FROM SETS TO BRAIDS

FROM SETS TO BRAIDS

Patrick Dehornoy

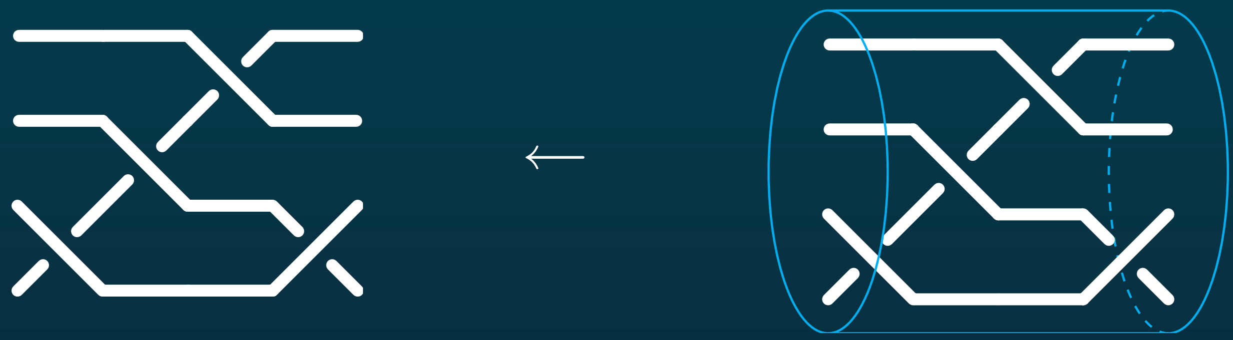
Laboratoire de Mathématiques
Nicolas Oresme, Caen

- A 4-strand braid diagram

- A 4-strand braid diagram = 2D-projection of a 3D-figure

$\longleftarrow$

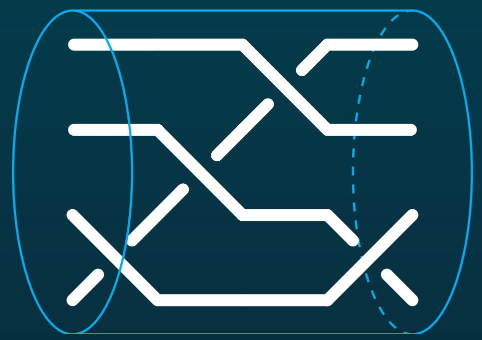
- A 4-strand braid diagram = 2D-projection of a 3D-figure



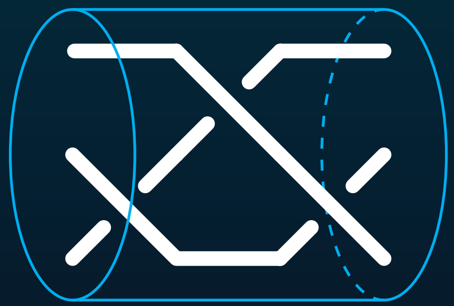
- isotopy = move the strands on the 3D-figure keeping the ends fixed

- A 4-strand braid diagram = 2D-projection of a 3D-figure

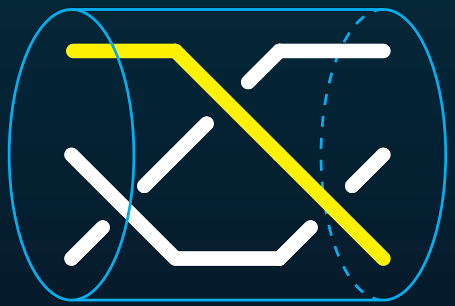
$\longleftarrow$



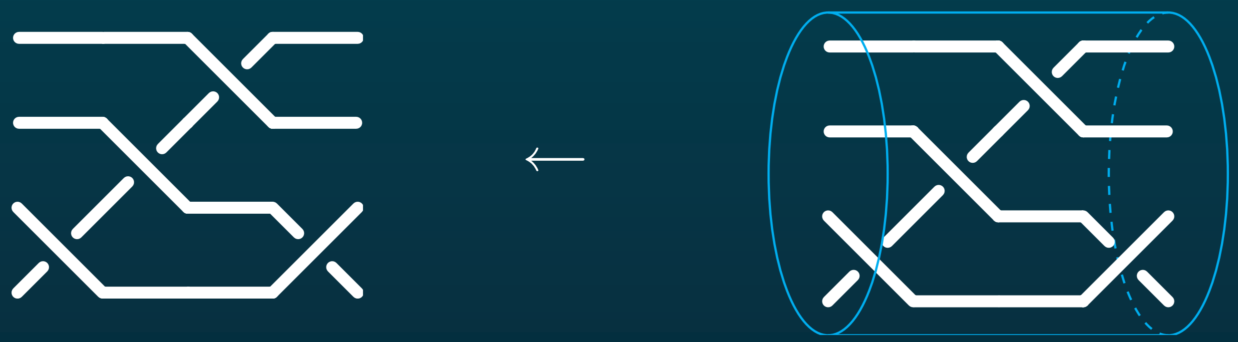
- isotopy = move the strands on the 3D-figure keeping the ends fixed



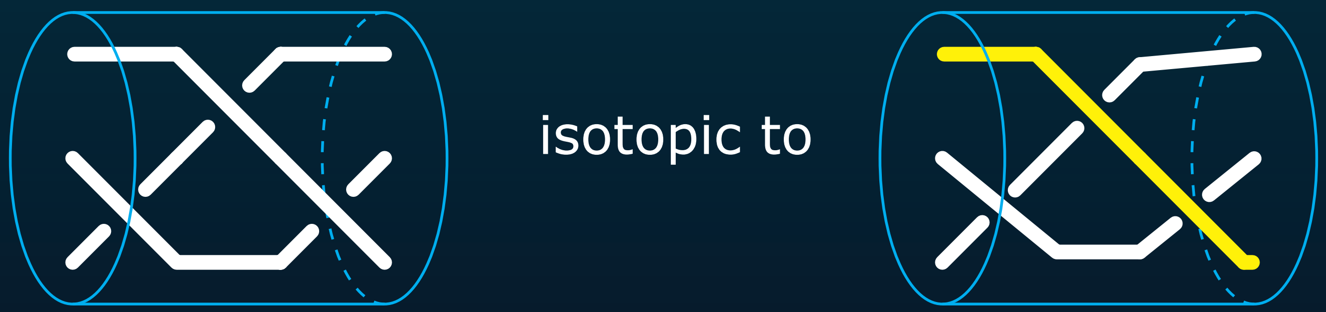
isotopic to



- A 4-strand braid diagram = 2D-projection of a 3D-figure



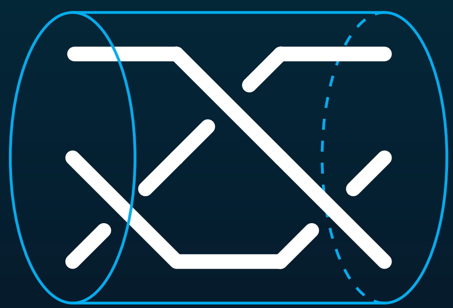
- isotopy = move the strands on the 3D-figure keeping the ends fixed



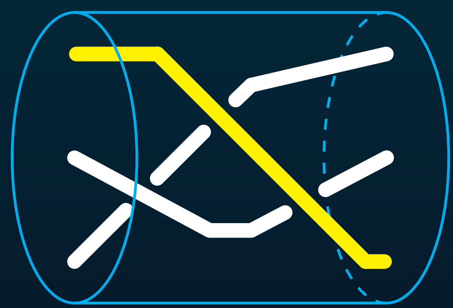
- A 4-strand braid diagram = 2D-projection of a 3D-figure

$\longleftarrow$

- isotopy = move the strands on the 3D-figure keeping the ends fixed



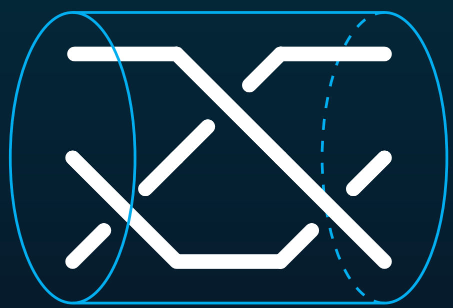
isotopic to



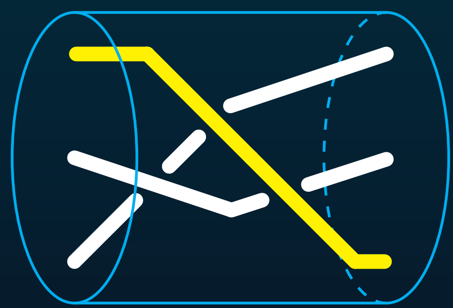
- A 4-strand braid diagram = 2D-projection of a 3D-figure

$\longleftarrow$

- isotopy = move the strands on the 3D-figure keeping the ends fixed



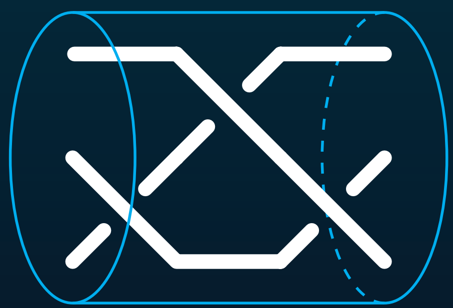
isotopic to



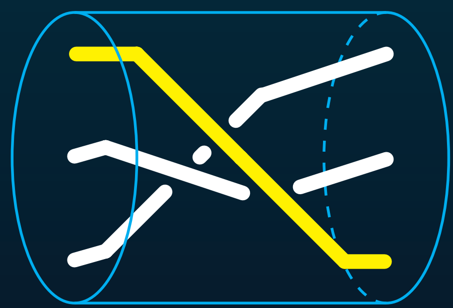
- A 4-strand braid diagram = 2D-projection of a 3D-figure

$\longleftarrow$

- isotopy = move the strands on the 3D-figure keeping the ends fixed



isotopic to

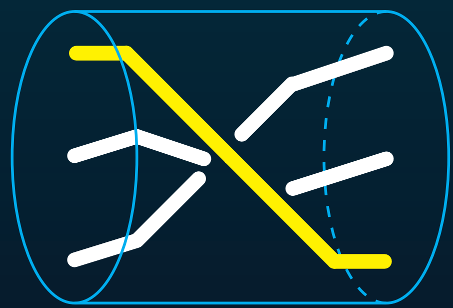


- A 4-strand braid diagram = 2D-projection of a 3D-figure

$\longleftarrow$

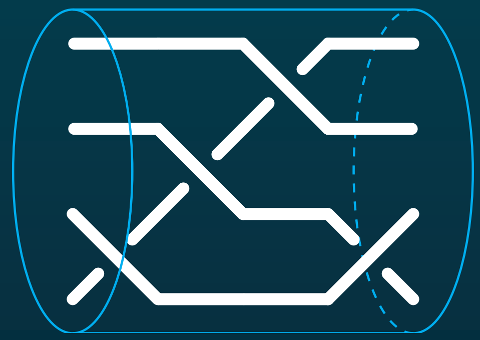
- isotopy = move the strands on the 3D-figure keeping the ends fixed

isotopic to

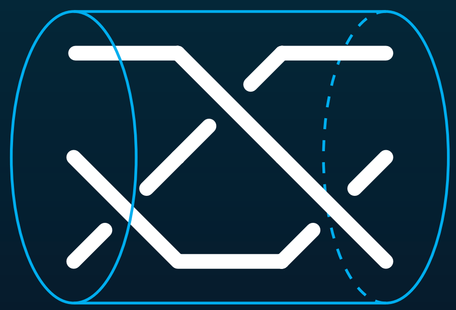


- A 4-strand braid diagram = 2D-projection of a 3D-figure

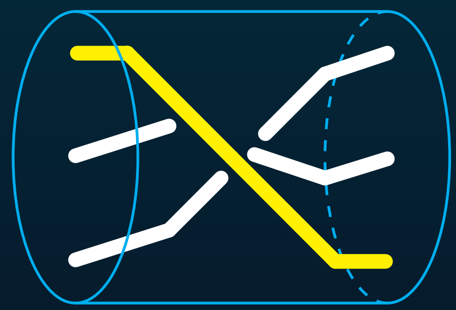
$\longleftarrow$



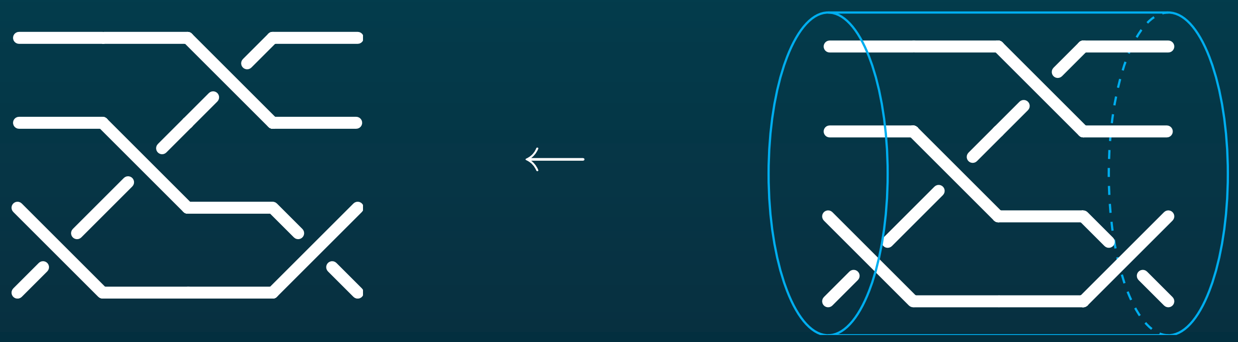
- isotopy = move the strands on the 3D-figure keeping the ends fixed



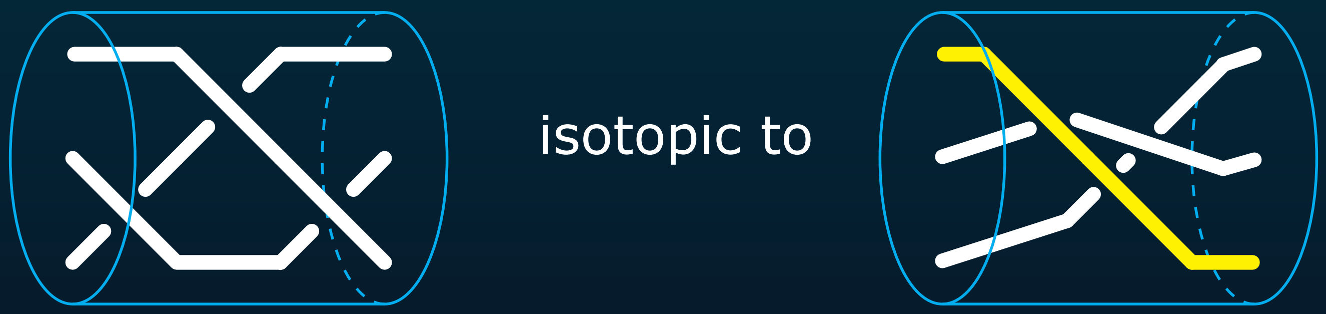
isotopic to



- A 4-strand braid diagram = 2D-projection of a 3D-figure



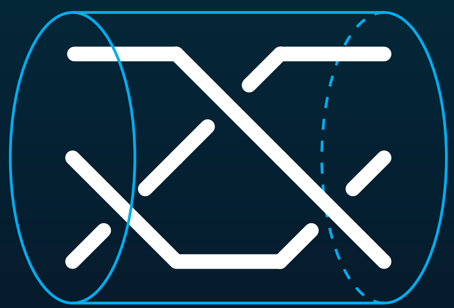
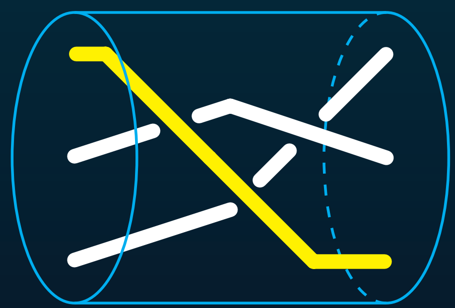
- isotopy = move the strands on the 3D-figure keeping the ends fixed



- A 4-strand braid diagram = 2D-projection of a 3D-figure

 $\longleftarrow$ 

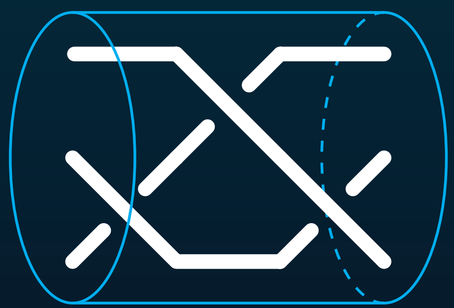
- isotopy = move the strands on the 3D-figure keeping the ends fixed

 isotopic to 

- A 4-strand braid diagram = 2D-projection of a 3D-figure

$\longleftarrow$

- isotopy = move the strands on the 3D-figure keeping the ends fixed

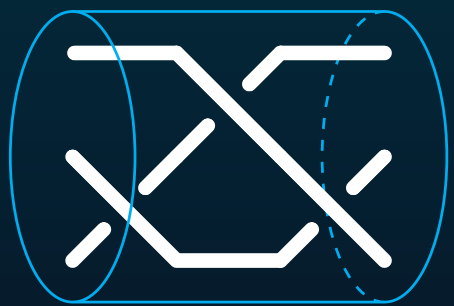


isotopic to

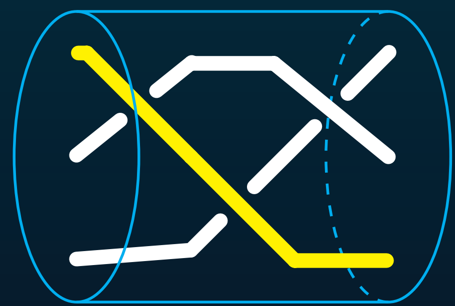
- A 4-strand braid diagram = 2D-projection of a 3D-figure

 $\longleftarrow$ 

- isotopy = move the strands on the 3D-figure keeping the ends fixed

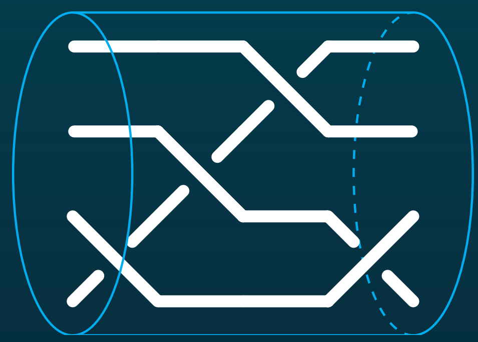


isotopic to

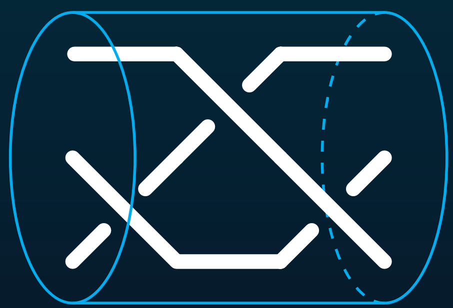


- A 4-strand braid diagram = 2D-projection of a 3D-figure

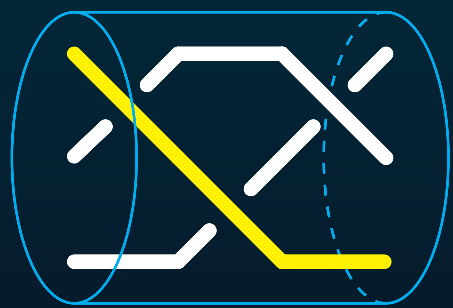
$\longleftarrow$



- isotopy = move the strands on the 3D-figure keeping the ends fixed



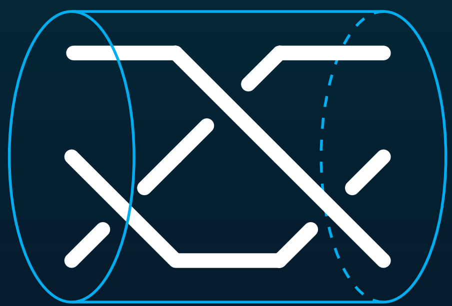
isotopic to



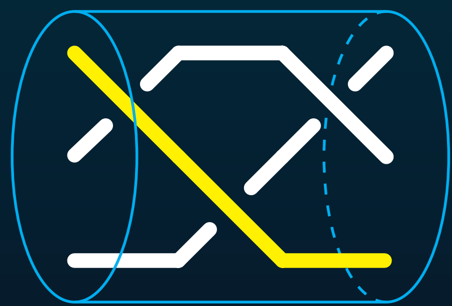
- A 4-strand braid diagram = 2D-projection of a 3D-figure

$\longleftarrow$

- isotopy = move the strands on the 3D-figure keeping the ends fixed

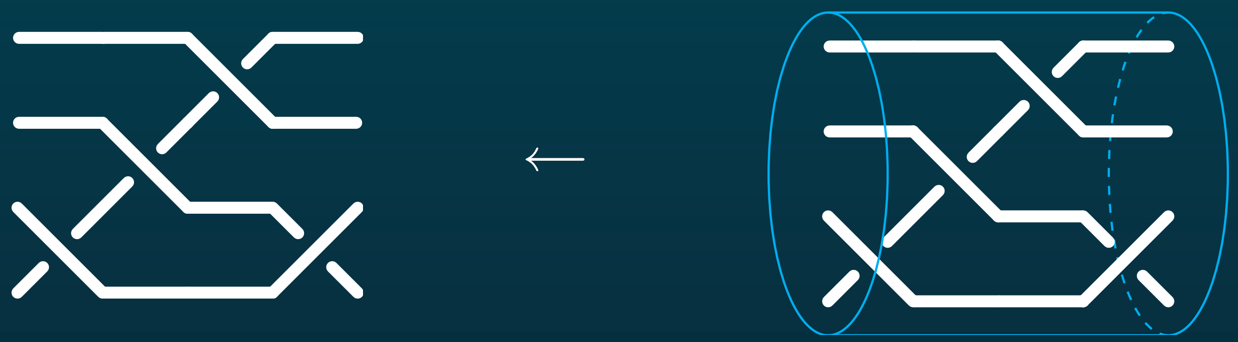


isotopic to

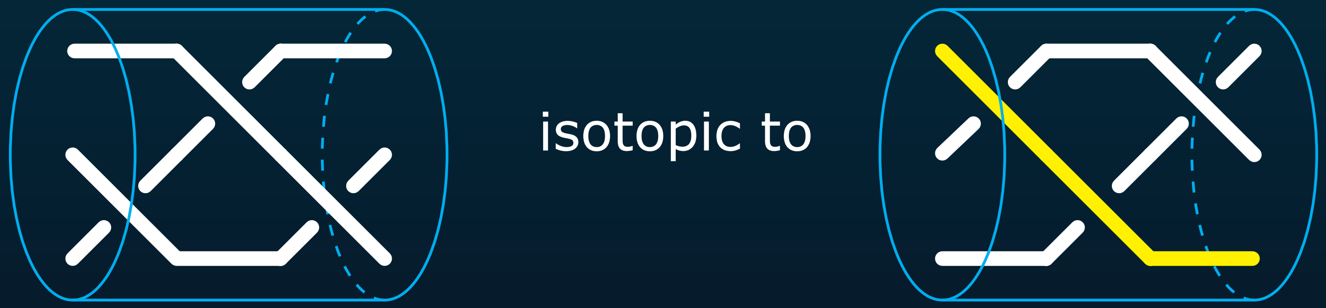


- a braid = an isotopy class $\rightsquigarrow$ represented by 2D-diagram,

- A 4-strand braid diagram = 2D-projection of a 3D-figure



- isotopy = move the strands on the 3D-figure keeping the ends fixed

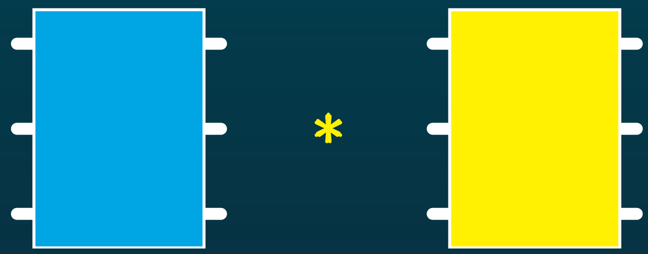


- a braid = an isotopy class $\rightsquigarrow$ represented by 2D-diagram,

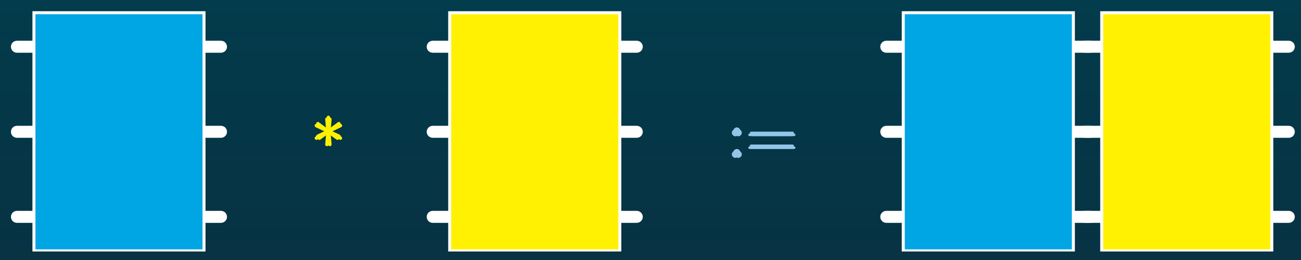
  but different 2D-diagrams may give rise to the same braid.

