- General principle (Brieskorn, Alexander): Colour the arcs of a braid or a link diagram

  $\rightsquigarrow$ extract information about the braid or the link.

  $\rightsquigarrow$ Self-distributivity $\quad x * (y * z) = (x * y) * (x * z).$

  $\rightsquigarrow$ algebraic translation of Reidemeister move of type III.

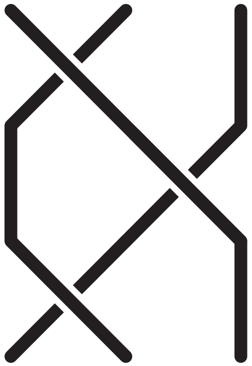
  $\rightsquigarrow$ Use various types of self-distributive operations (classical and non-classical)

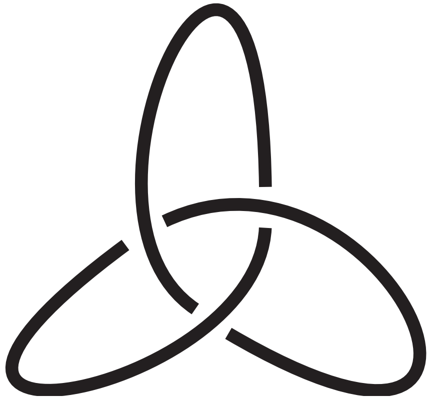
  $\rightsquigarrow$ various applications.

- Aim: To show how various colouring techniques can be used.

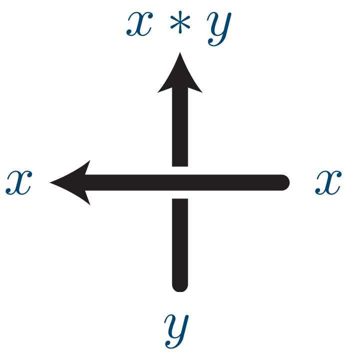
Arc colouring

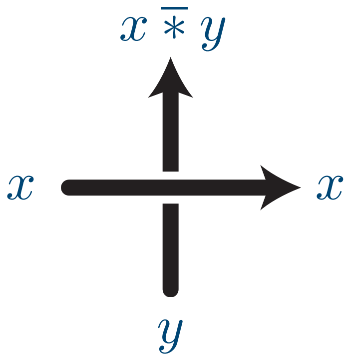
- Consider a standard braid or link diagram D:





- Attach colours from a set S to the arcs of D, and propagate them along the arcs.
  - ⇝ Not much to learn if colours never change;
  - ⇝ More interesting if colours may change: ⇝ Fix rules for crossings:





Invariance under isotopy

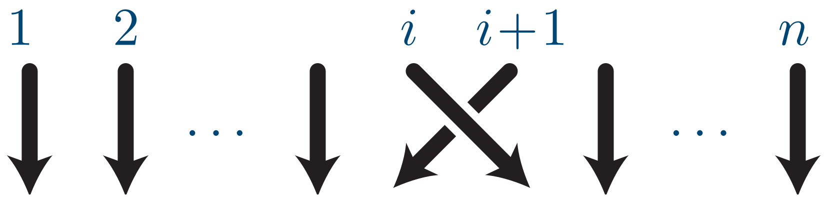
- Want information about the braid or the link represented by the diagram, not about the diagram

  ⇝ require invariance under isotopy.

- Case of braids:

  - Standard generators:

σ_i :



  - Standard presentation for

    ⇝ the braid group B_n, and ⇝ the braid monoid B_n^+:

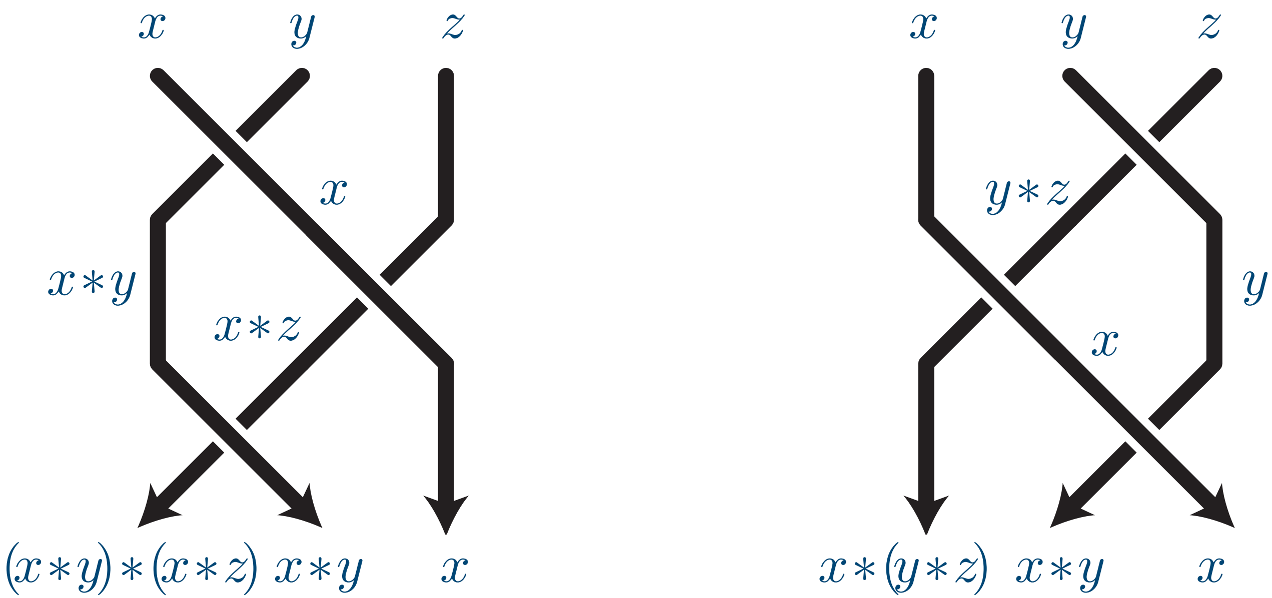
$$\left\langle \sigma_1, \ldots, \sigma_{n-1} \,;\, \begin{cases} \sigma_i \sigma_j = \sigma_j \sigma_i & \text{for } |i-j| \geqslant 2 \\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{for } |i-j| = 1 \end{cases} \right\rangle$$

  ⇝ Then: invariance under isotopy = compatibility with braid relations.

● Fact.- Colouring is compatible with isotopy iff $*$ satisfies Identity LD:

$$x * (y * z) = (x * y) * (x * z). \tag{1}$$

Proof:

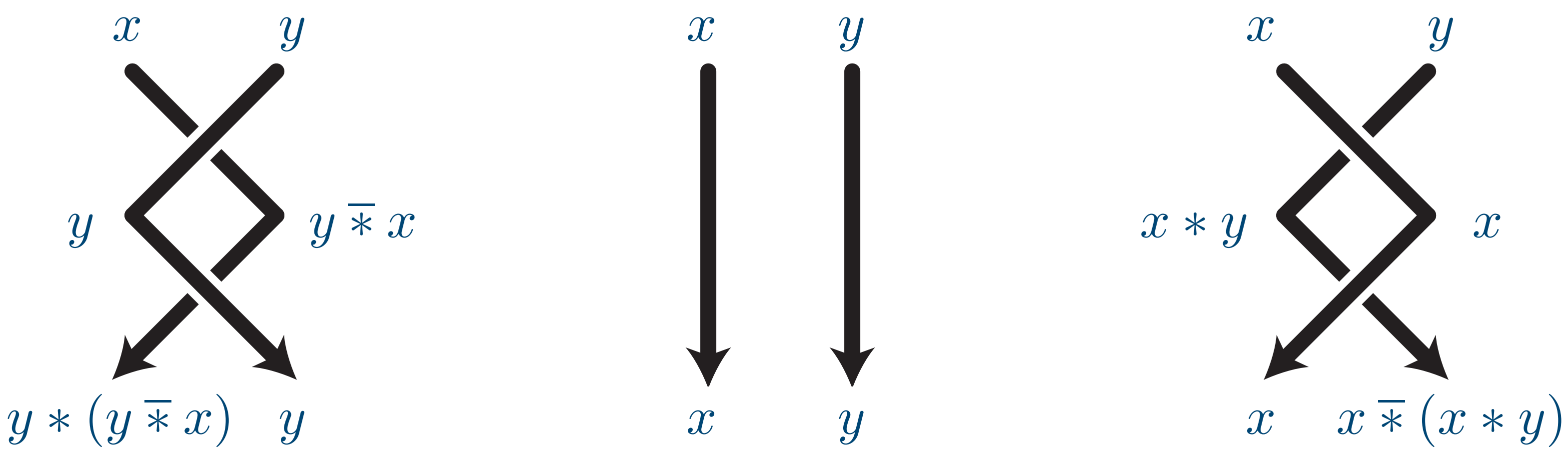


● Def.– $(S, *)$ is an LD-system if $*$ satisfies (1).

- Fact.- Colouring is compatible with isotopy iff $*$ satisfies Identity LD, plus

$$x * (x \mathbin{\overline{*}} y) = x \mathbin{\overline{*}} (x * y) = y. \tag{2}$$

Proof:



⇝ $\overline{*}$ is a left inverse for $*$: left translations rel to $*$ and $\overline{*}$ are bijections,

⇝ left cancellation is allowed for $*$ and $\overline{*}$

⇝ $*$ determines $\overline{*}$: $x \mathbin{\overline{*}} y$ = the unique z satisfying $x * z = y$.

- Def.– $(R, *, \overline{*})$ is a rack if $*$ satisfies (1) plus (2).

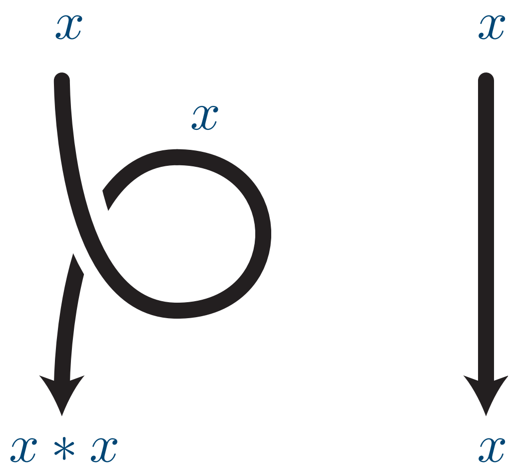
Case of links

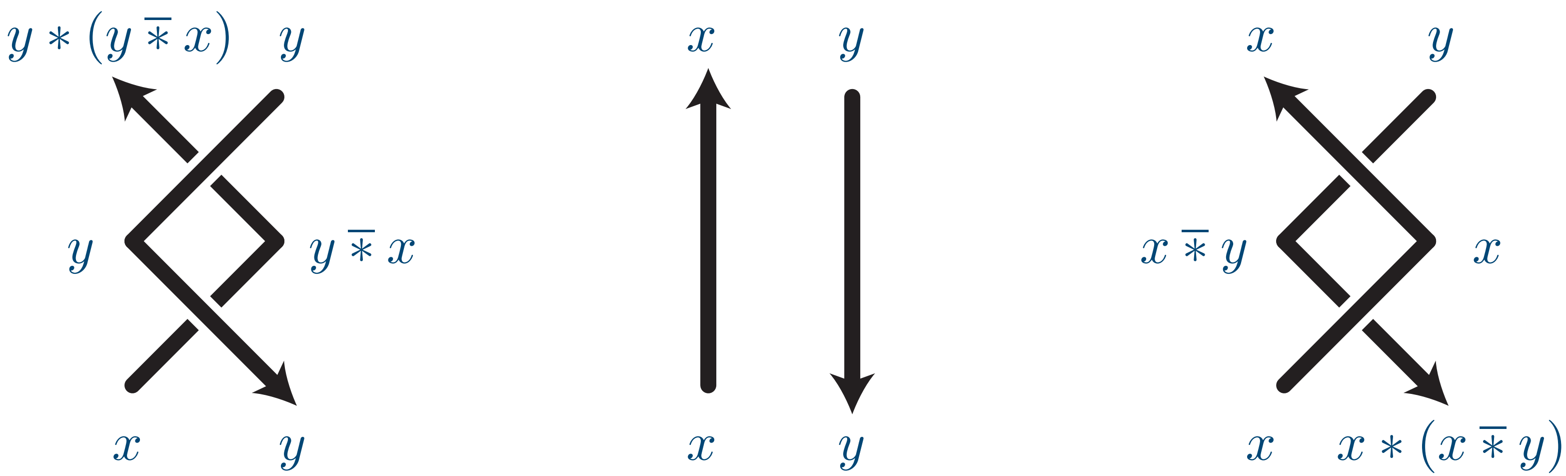
- Invariance under isotopy = compatibility with Reidemeister moves

