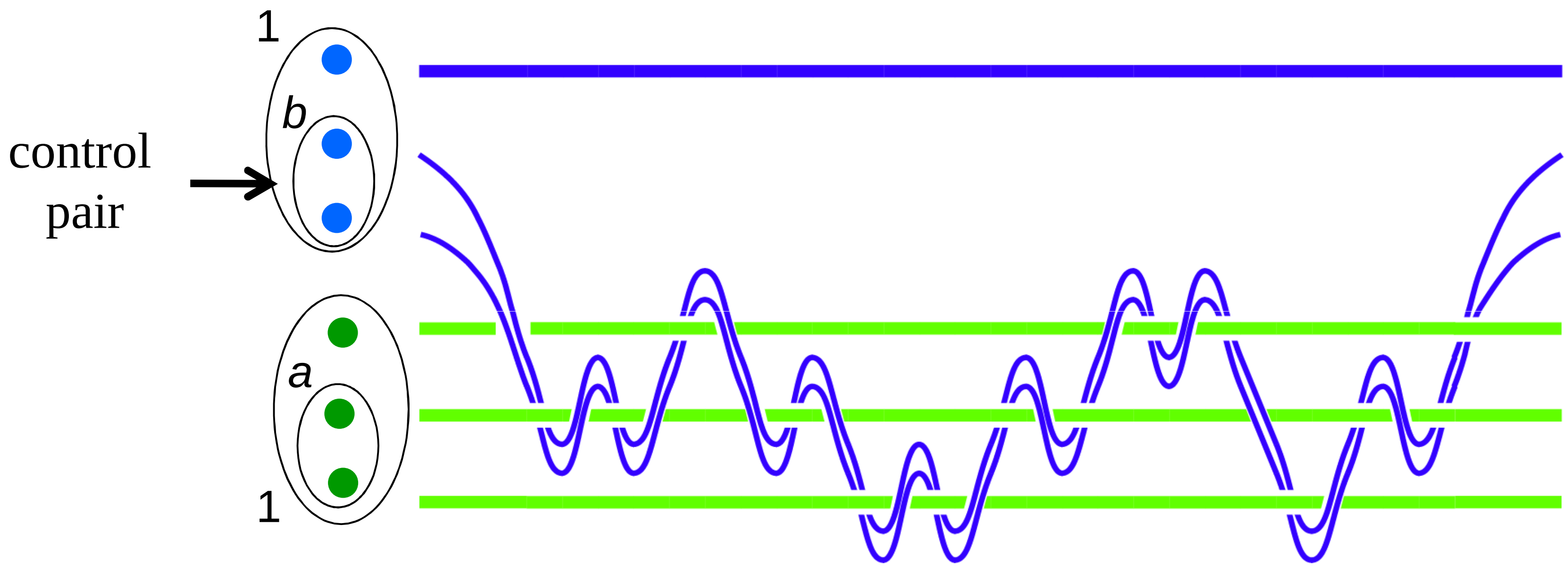
Two Qubit Controlled Gates



Goal: Find a braid in which some rotation is performed on the target qubit only if the control qubit is in the state 1. (***b=1***)

"Weaving" a Two Qubit Gate

Weave a *pair* of anyons from the control qubit between anyons in the target qubit.



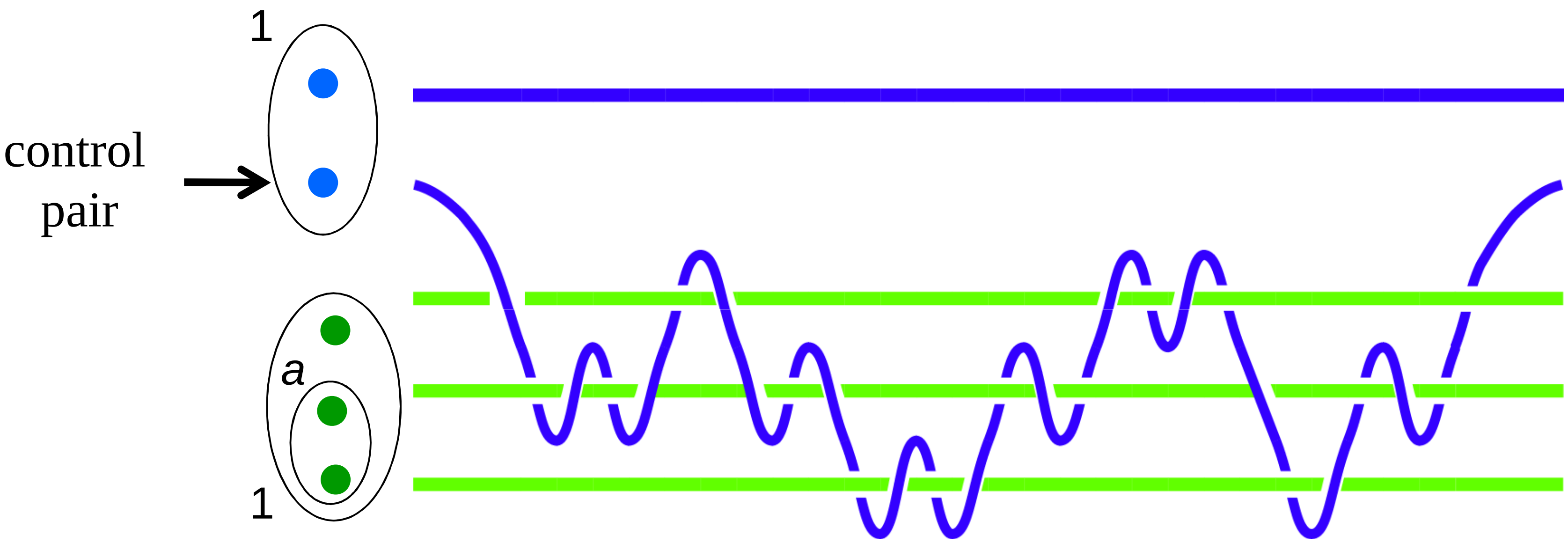
Important Rule: Braiding a q-spin 0 object does not induce transitions.

→ Target qubit is only affected if control qubit is in state $|1\rangle$

(b = 1)

“Weaving” a Two Qubit Gate

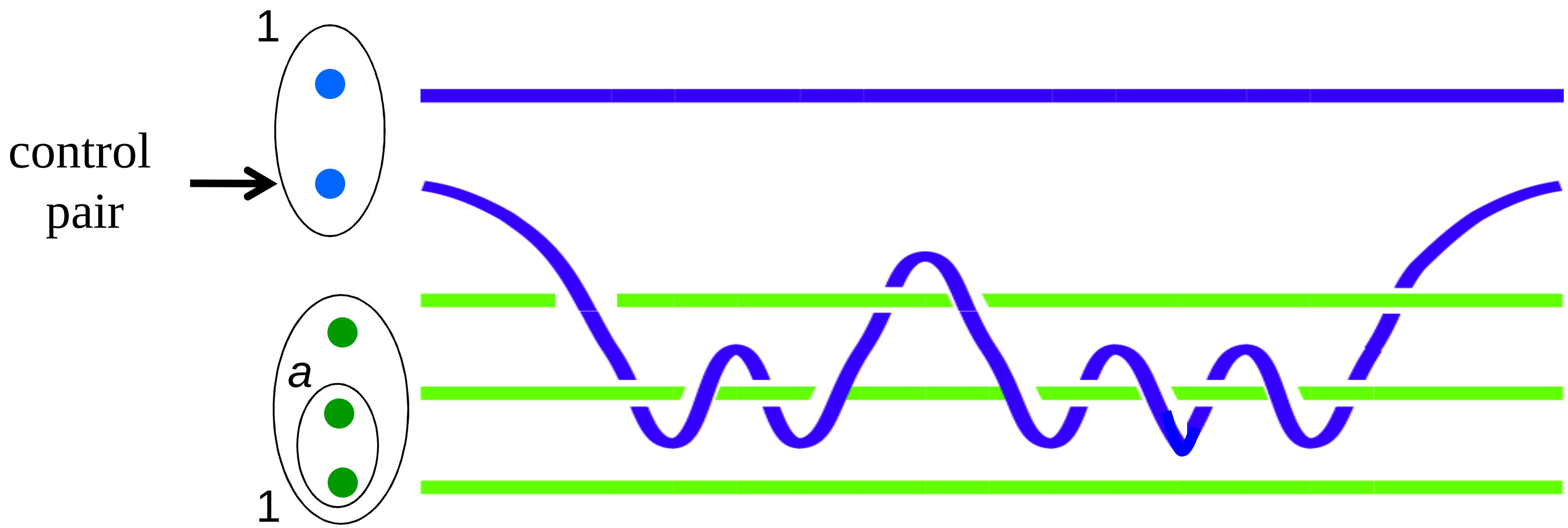
Only nontrivial case is when the control pair has q-spin 1.



We’ve reduced the problem to weaving one anyon around three others. **Still too hard for brute force approach!**

Try Weaving Around Just Two Anyons

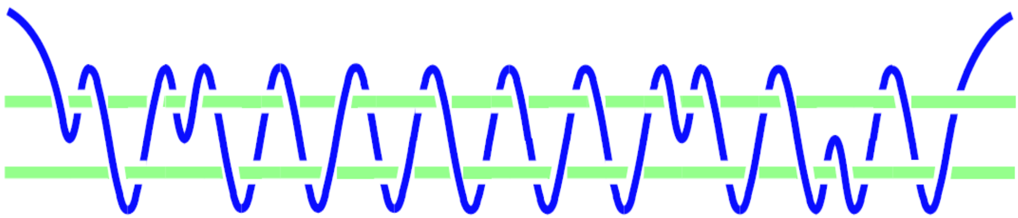
We're back to B_3, so this is numerically feasible.



Question: Can we find a weave which does not lead to **leakage errors**?

A Trick: Effective Braiding

Actual Weaving | *Effective* Braiding

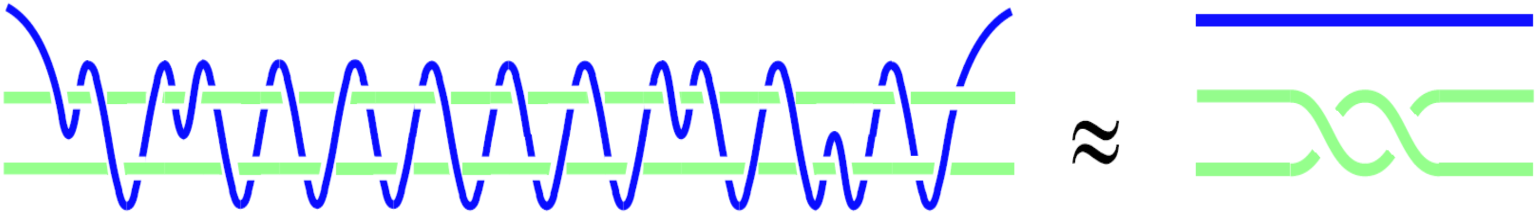


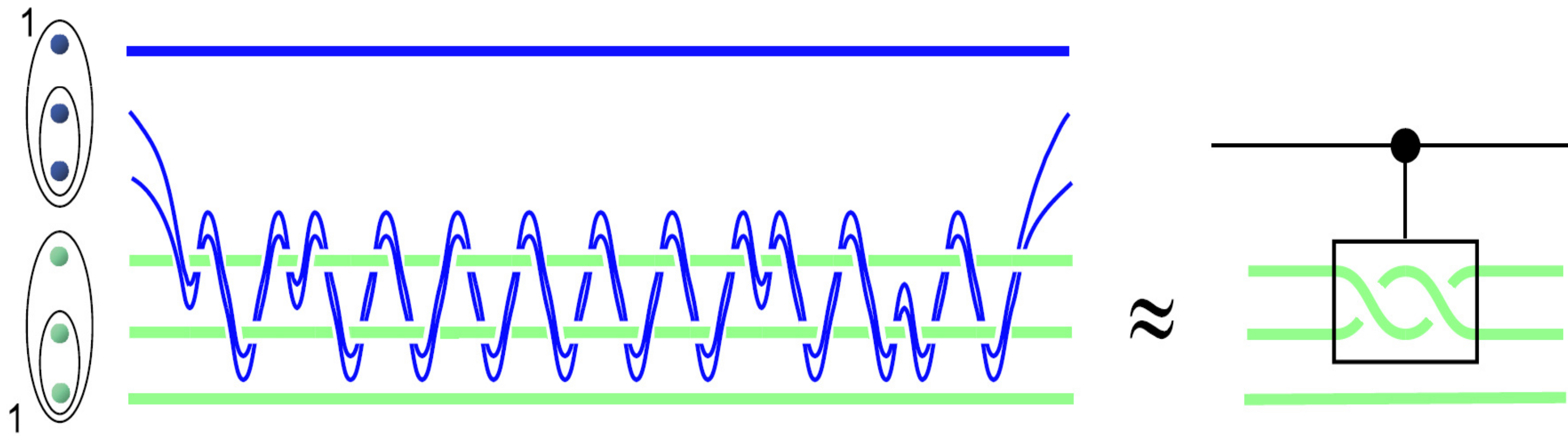
≈

$$\sigma_2^3\sigma_1^2\sigma_2^{-4}\sigma_1^2\sigma_2^2\sigma_1^{-2}\sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2\sigma_2^2\sigma_1^{-2}\sigma_2^2\sigma_1^{-2}\sigma_2^4\sigma_1^{-2}\sigma_2^2\sigma_1^4\sigma_2^2\sigma_1^{-2}\sigma_2 \approx \sigma_1^2$$

The effect of weaving the **blue anyon** through the two **green anyons** has approximately the same effect as braiding the two **green anyons** twice.

