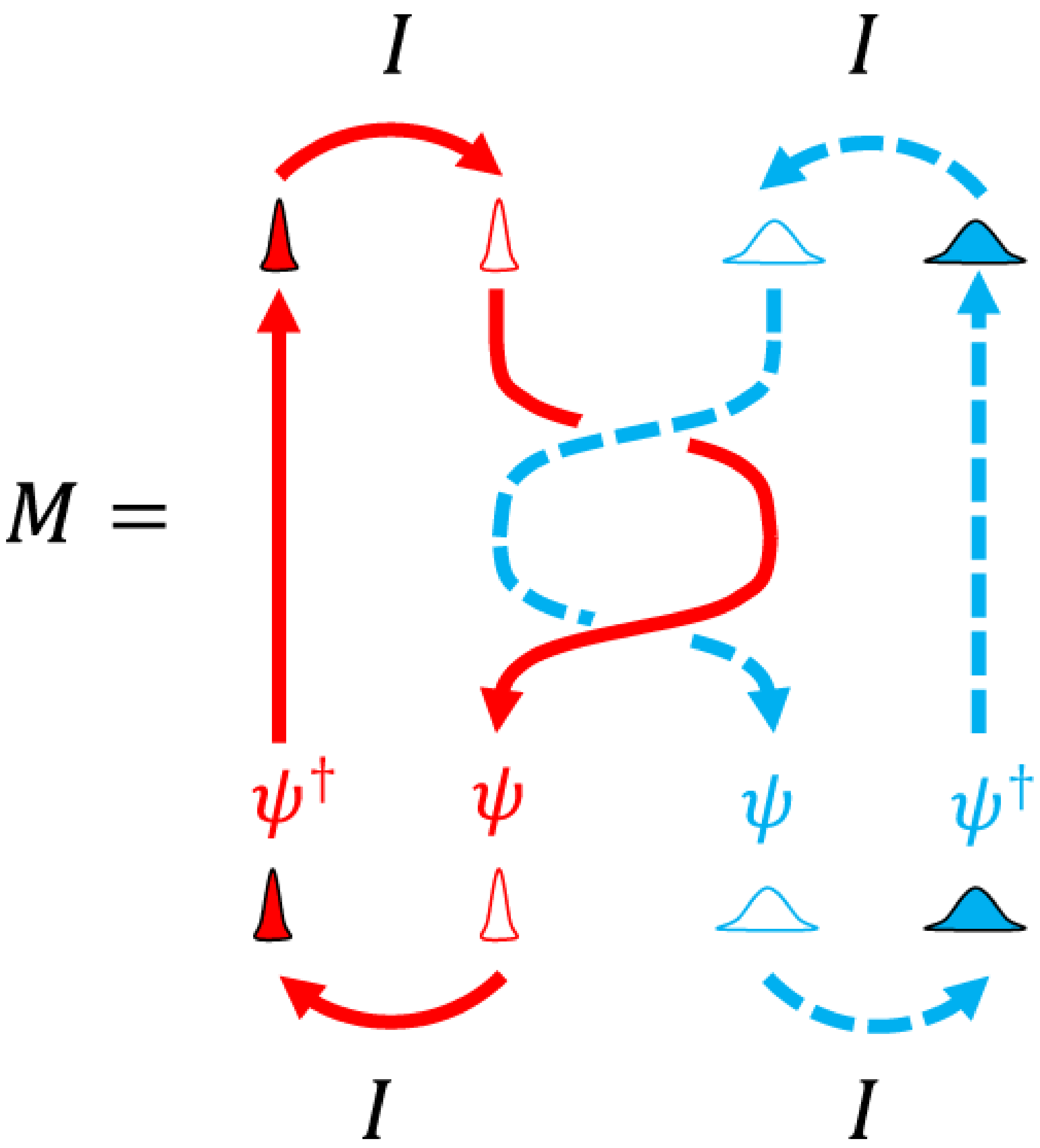
Topological Quantum Computing Through Braids

Borishan Ghosh
Hansraj College
BSc (H) Physics, 2nd Year
borishan.gh@gmail.com



Outline

1. Statistics at the quantum scale
2. Bosons, Fermions and Anyons
3. The Braid Group
4. Quantum Circuits
5. Topological QC
6. Universality under TQC

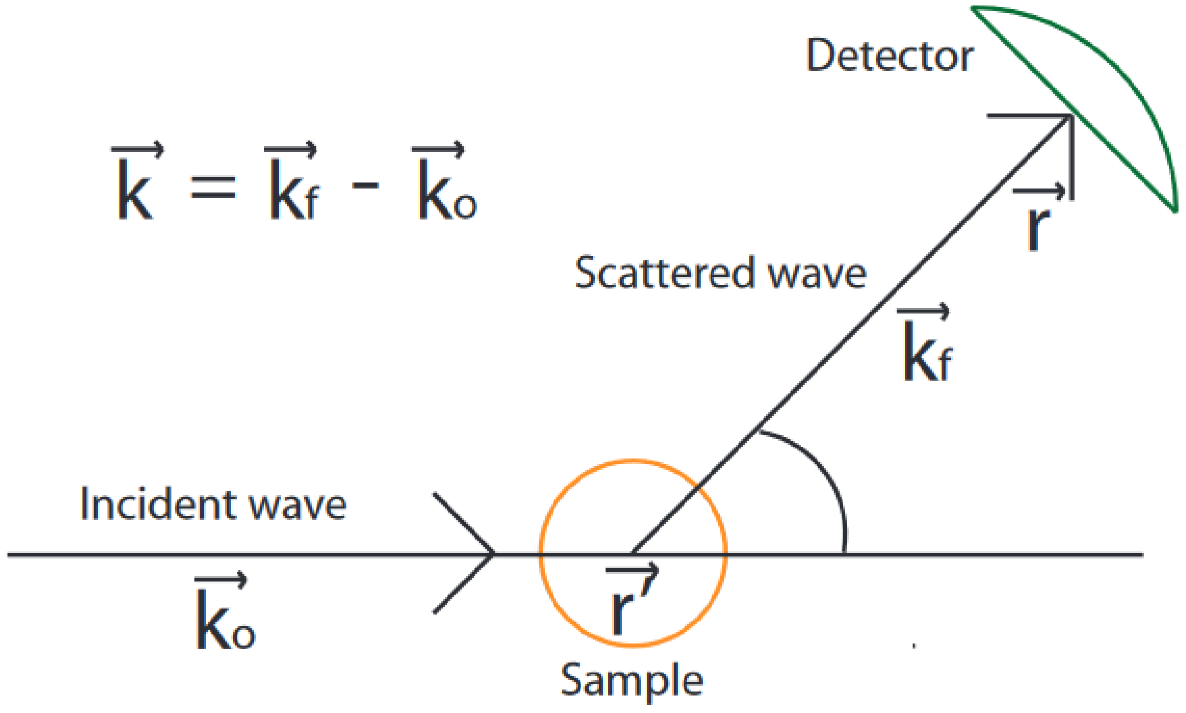
Can we tell apart classical particles under exchange?