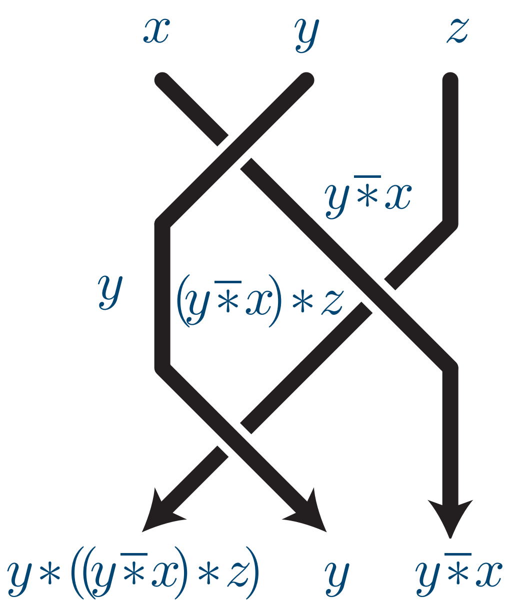
- Fact.- Colouring is compatible with Reidemeister moves iff $*$, $\overline{*}$ satisfies the rack identities, plus

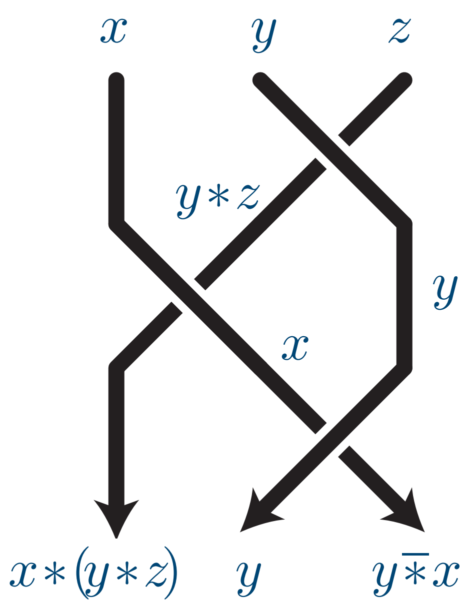
$$x * x = x. \tag{3}$$

Proof:









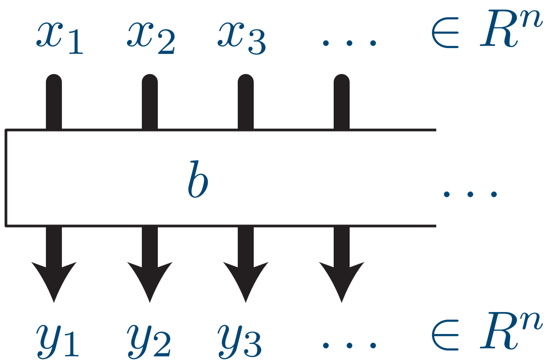
- Def.– $(Q, *, \overline{*})$ is a quandle if $*$ satisfies (1), (2), (3).

Two ways of using colourings

Braids are open, knots and links are closed $\rightsquigarrow$ different ways of using colourings.

- Braids: The Hurwitz action of braids on sequences of colours.