Controlled-“Knot” Gate

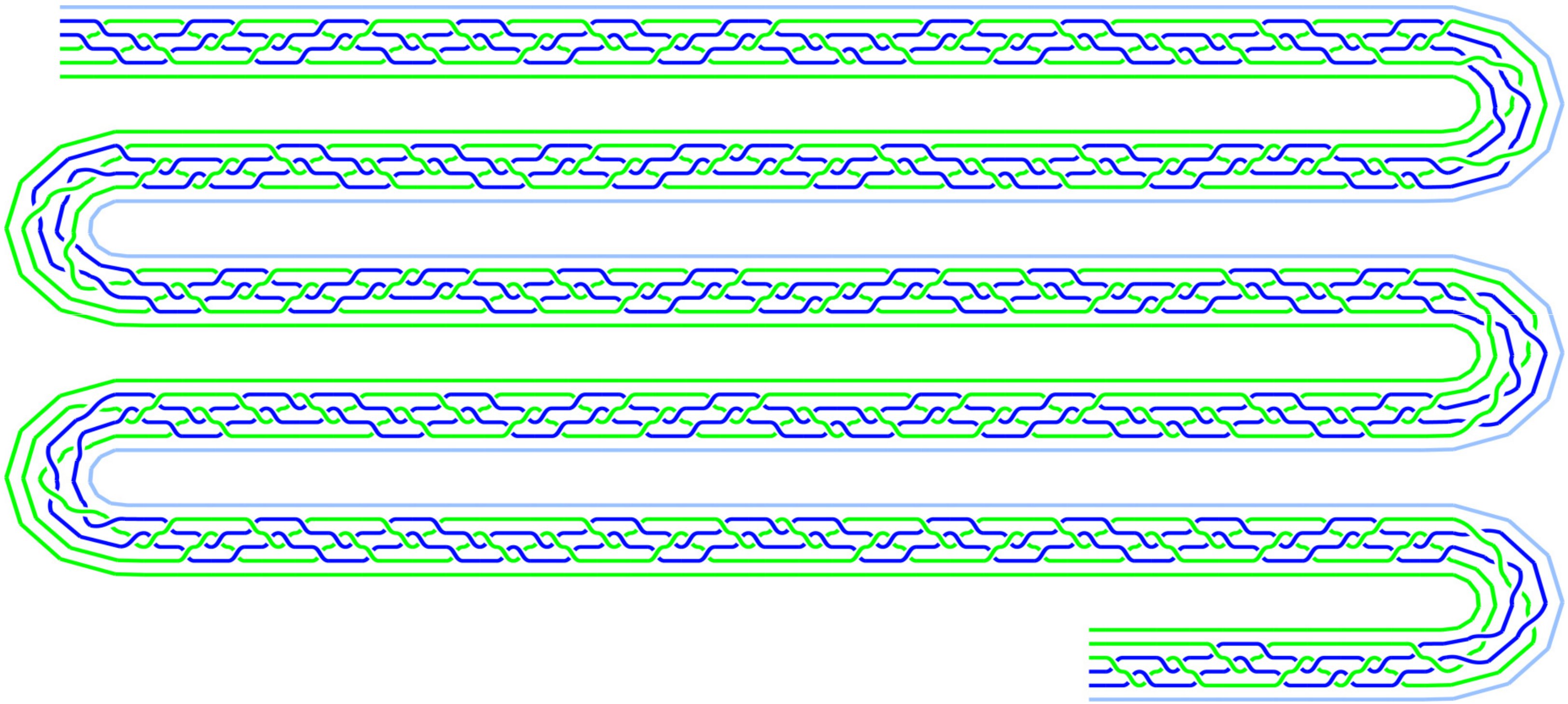




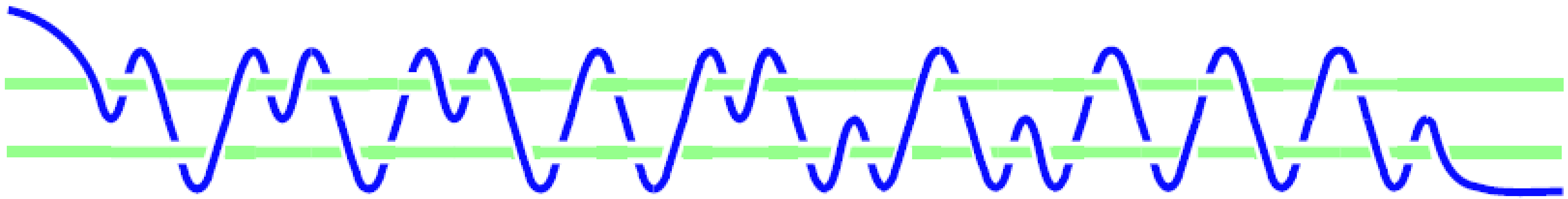
Effective braiding is all within the target qubit → No leakage!

Not a CNOT, but sufficient for universal quantum computation.

SK Improved Controlled-“Knot” Gate

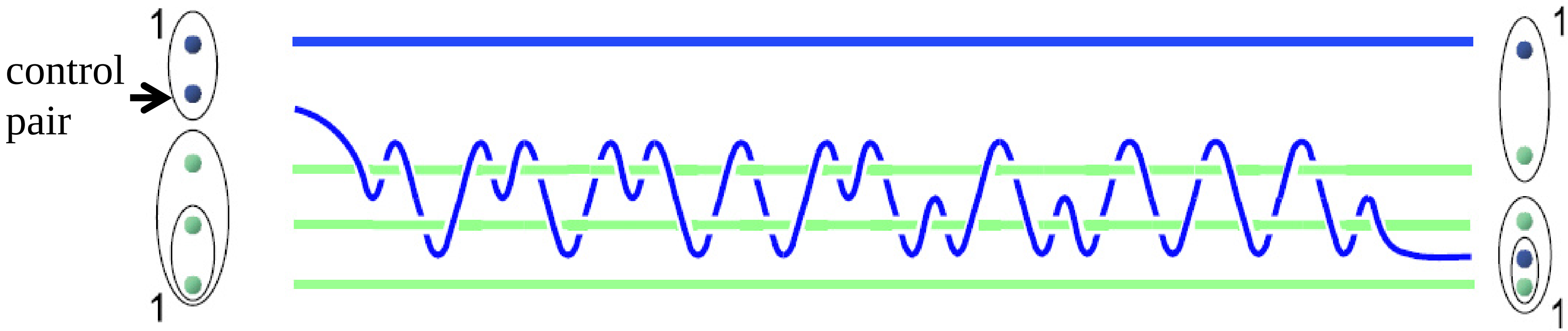


Another Trick: Injection Weaving

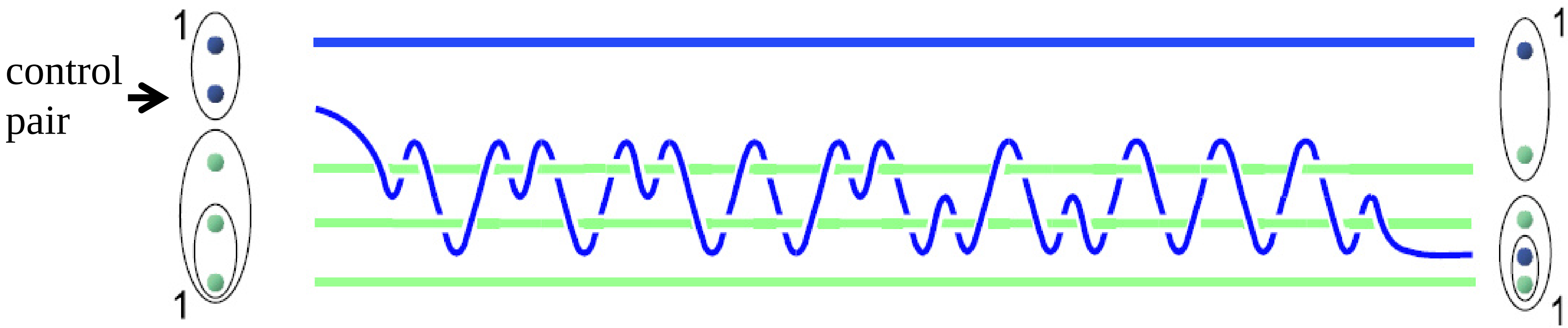


$$\sigma_2^{3}\sigma_1^{-2}\sigma_2^{-4}\sigma_1^{2}\sigma_2^{4}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{-2}\sigma_2^{-4}\sigma_1^{-4}\sigma_2^{-2}\sigma_1^{4}\sigma_2^{2}\sigma_1^{-2}\sigma_2^{2}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{3} \approx \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$

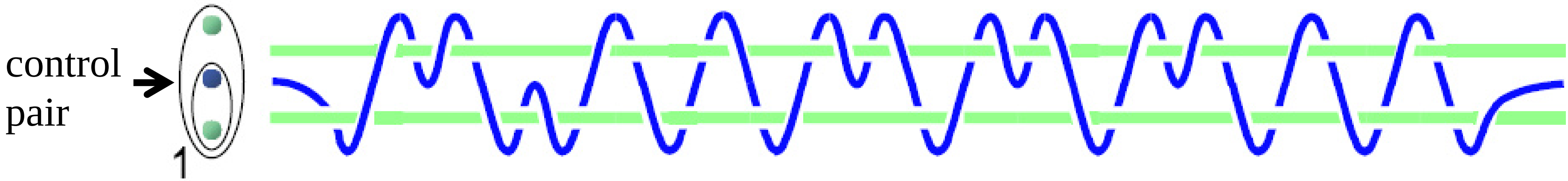
Step 1: Inject the control pair into the target qubit.



Another Trick: Injection Weaving



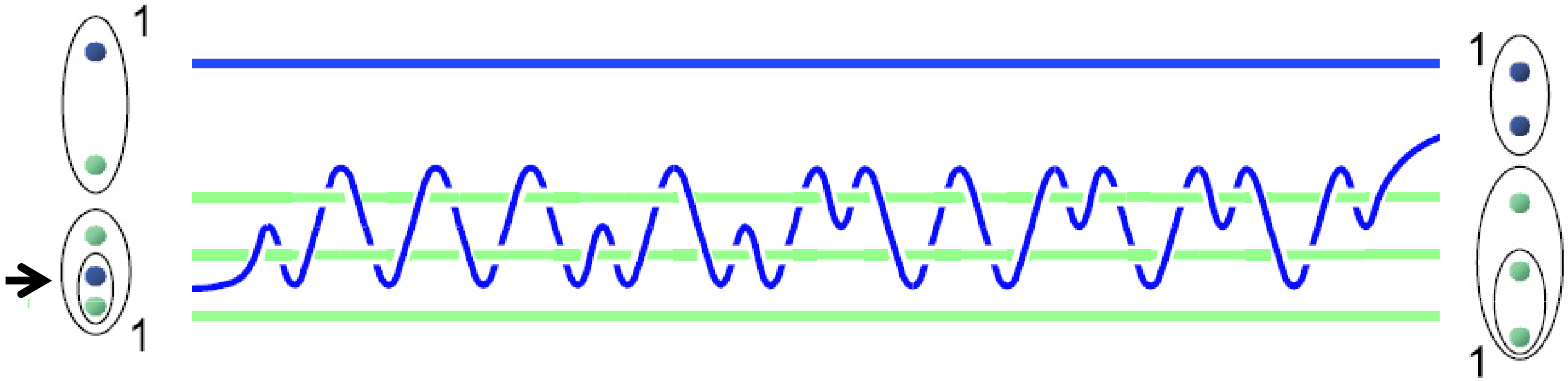
Step 2: Weave the control pair inside the injected target qubit.



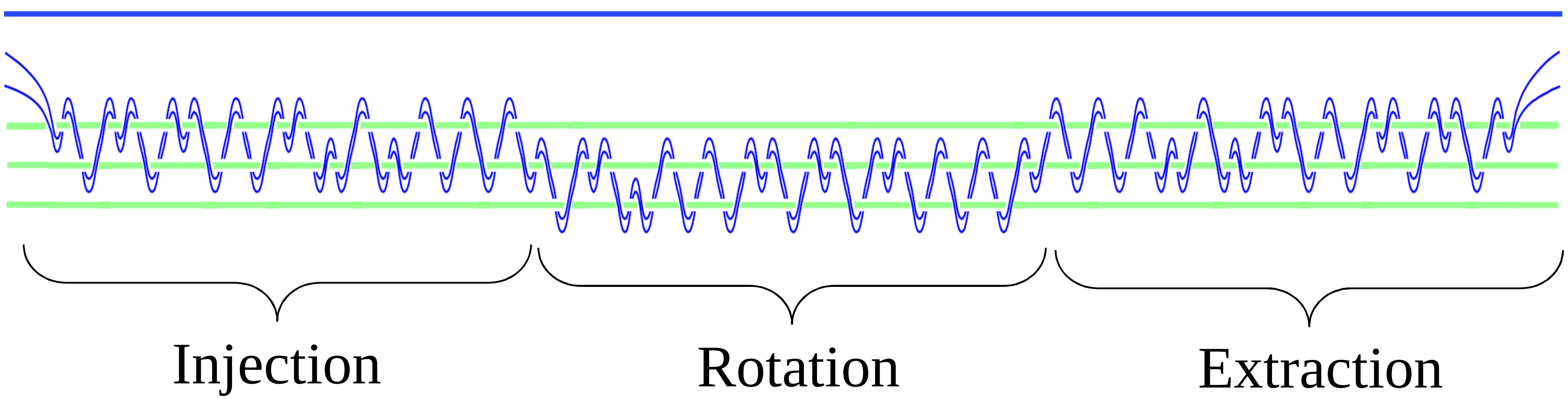
$$\sigma_1^{-2}\sigma_2^{-4}\sigma_1^{4}\sigma_2^{-2}\sigma_1^{2}\sigma_2^{2}\sigma_1^{-2}\sigma_2^{4}\sigma_1^{-2}\sigma_2^{4}\sigma_1^{2}\sigma_2^{-4}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{2}\sigma_2^{-2}\sigma_1^{-2} \approx \left(\begin{array}{cc|c} 0 & i & 0 \\ i & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$