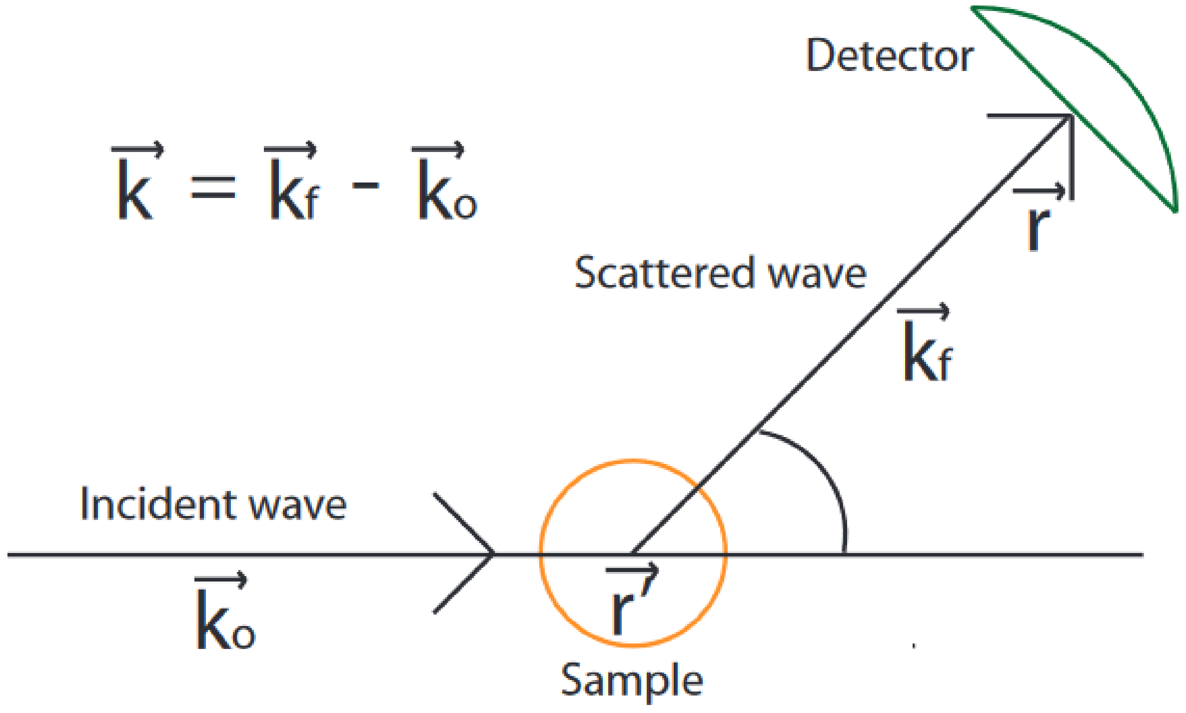
Pool table before and after break

Yes, no matter the permutation of the colours, we can always distinguish between two balls with full knowledge of the system and hence the trajectory

Can we say the same for quantum particles?

Quantum States are completelely specified by wavefuntions, when two wavefuntions overlap and then scatter, they completely lose identity.

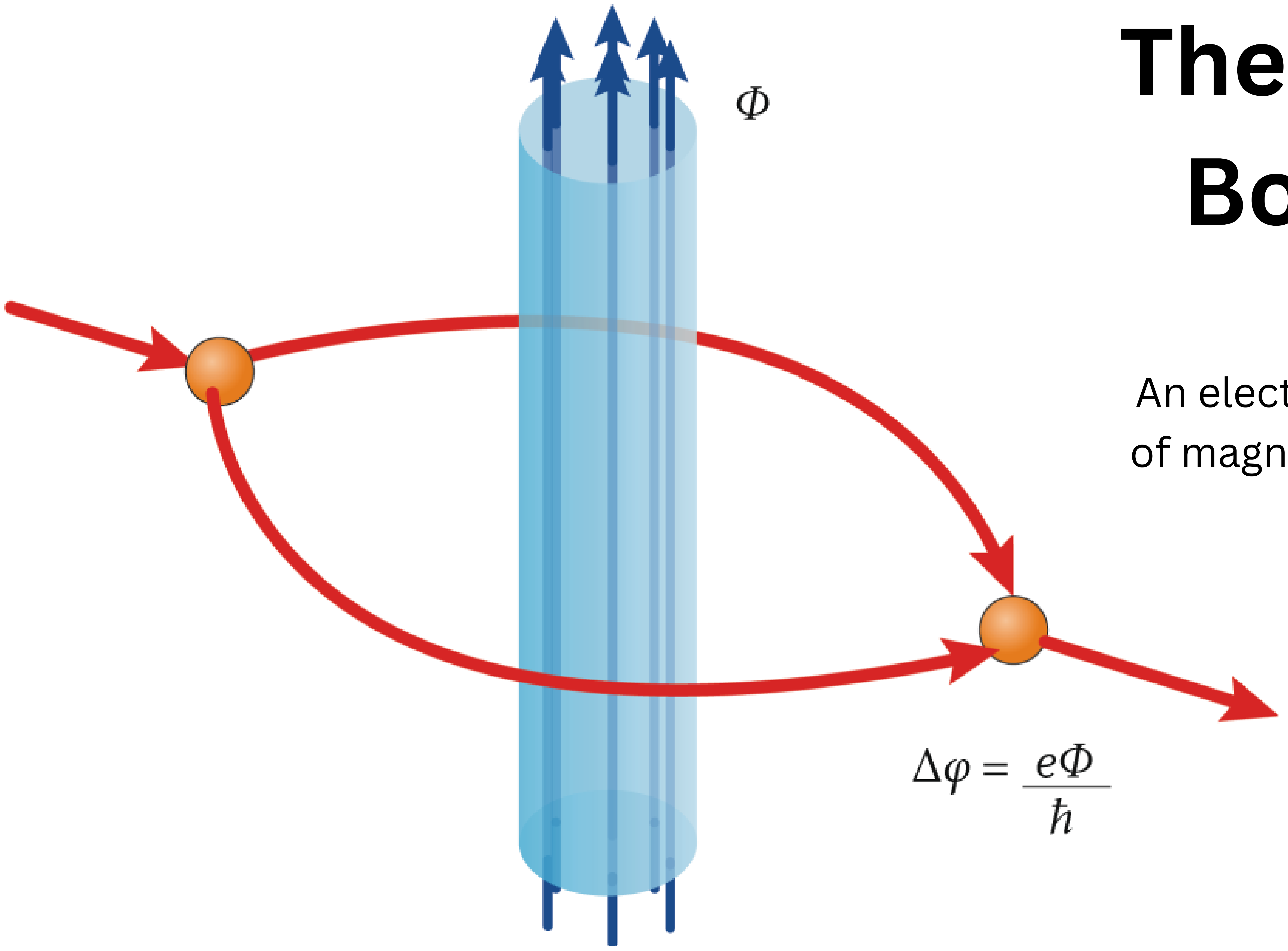




Can we say the same for quantum particles?

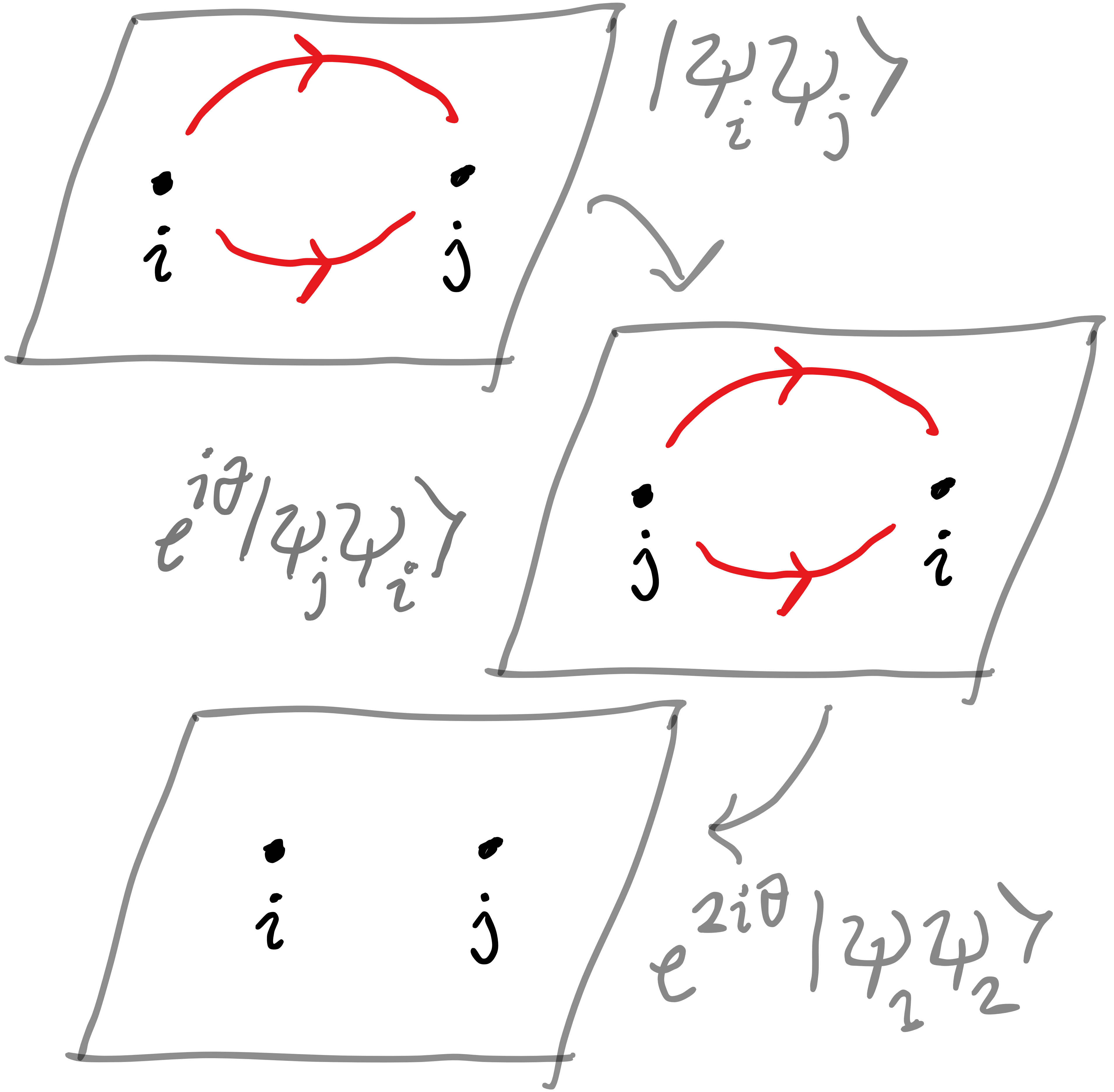
Quantum States are completelely specified by wavefuntions, when two wavefuntions overlap and then scatter, they completely lose identity.