- Product of two braids:

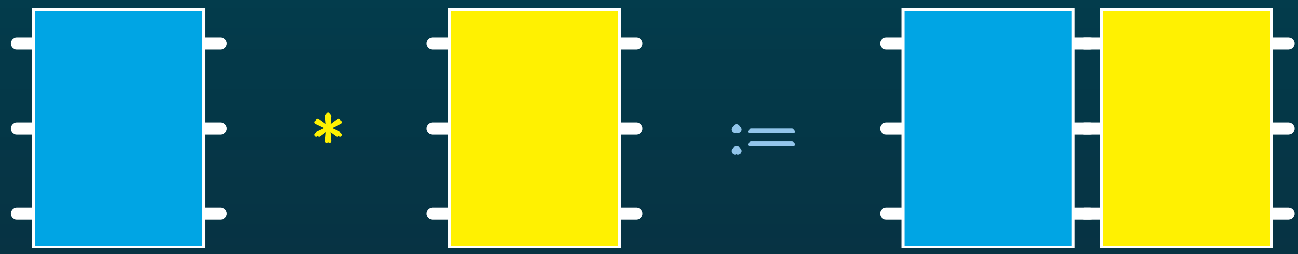
- Product of two braids:



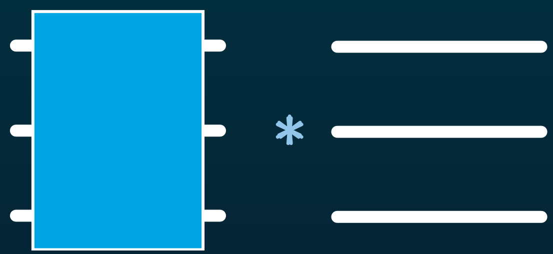
- Product of two braids:



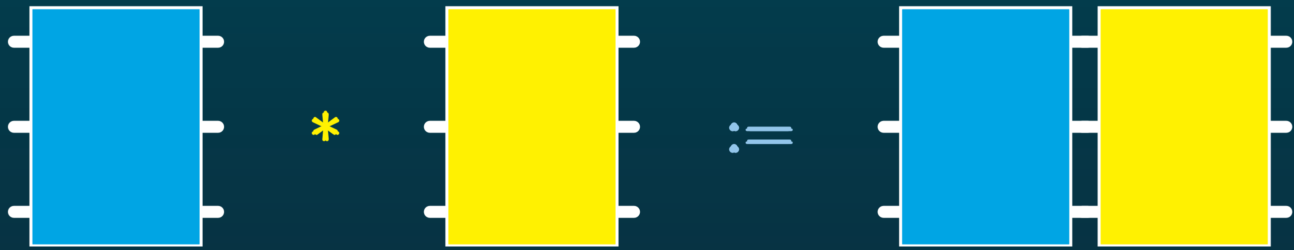
- Product of two braids:



- Then

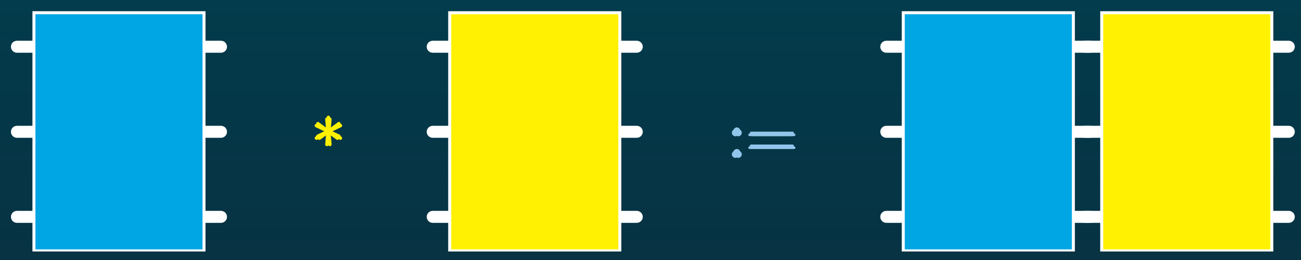


- Product of two braids:

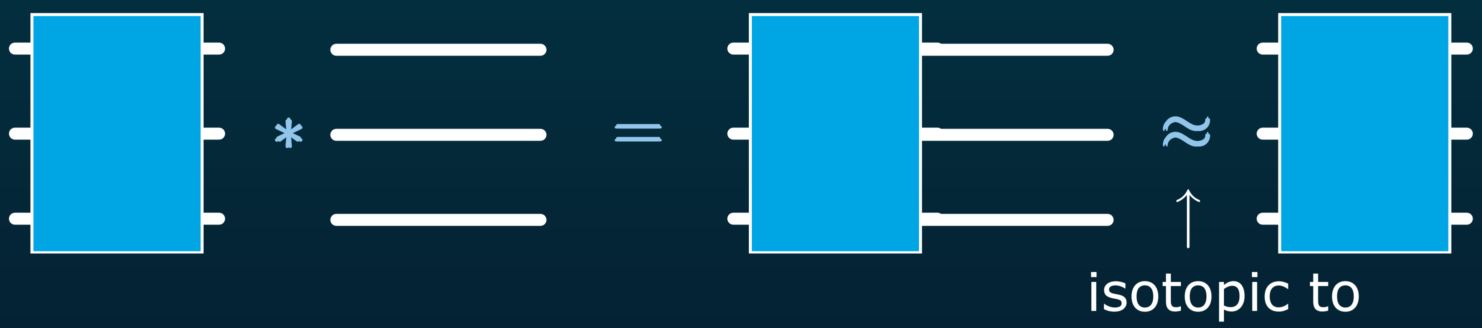


- Then

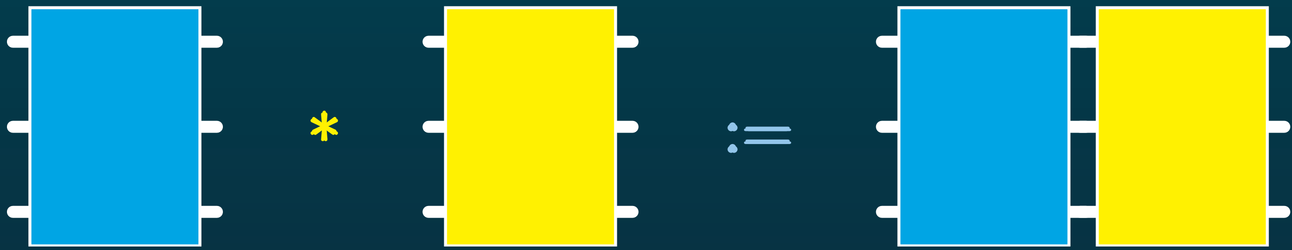
- Product of two braids:



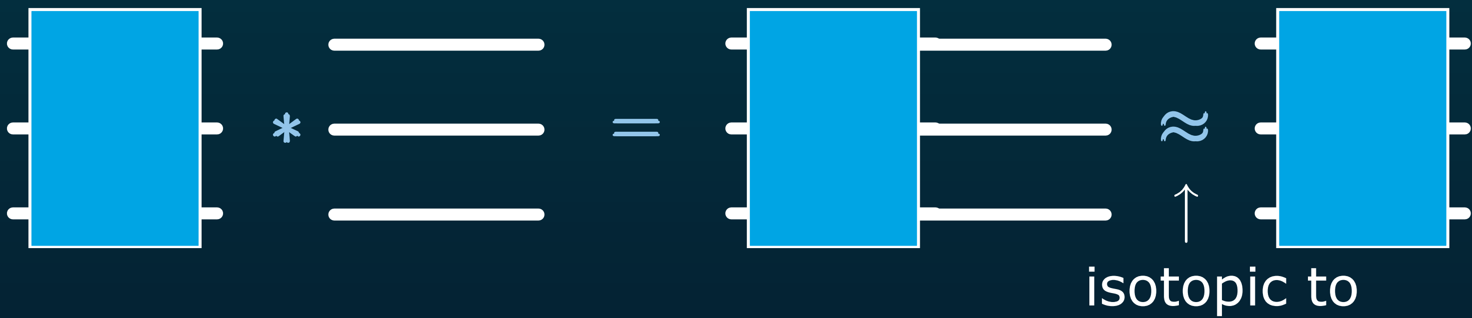
- Then



- Product of two braids:

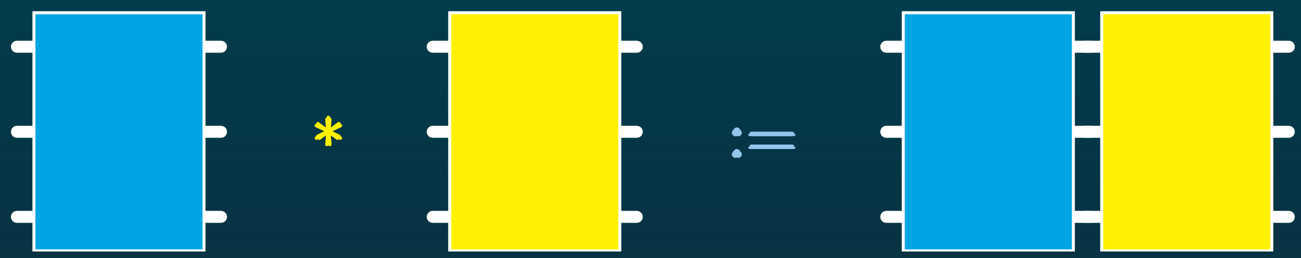


- Then

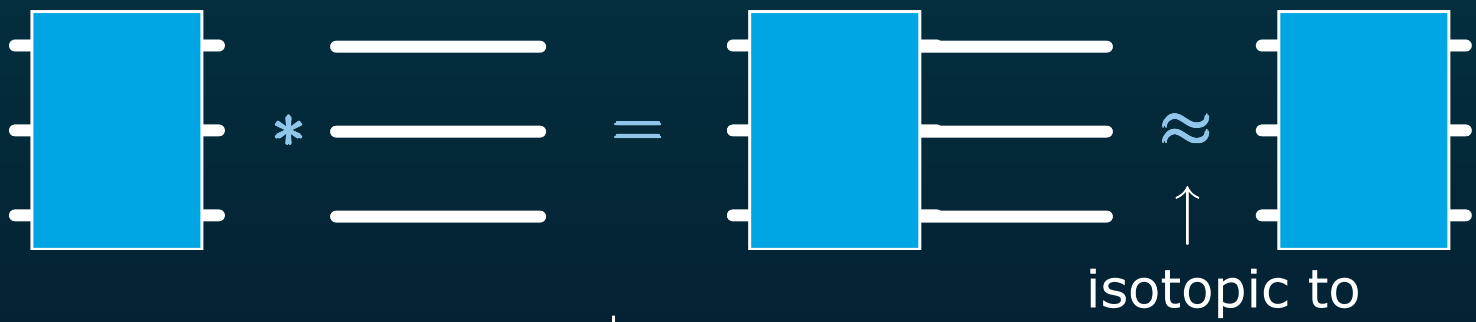


- and

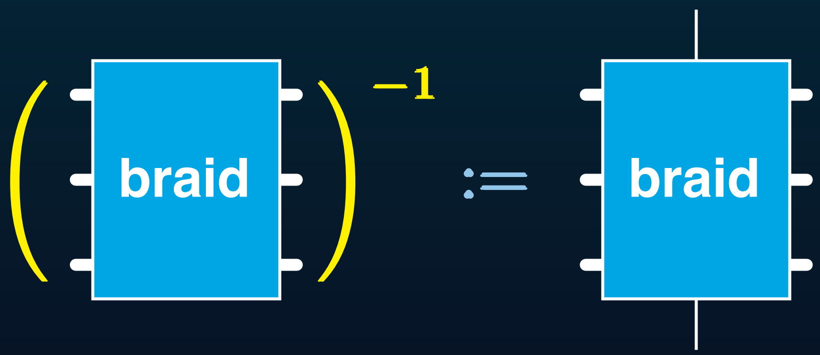
- Product of two braids:



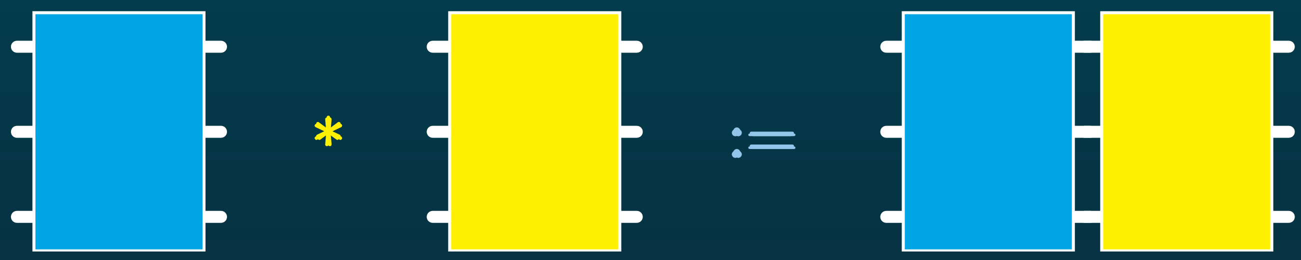
- Then



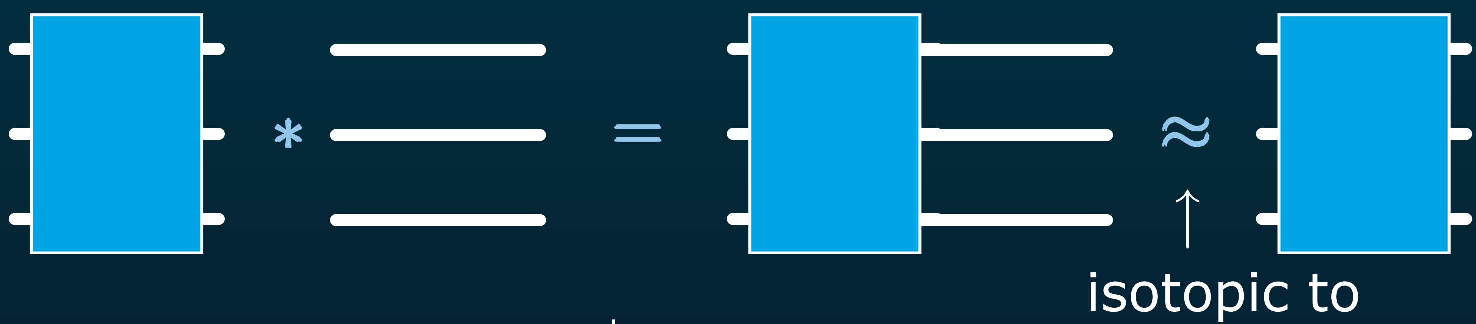
- and



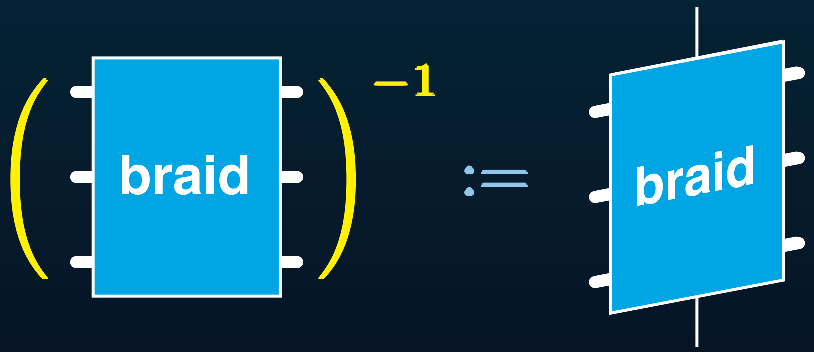
- Product of two braids:



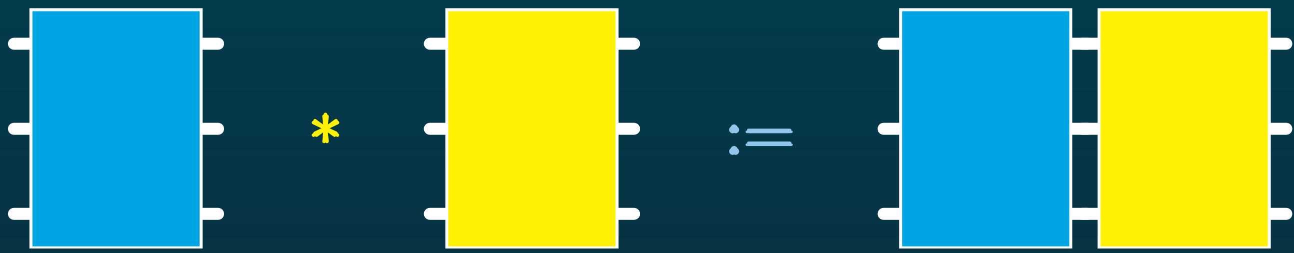
- Then



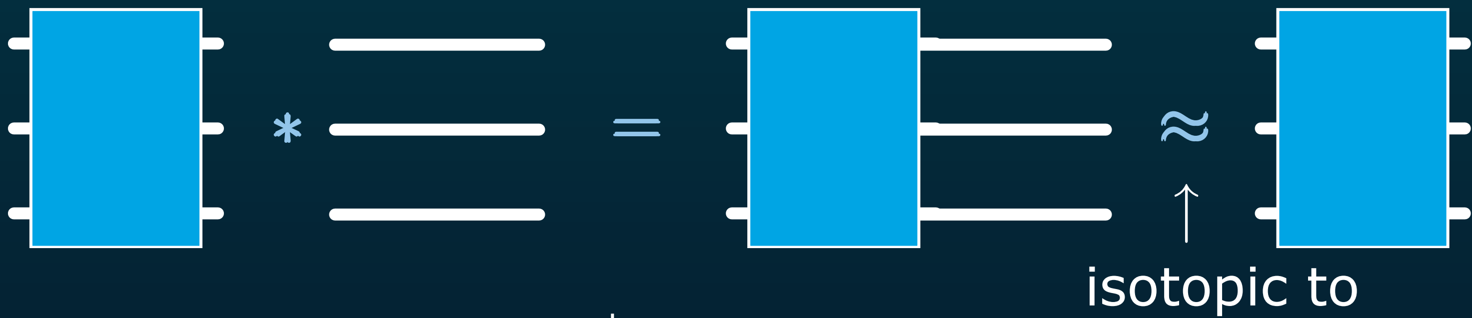
- and



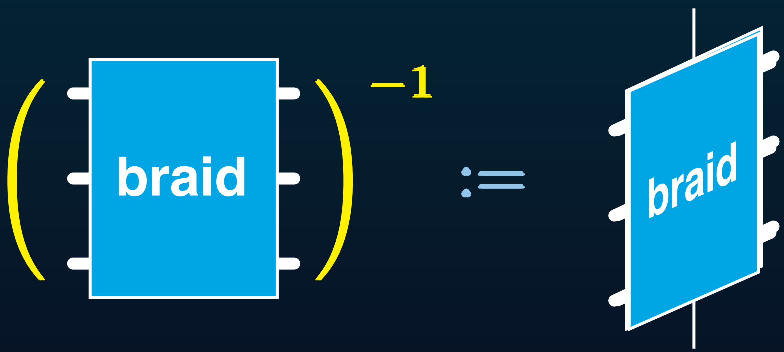
- Product of two braids:



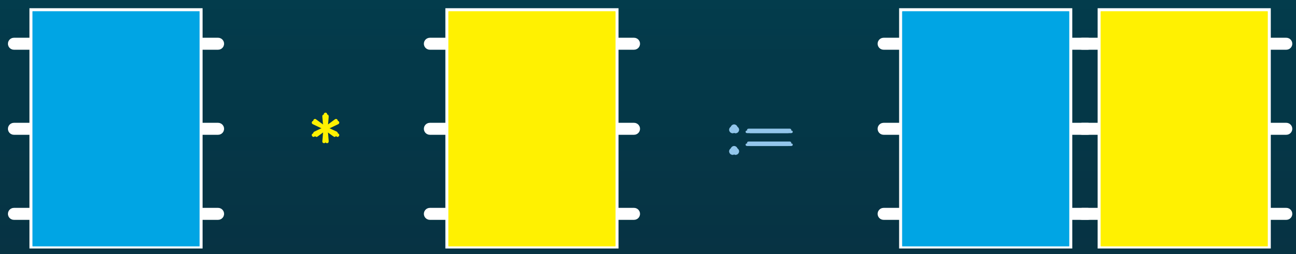
- Then



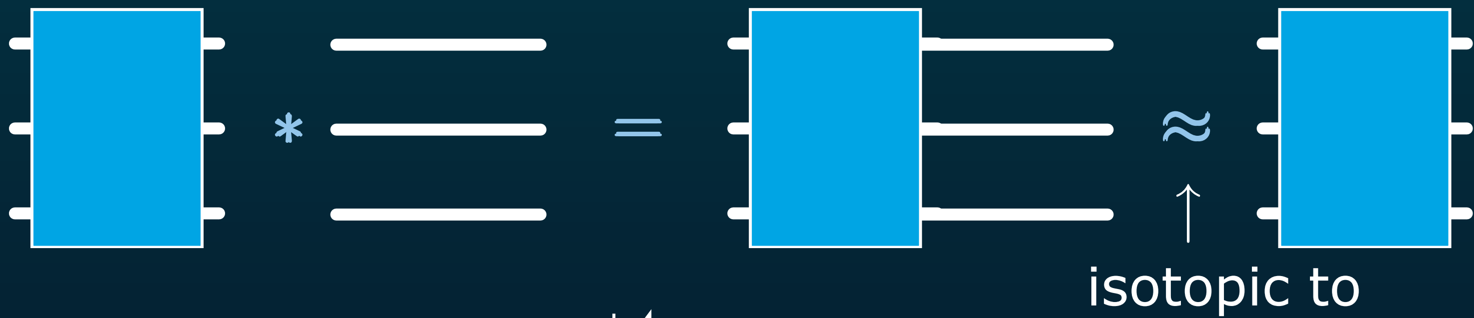
- and



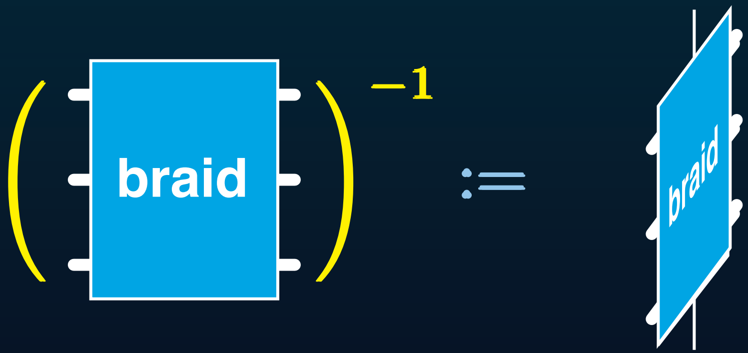
- Product of two braids:



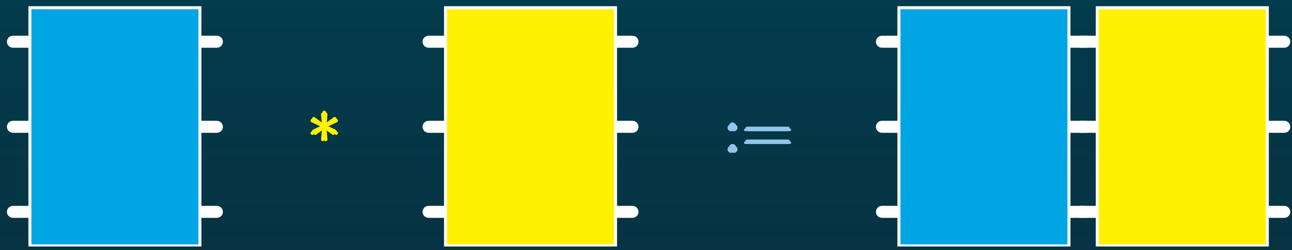
- Then



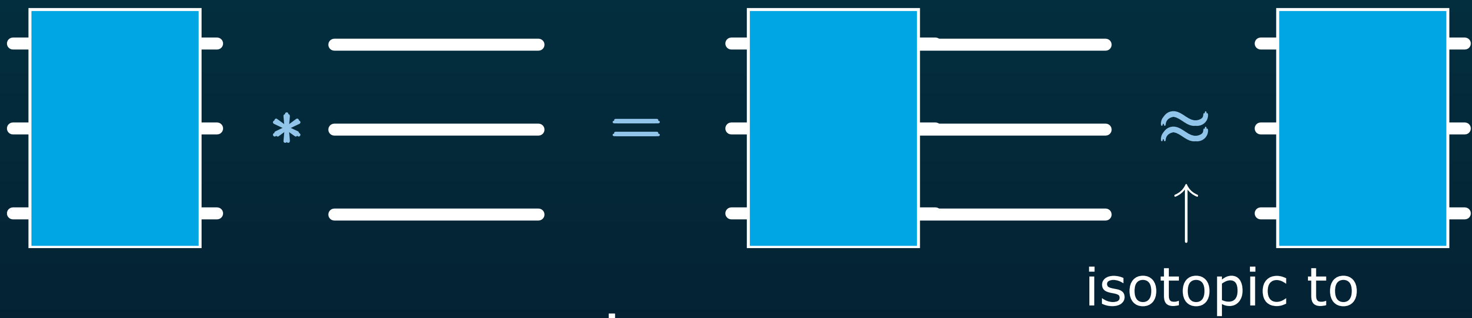
- and



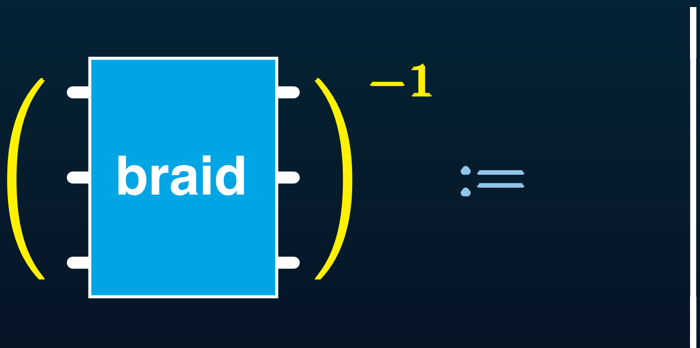
- Product of two braids:



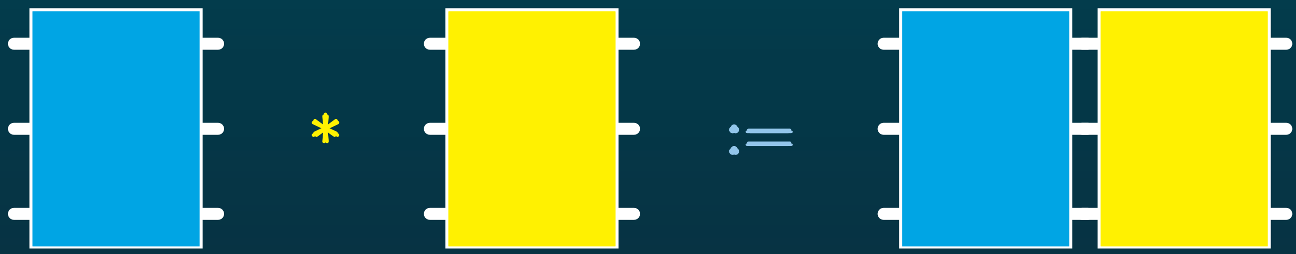
- Then



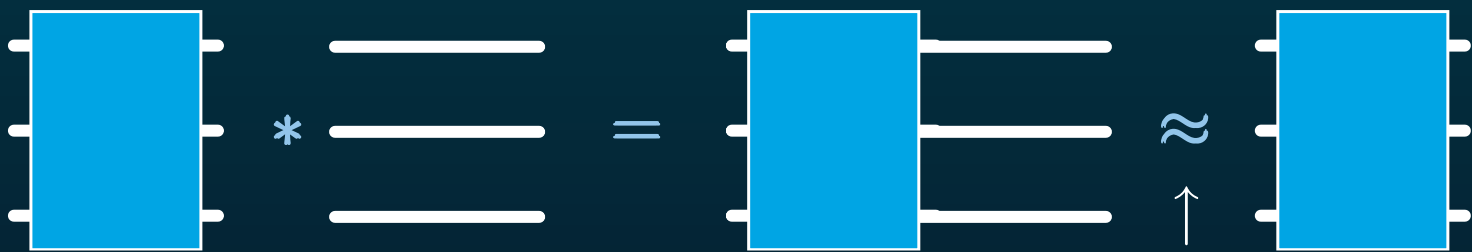
- and



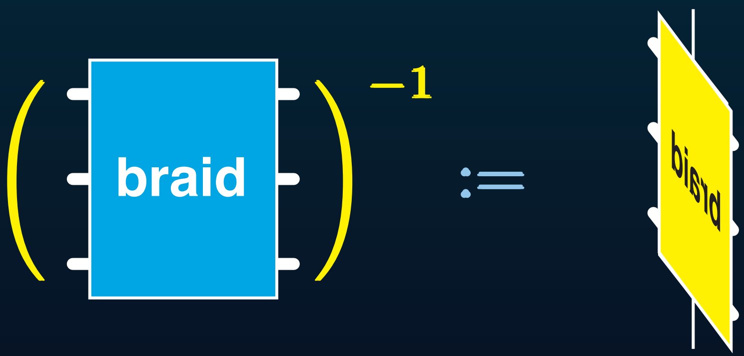
- Product of two braids:



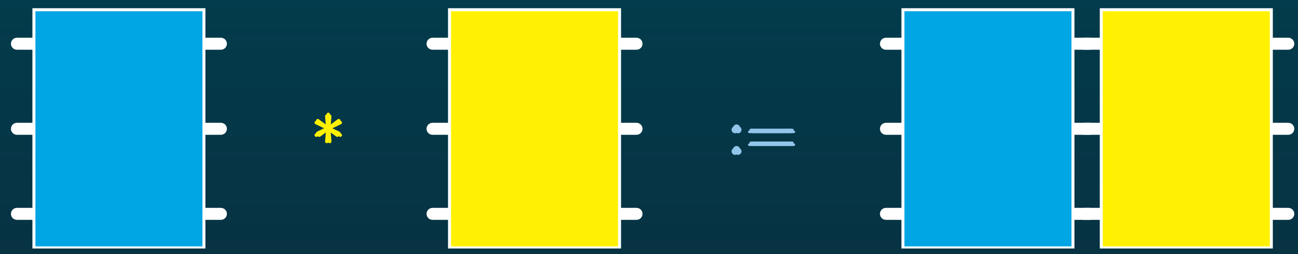
- Then



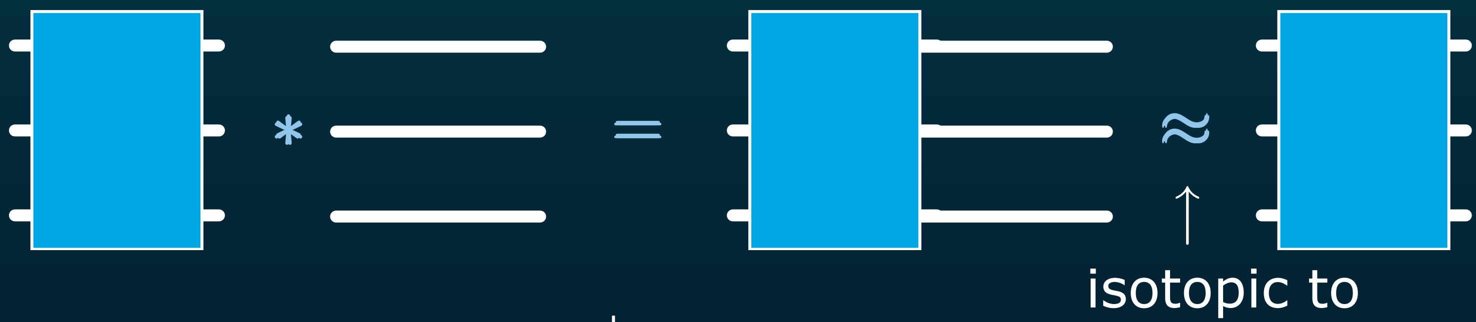
- and



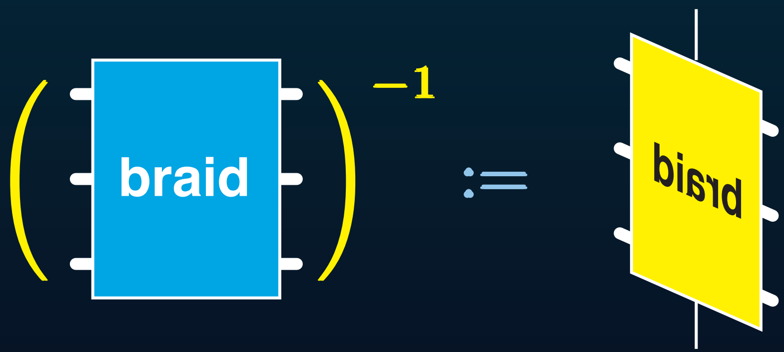
- Product of two braids:



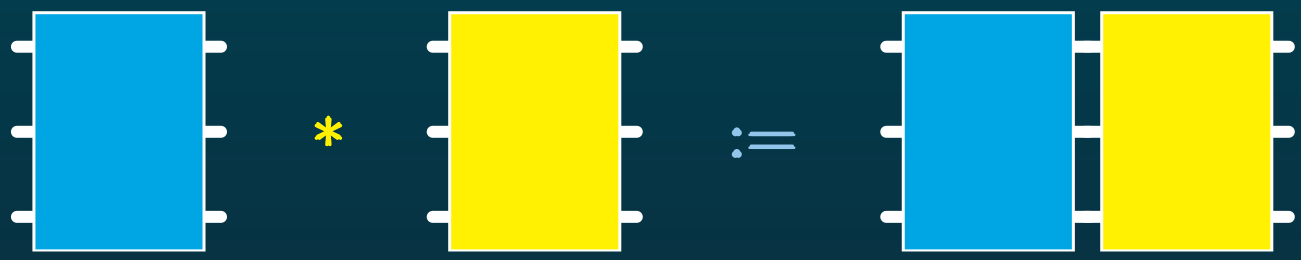
- Then



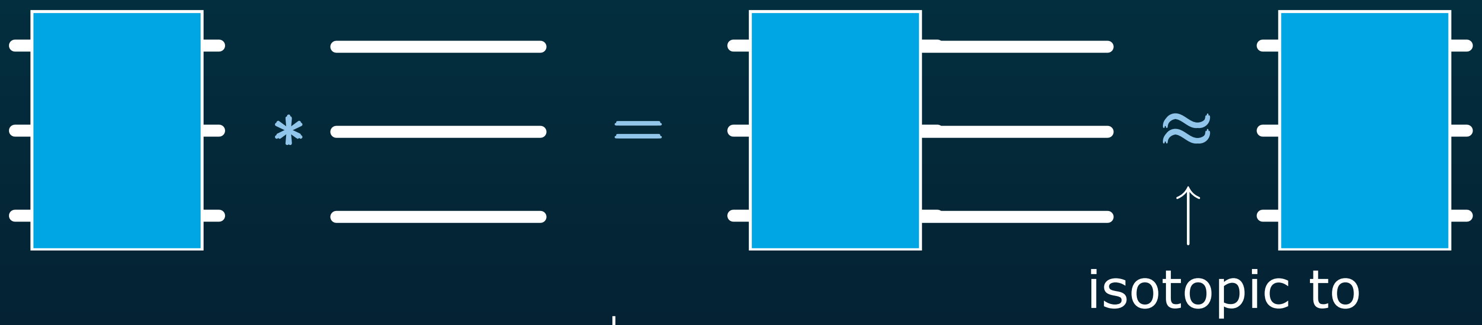
- and



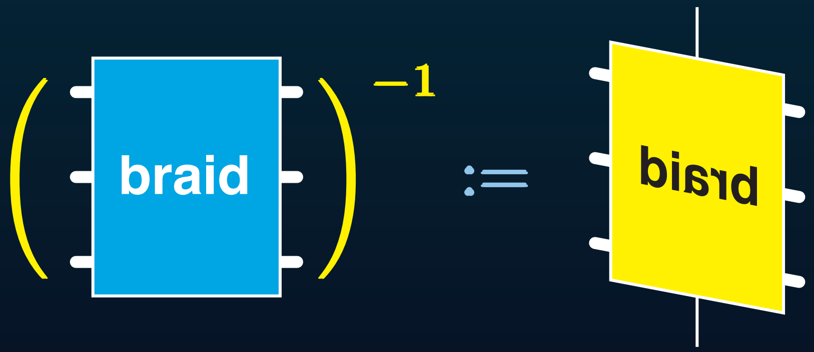
- Product of two braids:



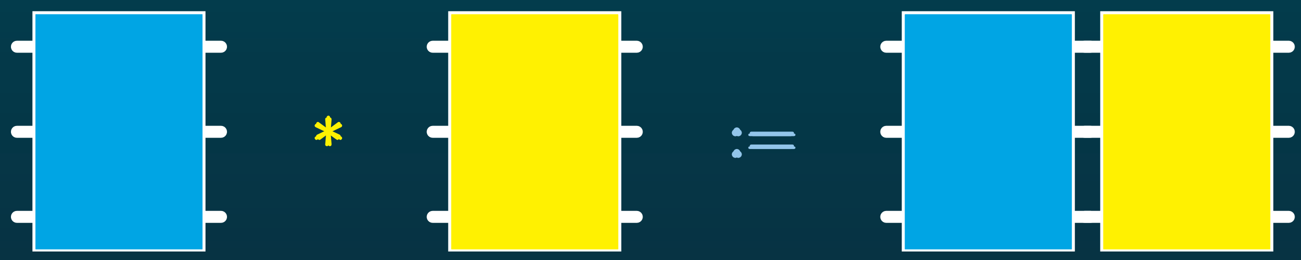
- Then



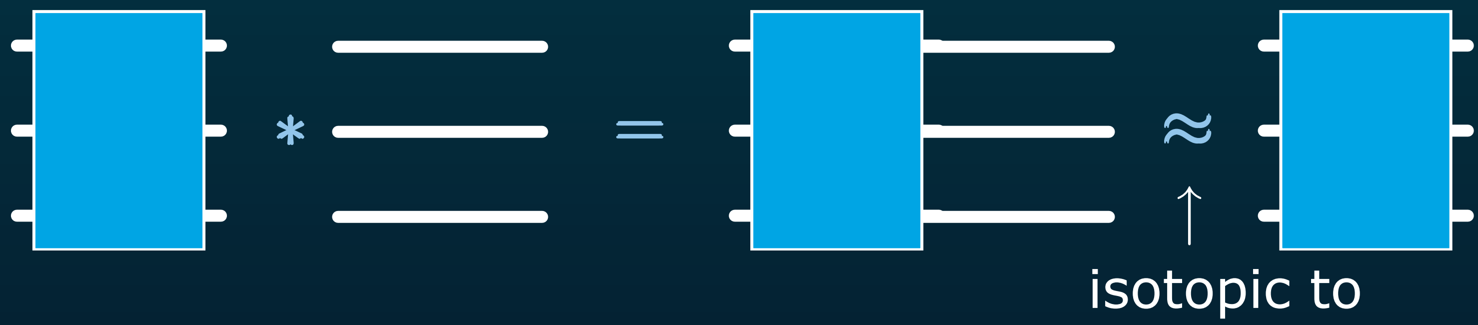
- and



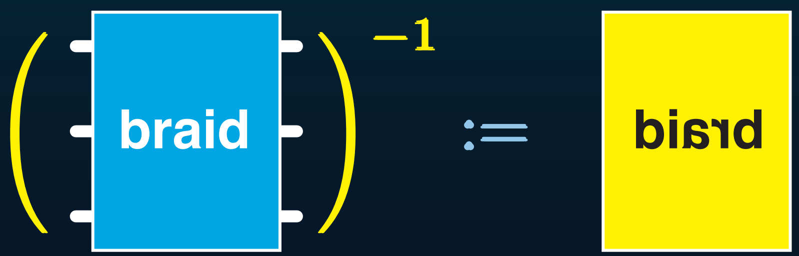
- Product of two braids:



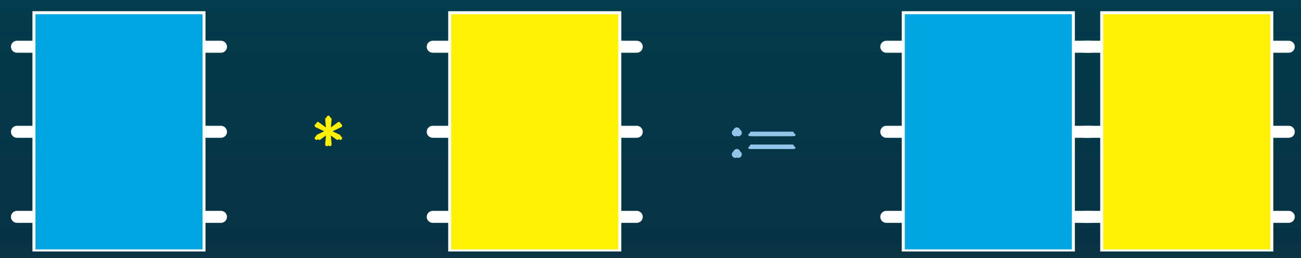
- Then



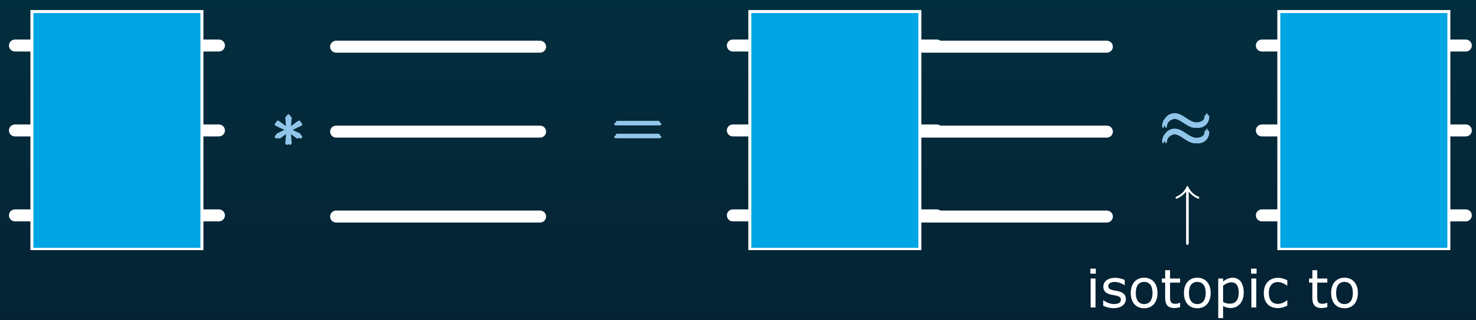
- and



- Product of two braids:

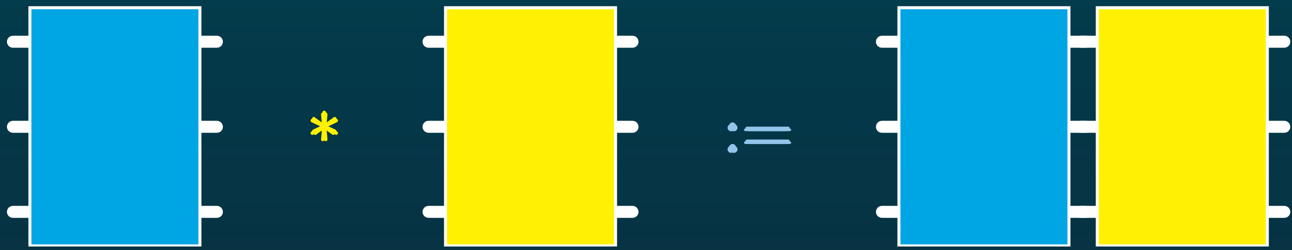


- Then

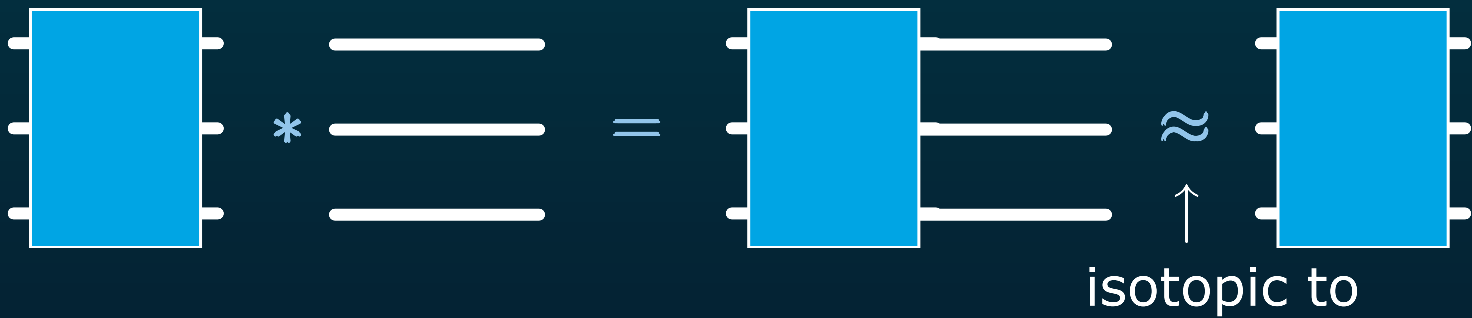


- and

- Product of two braids:

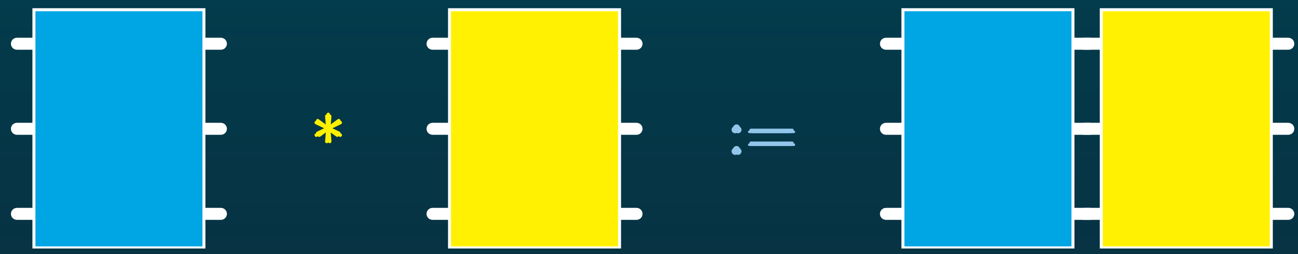


- Then

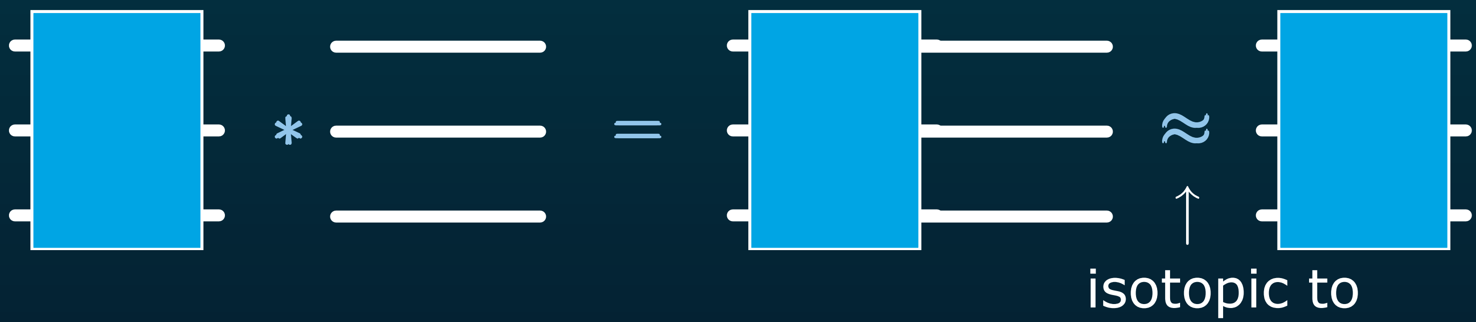


- and

- Product of two braids:

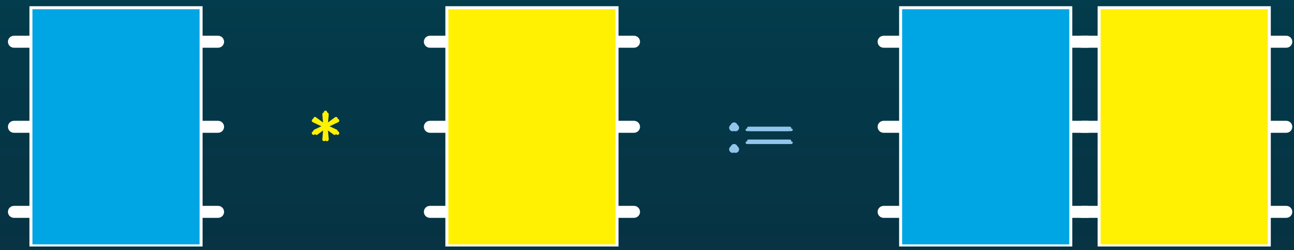


- Then

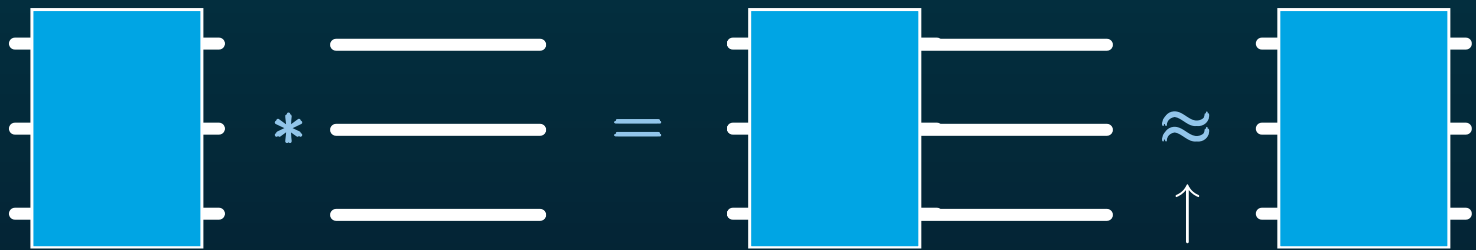


- and

- Product of two braids:

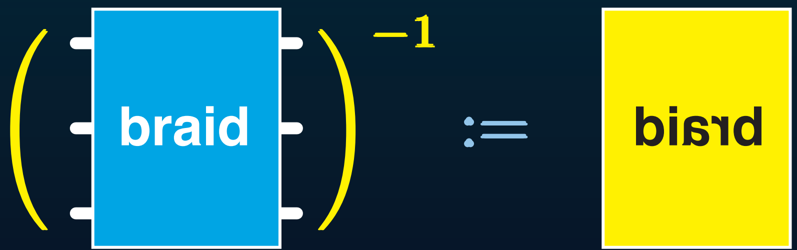


- Then



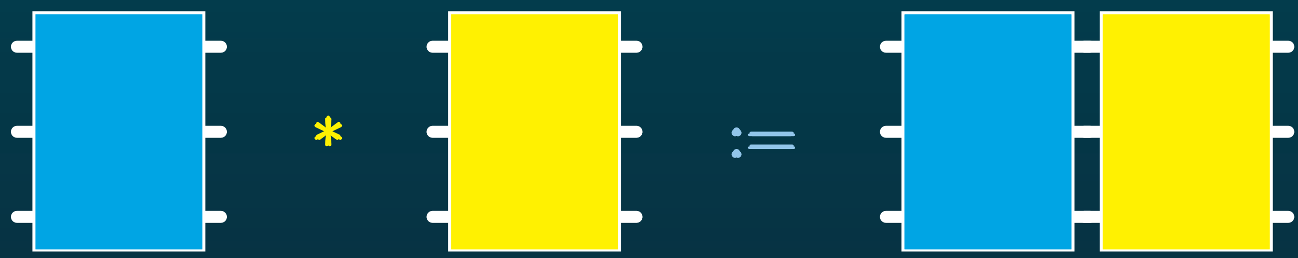
isotopic to

- and

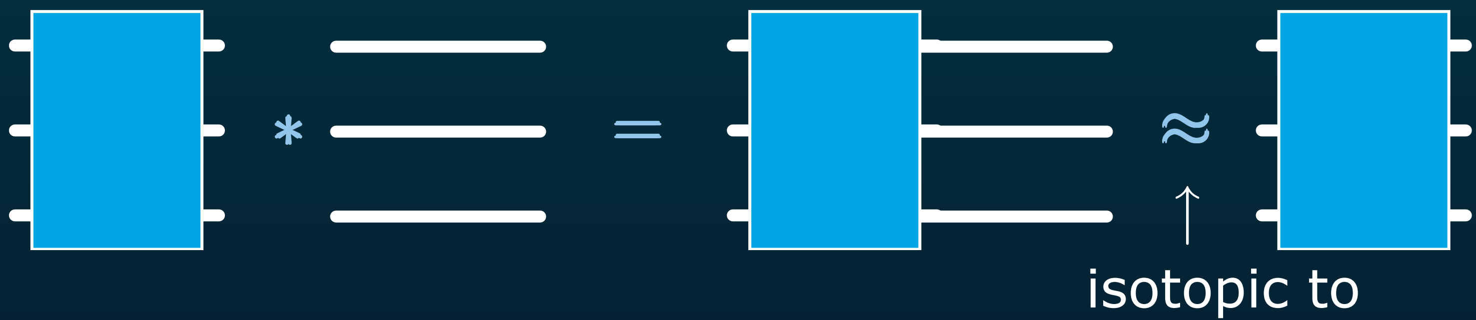


as

- Product of two braids:



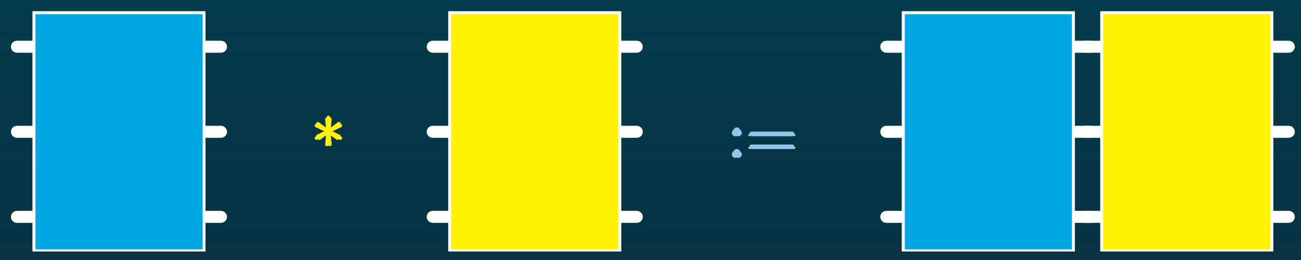
- Then



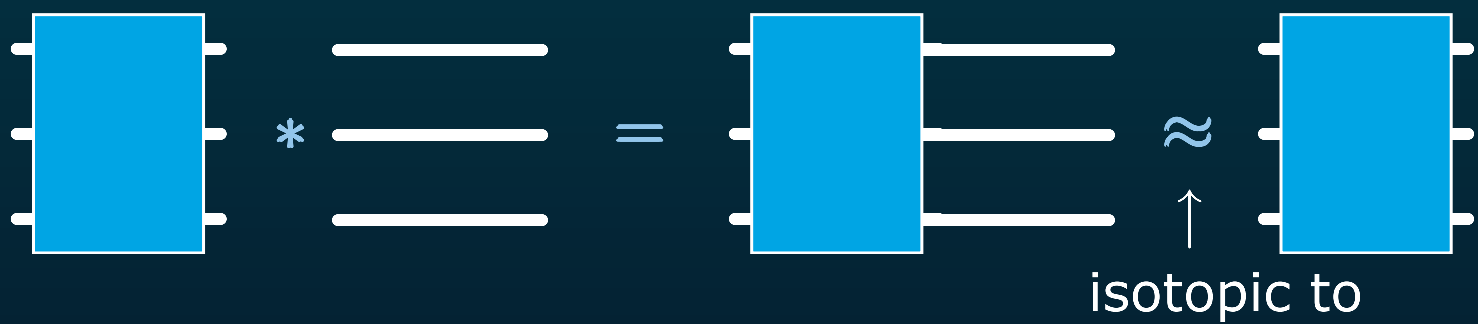
- and

THE BRAID GROUPS

- Product of two braids:

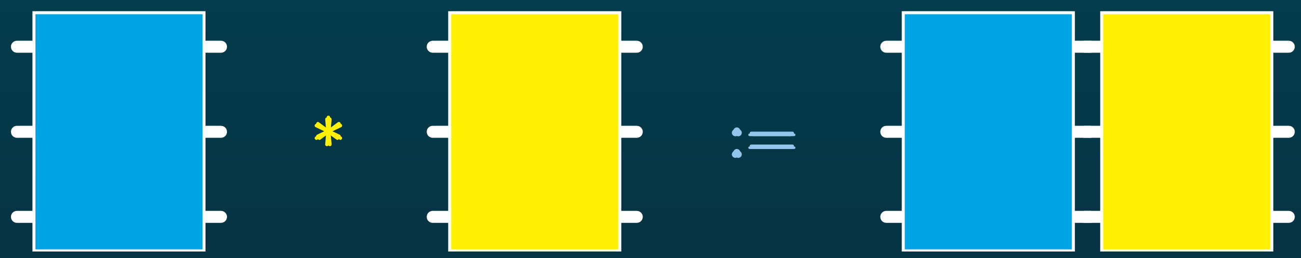


- Then

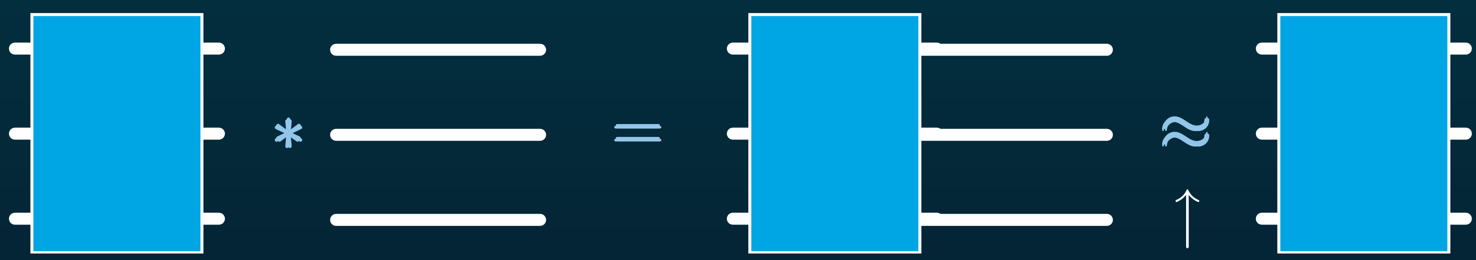


- and

- Product of two braids:



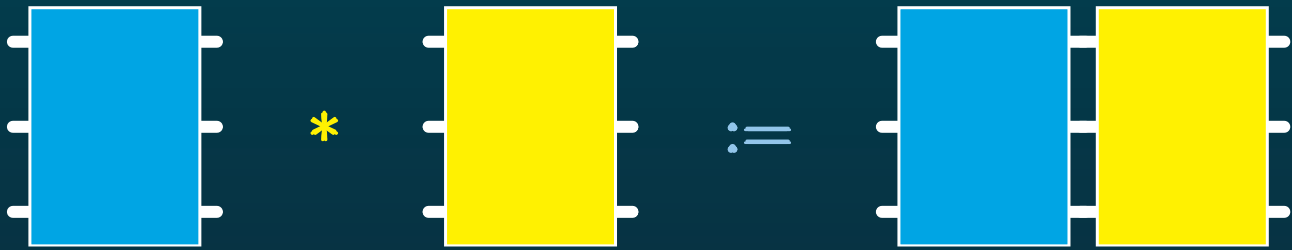
- Then



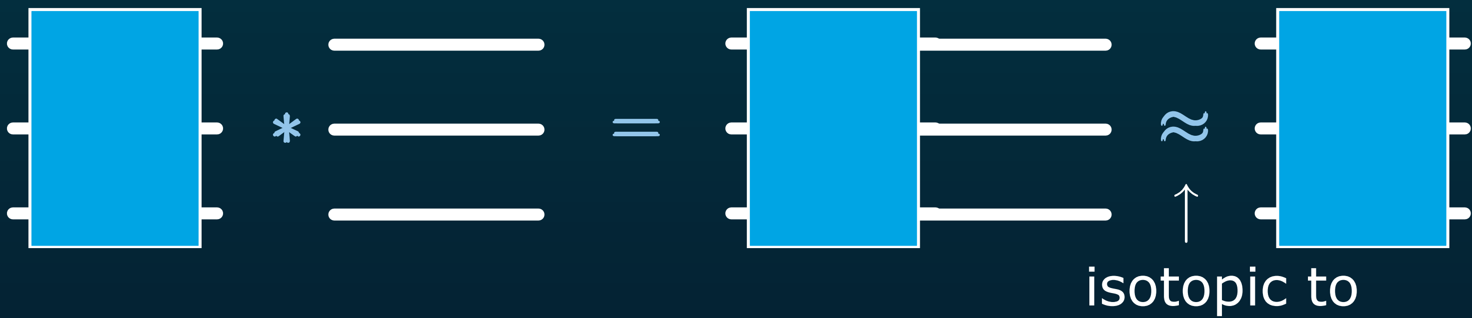
isotopic to

- and

- Product of two braids:

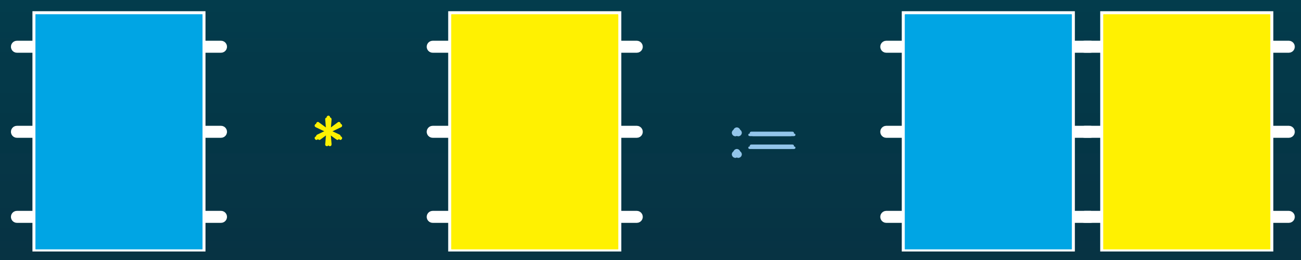


- Then

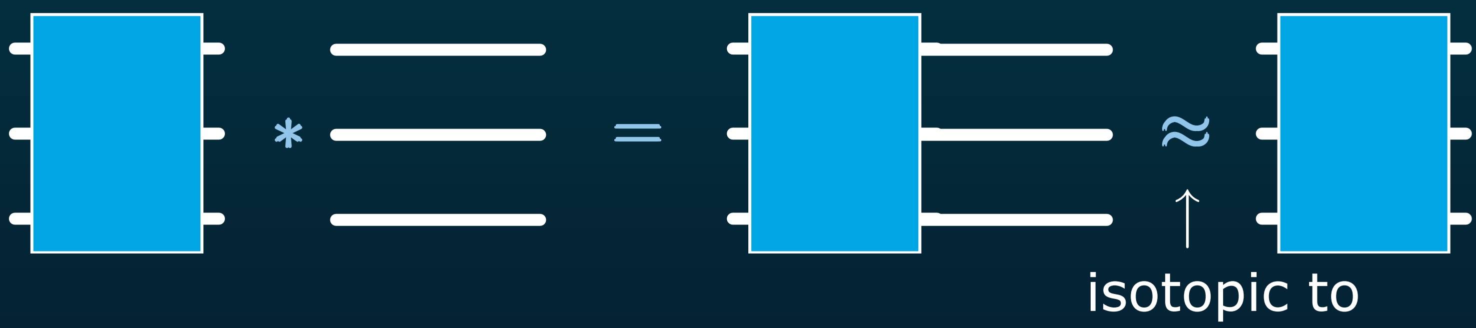


- and

- Product of two braids:

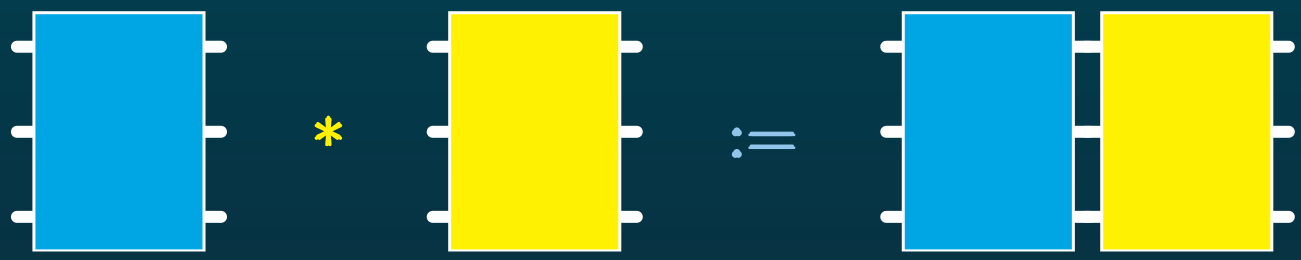


- Then

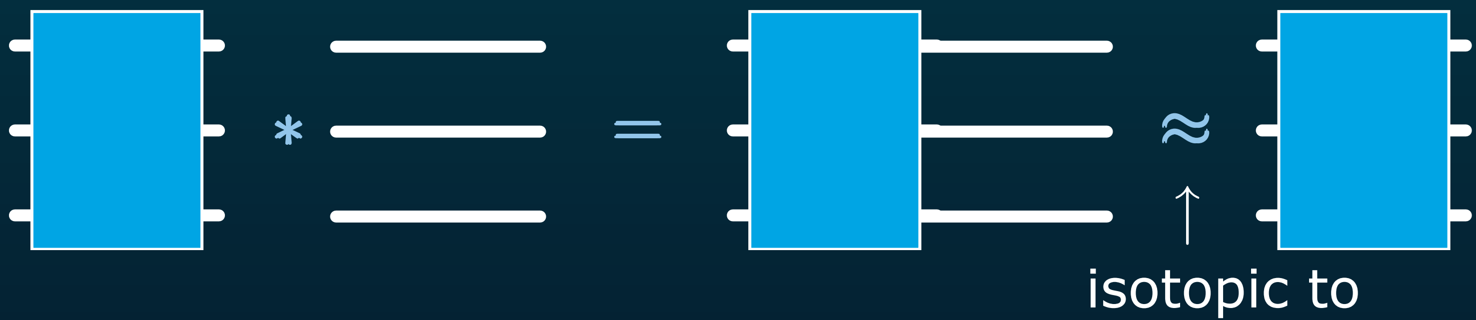


- and

- Product of two braids:

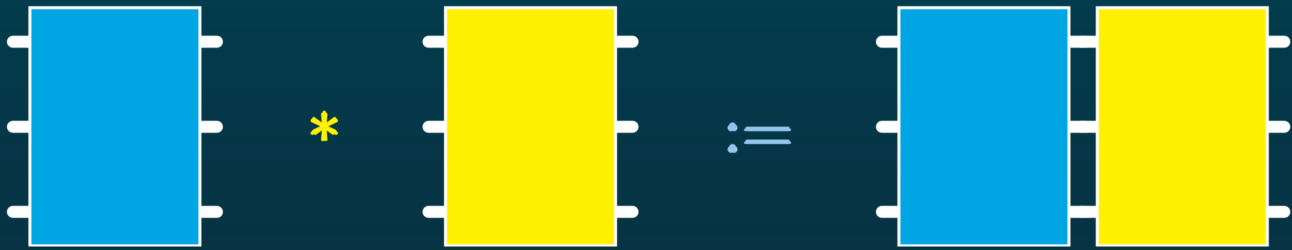


- Then

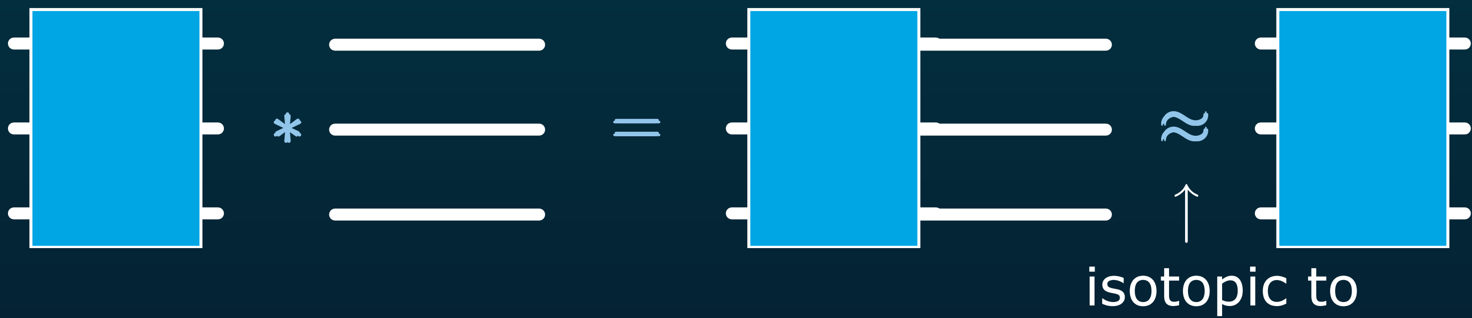


- and

- Product of two braids:

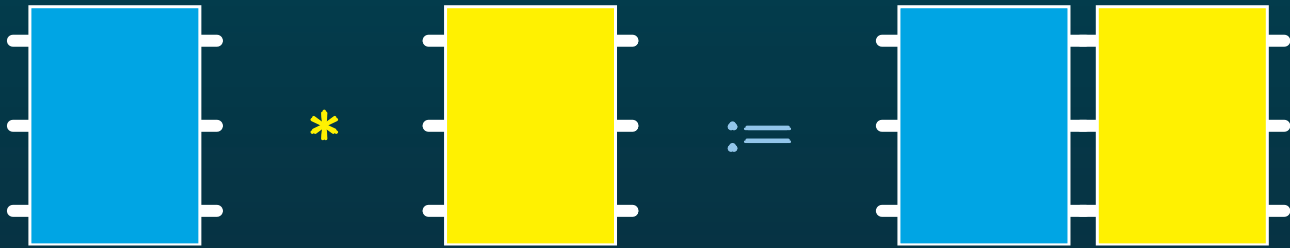


- Then

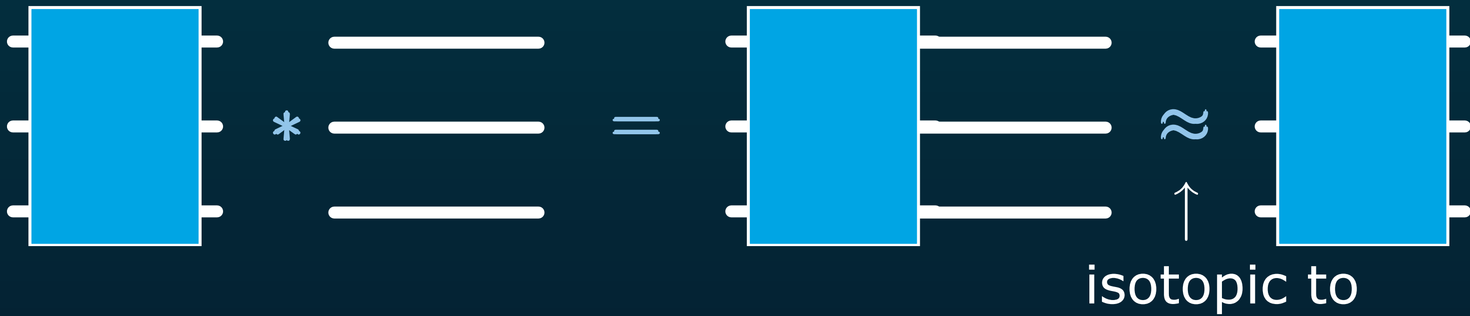


- and

- Product of two braids:



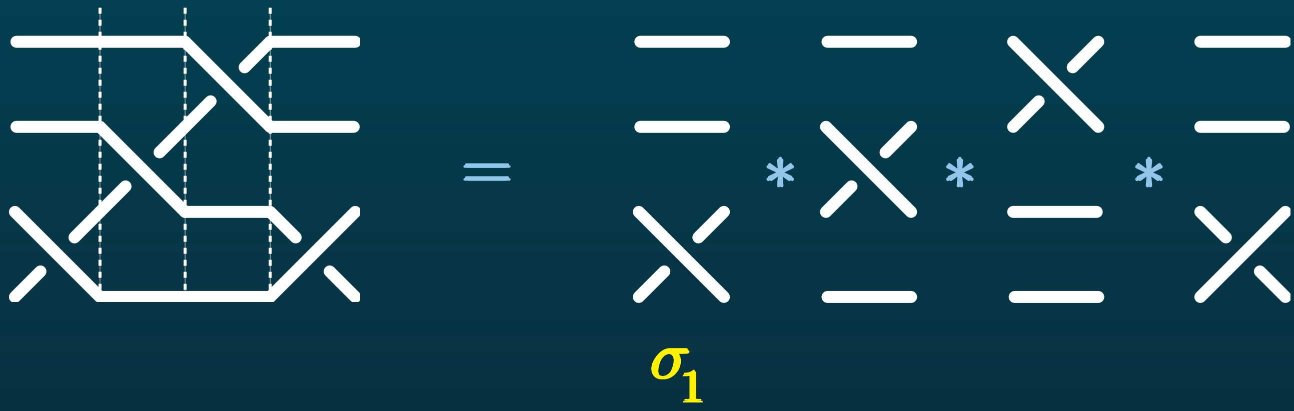
- Then

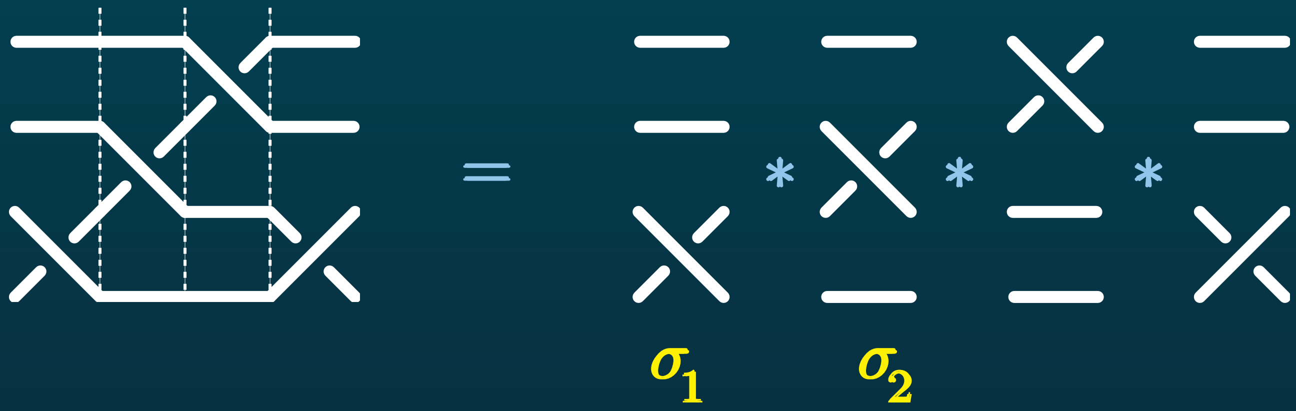


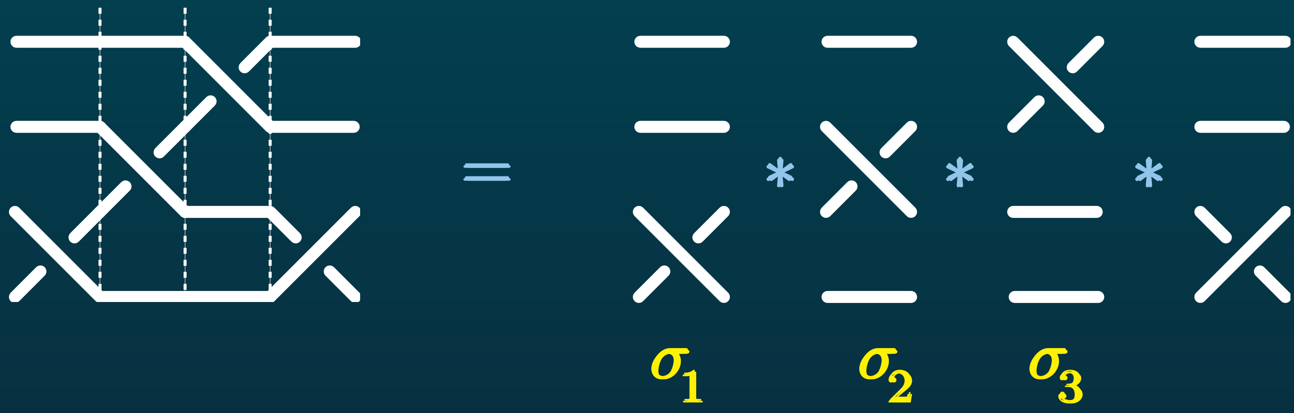
- and

$\rightsquigarrow$ For each n, the group B_n of n strand braids (E. Artin, $\sim$1925).

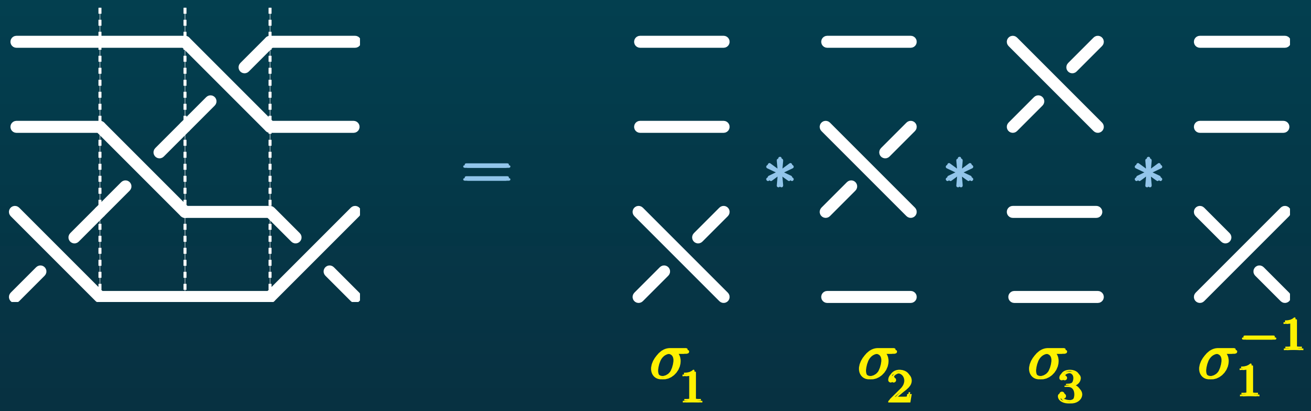
A PRESENTATION OF B_n

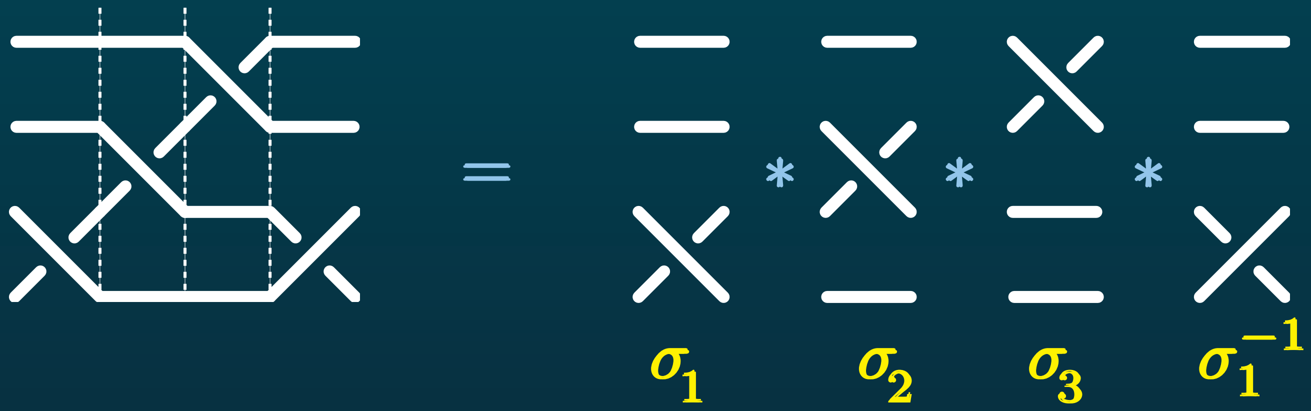



σ_1
σ_2


=
*
*
*
σ_1
σ_2
σ_3

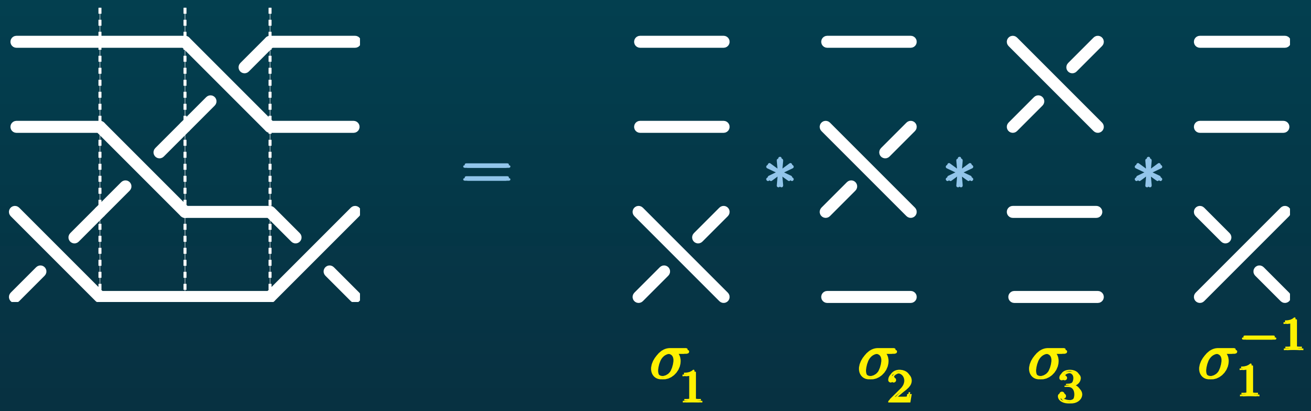
A PRESENTATION OF B_n



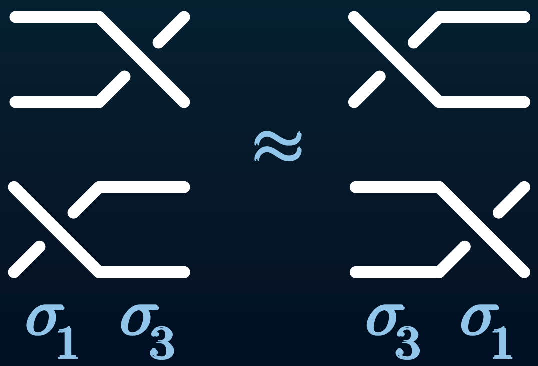


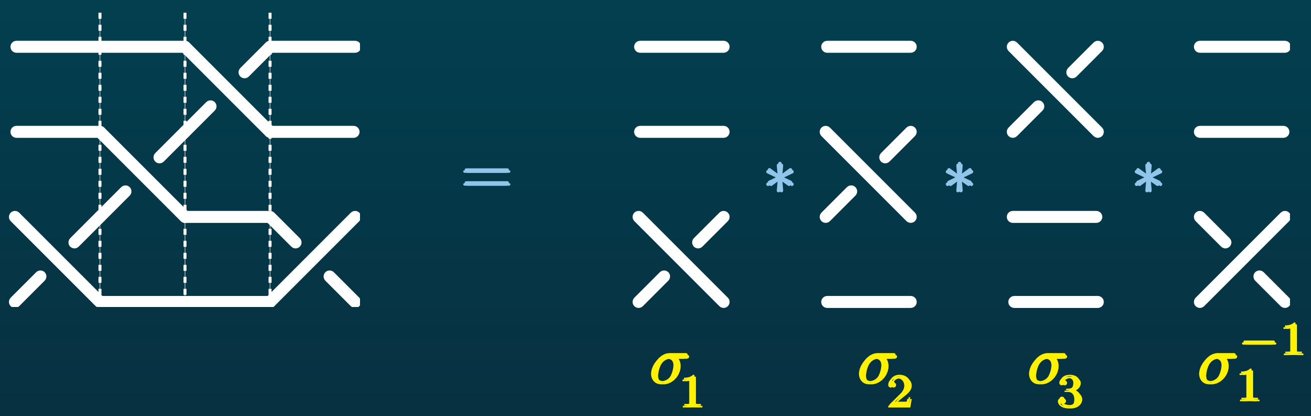
- Theorem (Artin): The group B_n is generated by $\sigma_1, \ldots, \sigma_{n-1}$, subject to $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $|i-j| \geqslant 2$, and $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ for $|i-j| = 1$.

A PRESENTATION OF B_n

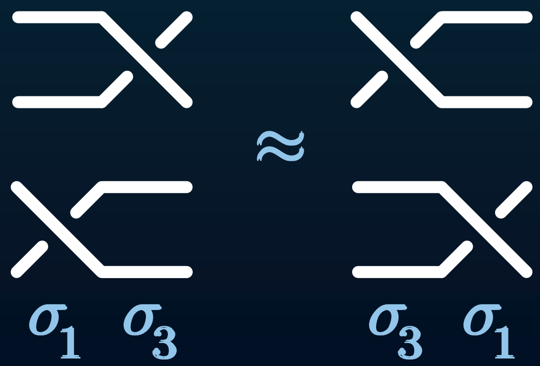


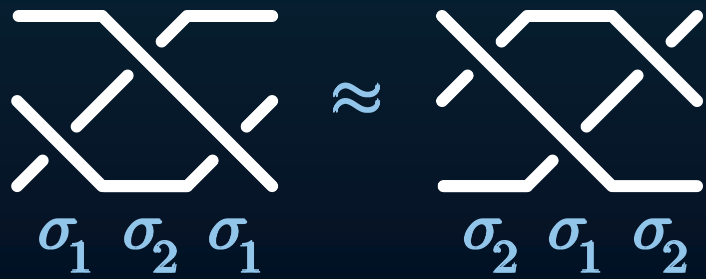
- Theorem (Artin): The group B_n is generated by $\sigma_1, \dots, \sigma_{n-1}$, subject to $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $|i - j| \geqslant 2$, and $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ for $|i - j| = 1$.





- Theorem (Artin): The group B_n is generated by $\sigma_1, \ldots, \sigma_{n-1}$, subject to
  $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $|i-j| \geqslant 2$, and $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ for $|i-j| = 1$.





- The isotopy problem of braids:

  Recognize if a braid diagram is isotopic to the trivial diagram

  $\Leftrightarrow$ Recognize if a braid word w represents 1 in the braid group.

- The isotopy problem of braids:

  Recognize if a braid diagram is isotopic to the trivial diagram

  $\Leftrightarrow$ Recognize if a braid word w represents 1 in the braid group.

  $\rightsquigarrow$ Problem #0 for possible applications, ***e.g.***, in cryptography

- The isotopy problem of braids:

  Recognize if a braid diagram is isotopic to the trivial diagram

  $\Leftrightarrow$ Recognize if a braid word w represents 1 in the braid group.

  $\rightsquigarrow$ Problem #0 for possible applications, ***e.g.***, in cryptography

- In a free group, w represents 1 iff w reduces to the empty word:

  iteratively delete patterns xx^{-1} and $x^{-1}x$.

- The isotopy problem of braids:

  Recognize if a braid diagram is isotopic to the trivial diagram

  $\Leftrightarrow$ Recognize if a braid word w represents 1 in the braid group.

  $\rightsquigarrow$ Problem #0 for possible applications, ***e.g.***, in cryptography

- In a free group, w represents 1 iff w reduces to the empty word:

  iteratively delete patterns xx^{-1} and $x^{-1}x$.

- In a non-free group, does not work:

  $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ represents 1 in B_n, but contains no $\sigma_i\sigma_i^{-1}$ or $\sigma_i^{-1}\sigma_i$.

- The isotopy problem of braids:

  Recognize if a braid diagram is isotopic to the trivial diagram

  $\Leftrightarrow$ Recognize if a braid word w represents 1 in the braid group.

  $\rightsquigarrow$ Problem #0 for possible applications, ***e.g.***, in cryptography

- In a free group, w represents 1 iff w reduces to the empty word:

  iteratively delete patterns xx^{-1} and $x^{-1}x$.

- In a non-free group, does not work:

  $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ represents 1 in B_n, but contains no $\sigma_i\sigma_i^{-1}$ or $\sigma_i^{-1}\sigma_i$.

  $\rightsquigarrow$ Question: Does some reduction work for B_n?

...yes, handle reduction.

...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$
  $\rightsquigarrow$ a pair $\sigma_1 ... \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.

...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  $\rightsquigarrow$ a pair $\sigma_1 \ldots \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.

...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  $\rightsquigarrow$ a pair $\sigma_1 \ldots \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.

...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$
  $\rightsquigarrow$ a pair $\sigma_1 ... \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.

...yes, handle reduction.

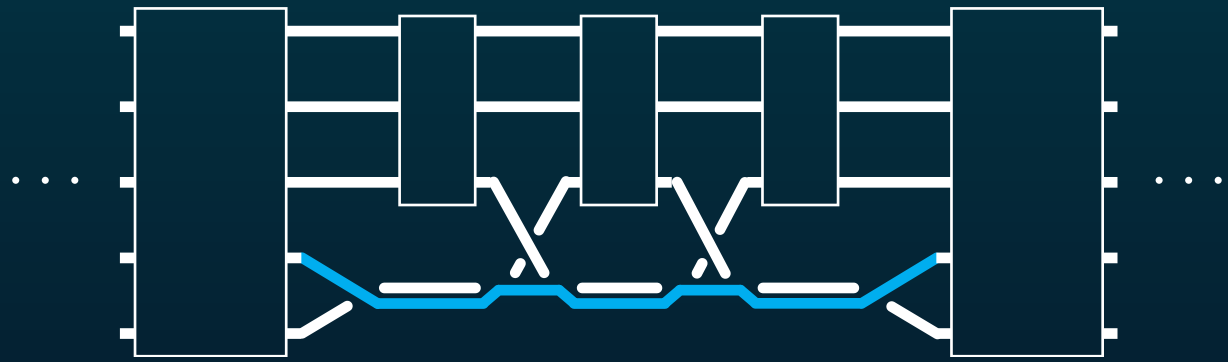
- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  $\rightsquigarrow$ a pair $\sigma_1 \ldots \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.