Another Trick: Injection Weaving

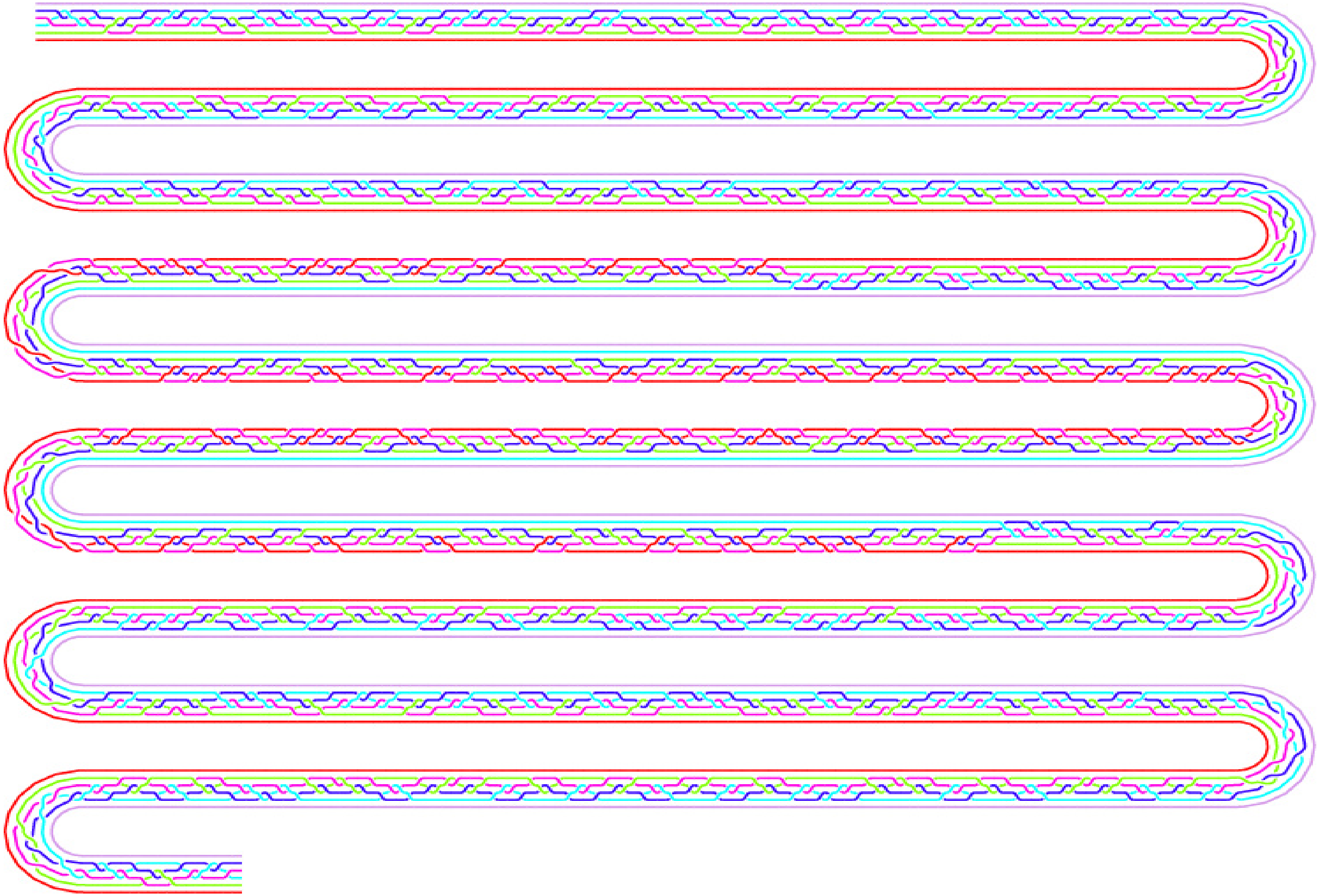
Step 3: Extract the control pair from the target using the inverse of the injection weave.



Putting it all together we have a CNOT gate:

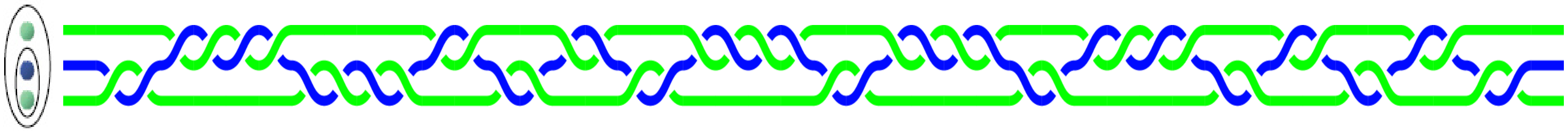


SK Improved Controlled-NOT Gate

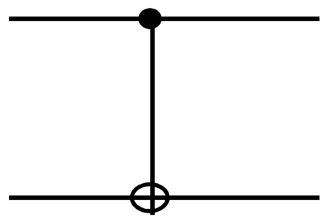


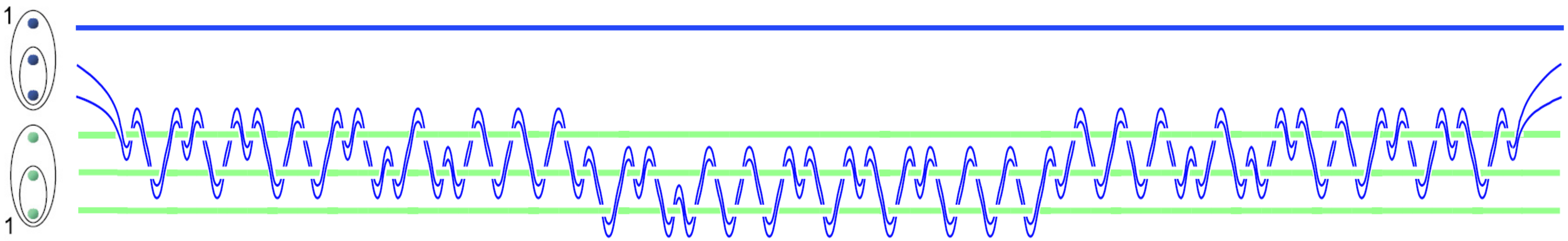
Universal Set of Gates

Single qubit rotations: $|\psi\rangle \;-\!\boxed{U_{\vec{\phi}}}\!-\; U_{\vec{\phi}}\,|\psi\rangle$



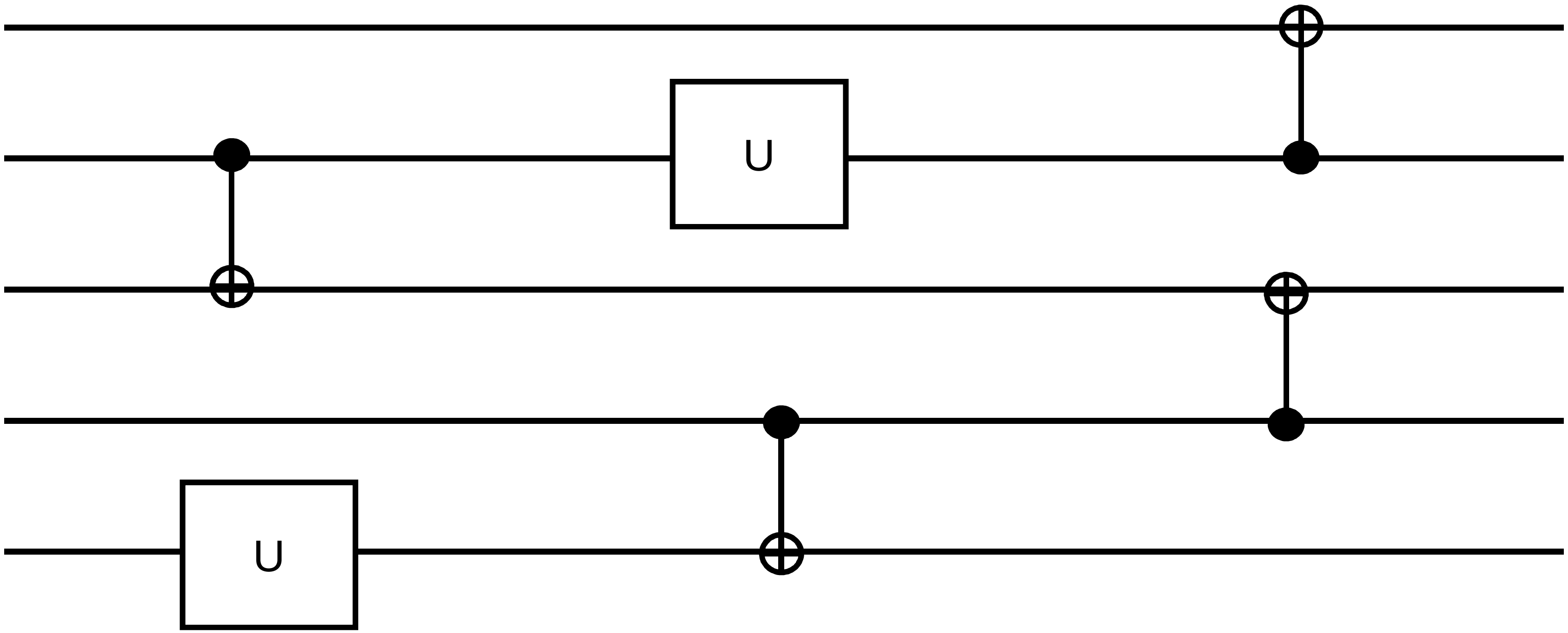
Controlled NOT:





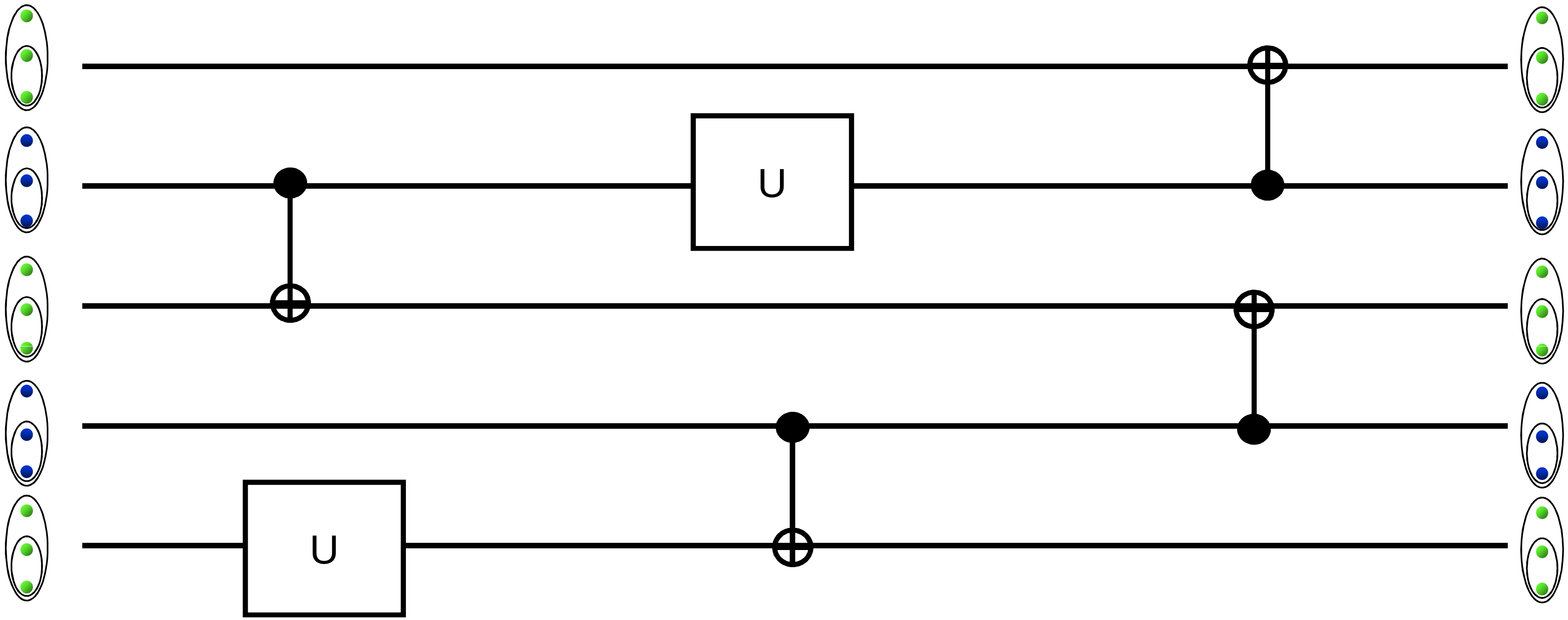
NEB, L. Hormozi, G. Zikos, S.H. Simon, Phys. Rev. Lett. 95 140503 (2005)

Quantum Circuit

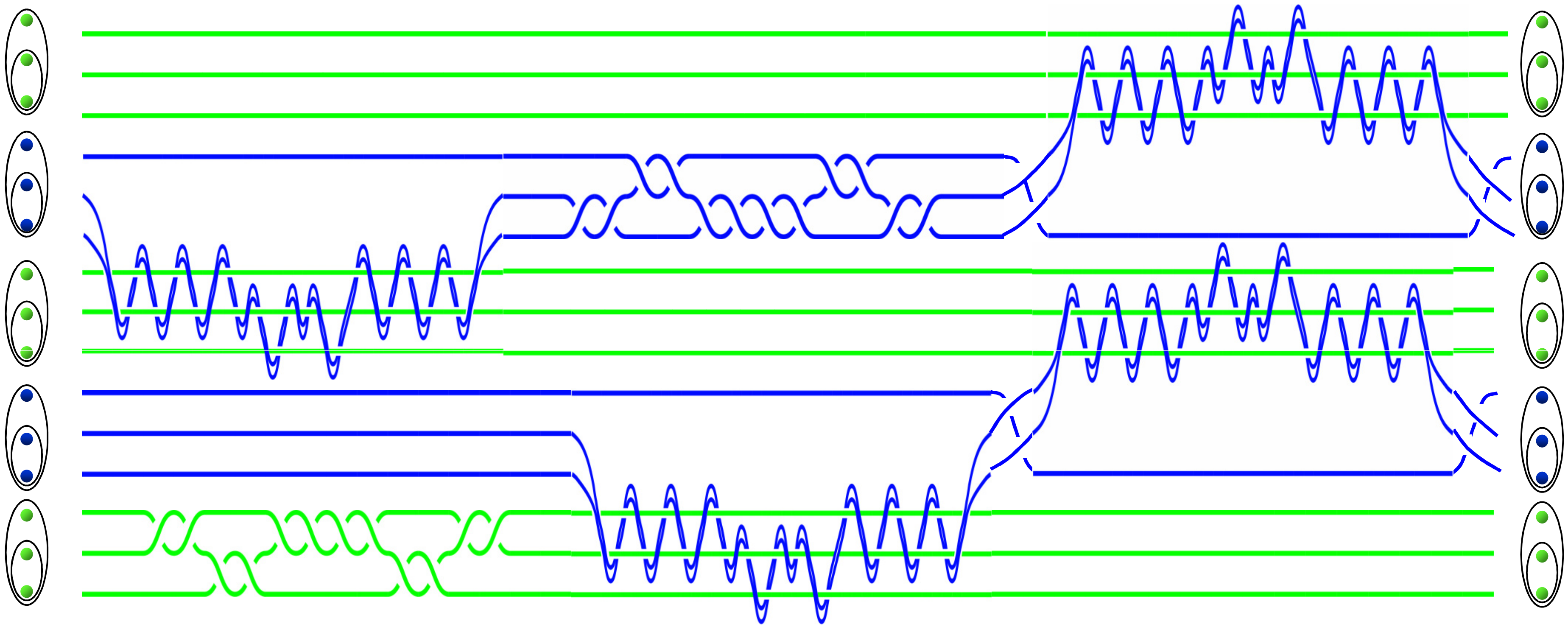


What braid corresponds to this circuit?