In quantum physics, identical states are indistinguishable.



The Aharonov–Bohm effect

An electron moving around a tube of magnetic field picks up a phase.



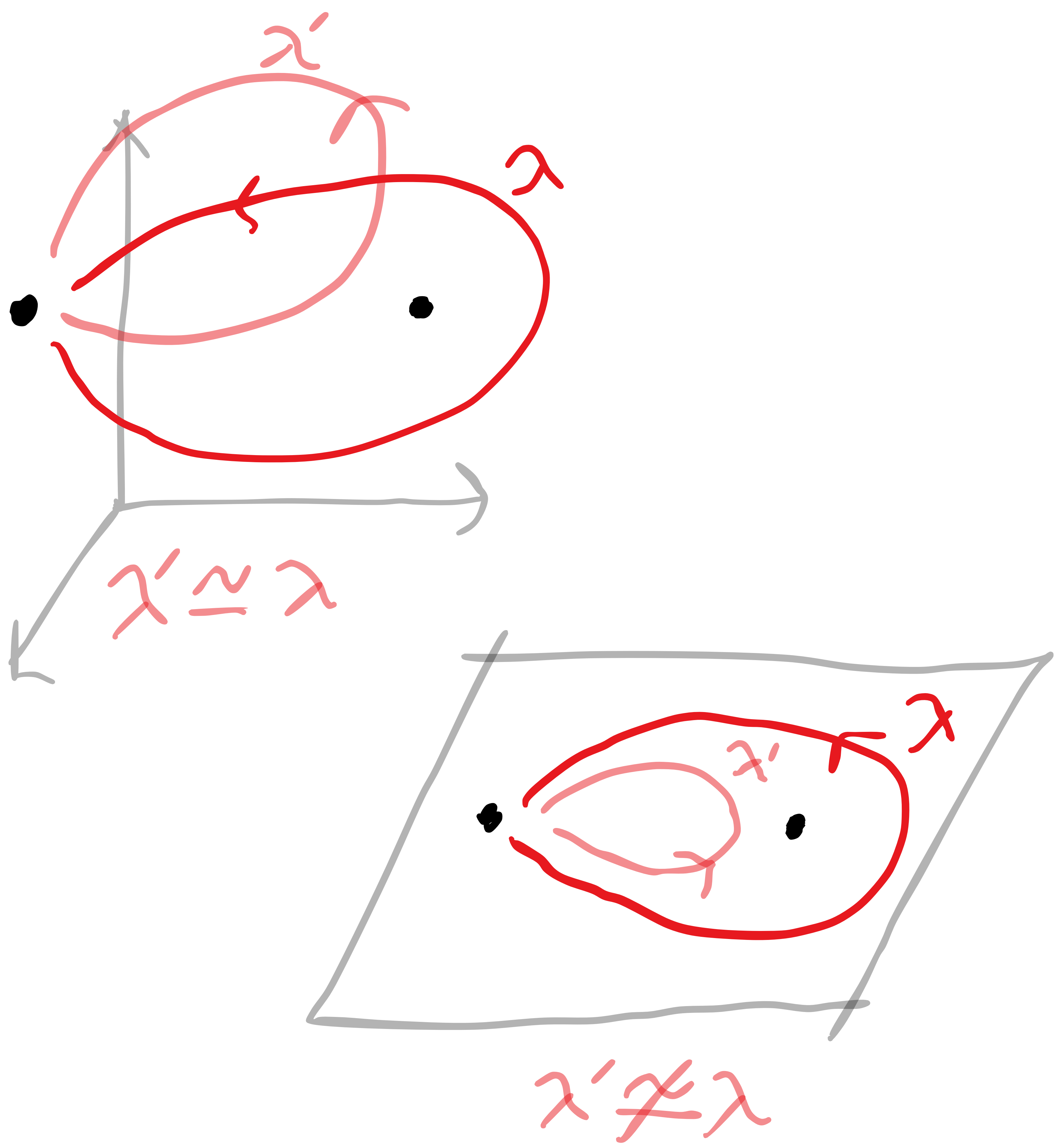
There are two worlds

Bosons follow Bose-Einstein Statistics, are Symmetric under exchange.

$$|\psi_1\psi_2\rangle = |\psi_2\psi_1\rangle$$

Fermions follow Fermi-Dirac Statistics, are Anti-symmetric under exchange.

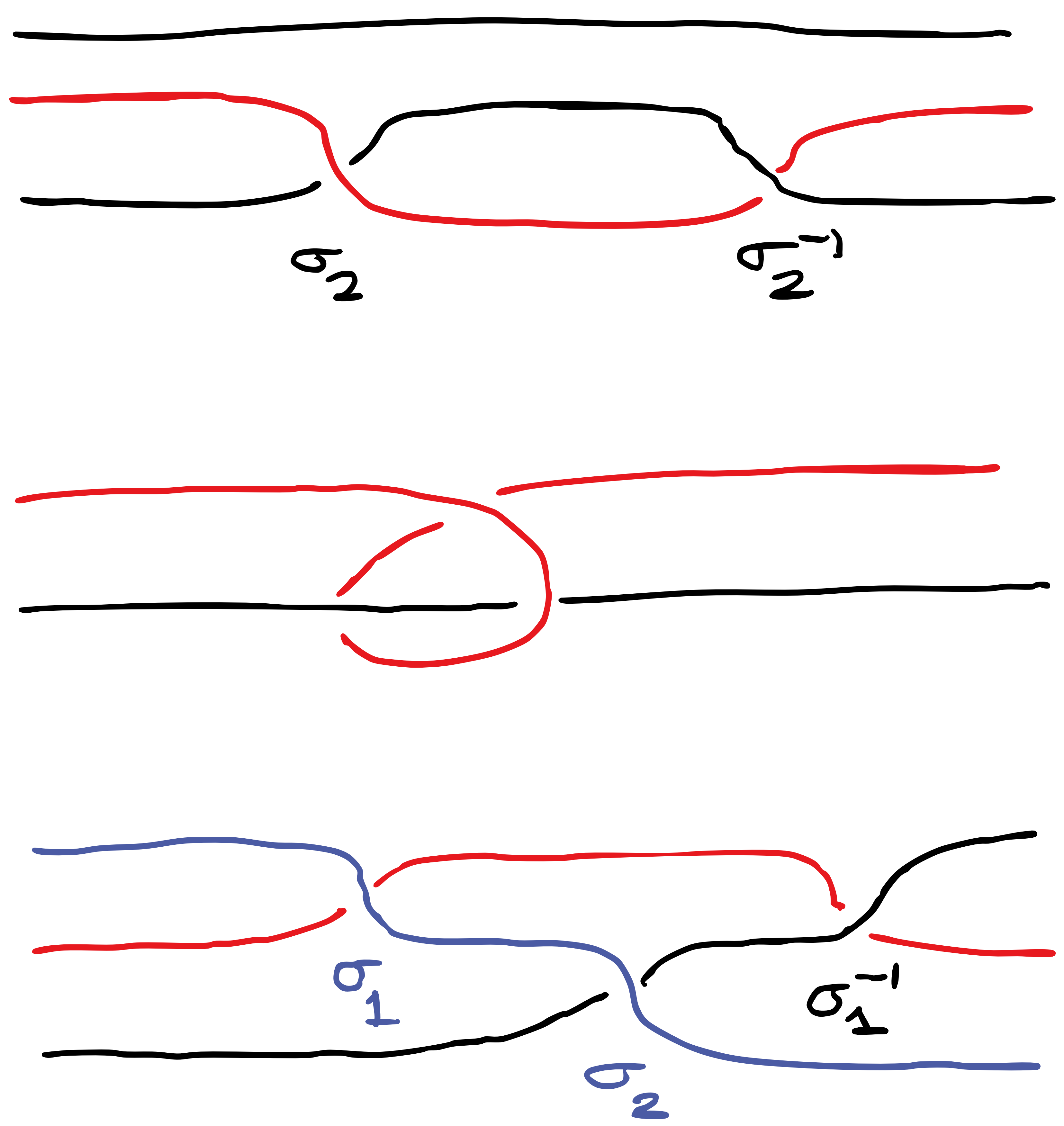
$$|\psi_1\psi_2\rangle = -|\psi_2\psi_1\rangle$$