...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

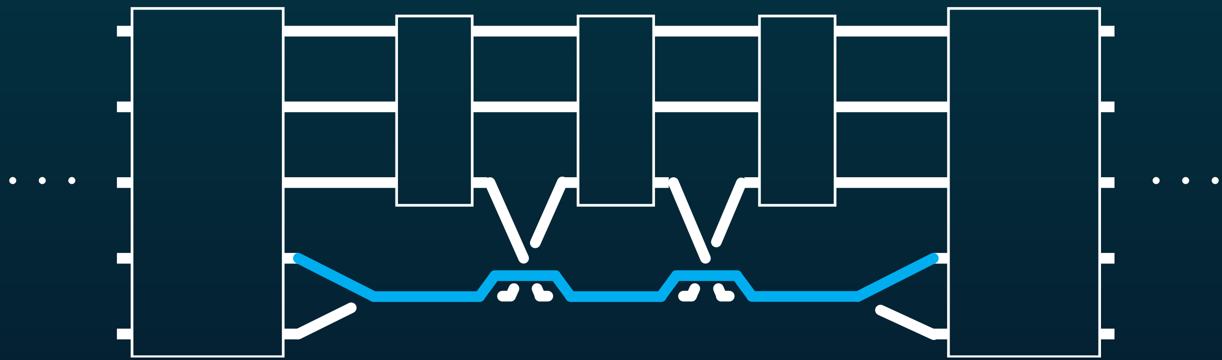
  $\rightsquigarrow$ a pair $\sigma_1 \ldots \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.



...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

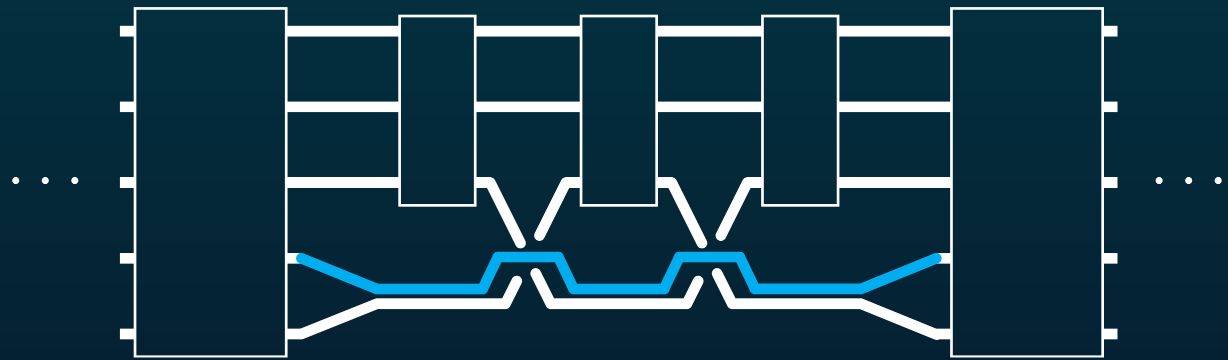
  $\rightsquigarrow$ a pair $\sigma_1 ... \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.



...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

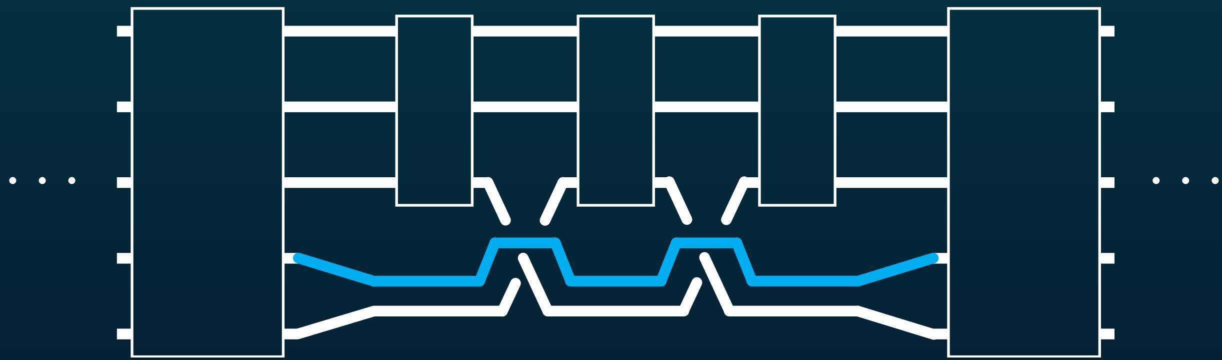
  $\rightsquigarrow$ a pair $\sigma_1 \ldots \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.



...yes, handle reduction.

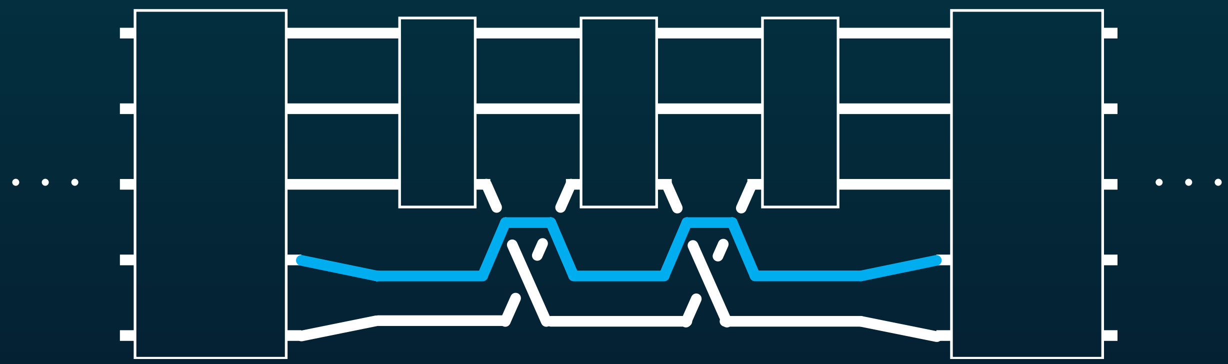
- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  $\rightsquigarrow$ a pair $\sigma_1 ... \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.



...yes, handle reduction.

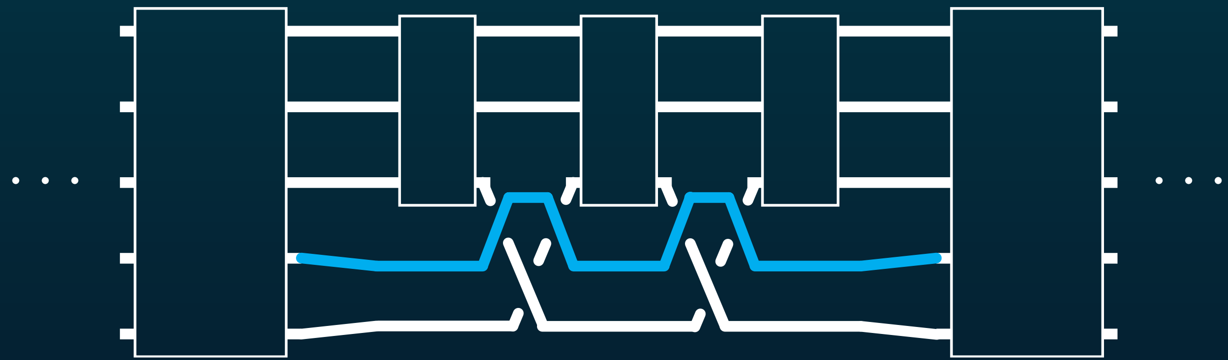
- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$
  $\rightsquigarrow$ a pair $\sigma_1 \dots \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.



...yes, handle reduction.

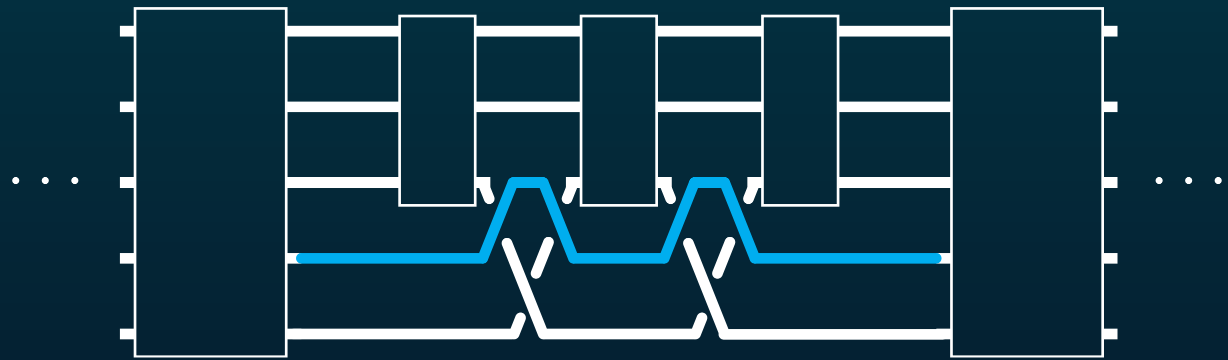
- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

$\rightsquigarrow$ a pair $\sigma_1 ... \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.



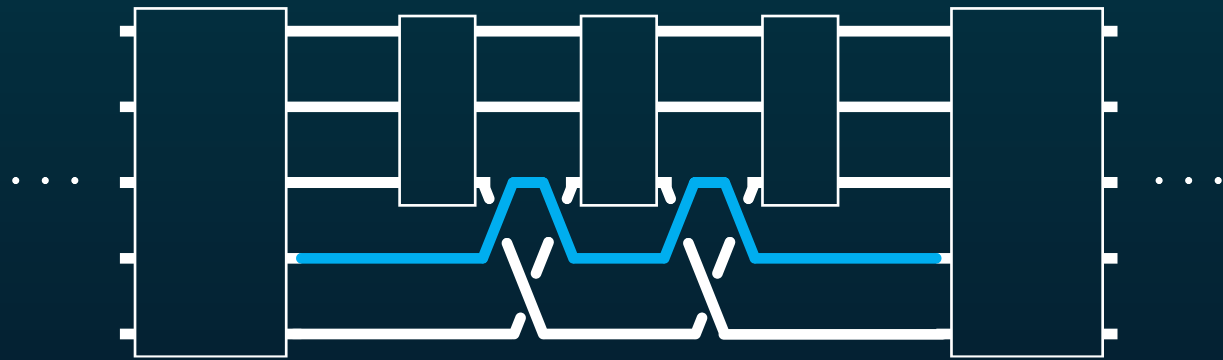
...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$
  $\rightsquigarrow$ a pair $\sigma_1 ... \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.



...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$
  $\rightsquigarrow$ a pair $\sigma_1 ... \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.

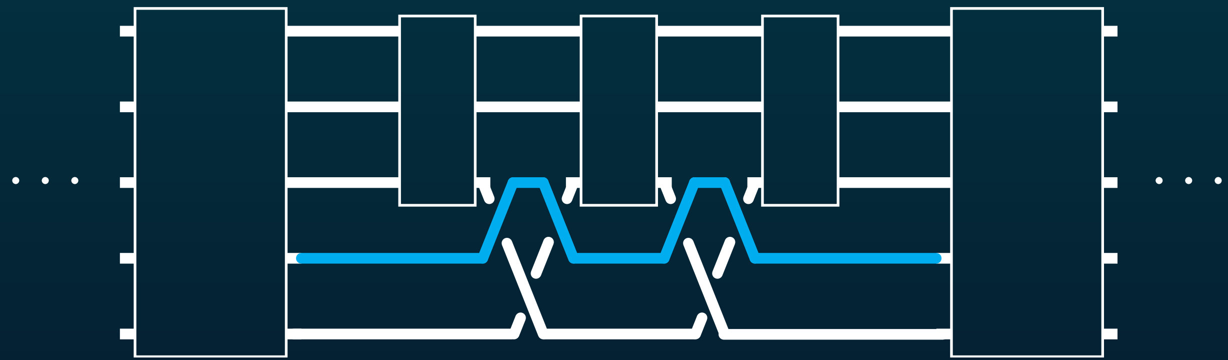


- Definition: Reducing a σ_1-handle $\sigma_1^e w \sigma_1^{-e}$:

...yes, handle reduction.

- The word $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contains $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  $\rightsquigarrow$ a pair $\sigma_1 \ldots \sigma_1^{-1}$ with no $\sigma_1^{\pm 1}$ in the middle: a $\boldsymbol{\sigma_1}$-handle.



- Definition: Reducing a σ_1-handle $\sigma_1^e w \sigma_1^{-e}$:

  - deleting the initial and final σ_1,
  - replacing each $\sigma_2^{\pm 1}$ in w with $\sigma_2^{-e}\sigma_1^{\pm 1}\sigma_2^{e}$.

- Facts: - Handle reduction is an isotopy;

- Facts: - Handle reduction is an isotopy;
  - It extends free group reduction;

- Facts: - Handle reduction is an isotopy;
  - It extends free group reduction;
  - Irreducible words are those not containing both σ_1 and σ_1^{-1}.

- Facts: - Handle reduction is an isotopy;
  - It extends free group reduction;
  - Irreducible words are those not containing both σ_1 and σ_1^{-1}.

- Theorem 1: (D. 1995) Braid reduction always terminates in finite time.
  A braid word represents 1 iff it reduces to the empty word.

- Facts: - Handle reduction is an isotopy;
  - It extends free group reduction;
  - Irreducible words are those not containing both σ_1 and σ_1^{-1}.

- Theorem 1: (D. 1995) Braid reduction always terminates in finite time.
  A braid word represents 1 iff it reduces to the empty word.

- Additional rule: nested handles must be reduced first.

- Facts: - Handle reduction is an isotopy;
  - It extends free group reduction;
  - Irreducible words are those not containing both σ_1 and σ_1^{-1}.

- Theorem 1: (D. 1995) Braid reduction always terminates in finite time.
  A braid word represents 1 iff it reduces to the empty word.

- Additional rule: nested handles must be reduced first.
- Extremely efficient in practice $\rightsquigarrow$ suitable for cryptographic applications.

- Facts: - Handle reduction is an isotopy;
  - It extends free group reduction;
  - Irreducible words are those not containing both σ_1 and σ_1^{-1}.

- Theorem 1: (D. 1995) Braid reduction always terminates in finite time.
  A braid word represents 1 iff it reduces to the empty word.

- Additional rule: nested handles must be reduced first.
- Extremely efficient in practice ⇝ suitable for cryptographic applications.

⇝ Question: Where does this reduction come from, why does it work?

... because of the braid ordering.

... because of the braid ordering.

• Theorem 2: (D. 1992) For a, b in B_n, let $a < b$ mean that $a^{-1}b$ can be represented by a word in which the generator σ_i with minimal i appears only positively. Then $<$ is a linear ordering on B_n.

... because of the braid ordering.

• Theorem 2: (D. 1992) For a, b in B_n, let $a < b$ mean that $a^{-1}b$ can be represented by a word in which the generator σ_i with minimal i appears only positively. Then $<$ is a linear ordering on B_n.

• Decomposes into:
- (A): a braid word containing σ_1 and not σ_1^{-1} does not represent 1;

... because of the braid ordering.

• Theorem 2: (D. 1992) For a, b in B_n, let $a < b$ mean that $a^{-1}b$ can be represented by a word in which the generator σ_i with minimal i appears only positively. Then $<$ is a linear ordering on B_n.

• Decomposes into:

- (A): a braid word containing σ_1 and not σ_1^{-1} does not represent 1;
- (C): each braid can be represented by a word with no σ_1 or no σ_1^{-1}.

... because of the braid ordering.

• Theorem 2: (D. 1992) For a, b in B_n, let $a < b$ mean that $a^{-1}b$ can be represented by a word in which the generator σ_i with minimal i appears only positively. Then $<$ is a linear ordering on B_n.

• Decomposes into:
- (A): a braid word containing σ_1 and not σ_1^{-1} does not represent 1;
- (C): each braid can be represented by a word with no σ_1 or no σ_1^{-1}.

• Theorem 1 comes from Theorem 2:

... because of the braid ordering.

• Theorem 2: (D. 1992) For a, b in B_n, let $a < b$ mean that $a^{-1}b$ can be represented by a word in which the generator σ_i with minimal i appears only positively. Then $<$ is a linear ordering on B_n.

• Decomposes into:
- (A): a braid word containing σ_1 and not σ_1^{-1} does not represent 1;
- (C): each braid can be represented by a word with no σ_1 or no σ_1^{-1}.

• Theorem 1 comes from Theorem 2: (C) gives the idea; (A) forbids cycles: if $\pi(w)$ is the prefix of w going to the first letter of the first σ_1-handle, then π decreases w.r.t. $<$ when reduction is performed.

... because of the braid ordering.

• Theorem 2: (D. 1992) For a, b in B_n, let $a < b$ mean that $a^{-1}b$ can be represented by a word in which the generator σ_i with minimal i appears only positively. Then $<$ is a linear ordering on B_n.

• Decomposes into:
- (A): a braid word containing σ_1 and not σ_1^{-1} does not represent 1;
- (C): each braid can be represented by a word with no σ_1 or no σ_1^{-1}.

• Theorem 1 comes from Theorem 2: (C) gives the idea; (A) forbids cycles: if $\pi(w)$ is the prefix of w going to the first letter of the first σ_1-handle,
then π decreases w.r.t. $<$ when reduction is performed.

$\rightsquigarrow$ Question: Where does this braid ordering come from?

... from self-distributivity.

... from self-distributivity.

• Braid colourings: Start with a set ("colours") S, apply colours at the left ends of the strands in a braid diagram and propagate to the right. Then compare the initial and final colours.

BRAID COLOURING

... from self-distributivity.

• Braid colourings: Start with a set ("colours") S, apply colours at the left ends of the strands in a braid diagram and propagate to the right. Then compare the initial and final colours.

• Choice 1: Colours are preserved in crossings:

BRAID COLOURING

... from self-distributivity.

• Braid colourings: Start with a set ("colours") S, apply colours at the left ends of the strands in a braid diagram and propagate to the right. Then compare the initial and final colours.

• Choice 1: Colours are preserved in crossings:

$\rightsquigarrow$ permutation of colours $\rightsquigarrow$ $B_n \twoheadrightarrow S_n$.

BRAID COLOURING

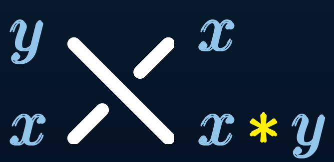
... from self-distributivity.

- Braid colourings: Start with a set ("colours") S, apply colours at the left ends of the strands in a braid diagram and propagate to the right. Then compare the initial and final colours.

- Choice 1: Colours are preserved in crossings:

$\rightsquigarrow$ permutation of colours $\rightsquigarrow$ $B_n \twoheadrightarrow S_n$.

- Choice 2: (Joyce, Matveev, Brieskorn, ...) Colours change under



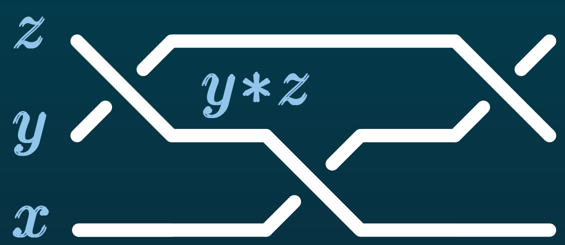
where $*$ is some binary operation on S

- For an action of B_n on S^n, need compatibility with braid relations:

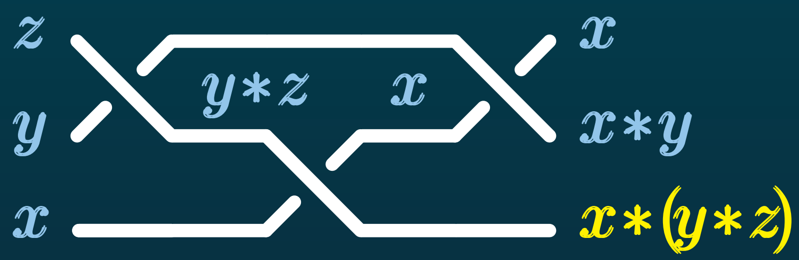
- For an action of B_n on S^n, need compatibility with braid relations:

- For an action of B_n on S^n, need compatibility with braid relations:

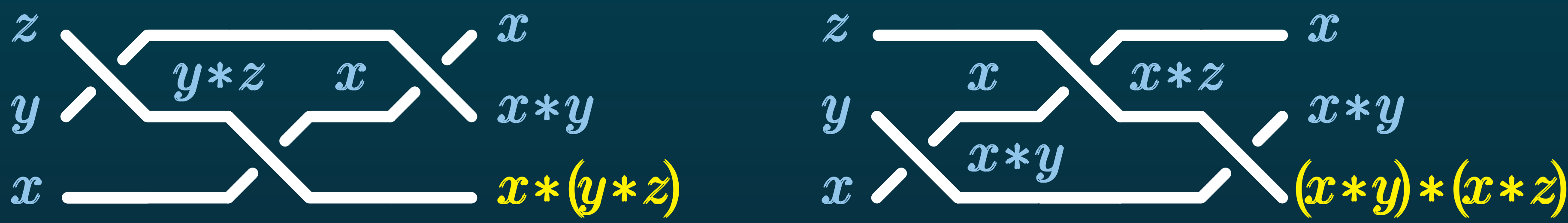
- For an action of B_n on S^n, need compatibility with braid relations:



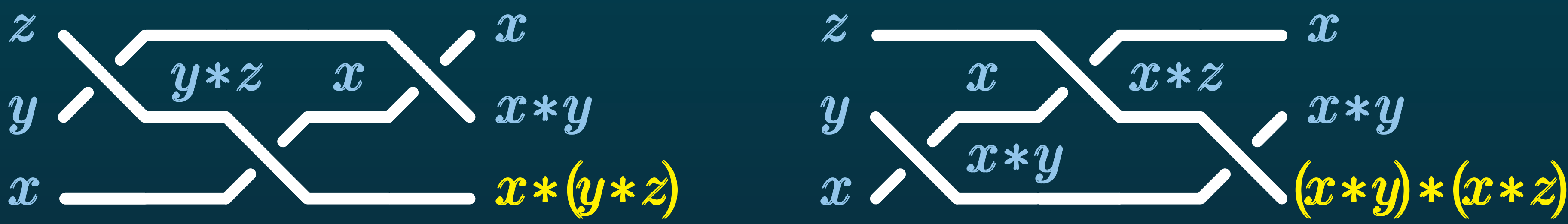
- For an action of B_n on S^n, need compatibility with braid relations:



- For an action of B_n on S^n, need compatibility with braid relations:



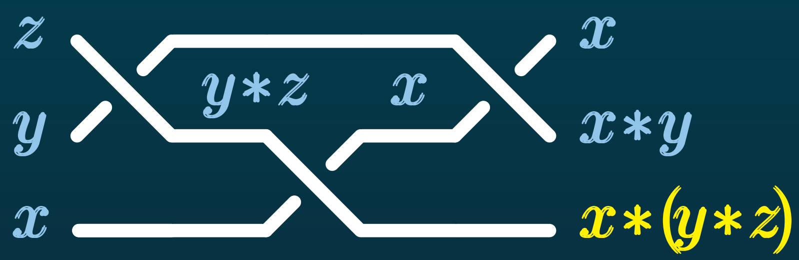
- For an action of B_n on S^n, need compatibility with braid relations:

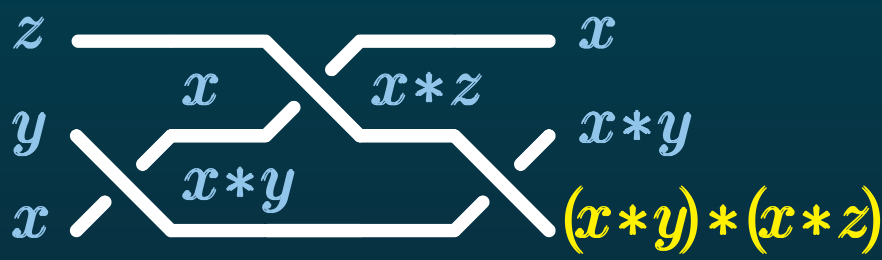


$\rightsquigarrow$ $(S,*)$ must be an LD-system, i.e., satisfy the left self-distributivity law:

$$x*(y*z)=(x*y)*(x*z). \tag{LD}$$

- For an action of B_n on S^n, need compatibility with braid relations:



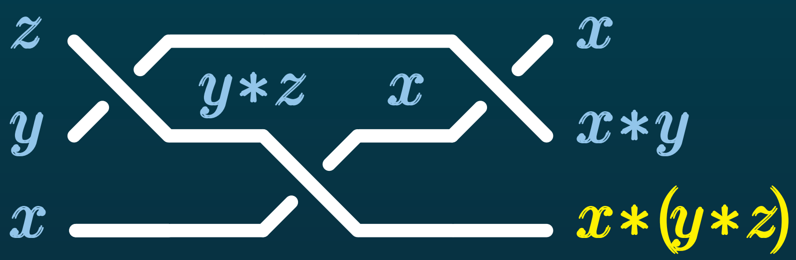


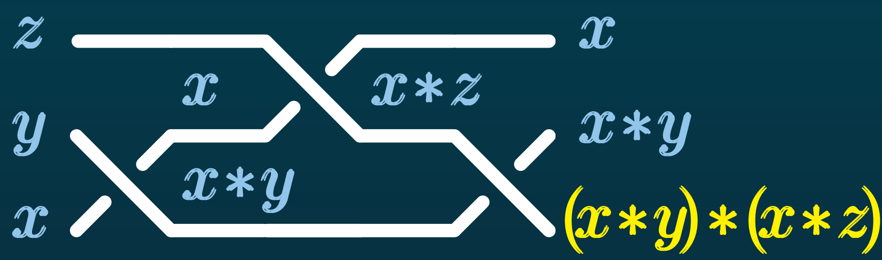
$\rightsquigarrow$ $(S, *)$ must be an LD-system, i.e., satisfy the left self-distributivity law:

$$x * (y * z) = (x * y) * (x * z). \qquad \text{(LD)}$$

- Standard examples:
  - $x * y = y$, leads to $B_n \twoheadrightarrow S_n$.