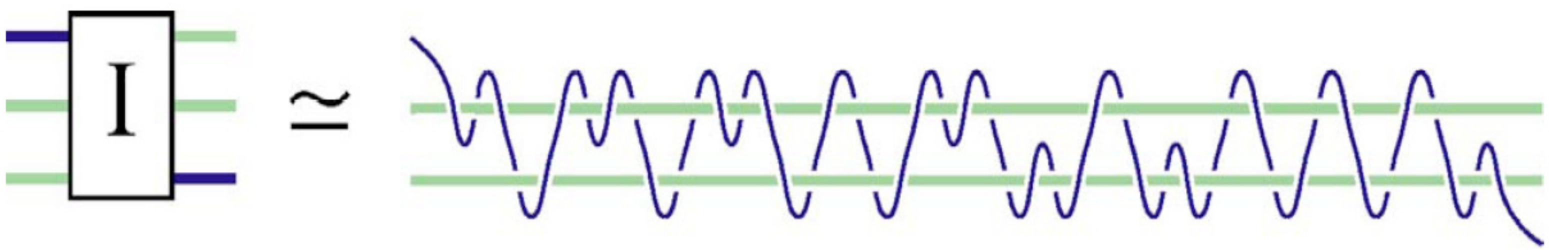
Quantum Circuit

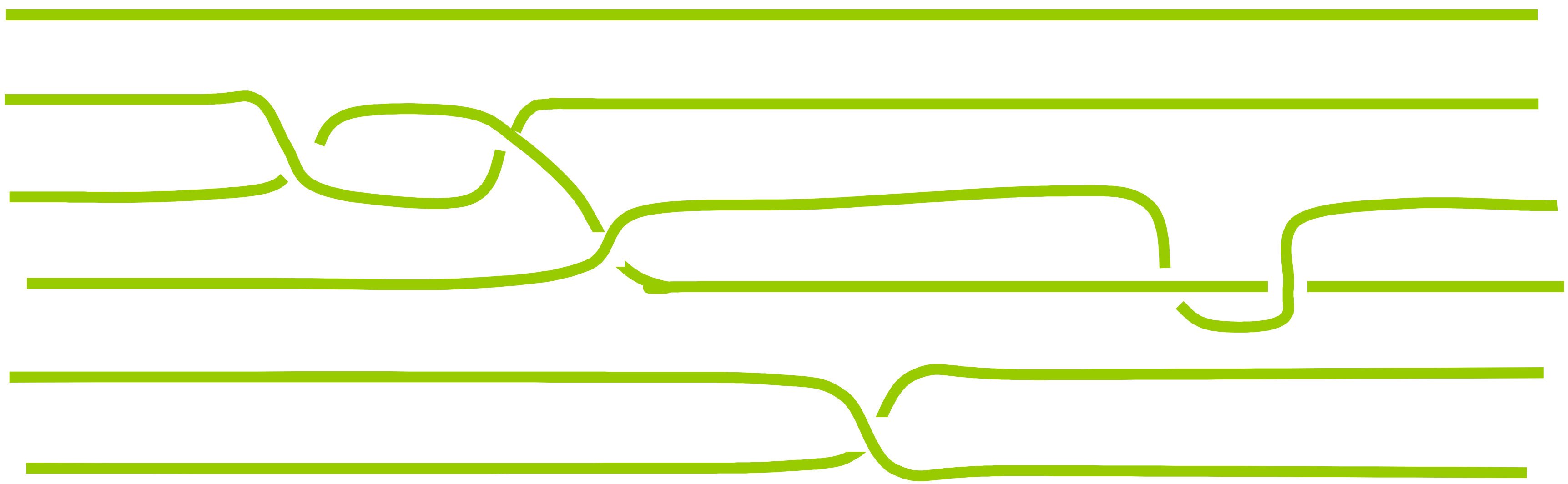


Braid

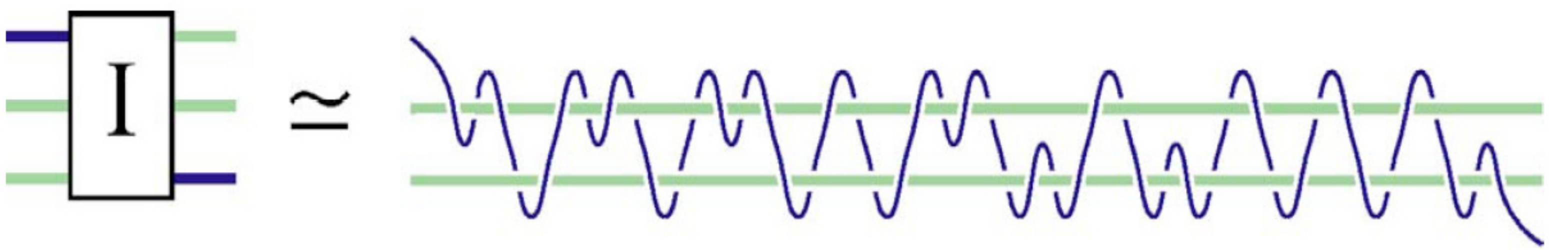


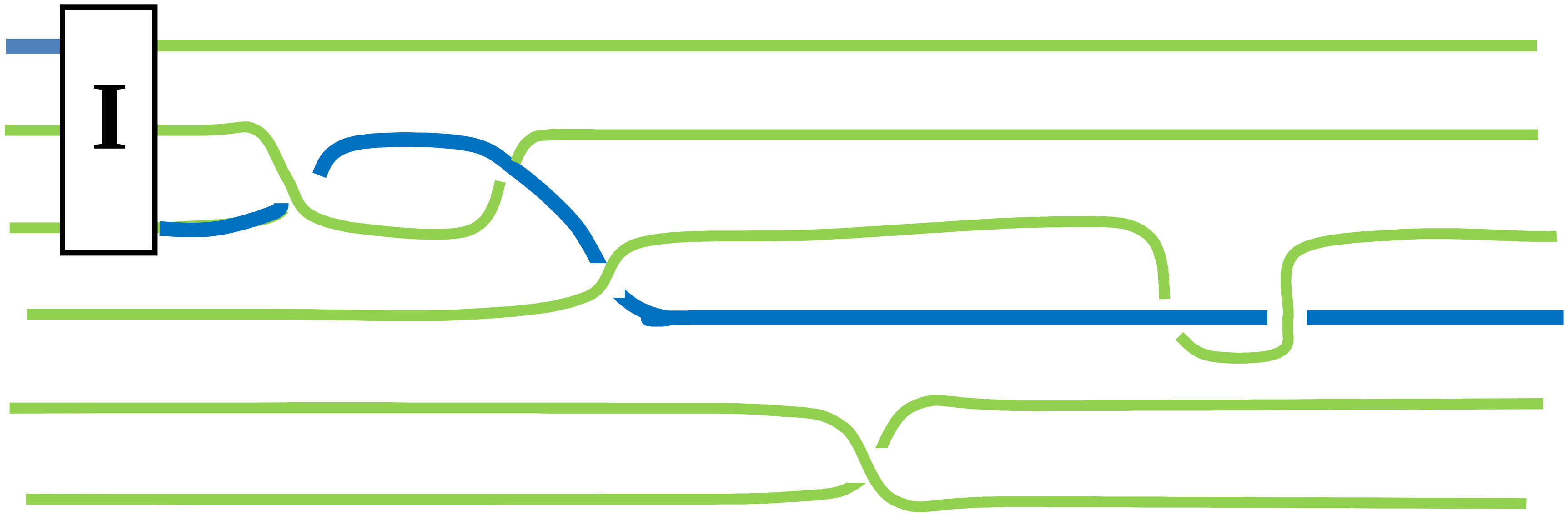
Turning any Braid into a Weave



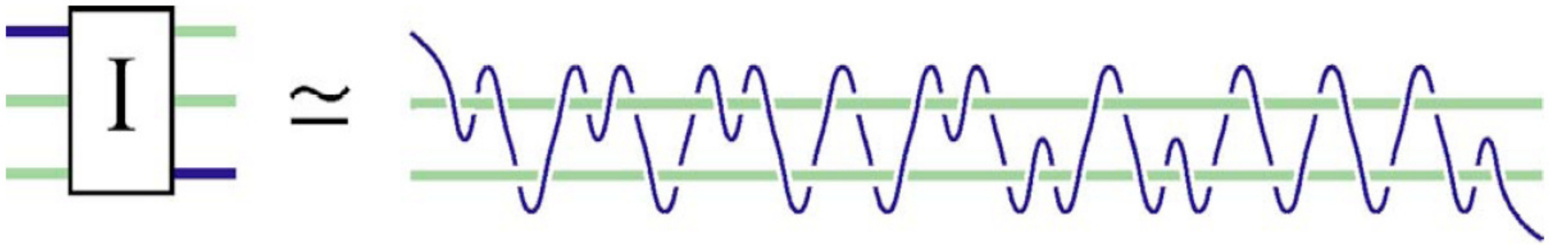


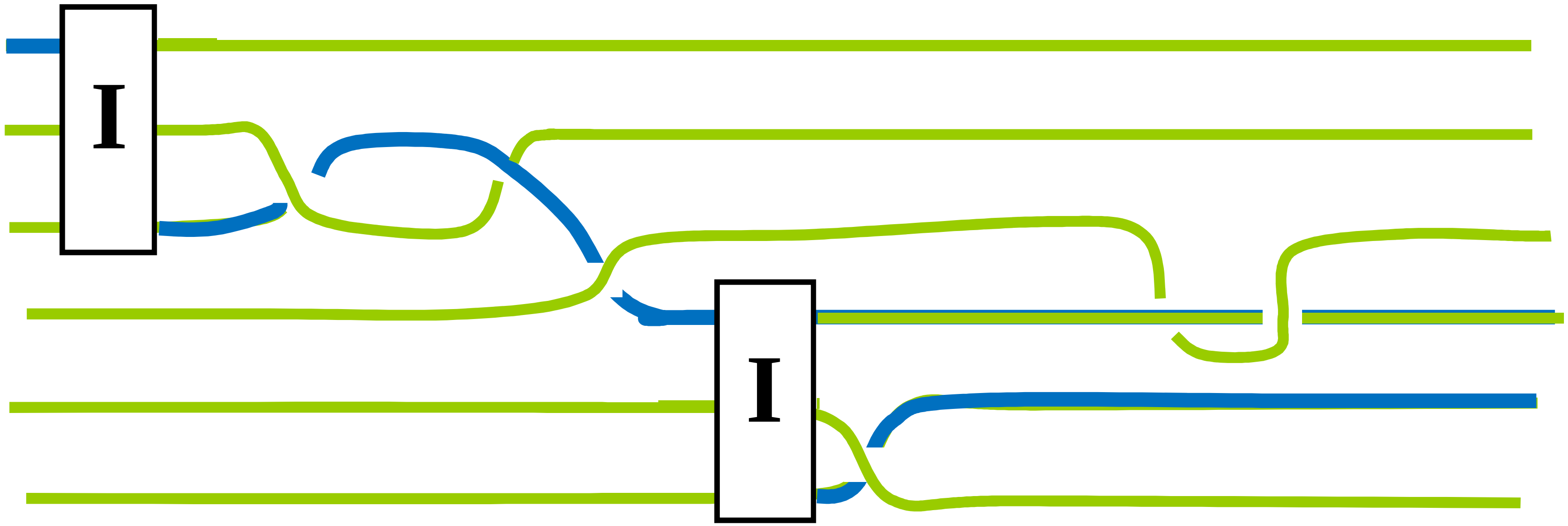
Turning any Braid into a Weave



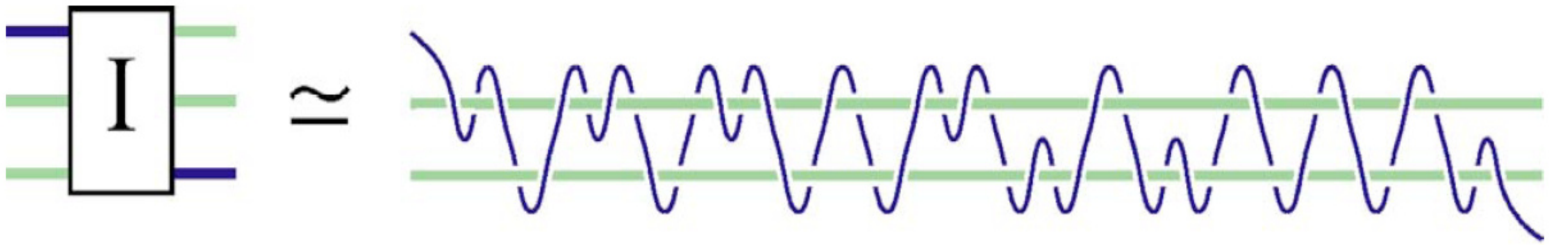


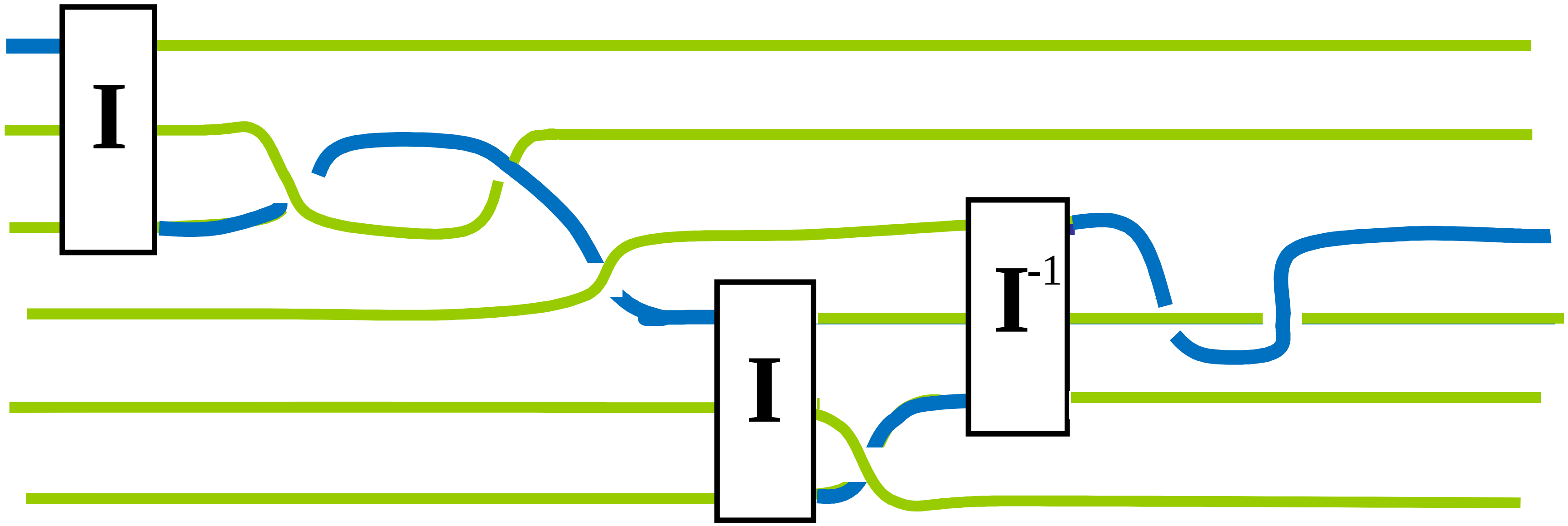
Turning any Braid into a Weave



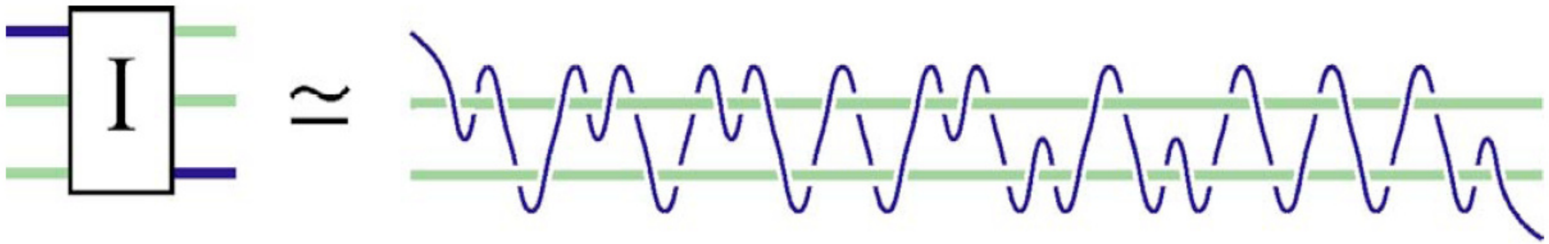


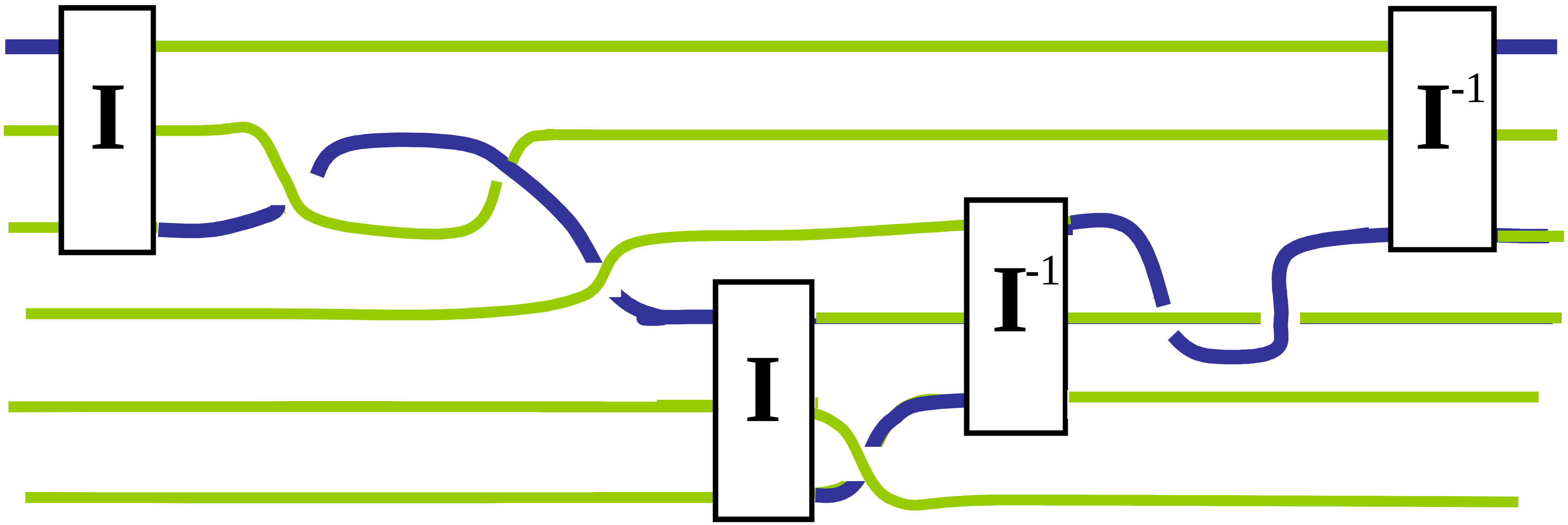
Turning any Braid into a Weave





Turning any Braid into a Weave





PRL **96,** 070503 (2006) PHYSICAL REVIEW LETTERS week ending 24 FEBRUARY 2006

Topological Quantum Computing with Only One Mobile Quasiparticle

S. H. Simon,[1] N. E. Bonesteel,[2] M. H. Freedman,[3] N. Petrovic,[1] and L. Hormozi[2]
[1]*Bell Laboratories, Lucent Technologies, 700 Mountain Avenue, Murray Hill, New Jersey 07974, USA*
[2]*Department of Physics and NHMFL, Florida State University, Tallahassee, Florida 32310, USA*