Onto R ^{2}

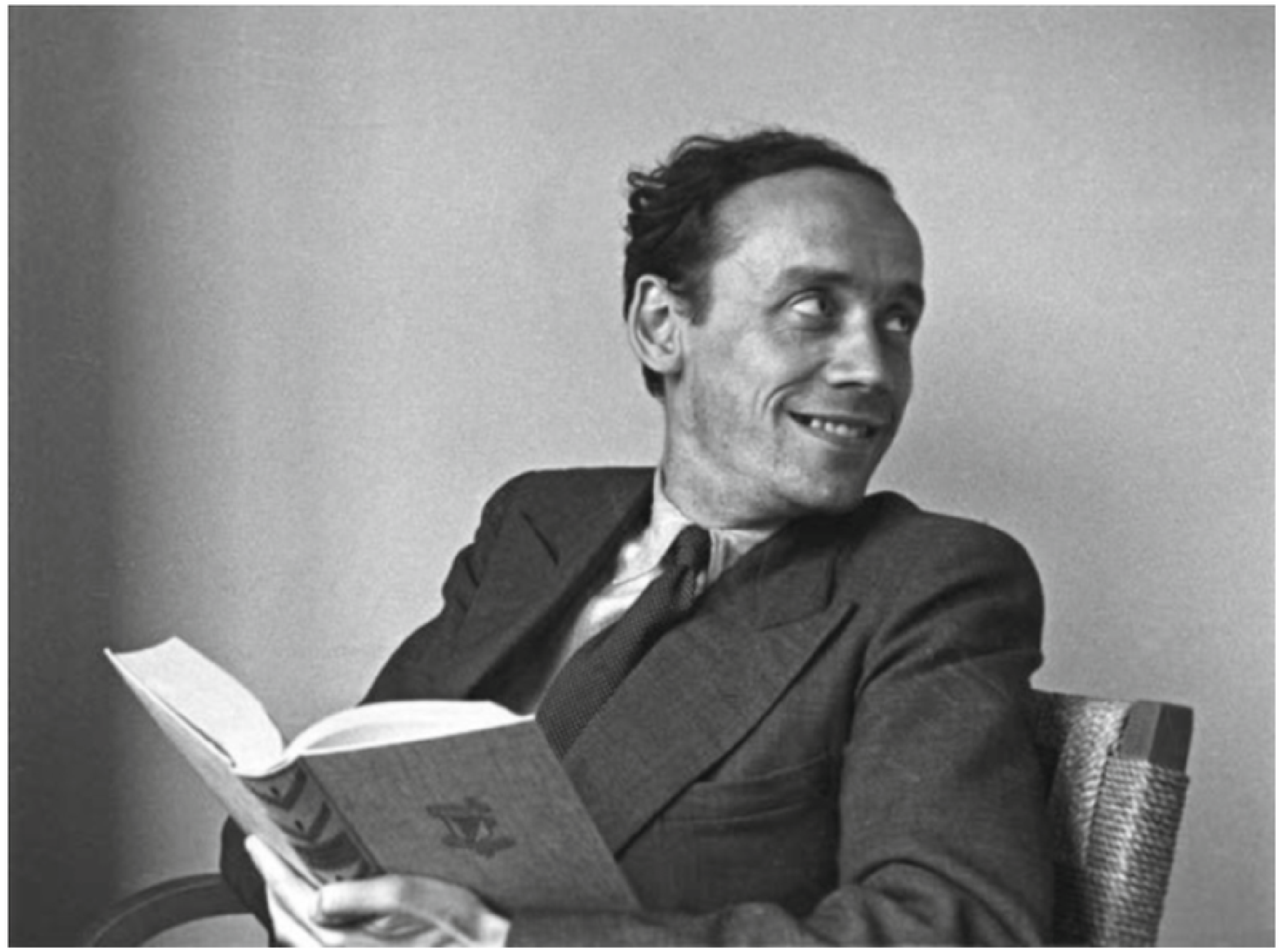
A loop around a point can be continuously deformed into itself in 3D space, *not in 2D*.

Consequently, in 2D space θ can lie any where between 0 and π. These particles with with intermediate phases are called ***any-ons***, with properties somewhere between bosons and fermions



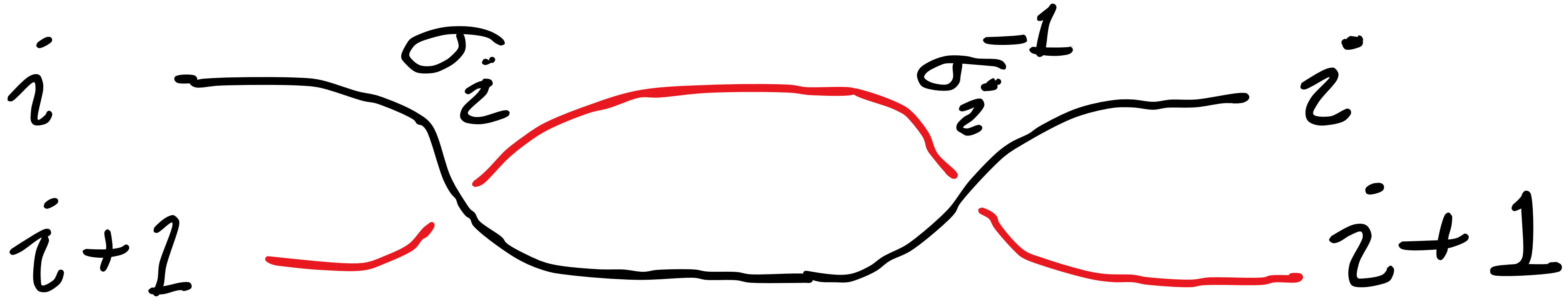
The Braid Group

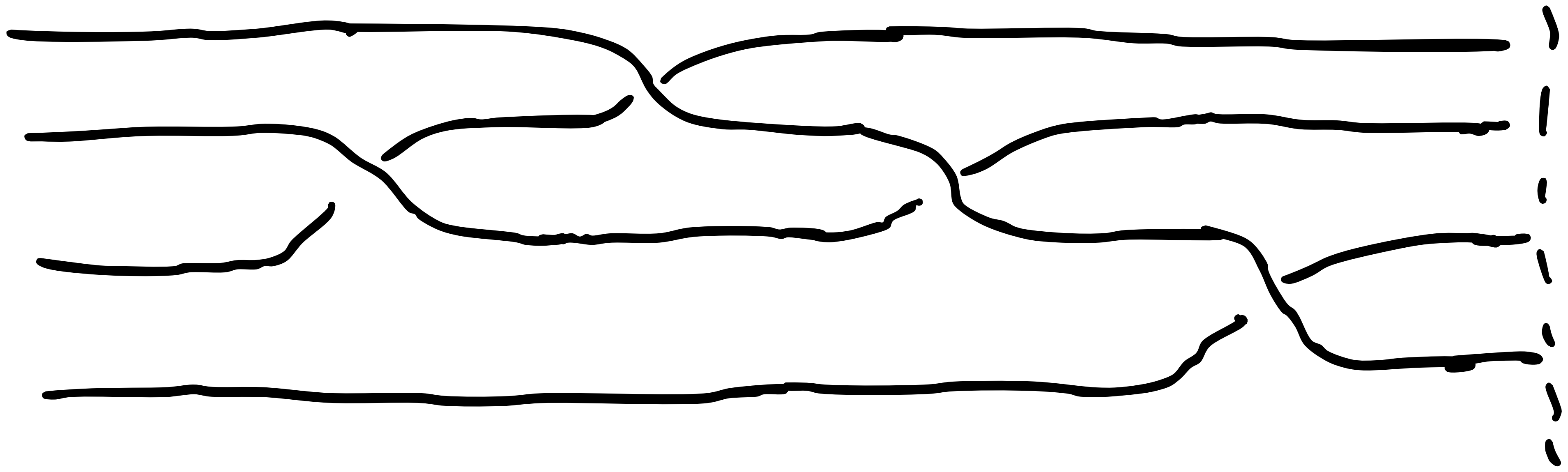
1. No strands can be tangent to each other at any point.
2. Only two strands can cross at any point.
3. No two crossings can occur at the same horizontal level.