- For an action of B_n on S^n, need compatibility with braid relations:





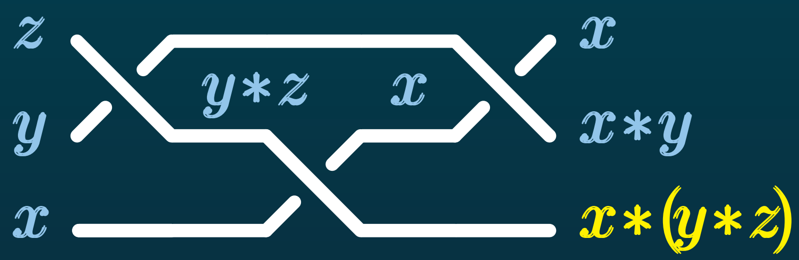
$\rightsquigarrow$ $(S, *)$ must be an LD-system, i.e., satisfy the left self-distributivity law:

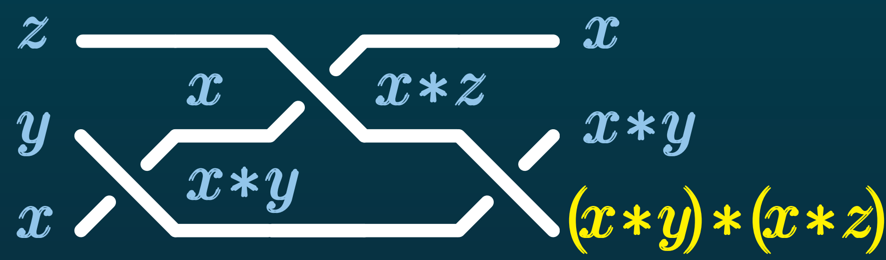
$$x * (y * z) = (x * y) * (x * z). \tag{LD}$$

- Standard examples:
  - $x * y = y$, leads to $B_n \twoheadrightarrow S_n$.
  - $x * y = xyx^{-1}$, leads to $B_n \rightarrow Aut(F_n)$ (Artin)

LD-SYSTEMS

- For an action of B_n on S^n, need compatibility with braid relations:



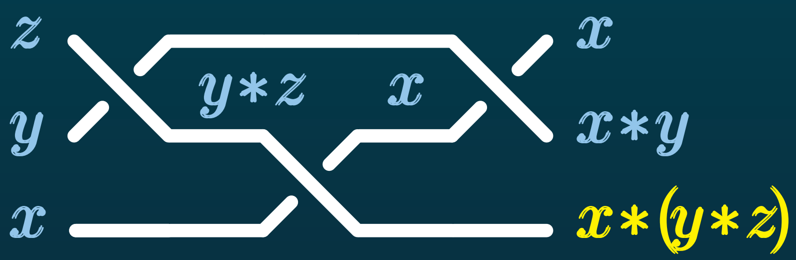


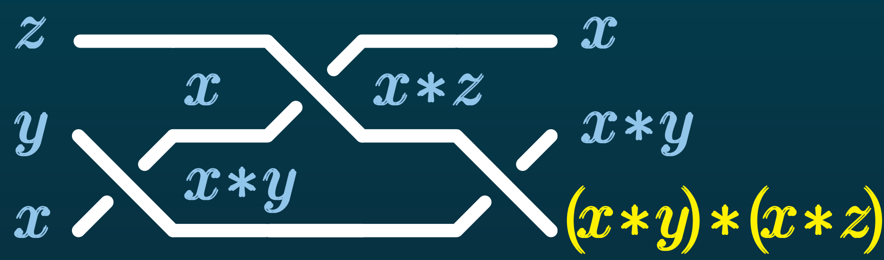
$\rightsquigarrow$ $(S,*)$ must be an LD-system, i.e., satisfy the left self-distributivity law:

$$x * (y * z) = (x * y) * (x * z). \tag{LD}$$

- Standard examples:
  - $x * y = y$, leads to $B_n \twoheadrightarrow S_n$.
  - $x * y = xyx^{-1}$, leads to $B_n \rightarrow Aut(F_n)$ (Artin)
  - $x * y = (1-t)x + ty$, leads to $B_n \rightarrow GL_n(\mathbb{Z}[t, t^{-1}])$ (Burau)

- For an action of B_n on S^n, need compatibility with braid relations:





$\rightsquigarrow$ $(S, *)$ must be an LD-system, i.e., satisfy the left self-distributivity law:

$$x * (y * z) = (x * y) * (x * z). \qquad \text{(LD)}$$

- Standard examples:
  - $x * y = y$, leads to $B_n \twoheadrightarrow S_n$.
  - $x * y = xyx^{-1}$, leads to $B_n \to Aut(F_n)$ (Artin)
  - $x * y = (1 - t)x + ty$, leads to $B_n \to GL_n(\mathbb{Z}[t, t^{-1}])$ (Burau)

Note: in these examples, $x * x = x$ always holds.

$\rightsquigarrow$ Other examples?

$\rightsquigarrow$ Other examples?

- Say that an LD-system $(S, *)$ is orderable if
  there is a linear ordering $<$ on S satisfying $x < x * y$ for all x, y.

⇝ Other examples?

- Say that an LD-system $(S, *)$ is orderable if
  there is a linear ordering $<$ on S satisfying $x < x * y$ for all x, y.

  ⇝ certainly of a new flavour: $x < x * x \neq x$.

$\rightsquigarrow$ Other examples?

- Say that an LD-system $(S, *)$ is orderable if
  there is a linear ordering $<$ on S satisfying $x < x * y$ for all x, y.

  $\rightsquigarrow$ certainly of a new flavour: $x < x * x \neq x$.

- Theorem 3: (D. 1991) There exist orderable LD-systems
  (namely: free LD-systems).

⇝ Other examples?

- Say that an LD-system $(S, *)$ is orderable if
  there is a linear ordering $<$ on S satisfying $x < x * y$ for all x, y.
  ⇝ certainly of a new flavour: $x < x * x \neq x$.

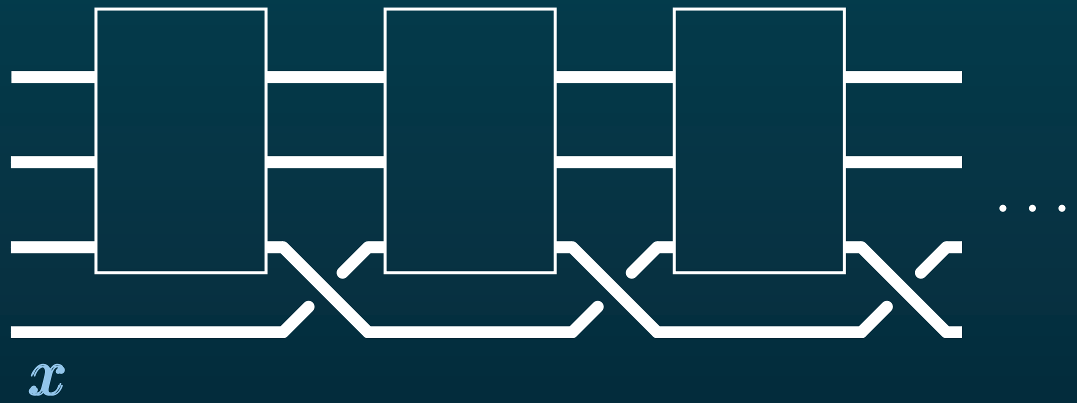
- Theorem 3: (D. 1991) There exist orderable LD-systems
  (namely: free LD-systems).

- Theorem 2 comes from Theorem 3:
  Use an orderable LD-system to colour braids. The points are:
  - (A): A braid word with σ_1 and no σ_1^{-1} does not represent 1,
  - (C): Linearity of the ordering.

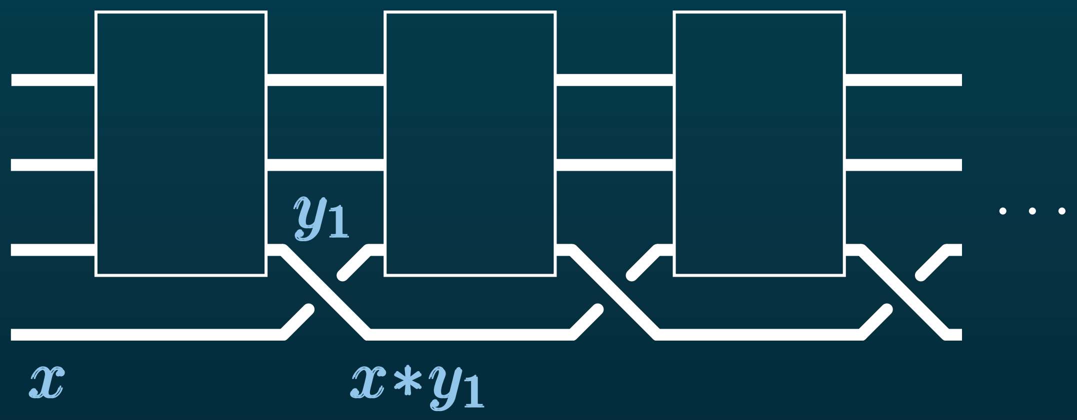
- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1

- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1

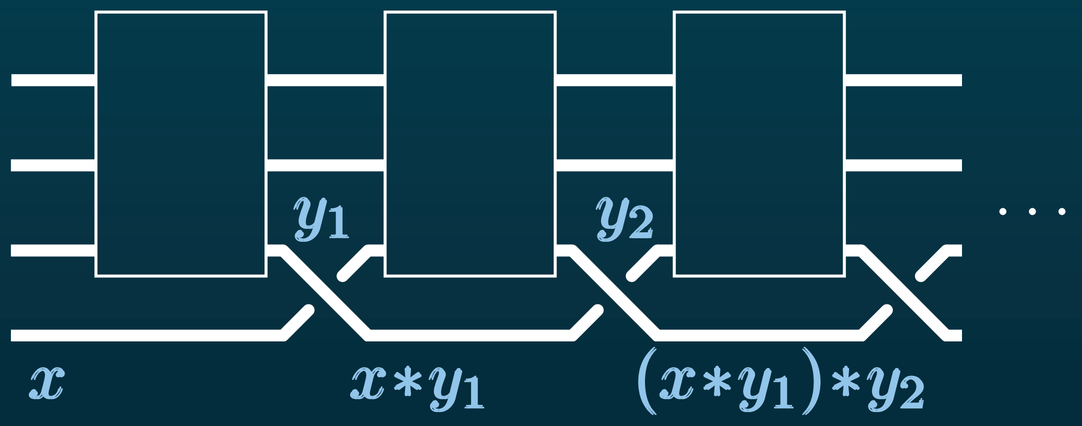
- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



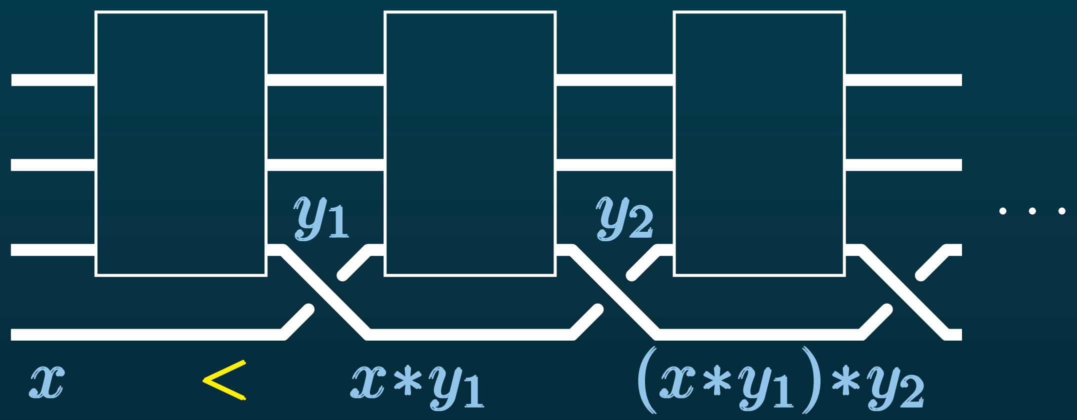
- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



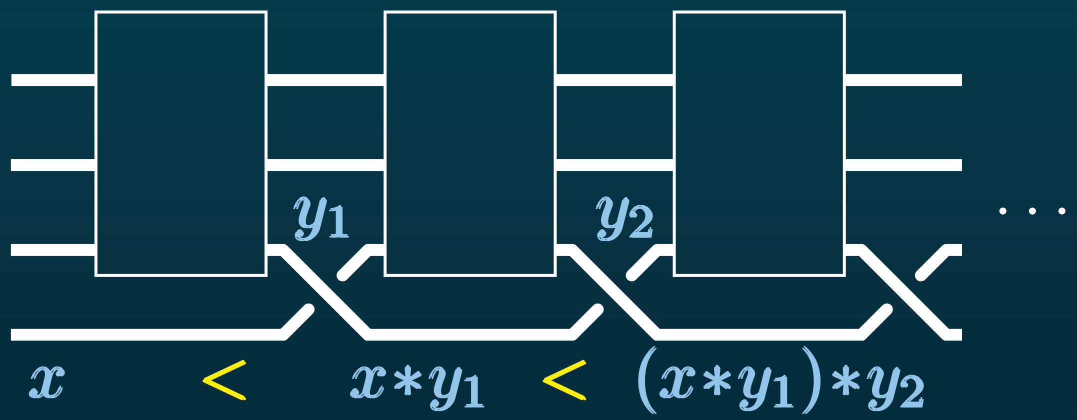
- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



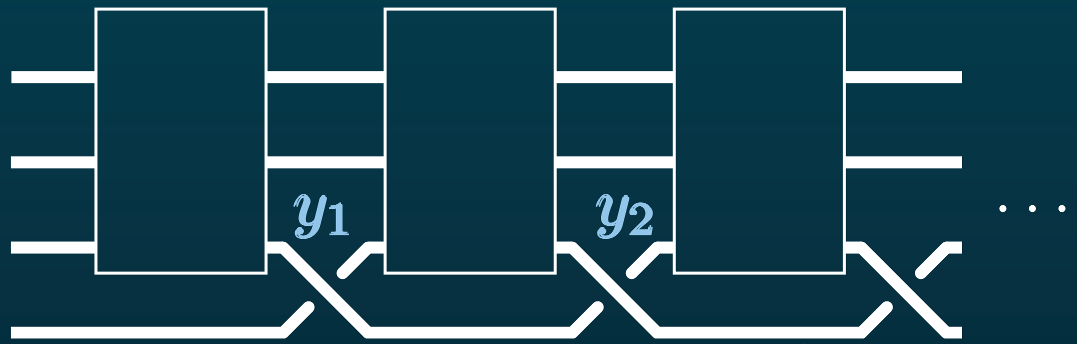
- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1

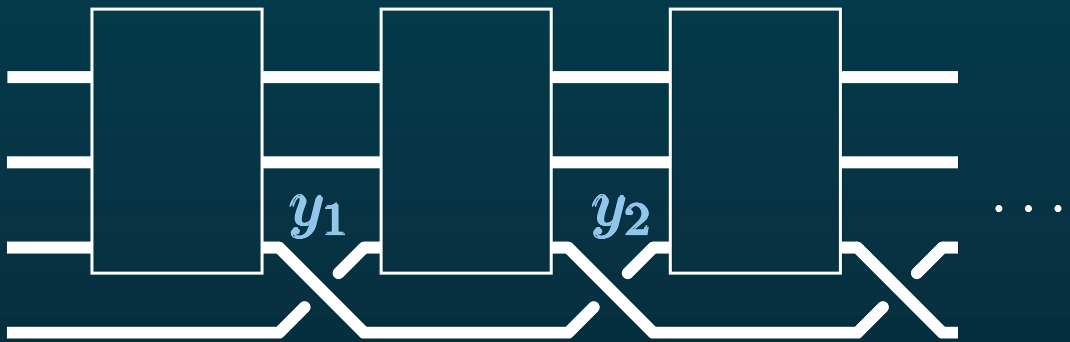


- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



$$x \quad < \quad x*y_1 \quad < \quad (x*y_1)*y_2 \quad < \ldots$$

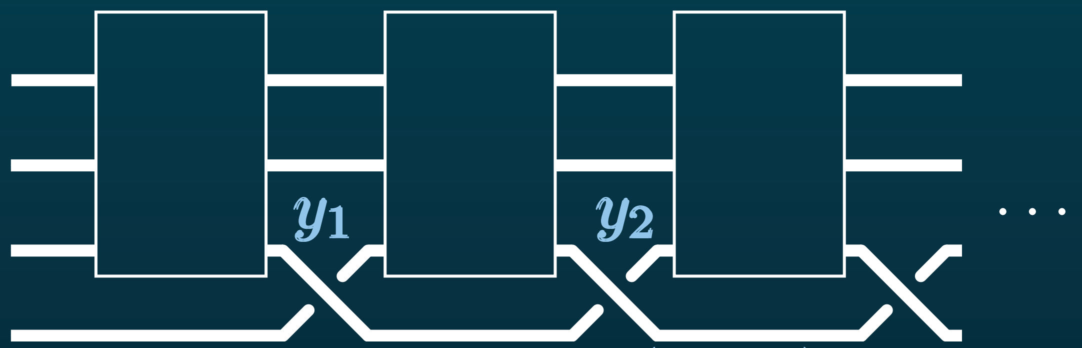
- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



$$x \quad < \quad x{*}y_1 \quad < \quad (x{*}y_1){*}y_2 \quad < \ldots \quad \neq x$$

PROOFS

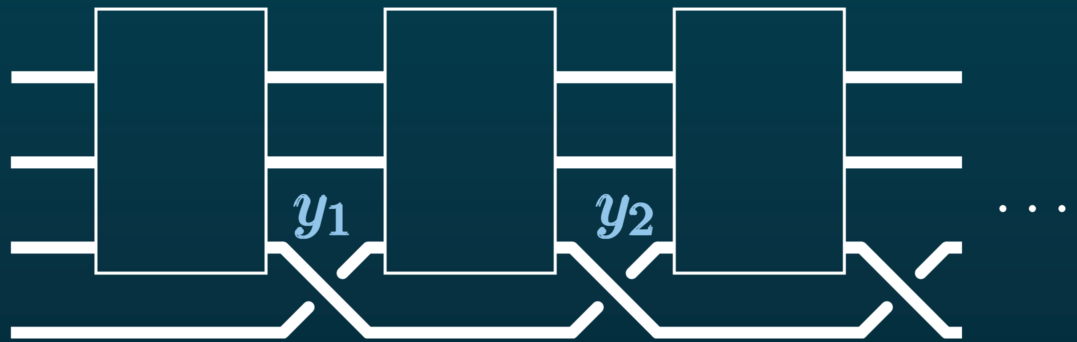
- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



$$x \;<\; x{*}y_1 \;<\; (x{*}y_1){*}y_2 \;<\; \dots \;\neq x$$

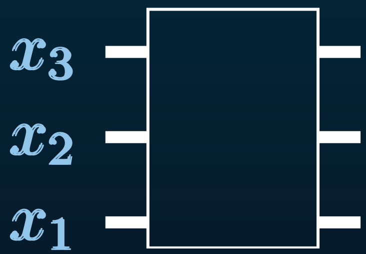
- Proof of (C) : A linear ordering on braids:

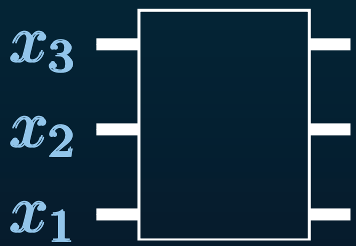
- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



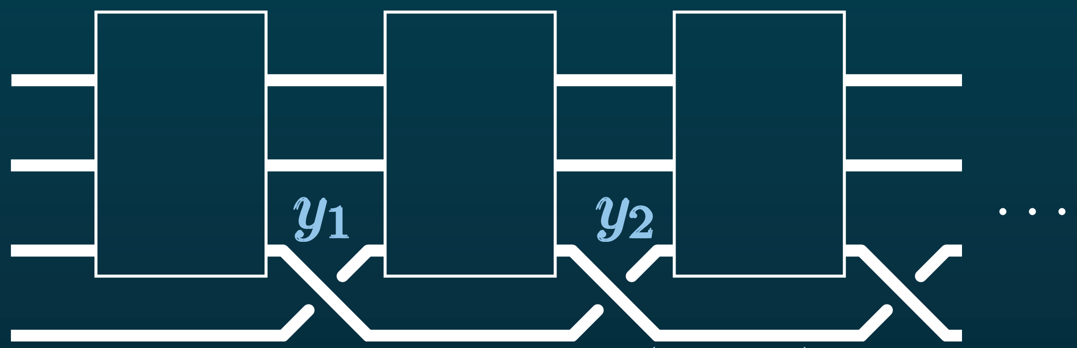
$$x \quad < \quad x*y_1 \quad < \quad (x*y_1)*y_2 \quad < \ldots \quad \neq x$$

- Proof of (C) : A linear ordering on braids:



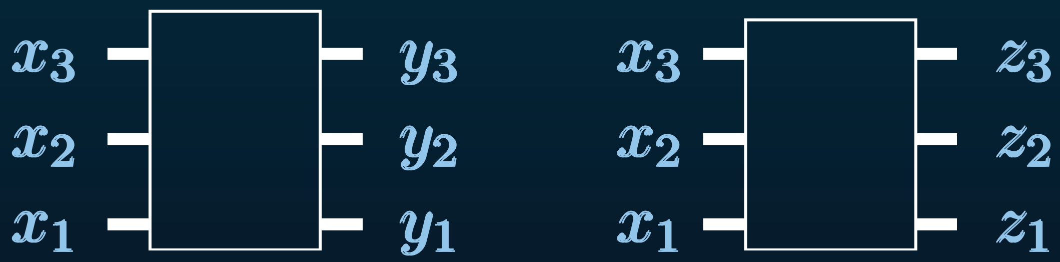


- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1

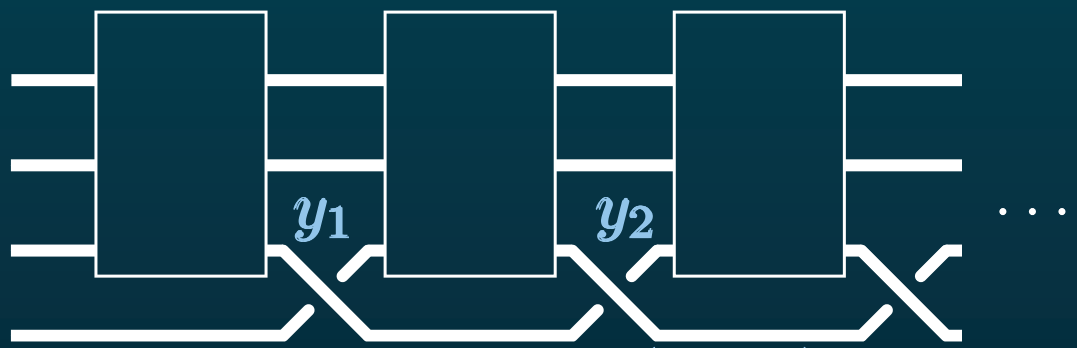


$$x \quad < \quad x{*}y_1 \quad < \quad (x{*}y_1){*}y_2 \quad < \ldots \quad \neq x$$

- Proof of (C) : A linear ordering on braids:

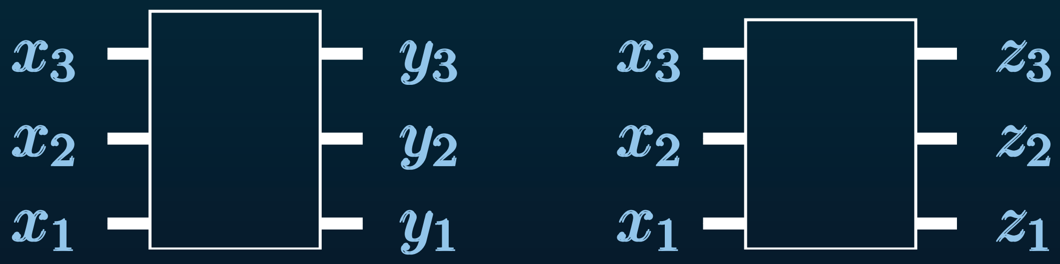


- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



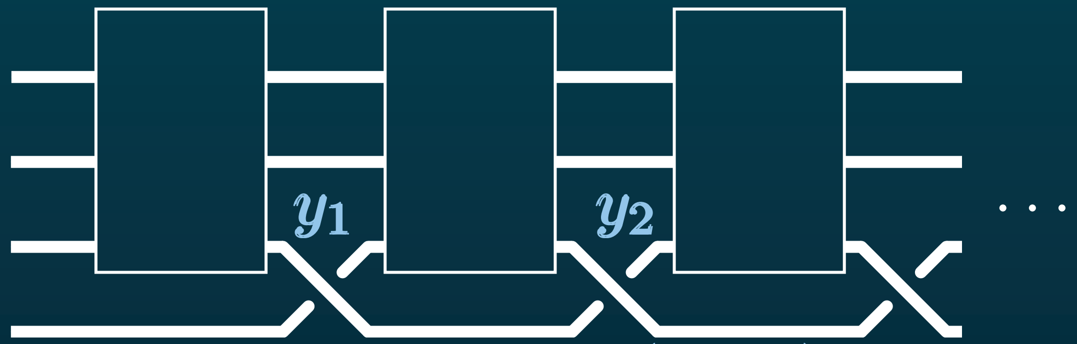
$$x \quad < \quad x{*}y_1 \quad < \quad (x{*}y_1){*}y_2 \quad < \dots \quad \neq x$$

- Proof of (C) : A linear ordering on braids:



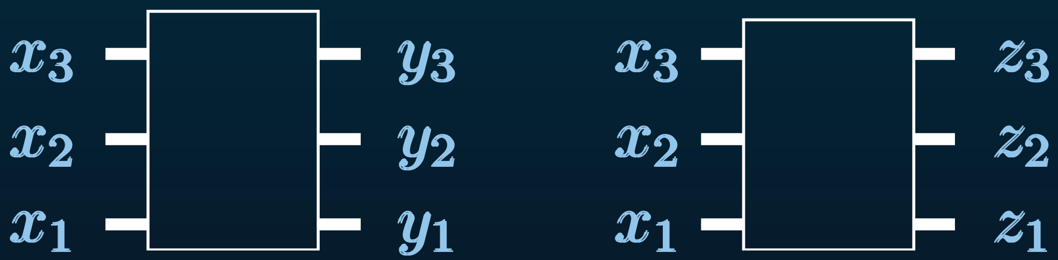
$\rightsquigarrow$ Compare $(y_1, y_2, \ldots)$ and $(z_1, z_2, \ldots)$ lexicographically.

- Proof of (A) : A braid word with σ_1 and no σ_1^{-1} does not represent 1



$$x \quad < \quad x * y_1 \quad < \quad (x * y_1) * y_2 \quad < \ldots \quad \neq x$$

- Proof of (C) : A linear ordering on braids:



$\rightsquigarrow$ Compare $(y_1, y_2, \ldots)$ and $(z_1, z_2, \ldots)$ lexicographically.

$\rightsquigarrow$ Question: Why to study orderable LD-systems?

... because Set Theory told us

... because Set Theory told us

• Set Theory studies infinity. By Gödel's theorem, every axiom system, in particular the standard Zermelo-Fraenkel system ZF, is incomplete.

... because Set Theory told us

• Set Theory studies infinity. By Gödel's theorem, every axiom system, in particular the standard Zermelo-Fraenkel system ZF, is incomplete.

$\rightsquigarrow$ (Gödel's program): Complete ZF with axioms asserting the existence of “hyper-infinite" sets (large cardinals).

... because Set Theory told us

• Set Theory studies infinity. By Gödel's theorem, every axiom system, in particular the standard Zermelo-Fraenkel system ZF, is incomplete.

$\rightsquigarrow$ (Gödel's program): Complete ZF with axioms asserting the existence of "hyper-infinite" sets (large cardinals).

• Strengthen "X is infinite iff $\exists j : X \to X$ injective non-surjective"
to "X is hyper-infinite (self-similar) iff $\exists j$ ... and, in addition,
j preserves what is definable from $\in$

... because Set Theory told us

• Set Theory studies infinity. By Gödel's theorem, every axiom system, in particular the standard Zermelo-Fraenkel system ZF, is incomplete.

$\rightsquigarrow$ (Gödel's program): Complete ZF with axioms asserting the existence of “hyper-infinite" sets (large cardinals).

• Strengthen “X is infinite iff $\exists j : X \to X$ injective non-surjective"
to “X is hyper-infinite (self-similar) iff $\exists j$ ... and, in addition,
j preserves what is definable from $\in$ (an elementary embedding)".

... because Set Theory told us

- Set Theory studies infinity. By Gödel's theorem, every axiom system, in particular the standard Zermelo-Fraenkel system ZF, is incomplete.

$\rightsquigarrow$ (Gödel's program): Complete ZF with axioms asserting the existence of "hyper-infinite" sets (large cardinals).

- Strengthen "X is infinite iff $\exists j : X \to X$ injective non-surjective"
  to "X is hyper-infinite (self-similar) iff $\exists j$ ... and, in addition,
  j preserves what is definable from $\in$ (an elementary embedding)".

- As $j : n \mapsto n+1$ is injective nonsurjective, $\mathbb{N}$ is infinite;
  Now j preserves $<$, but not $+$: j is not an e.e.;
  Actually, no e.e. of $\mathbb{N}$ exists: $\mathbb{N}$ is not self-similar.

... because Set Theory told us

• Set Theory studies infinity. By Gödel's theorem, every axiom system, in particular the standard Zermelo-Fraenkel system ZF, is incomplete.

$\rightsquigarrow$ (Gödel's program): Complete ZF with axioms asserting the existence of “hyper-infinite" sets (large cardinals).

• Strengthen “X is infinite iff $\exists j : X \to X$ injective non-surjective"
to “X is hyper-infinite (self-similar) iff $\exists j$ ... and, in addition,
j preserves what is definable from $\in$ (an elementary embedding)".

• As $j : n \mapsto n+1$ is injective nonsurjective, $\mathbb{N}$ is infinite;
Now j preserves $<$, but not $+$: j is not an e.e.;
Actually, no e.e. of $\mathbb{N}$ exists: $\mathbb{N}$ is not self-similar.

- A rank is a set R s.t. $f : R \longrightarrow R$ implies $f \in R$. (??)

- A rank is a set R s.t. $f : R \to R$ implies $f \in R$. (??)

there exists an e.e. of... into itself

- If R is a self-similar rank, and i, j are e.e.'s of R, we can apply i to j.

- A rank is a set R s.t. $f : R \to R$ implies $f \in R$. (??)

there exists an e.e. of... into itself

- If R is a self-similar rank, and i, j are e.e.'s of R, we can apply i to j.
  - "Being an e.e." is definable from $\in$, so $i(j)$ is an e.e. too;

    $\rightsquigarrow$ a binary operation on e.e.'s defined on R.

- A rank is a set R s.t. $f : R \to R$ implies $f \in R$. (??)

there exists an e.e. of... into itself

- If R is a self-similar rank, and i, j are e.e.'s of R, we can apply i to j.
  - "Being an e.e." is definable from $\in$, so $i(j)$ is an e.e. too;
    $\rightsquigarrow$ a binary operation on e.e.'s defined on R.
  - "Being the image under" is definable from $\in$,
    so $\ell = j(k)$ implies $i(\ell) = i(j)(i(k))$, ***i.e.***, $i(j(k)) = i(j)(i(k))$.
    $\rightsquigarrow$ this operation satisfies the LD law.

- A rank is a set R s.t. $f : R \to R$ implies $f \in R$. (??)

there exists an e.e. of... into itself

- If R is a self-similar rank, and i, j are e.e.'s of R, we can apply i to j.

  - "Being an e.e." is definable from $\in$, so $i(j)$ is an e.e. too;

    $\rightsquigarrow$ a binary operation on e.e.'s defined on R.

  - "Being the image under" is definable from $\in$,

    so $\ell = j(k)$ implies $i(\ell) = i(j)(i(k))$, ***i.e.***, $i(j(k)) = i(j)(i(k))$.

    $\rightsquigarrow$ this operation satisfies the LD law.

$\rightsquigarrow$ For every e.e. j, a new LD-system $I(j)$, the iterates of j: $j(j)$, $j(j)(j)$...

- A rank is a set R s.t. $f : R \to R$ implies $f \in R$. (??)

there exists an e.e. of... into itself

- If R is a self-similar rank, and i, j are e.e.'s of R, we can apply i to j.
  - "Being an e.e." is definable from $\in$, so $i(j)$ is an e.e. too;
    $\rightsquigarrow$ a binary operation on e.e.'s defined on R.
  - "Being the image under" is definable from $\in$,
    so $\ell = j(k)$ implies $i(\ell) = i(j)(i(k))$, ***i.e.***, $i(j(k)) = i(j)(i(k))$.
    $\rightsquigarrow$ this operation satisfies the LD law.

$\rightsquigarrow$ For every e.e. j, a new LD-system $I(j)$, the iterates of j: $j(j)$, $j(j)(j)$...

Proposition: (D. 1986) If j is an e.e. of a self-similar rank, then the LD-structure of $I(j)$ implies Π^1_1-determinacy. $\rightsquigarrow$ "$I(j)$ is not trivial."

- Theorem: (D. 1989) If there exists at least one orderable LD-system,
  then the word problem of LD is solvable.

  deciding if terms are equal mod. LD

- Theorem: (D. 1989) If there exists at least one orderable LD-system, then the word problem of LD is solvable.

deciding if terms are equal mod. LD

- Theorem: (Laver, 1989) If j is an e.e. of a self-similar rank, then $I(j)$ is an orderable LD-system.

- Theorem: (D. 1989) If there exists at least one orderable LD-system,
  then the word problem of LD is solvable.
  deciding if terms are equal mod. LD

- Theorem: (Laver, 1989) If j is an e.e. of a self-similar rank,
  then $I(j)$ is an orderable LD-system.

- Corollary: If there exists a self-similar rank, the word pb. of LD is solvable.

- Theorem: (D. 1989) If there exists at least one orderable LD-system, then the word problem of LD is solvable.

  deciding if terms are equal mod. LD

- Theorem: (Laver, 1989) If j is an e.e. of a self-similar rank, then $I(j)$ is an orderable LD-system.

- Corollary: If there exists a self-similar rank, the word pb. of LD is solvable.

- But the existence of a self-similar rank is an unprovable axiom.

  $\rightsquigarrow$ The corollary is not a solution for the word problem of LD (???)

- Theorem: (D. 1989) If there exists at least one orderable LD-system,
  then the word problem of LD is solvable.
  deciding if terms are equal mod. LD

- Theorem: (Laver, 1989) If j is an e.e. of a self-similar rank,
  then $I(j)$ is an orderable LD-system.

- Corollary: If there exists a self-similar rank, the word pb. of LD is solvable.

- But the existence of a self-similar rank is an unprovable axiom.
  - ⇝ The corollary is not a solution for the word problem of LD (???)
    - ⇝ Construct a true orderable LD-system

- Theorem: (D. 1989) If there exists at least one orderable LD-system,
  then the word problem of LD is solvable.
  deciding if terms are equal mod. LD

- Theorem: (Laver, 1989) If j is an e.e. of a self-similar rank,
  then $I(j)$ is an orderable LD-system.

- Corollary: If there exists a self-similar rank, the word pb. of LD is solvable.

- But the existence of a self-similar rank is an unprovable axiom.
  - ⇝ The corollary is not a solution for the word problem of LD (???)
    - ⇝ Construct a true orderable LD-system
      - ⇝ Theorem 3 ("free LD-systems are orderable") by investigating the "geometry group of LD"

- Theorem: (D. 1989) If there exists at least one orderable LD-system,
  then the word problem of LD is solvable.
  deciding if terms are equal mod. LD

- Theorem: (Laver, 1989) If j is an e.e. of a self-similar rank,
  then $I(j)$ is an orderable LD-system.

- Corollary: If there exists a self-similar rank, the word pb. of LD is solvable.

- But the existence of a self-similar rank is an unprovable axiom.
  - $\rightsquigarrow$ The corollary is not a solution for the word problem of LD (???)
    - $\rightsquigarrow$ Construct a true orderable LD-system
      - $\rightsquigarrow$ Theorem 3 ("free LD-systems are orderable") by investigating the "geometry group of LD"
        - $\rightsquigarrow$ As the latter extends Artin's braid group: braid applications

$\rightsquigarrow$ A continuous path from Set Theory to braid applications.

$\rightsquigarrow$ A continuous path from Set Theory to braid applications.

- Question: Are the braids results applications of Set Theory?

$\rightsquigarrow$ A continuous path from Set Theory to braid applications.

- Question: Are the braids results applications of Set Theory?

- Formally, no: Braids appear when Set Theory vanishes:

$\rightsquigarrow$ A continuous path from Set Theory to braid applications.

- Question: Are the braids results applications of Set Theory?

- Formally, no: Braids appear when Set Theory vanishes:
  - Set Theory gives a (hypothetical) example of a certain object (an orderable LD-system),

$\rightsquigarrow$ A continuous path from Set Theory to braid applications.

- Question: Are the braids results applications of Set Theory?

- Formally, no: Braids appear when Set Theory vanishes:
  - Set Theory gives a (hypothetical) example of a certain object (an orderable LD-system),
  - Braids and their ordering appear in the process of constructing an alternative ("true") example.

$\rightsquigarrow$ A continuous path from Set Theory to braid applications.

- Question: Are the braids results applications of Set Theory?

- Formally, no: Braids appear when Set Theory vanishes:
  - Set Theory gives a (hypothetical) example of a certain object (an orderable LD-system),
  - Braids and their ordering appear in the process of constructing an alternative ("true") example.

- In essence, yes: if Set Theory had not shown that the LD law is involved in deep phenomena, and made the existence of orderable LD-systems plausible, it is unlikely that such objects would have been investigated...

- In physics: using physical intuition and/or evidence,
  - guess some statement, then
  - then pass it to mathematicians for a formal proof.

- In physics: using physical intuition and/or evidence,
  - guess some statement, then
  - then pass it to mathematicians for a formal proof.

- Here: using logical intuition and/or evidence ($\exists$ self-similar rank),

- In physics: using physical intuition and/or evidence,
  - guess some statement, then
  - then pass it to mathematicians for a formal proof.

- Here: using logical intuition and/or evidence ($\exists$ self-similar rank),
  - guess some statement ($\exists$ orderable LD-system),

- In physics: using physical intuition and/or evidence,
  - guess some statement, then
  - then pass it to mathematicians for a formal proof.

- Here: using logical intuition and/or evidence ($\exists$ self-similar rank),
  - guess some statement ($\exists$ orderable LD-system),
  - then pass it to mathematicians for a formal proof.

- In physics: using physical intuition and/or evidence,
  - guess some statement, then
  - then pass it to mathematicians for a formal proof.

- Here: using logical intuition and/or evidence ($\exists$ self-similar rank),
  - guess some statement ($\exists$ orderable LD-system),
  - then pass it to mathematicians for a formal proof.

- An argument in favour of Set Theory: For this use of Set Theory,
  the point is not that the axioms are plausible, but that they are powerful.

- In physics: using physical intuition and/or evidence,
  - guess some statement, then
  - then pass it to mathematicians for a formal proof.

- Here: using logical intuition and/or evidence ($\exists$ self-similar rank),
  - guess some statement ($\exists$ orderable LD-system),
  - then pass it to mathematicians for a formal proof.

- An argument in favour of Set Theory: For this use of Set Theory, the point is not that the axioms are plausible, but that they are powerful.

$\rightsquigarrow$ Even if one does not believe in the existence of (hyper)infinite sets, one should agree that, in this case, they led to applicable mathematics.

- More about the braid ordering...

- More about the braid ordering...
- Another similar application of set theory?

- More about the braid ordering...

- Another similar application of set theory?

- Start with

$$\begin{array}{c|cccc} & 1 & 2 & \dots & N \\ \hline 1 & 2 & & & \\ 2 & 3 & & & \\ \vdots & & & & \\ N{-}1 & N & & & \\ N & 1 & & & \end{array}$$

and try to construct an LD table.

- More about the braid ordering...

- Another similar application of set theory?

- Start with

$$\begin{array}{c|cccc} & 1 & 2 & \dots & N \\ \hline 1 & 2 & & & \\ 2 & 3 & & & \\ \vdots & & & & \\ N-1 & N & & & \\ N & 1 & & & \end{array}$$

and try to construct an LD table.

  - at most one solution for each N;

- More about the braid ordering...

- Another similar application of set theory?

- Start with

	1	2	$\dots$	N
1	2			
2	3			
$\vdots$				
$N{-}1$	N			
N	1			

and try to construct an LD table.

  - at most one solution for each N;
  - actually an LD-table iff N is a power of 2,

- More about the braid ordering...

- Another similar application of set theory?

- Start with

	1	2	...	N
1	2			
2	3			
$\vdots$				
$N-1$	N			
N	1			

and try to construct an LD table.

  - at most one solution for each N;
  - actually an LD-table iff N is a power of 2, ***e.g.***,

	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

- More about the braid ordering...

- Another similar application of set theory?

- Start with

	1	2	...	N
1	2			
2	3			
$\vdots$				
$N{-}1$	N			
N	1			

and try to construct an LD table.

 - at most one solution for each N;
 - actually an LD-table iff N is a power of 2, ***e.g.***,

	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

$\rightsquigarrow$ Define the n-th Laver table A_n to be the one with 2^n elements.

- Facts: - Each row in A_n is periodic;

- Facts: - Each row in A_n is periodic;
  - A_n is the projection of A_{n+1} mod. 2^n.

  $\rightsquigarrow$ period of first row in $A_{n+1} \geqslant$ period of first row in A_n.

- Facts: - Each row in A_n is periodic;
  - A_n is the projection of A_{n+1} mod. 2^n.

  $\rightsquigarrow$ period of first row in $A_{n+1} \geqslant$ period of first row in A_n.

- Theorem: (Laver, 1995) Assume that there exists a self-similar rank.
  Then the period of the first row in A_n goes to ∞ with n.

- Facts: - Each row in A_n is periodic;
  - A_n is the projection of A_{n+1} mod. 2^n.

  $\rightsquigarrow$ period of first row in $A_{n+1} \geqslant$ period of first row in A_n.

- Theorem: (Laver, 1995) Assume that there exists a self-similar rank.
  Then the period of the first row in A_n goes to ∞ with n.

- Open problem:
  - Prove that the period of the first row in A_n goes to ∞ with n...

- Facts: - Each row in A_n is periodic;
  - A_n is the projection of A_{n+1} mod. 2^n.
    $\rightsquigarrow$ period of first row in $A_{n+1} \geqslant$ period of first row in A_n.

- Theorem: (Laver, 1995) Assume that there exists a self-similar rank.
  Then the period of the first row in A_n goes to ∞ with n.

- Open problem:
  - Prove that the period of the first row in A_n goes to ∞ with n...

    $\uparrow$

    without using any unprovable hypothesis such as "$\exists$ a self-similar rank"

- Facts: - Each row in A_n is periodic;
  - A_n is the projection of A_{n+1} mod. 2^n.

  $\rightsquigarrow$ period of first row in $A_{n+1} \geqslant$ period of first row in A_n.

- Theorem: (Laver, 1995) Assume that there exists a self-similar rank. Then the period of the first row in A_n goes to ∞ with n.

- Open problem:
  - Prove that the period of the first row in A_n goes to ∞ with n...

  $\uparrow$
  without using any unprovable hypothesis such as "$\exists$ a self-similar rank"

  ... or prove that such an hypothesis is necessary.

- Facts: - Each row in A_n is periodic;
  - A_n is the projection of A_{n+1} mod. 2^n.

  $\rightsquigarrow$ period of first row in $A_{n+1} \geqslant$ period of first row in A_n.

> • Theorem: (Laver, 1995) Assume that there exists a self-similar rank.
> Then the period of the first row in A_n goes to ∞ with n.

- Open problem:
  - Prove that the period of the first row in A_n goes to ∞ with n...

    ↑

    without using any unprovable hypothesis such as "$\exists$ a self-similar rank"

    ... or prove that such an hypothesis is necessary.

- Only known negative result (Dougherty 1995):

  Not provable in Primitive Recursive Arithmetic (double recursion needed).

P. Dehornoy; Braids and Self-Distributivity; PM 192, Birkhauser (2000).

P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest; Why are braids orderable?; Panoramas & Syntheses vol. 14, Soc. Math. France (2002).

• http://www.math.unicaen.fr/$\sim$ dehornoy