[3]*Microsoft Research, One Microsoft Way, Redmond, Washington 98052, USA*

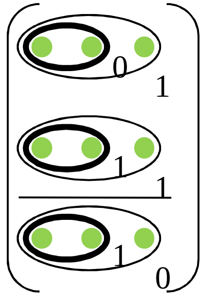
We know it is possible to carry out universal quantum computation by moving only a *single* particle.

Can we find an efficient CNOT construction in which only a single particle is woven through the other particles?

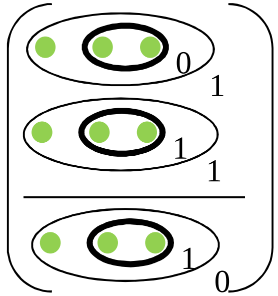
Another Useful Braid: The F-Braid

F-Matrix:

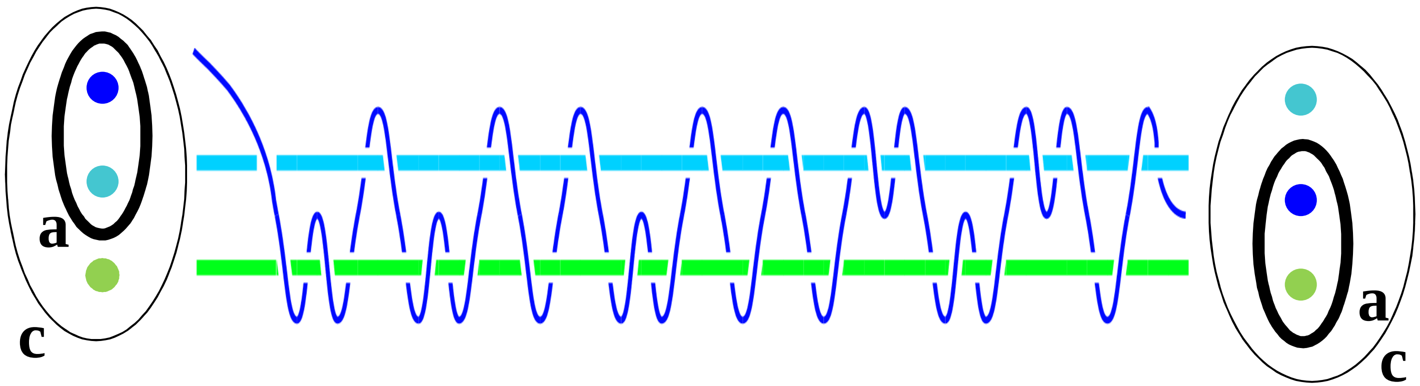
$$\left(\begin{array}{cc|c} \tau & \sqrt{\tau} & 0 \\ \sqrt{\tau} & -\tau & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$



=

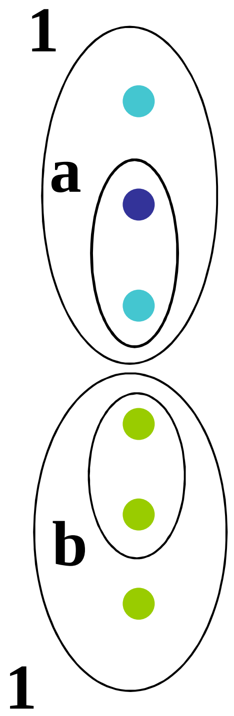


F-Braid:

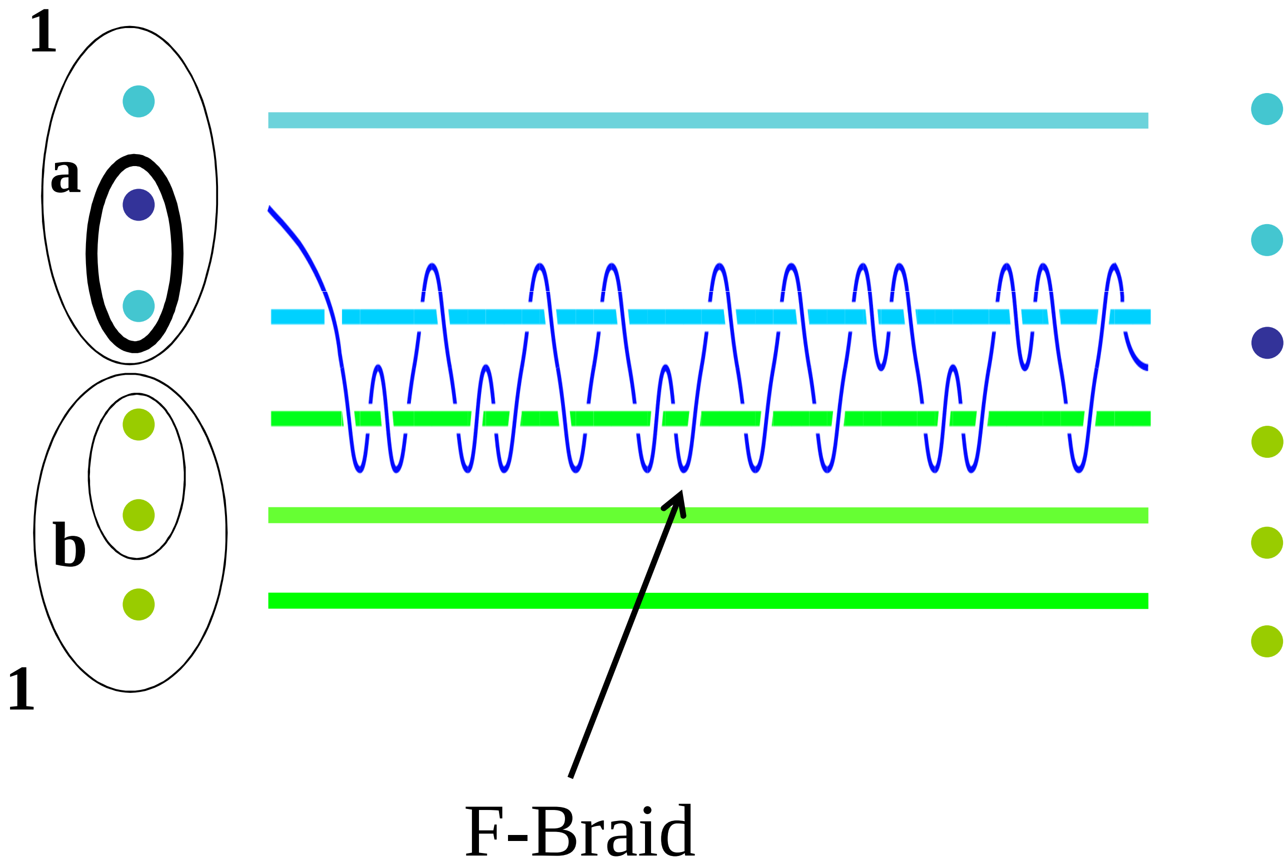


$$\sigma_2^1\sigma_1^4\sigma_2^2\sigma_1^{-4}\sigma_2^2\sigma_1^2\sigma_2^2\sigma_1^{-4}\sigma_2^2\sigma_1^{-2}\sigma_2^2\sigma_1^{-2}\sigma_2^4\sigma_1^{-4}\sigma_2^4\sigma_1^{-2}\sigma_2^{-2} \approx i\left(\begin{array}{cc|c} \tau & \sqrt{\tau} & 0 \\ \sqrt{\tau} & -\tau & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$