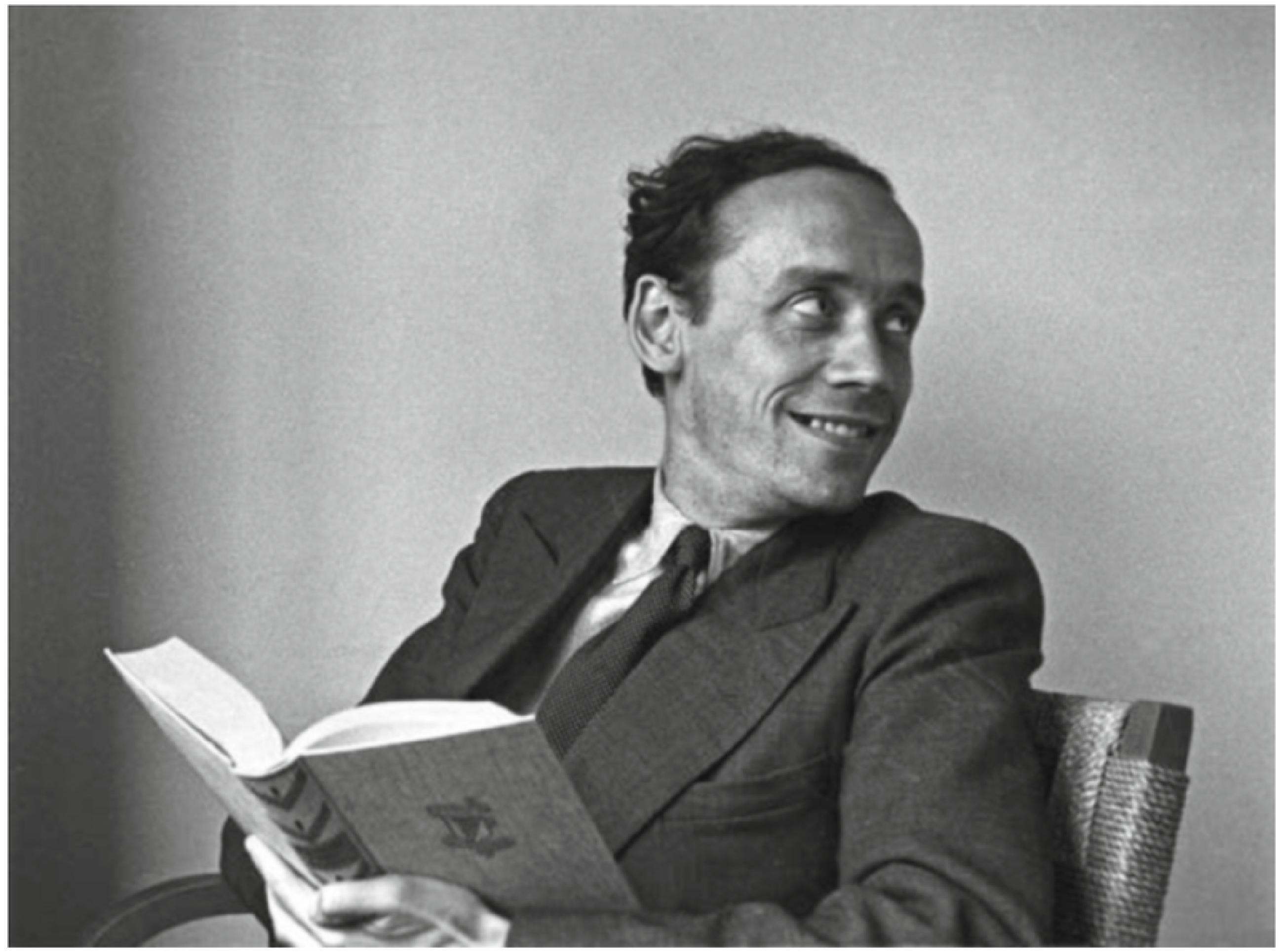
Artin Generators

$$B_n = \langle \sigma_1, \sigma_2 \ldots, \sigma_{n-1}, \sigma_1^{-1}, \sigma_2^{-1} \ldots, \sigma_{n-1}^{-1} \rangle$$



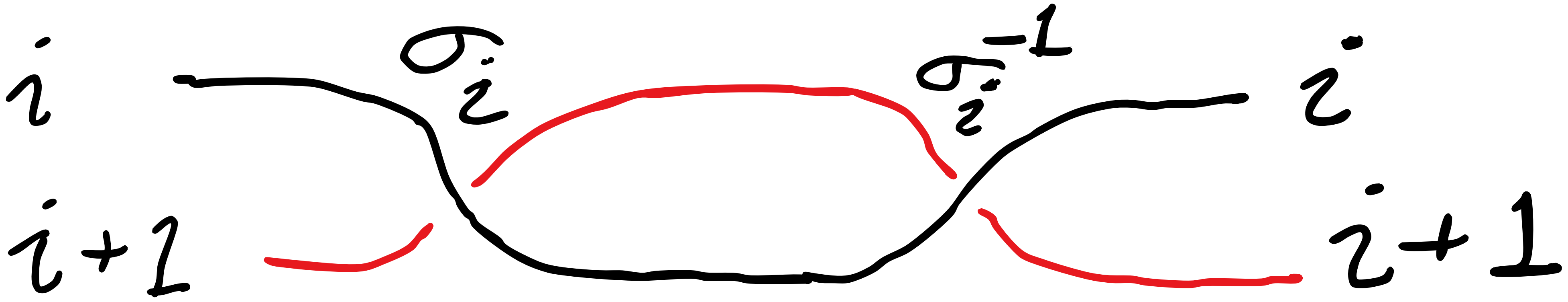


$\sigma_2\sigma_1\sigma_2\sigma_3$

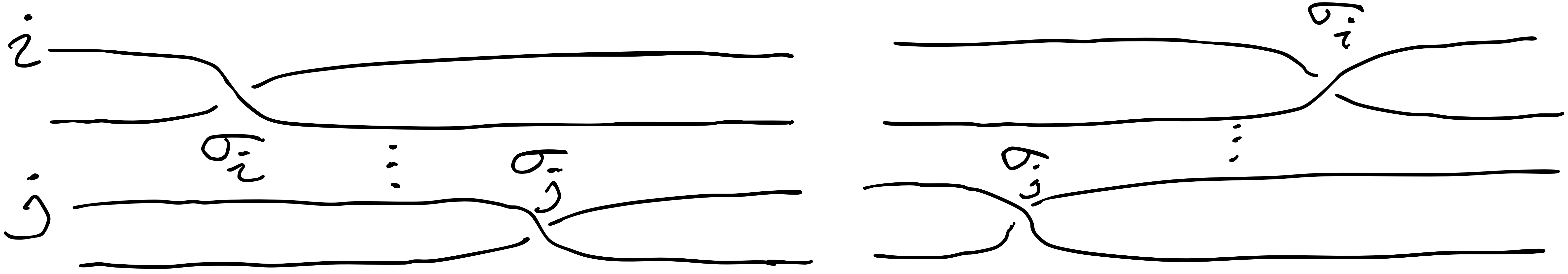


Artin Generators

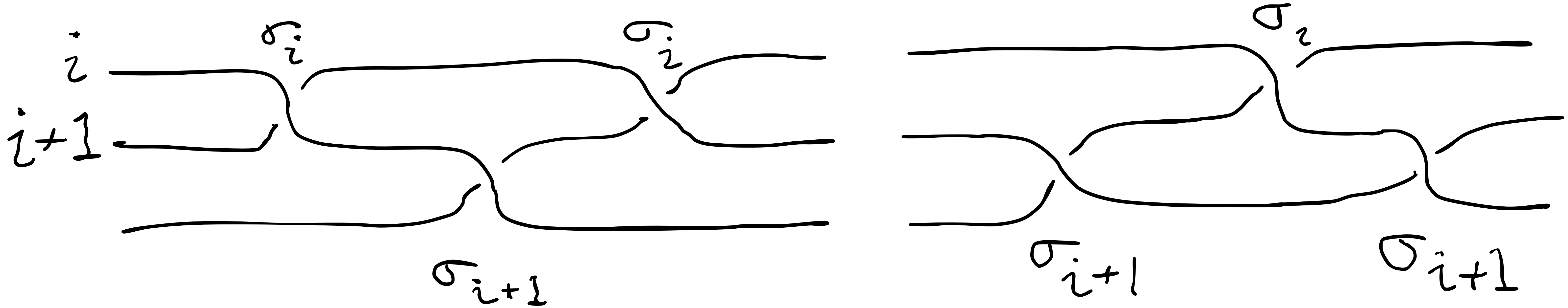
$$B_n = \langle \sigma_1, \sigma_2 \ldots, \sigma_{n-1}, \sigma_1^{-1}, \sigma_2^{-1} \ldots, \sigma_{n-1}^{-1} \rangle$$

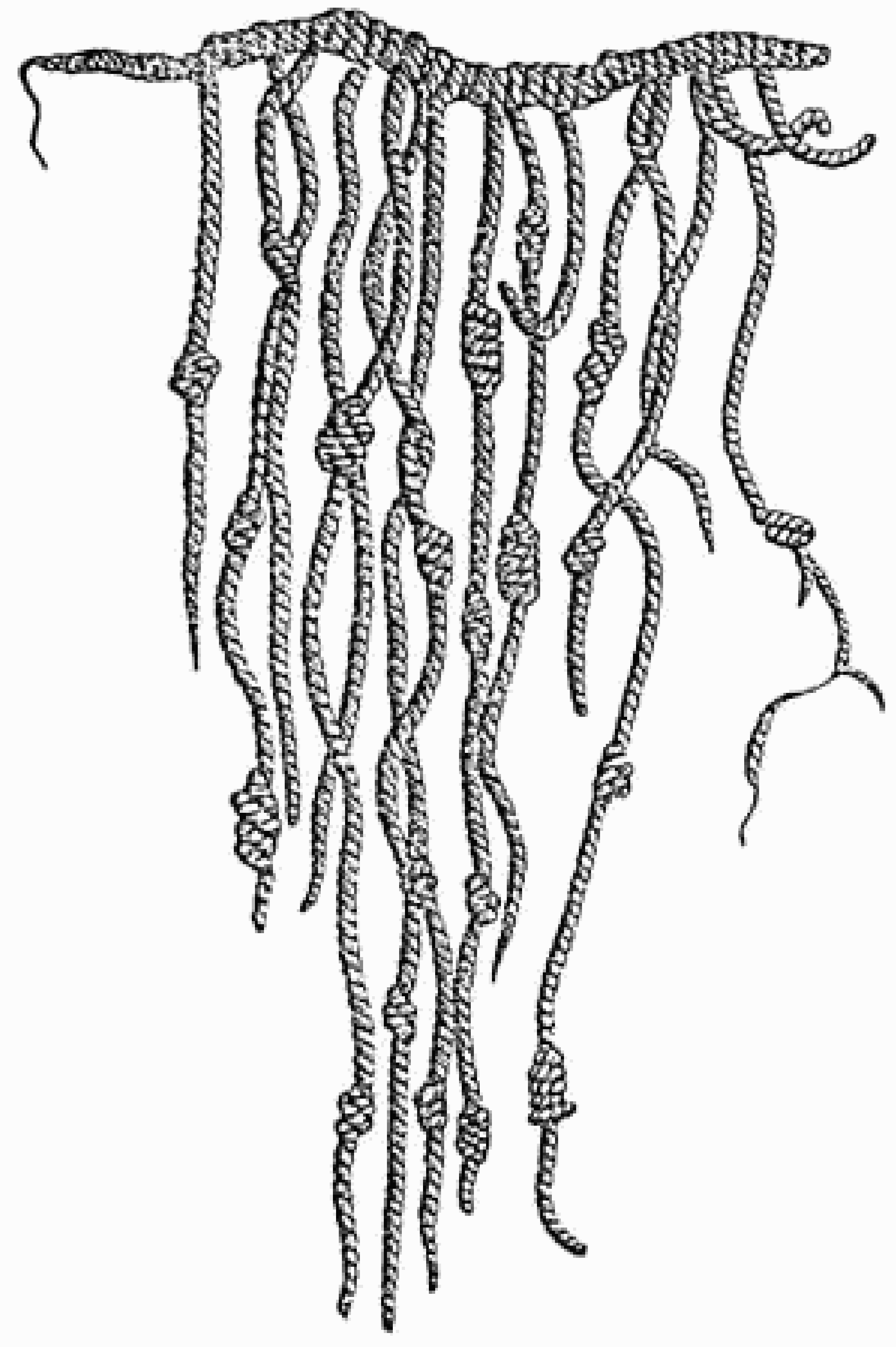


$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{when } |i-j| \geq 2$$



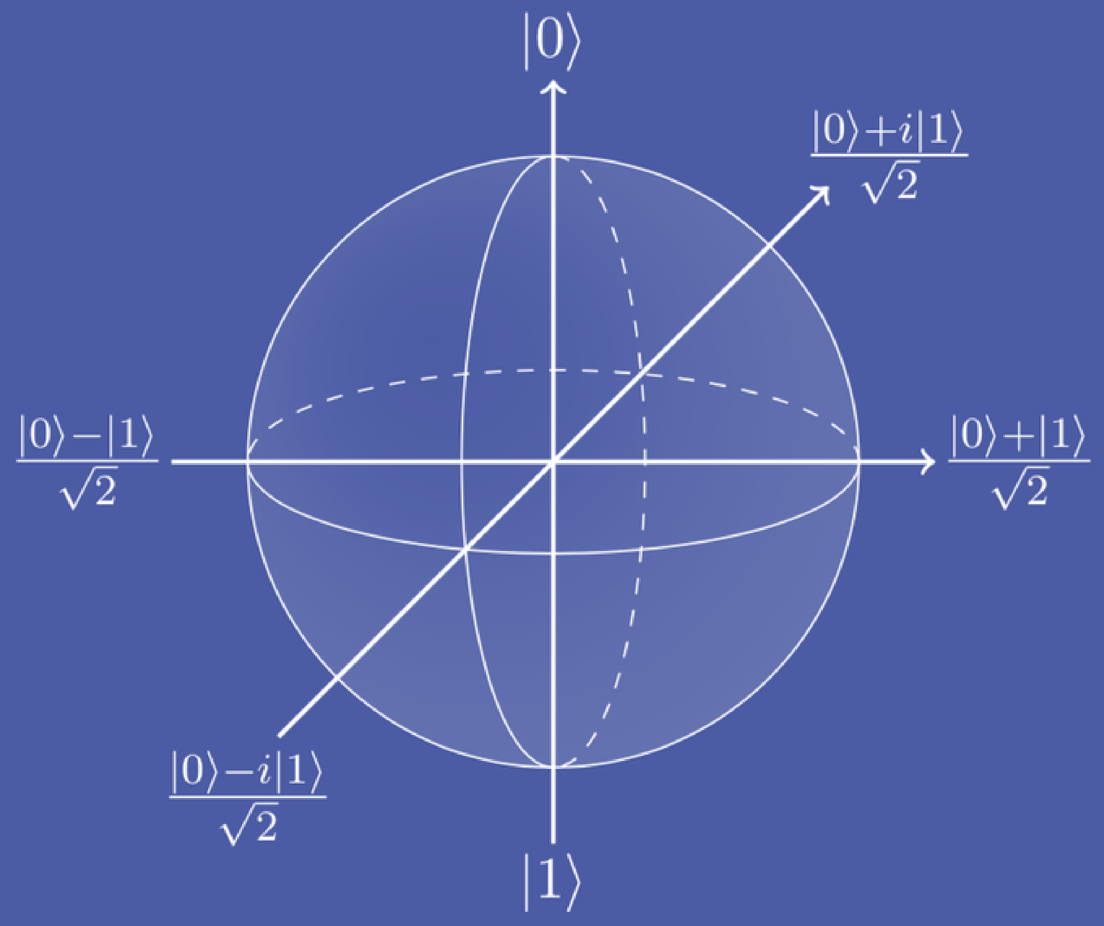
$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$$