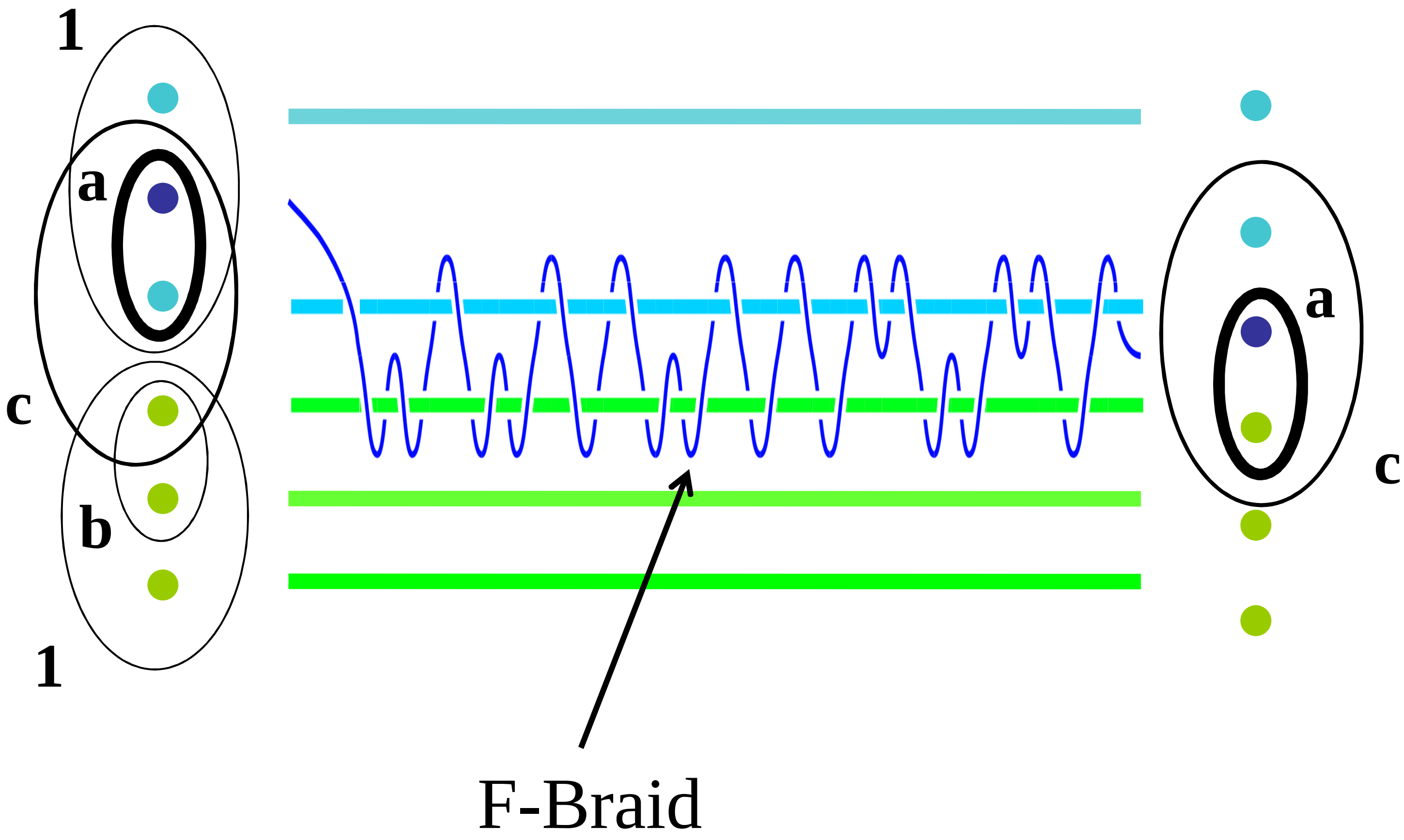
Single Particle Weave Gate: Part 1



Single Particle Weave Gate: Part 1

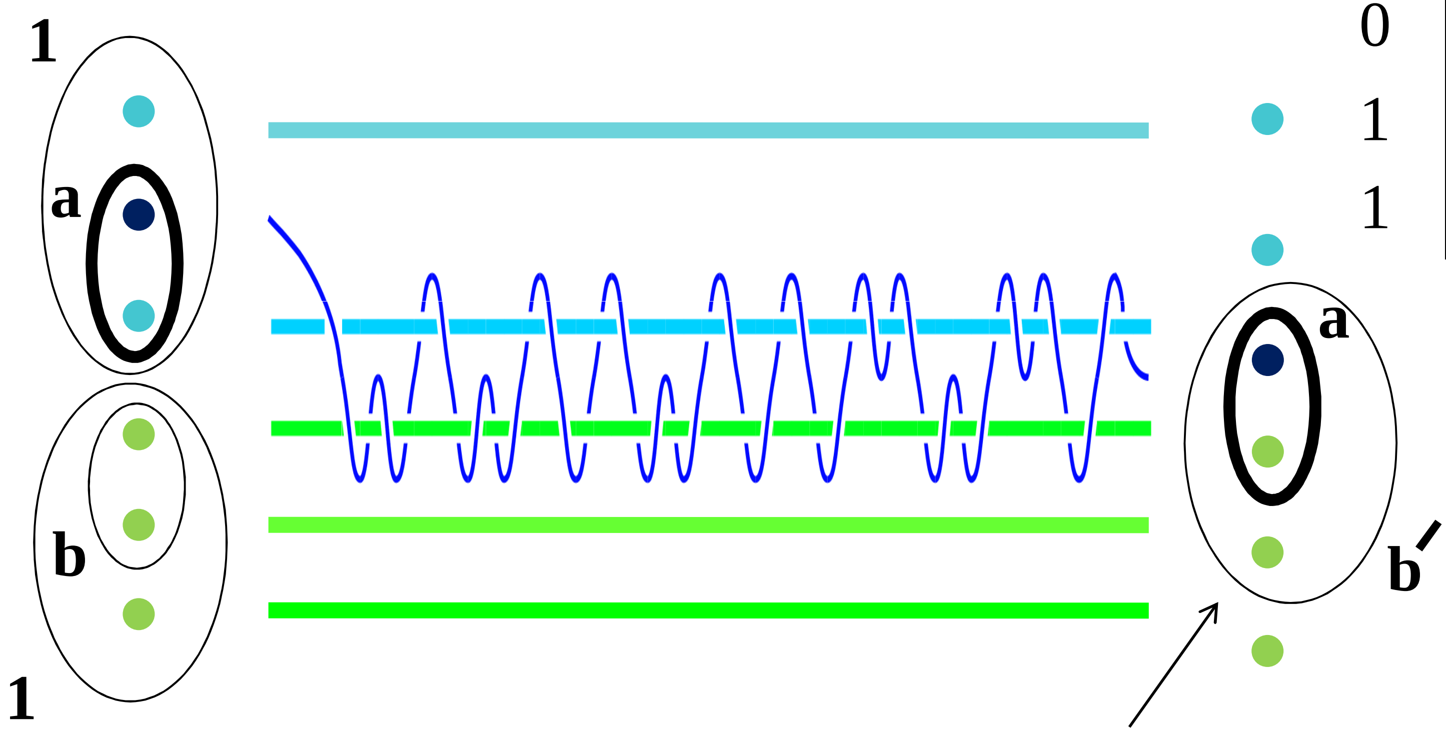


Single Particle Weave Gate: Part 1



Single Particle Weave Gate: Part 1

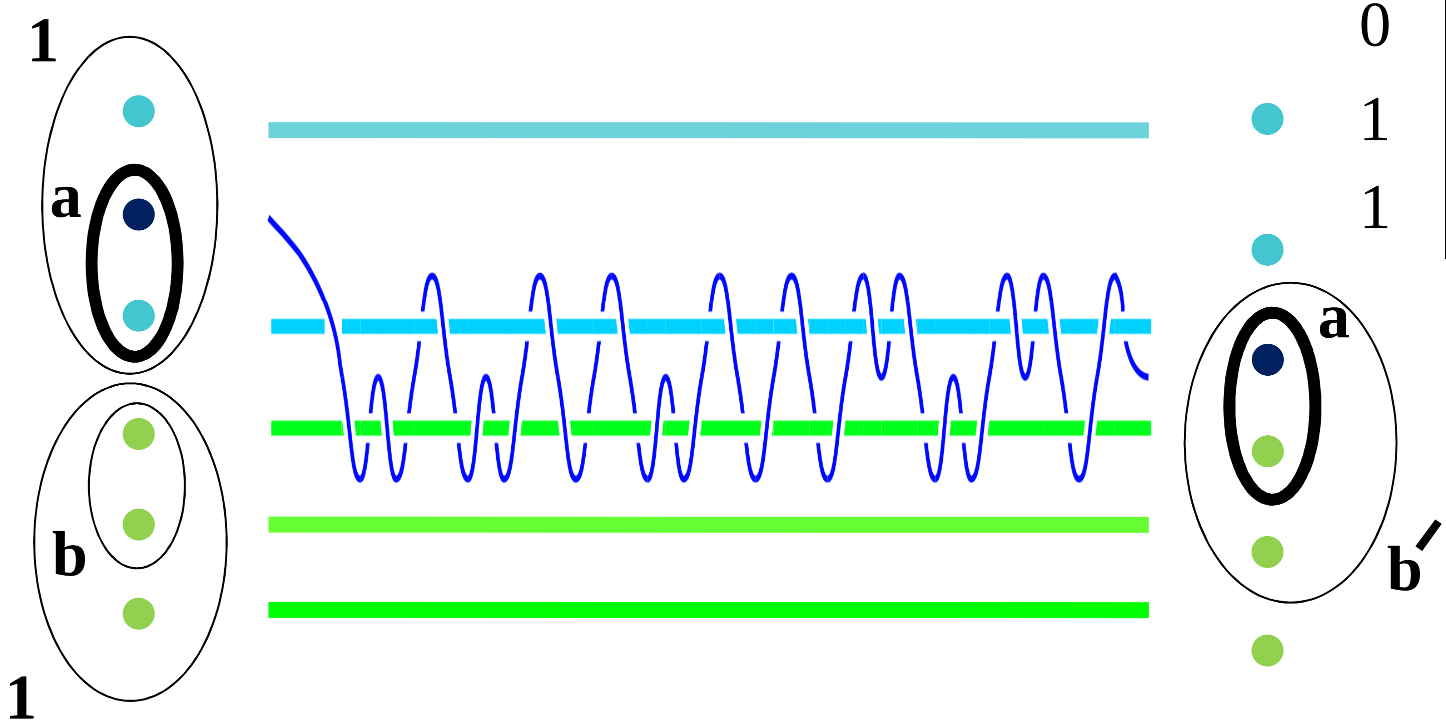
a	b	b′
0	0	1
0	1	1
1	0	0
1	1	1



Intermediate State

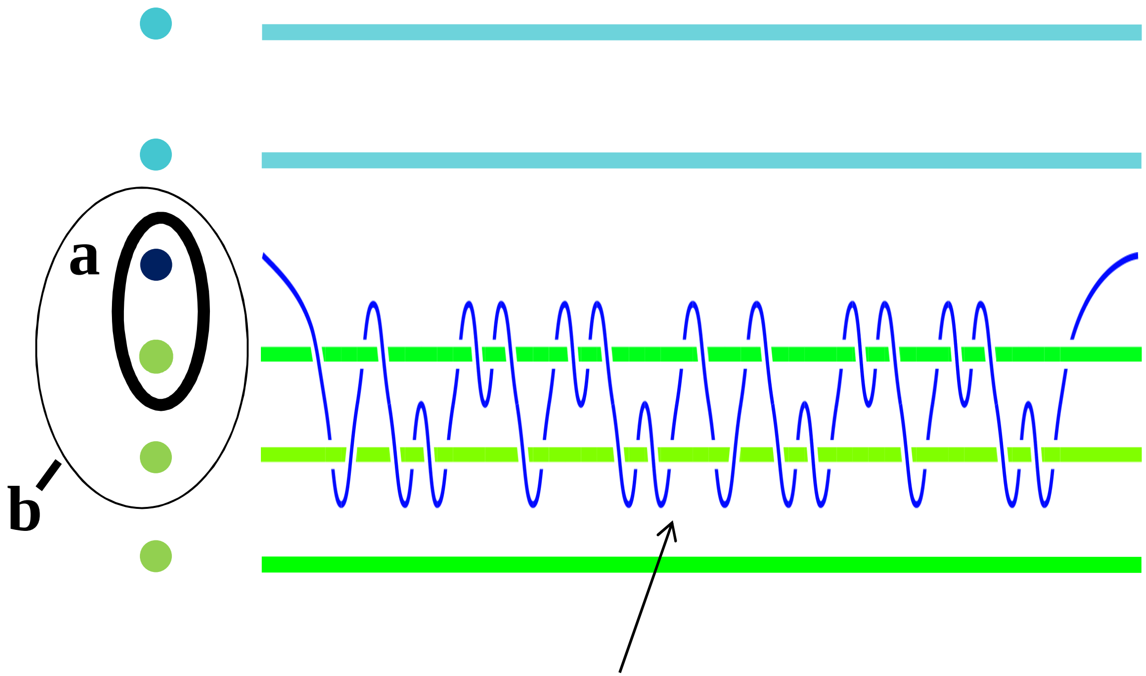
Single Particle Weave Gate: Part 1

a	b	b′
0	0	1
0	1	1
1	0	0
1	1	1



Single Particle Weave Gate: Part 2

a	b	b'	Phase
0	0	1	-1
0	1	1	-1
1	0	0	+1
1	1	1	-1

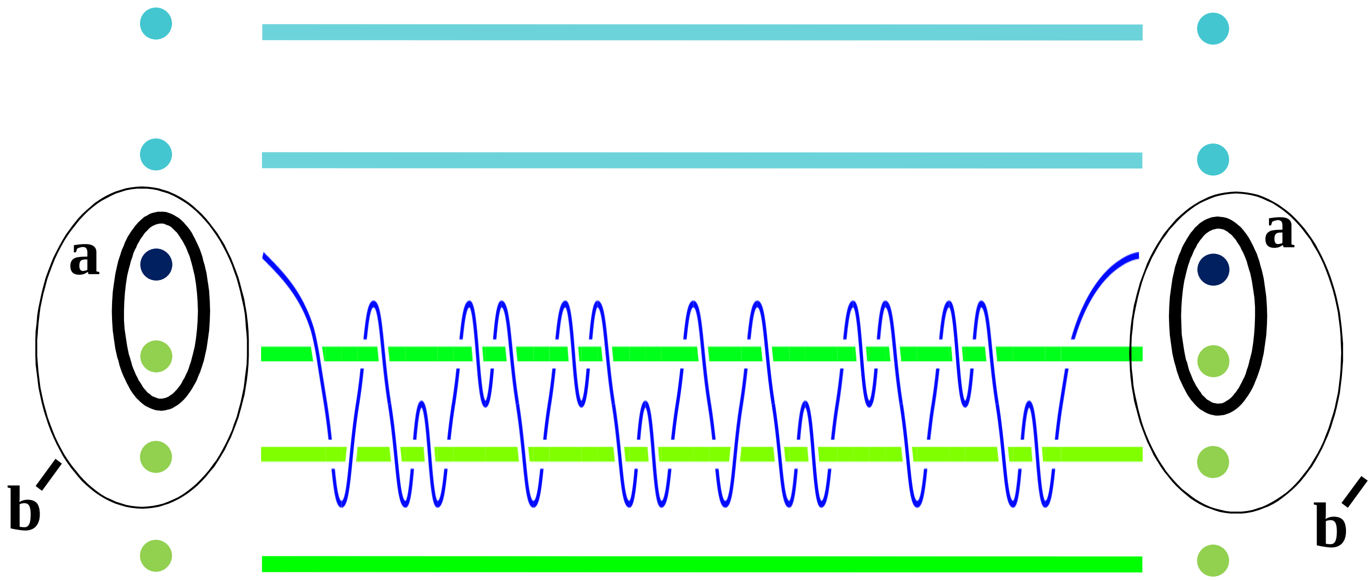