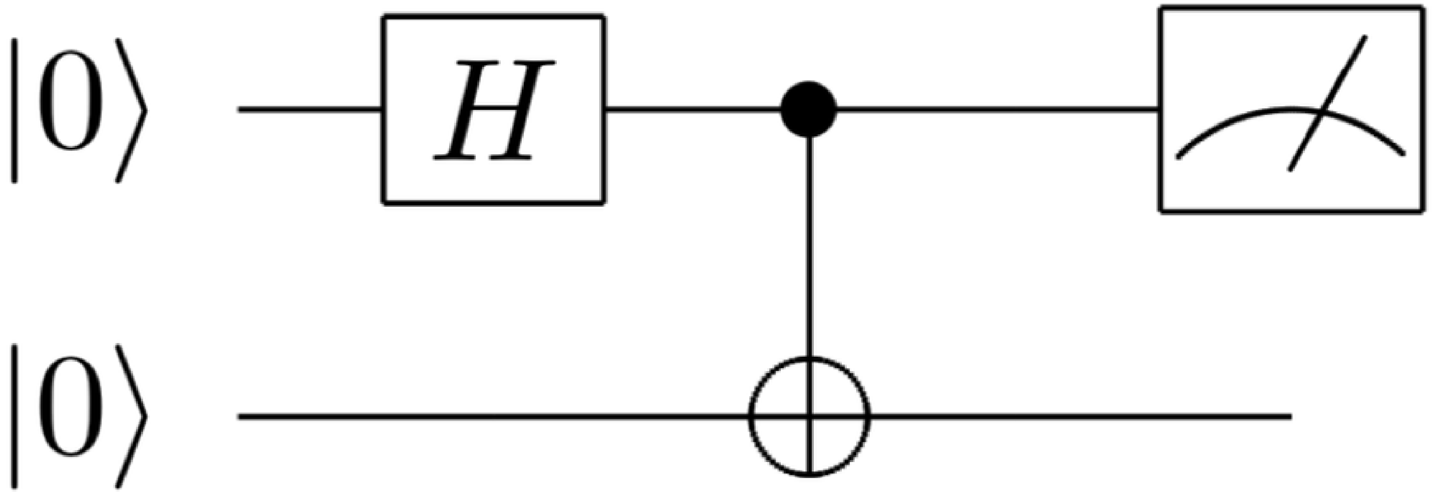
Quipu dating c. 2600 BC – 17th century

Quantum Circuits

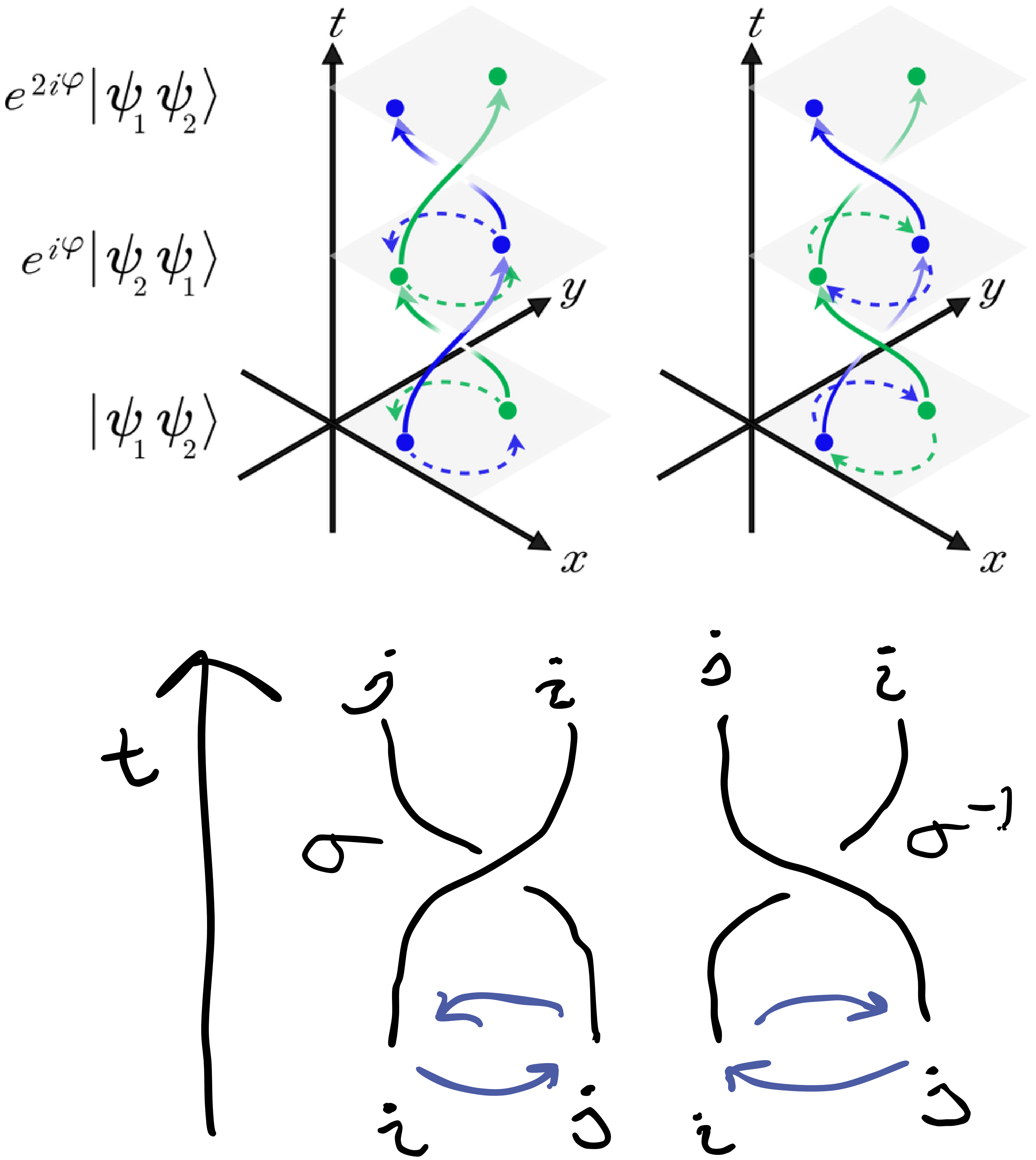


A qubit is a vector on the Bloch Sphere.

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



1. Initialize an input state
2. Apply unitary transformations (Rotations along the Bloch Sphere)
3. Measurement



Topological QC

Adding a time axis, to anyon exchanges resembles braids.

Every permutation of anyons can be written as an element in the braid group. With every braiding, the initial wavefuntion picks up a unique phase.

Just like the braids, these exchanges are not necessarily abelian.

Measurement by fusion

$$\chi \in \{\mathbb{I}, \tau\}$$

$$\mathbb{I} * \chi = \chi$$

$$\tau * \tau = \mathbb{I} + \tau$$

$$\begin{aligned} \tau * \tau * \tau &= \tau * (\mathbb{I} + \tau) \\ &= 2\tau + \mathbb{I} \end{aligned}$$

Measurement by fusion

$$\chi \in \{\mathbb{I}, \tau\}$$

$$\mathbb{I} * \chi = \chi$$

$$\tau * \tau = \mathbb{I} + \tau$$

$$\begin{aligned} \tau * \tau * \tau &= \tau * (\mathbb{I} + \tau) \\ &= 2\tau + \mathbb{I} \end{aligned}$$

$$\tau * \tau * \tau * \tau = 3\tau + 2\mathbb{I}$$

$$\tau * \tau * \tau * \tau * \tau = 5\tau + 3\mathbb{I}$$

$$\tau * \tau * \tau * \tau * \tau * \tau = 8\tau + 5\mathbb{I}$$

Measurement by fusion

$$\chi \in \{\mathbb{I}, \tau\}$$

$$\mathbb{I} * \chi = \chi$$

$$\tau * \tau = \mathbb{I} + \tau$$

$$\begin{aligned} \tau * \tau * \tau &= \tau * (\mathbb{I} + \tau) \\ &= 2\tau + \mathbb{I} \end{aligned}$$

$$\tau * \tau * \tau * \tau = 3\tau + 2\mathbb{I}$$

$$\tau * \tau * \tau * \tau * \tau = 5\tau + 3\mathbb{I}$$

$$\tau * \tau * \tau * \tau * \tau * \tau = 8\tau + 5\mathbb{I}$$

Fibonacci !

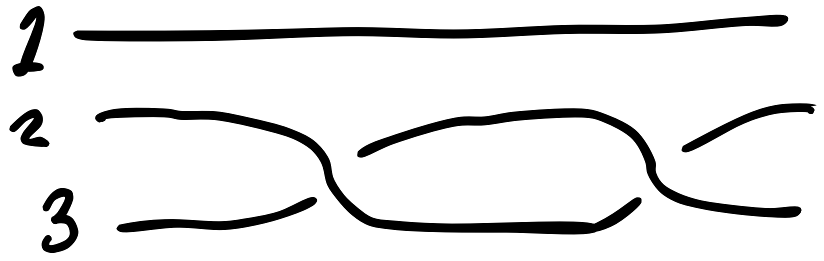
$$\tau * \ldots * \tau = f_{n-1}\tau + f_{n-2}\mathbb{I}$$

Qubit State, after braiding and measurements (fusion):

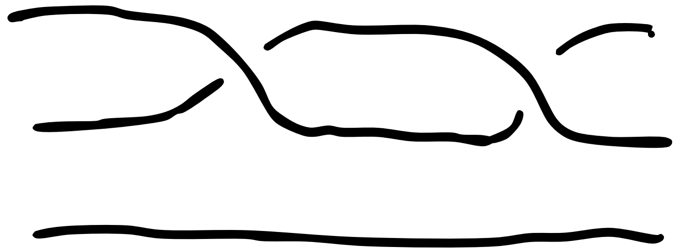
$$|\psi\rangle = \alpha(\tau * \tau)_\tau + \beta(\tau * \tau)_\mathbb{I}$$

Universality

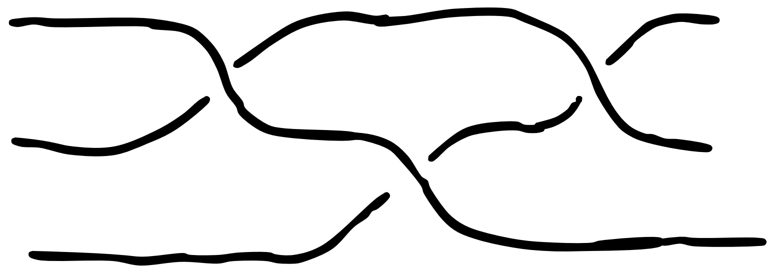
All operations in Quantum Computing can be written as a combination of Single Qubit rotations and the CNOT gate.



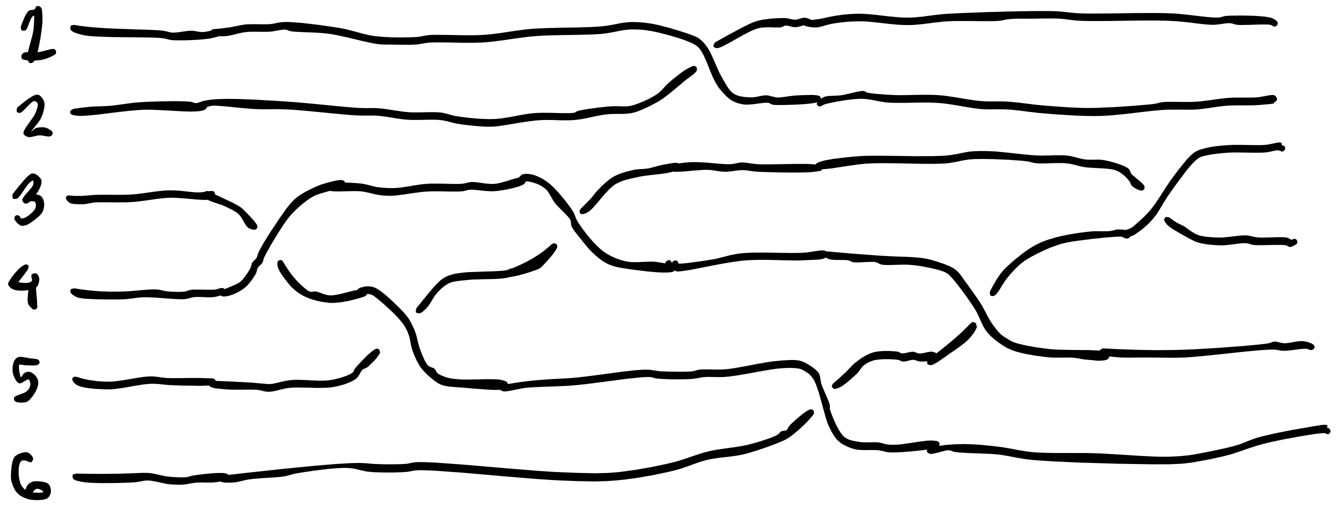
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



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

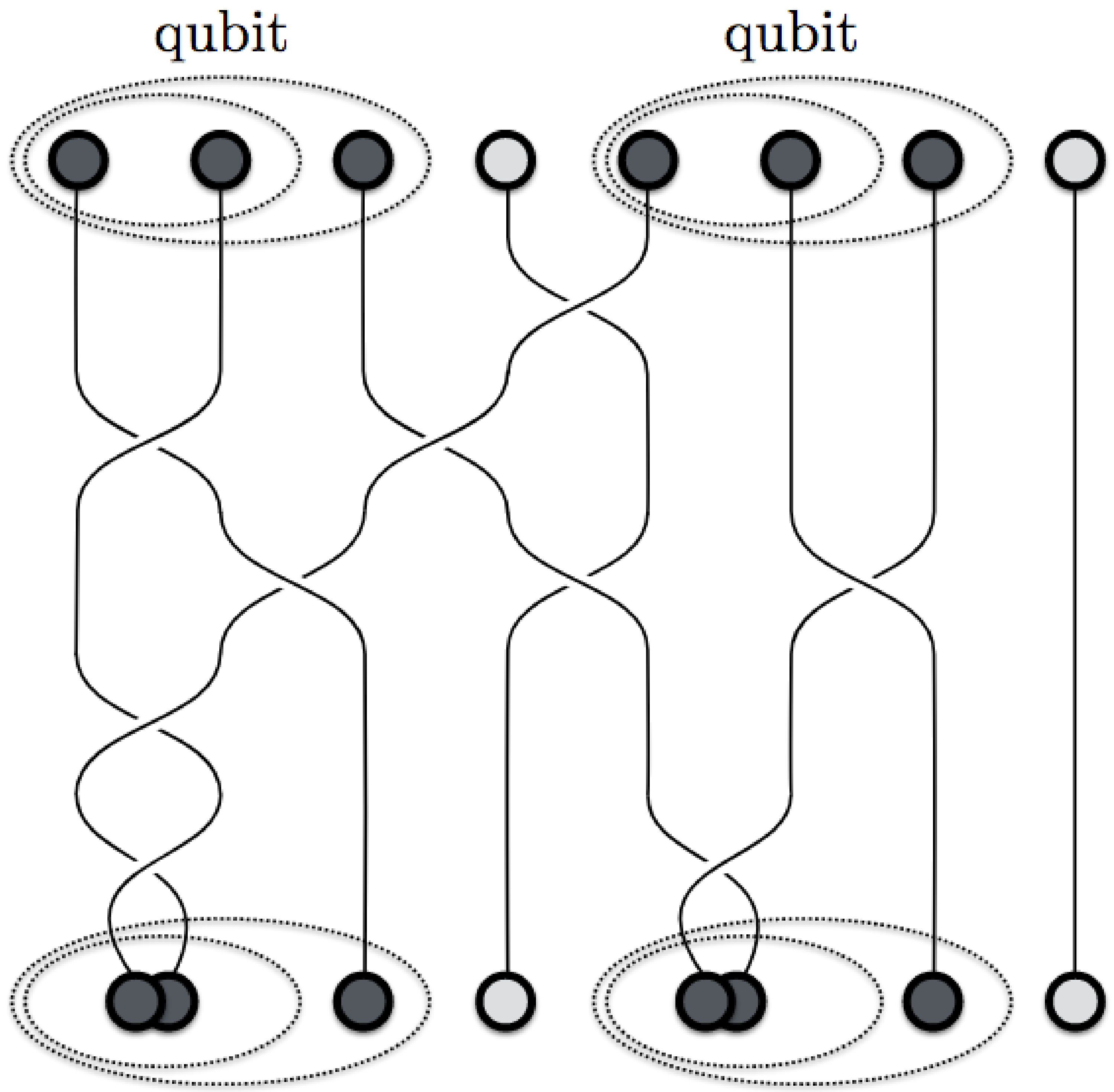


$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



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

$CNOT$



There you have it !

From Artin's simple Toy example from the 1950s to Quantum computers, you can today-

1. Break RSA encryption, or most of the encryption algorithms protecting banks, texts, digital vaults, and more ***(Shor's Algorithm)***
2. Have perfect end to end communication without espionage ***(BB84)***
3. Search faster than classically possible ***(Grover's Search)***

Thank you for your time

Any Questions?