$$\approx \begin{array}{c} \overbrace{\qquad\qquad}^{b'=1}\ \overbrace{\quad}^{b'=0} \\ \left(\begin{array}{cc|c} -1 & 0 & 0 \\ 0 & -1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \end{array}$$

Phase Braid

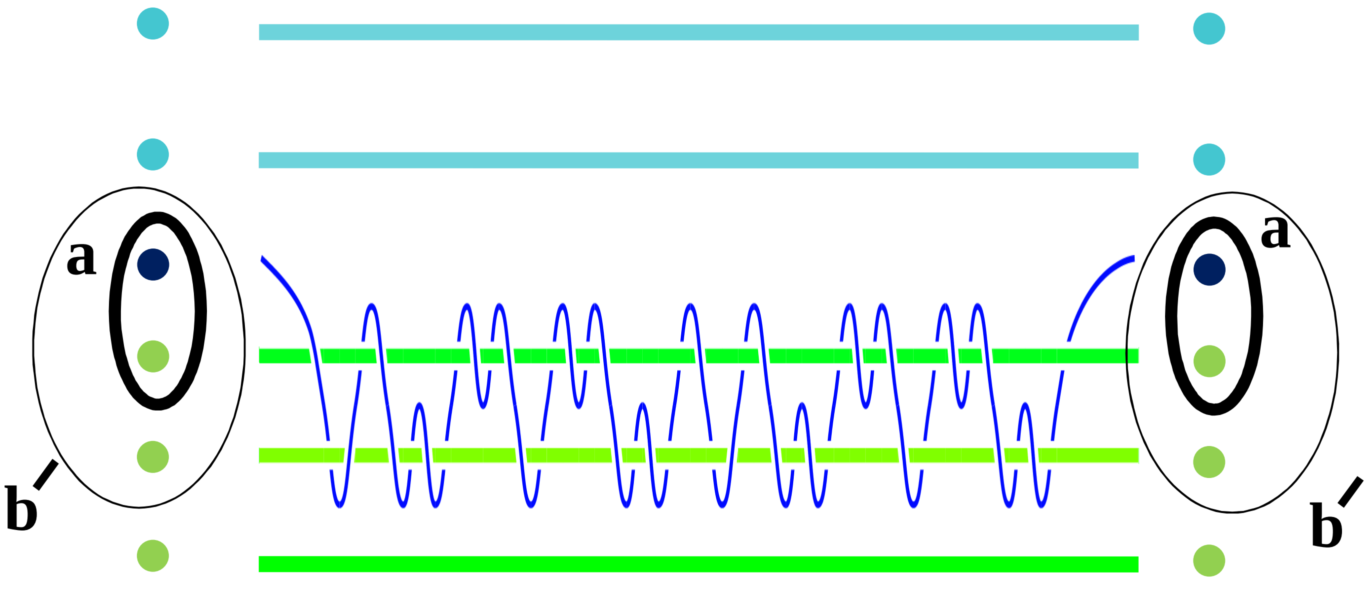
Single Particle Weave Gate: Part 2

a	b	b′	
0	0	1	-1
0	1	1	-1
1	0	0	+1
1	1	1	-1



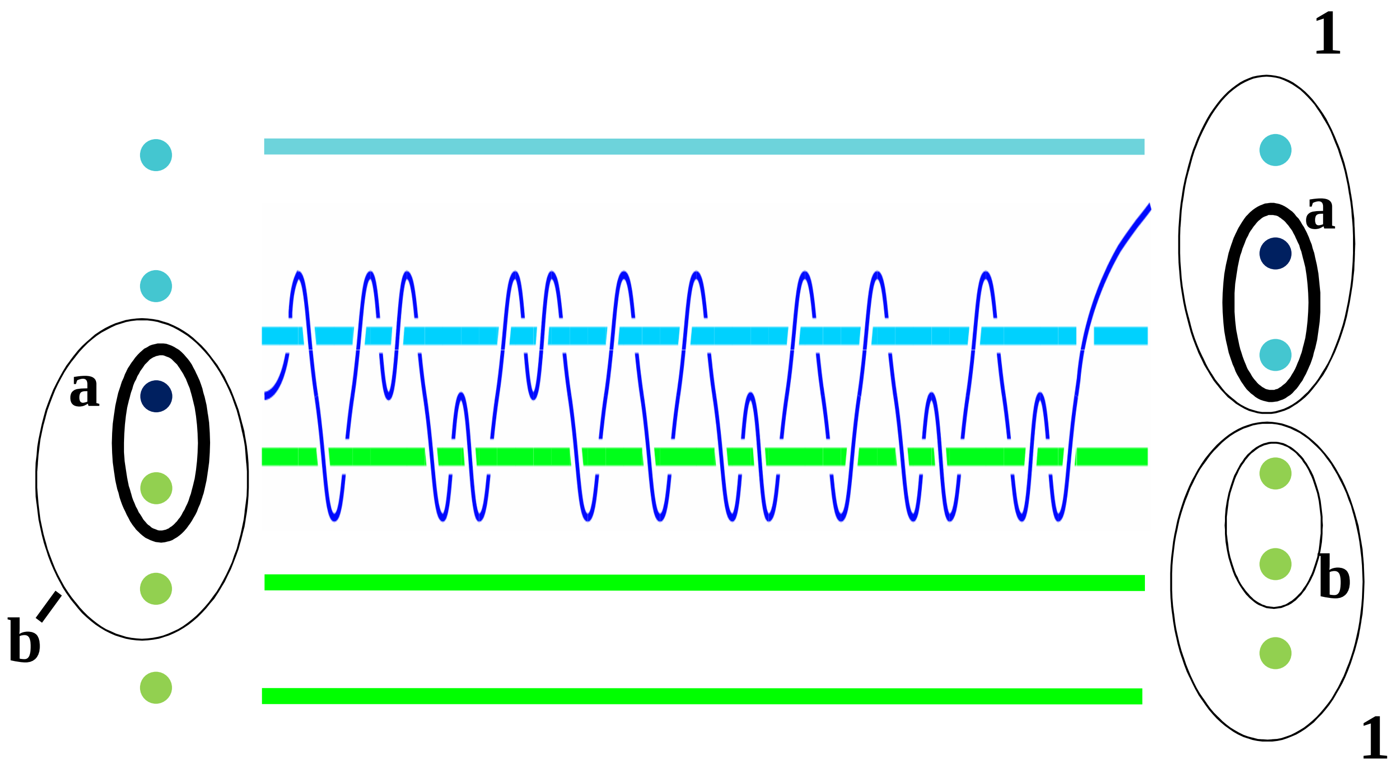
Single Particle Weave Gate: Part 2

a	b	b′	Phase
0	0	1	-1
0	1	1	-1
1	0	0	+1
1	1	1	-1

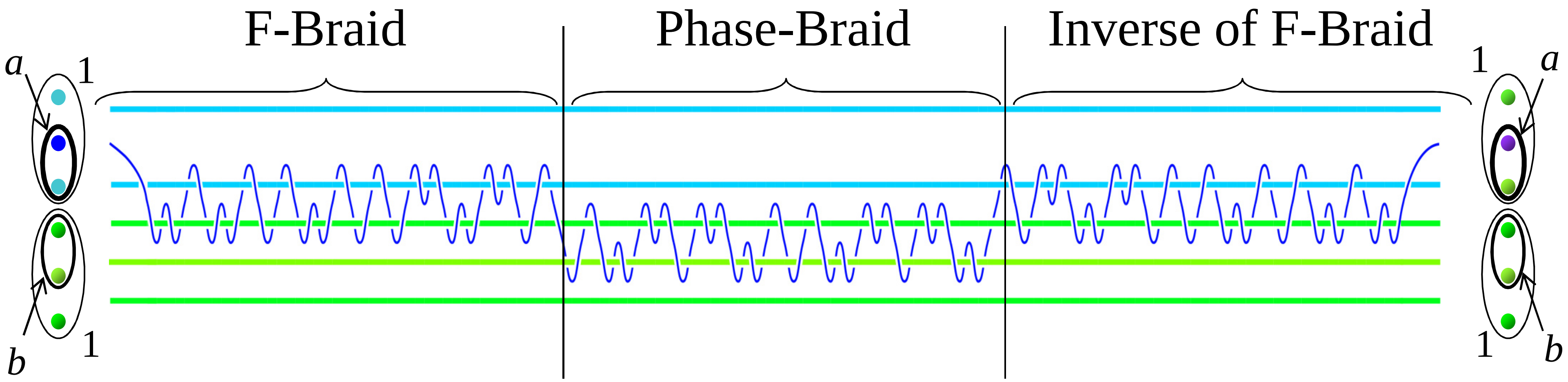


Single Particle Weave Gate: Part 3

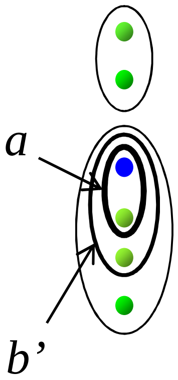
a	b	b′	Phase
0	0	1	-1
0	1	1	-1
1	0	0	+1
1	1	1	-1



Controlled-Phase Gate



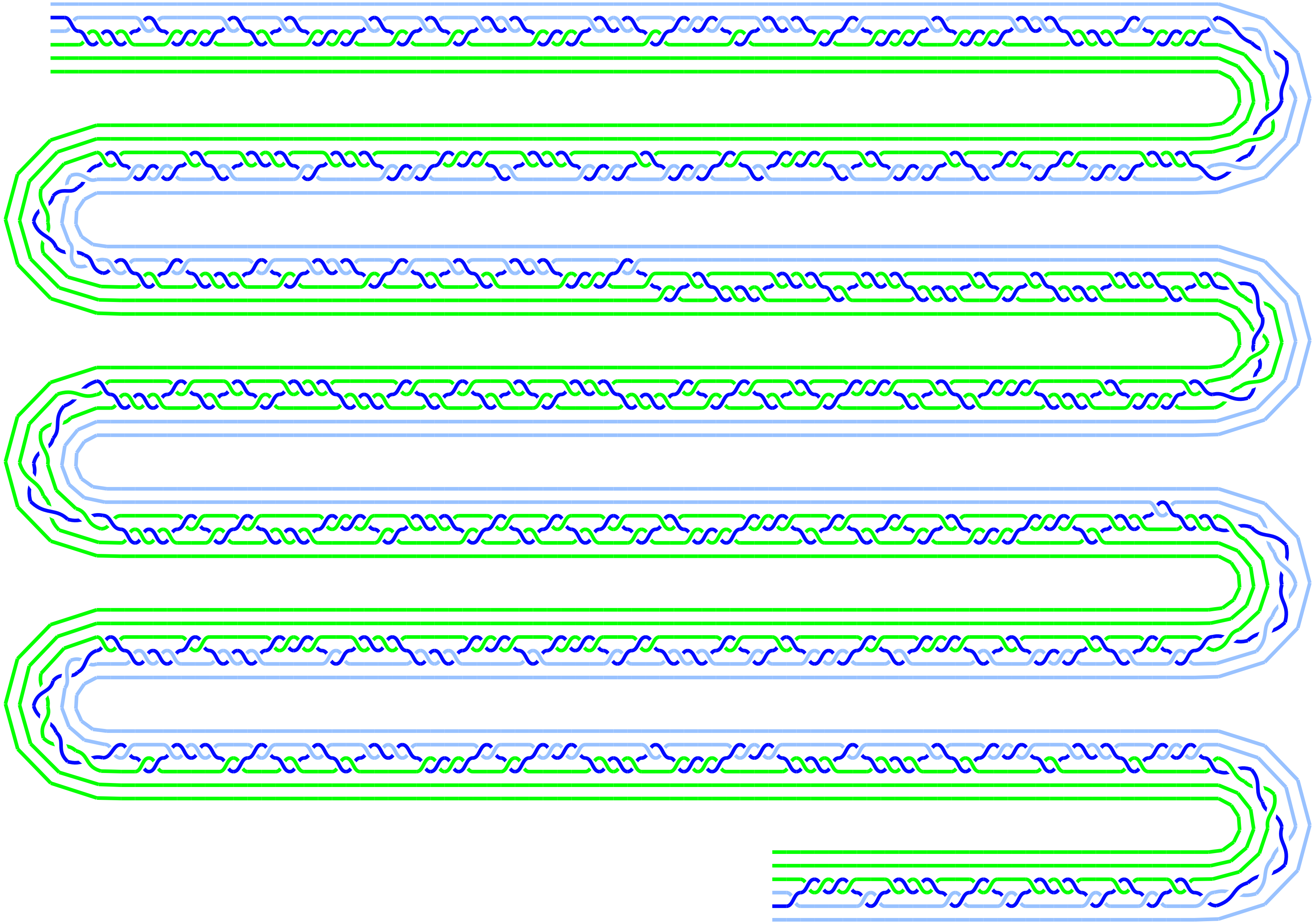
Intermediate state



Final result

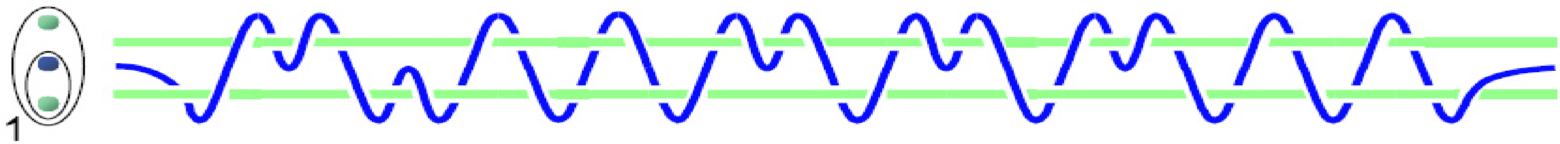
$$U = -\left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) + O(10^{-3})$$

SK Improved Controlled-Phase Gate

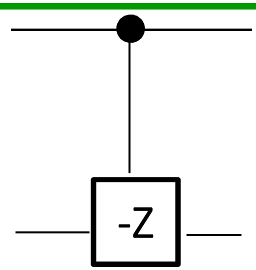


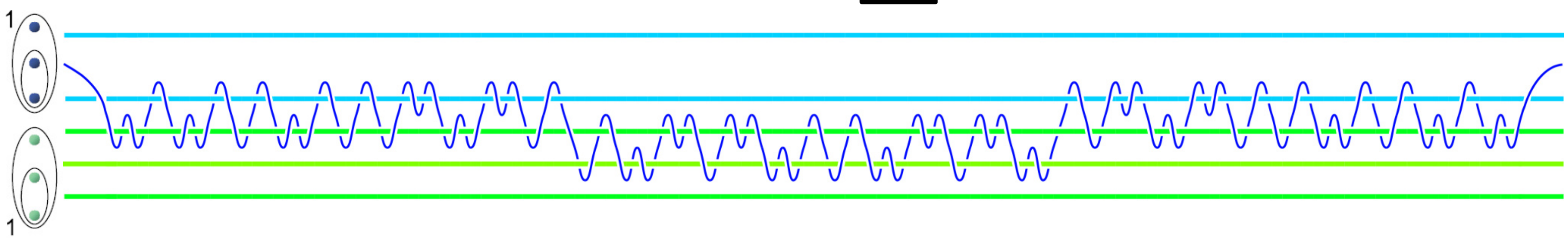
Universal "One-Particle Weave" Gates

Single qubit rotations: $|\psi\rangle \;-\!\boxed{U_{\vec{\phi}}}\!-\; U_{\vec{\phi}}\,|\psi\rangle$



Controlled-Phase gate:





L. Hormozi, G. Zikos, NEB, and S.H. Simon, Phys. Rev. B 75, 165310 (2007).

How Big is Shor's Braid?

How many elementary braids are required to factor a K-bit number N using Shor's algorithm?

Bottleneck: Modular Exponentiation requires ~ K^3 gates.

$$U_{\mathrm{mod\,exp}} \left|a\right\rangle_i \left|0\right\rangle_o = \left|a\right\rangle_i \left|x^a \,(\mathrm{mod}\, N)\right\rangle_o$$

Specific requirements:

~ 3 K Qubits

~ 40 K^3 NOT gates

~ 28 K^3 CNOT gates

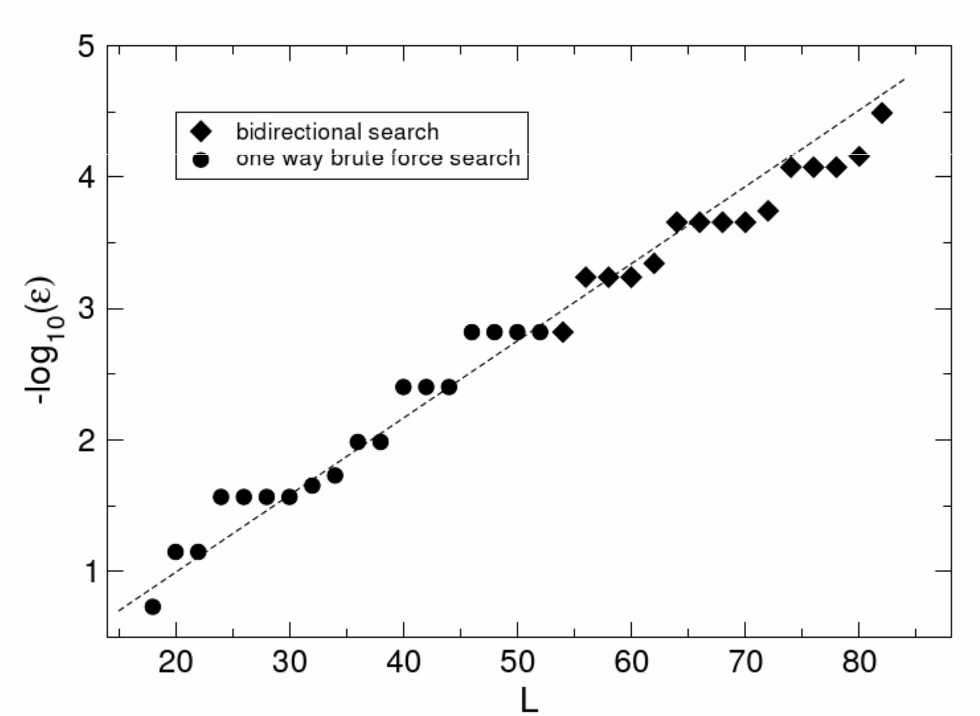
~ 92 K^3 CCNOT (Toffoli) gates

Beckman, Chari, Devabhaktuni, Preskill, PRA 54, 1034 (1996).

Quantum Gates for Modular Exp

NOT Gate:

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



G. Zikos, et al., Int. J. Mod. Phys. B 23, 2727 (2009).

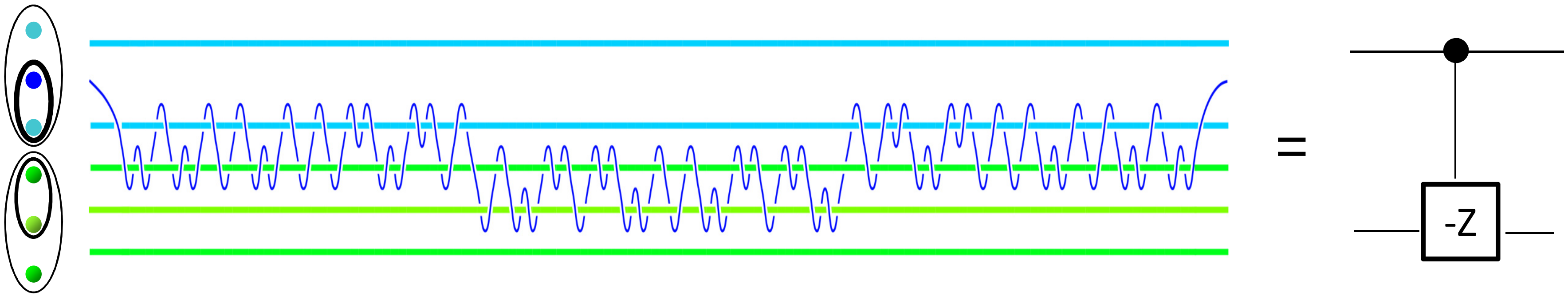
Length (measured in elementary braids) grows logarithmically with decreasing error:

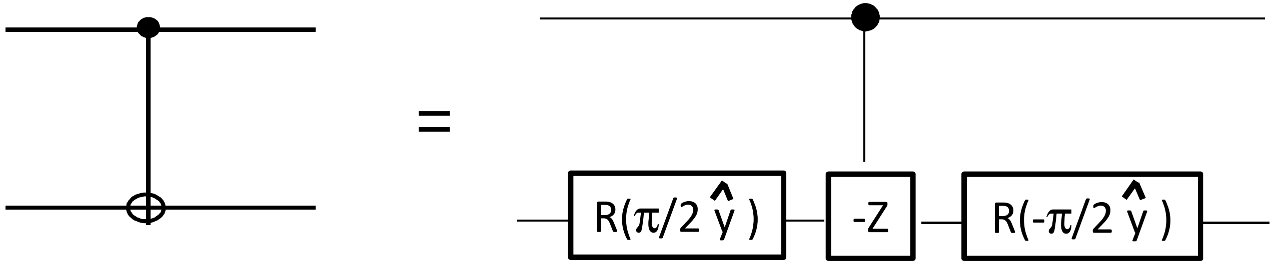
$$L_{NOT} \approx 18 \left| \log_{10} \varepsilon \right|$$

Roughly same scaling seen for all "three-weaves"

Quantum Gates for Modular Exp

CNOT Gate:





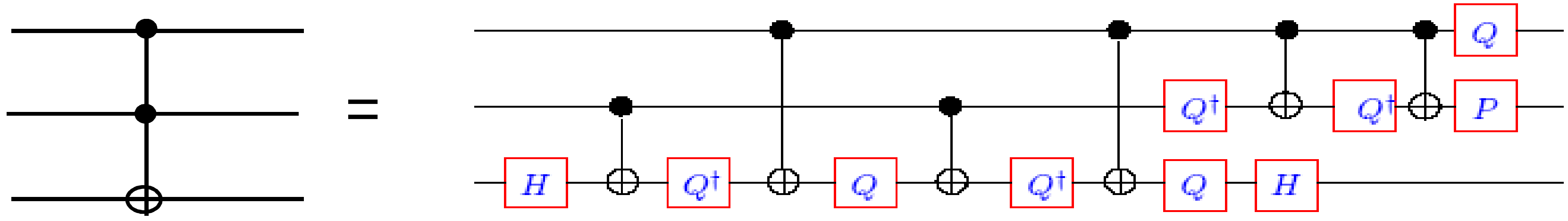
CNOT is constructed using 3 three-weaves plus 2 single qubit rotations for a total of 5 three-weaves.

$$L_{CNOT} \approx 5L_{NOT} \approx 90\left|\log_{10}\varepsilon\right|$$

Quantum Gates for Modular Exp

CCNOT (Toffoli) Gate:

(from http://www.cl.cam.ac.uk/teaching/0607/QuantComp/lecture4.pdf)



where, $P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, Q = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$

CCNOT can be constructed using 6 CNOTs (up to single qubit rotations on the target) and 9 single qubit rotations. So 6x3 = 18 “CNOT” three-weaves + 9 “single qubit rotation” three-weaves = 27 three-weaves.

$$L_{CCNOT} \approx 27 L_{NOT} \approx 486 \left| \log_{10} \varepsilon \right|$$

Number of Elementary Braids

Total number of elementary braids:

$$L_{Shor} \approx 50{,}000\,|\log_{10}\varepsilon|\,K^3$$

For a finite probability that no error occurs, we require:

$$|\varepsilon|^2 \sim \frac{1}{50{,}000\,K^3}$$

To factor a 128-bit number:

$$\varepsilon \sim 3\times 10^{-6} \rightarrow \boxed{\begin{array}{l}\text{Number of Fibonacci anyons } \approx 1000 \\ \text{Number of elementary braids} \approx 6\times 10^{11}\end{array}}$$

M. Baraban, NEB, and S. H. Simon, PRA **81**, 062317 (2010)