  $\rightsquigarrow$ Fix one rack $(R, *)$, and use it to colour every braid b: $\rightsquigarrow$ b defines a map of R^n to itself.



$$\longmapsto \qquad \rho_b : R^n \to R^n$$

- Def.– For $(R, *, \overline{*})$ a rack, put $\boldsymbol{x} \bullet \varepsilon = \boldsymbol{x}$ (for ε = empty word), and

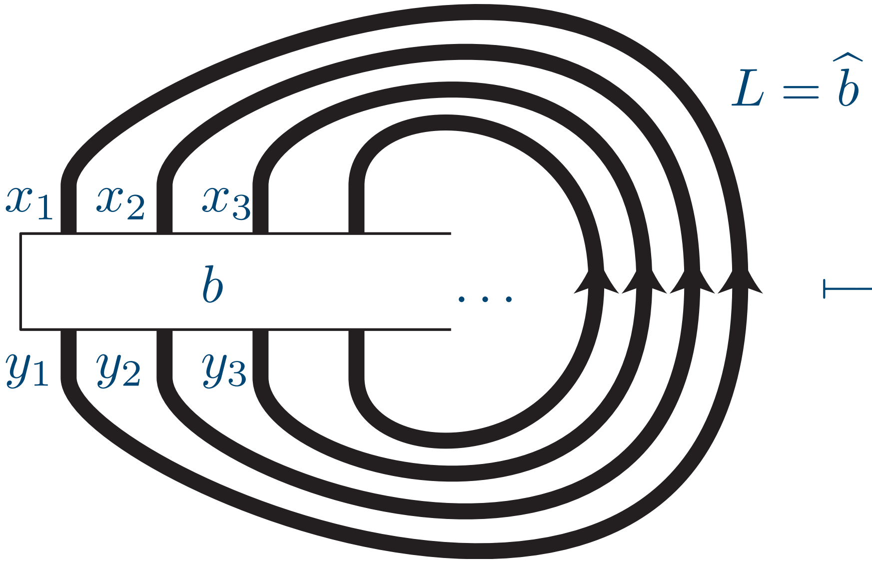
$$\boldsymbol{x} \bullet (\sigma_i\, w) = (x_1, \dots, x_{i-1}, x_i * x_{i+1}, x_i, x_{i+2} \dots) \bullet w$$
$$\boldsymbol{x} \bullet (\sigma_i^{-1} w) = (x_1, \dots, x_{i-1}, x_{i+1}, x_i \,\overline{*}\, x_{i+1}, x_{i+2} \dots) \bullet w.$$

- Proposition.- (Brieskorn) For each LD-system $(S, *)$ one obtains an action of B_n^+ on S^n.
  For each rack $(R, *, \overline{*})$ one obtains an action of B_n on R^n.

Two ways of using colourings (cont'd)

- Links: pushing the colours leads to obstructions

$\rightsquigarrow$ quotient of the initial quandle (depending on the link) $\rightsquigarrow$ invariant of that link



$$\longmapsto Q_L = Q/(y_1 = x_1, y_2 = x_2, \dots)$$

$\rightsquigarrow$ the more general the quandle, the most powerful the invariant.

$\rightsquigarrow$ fundamental quandle: Q_L for Q free on n generators if L closure of an n strand braid.

- Proposition.- (Joyce, Matveev) The fundamental quandle is a complete invariant of the isotopy type up to a mirror symmetry.

(BUT problem: how to compute Q_L?)

Example 1: trivial rack

- Take S = any set, and

$$x * y = y, \quad x \mathbin{\overline{*}} y = y.$$

  - $\rightsquigarrow$ a rack, even a quandle;
  - $\rightsquigarrow$ amounts to not changing colours.

- For braids: leads to

$$\boldsymbol{x} \bullet b = \mathsf{perm}(b)(\boldsymbol{x})$$

where $\mathsf{perm}(b)$ is the permutation associated with b.

  - $\rightsquigarrow$ Here, the Hurwitz action leads to

$$\mathsf{perm} : B_n \twoheadrightarrow \mathfrak{S}_n.$$

- For links: identifying output colours with input colours yields a quotient with k elements for a link L with k components.

Example 2: shift rack

- Take $\mathbf{Z}$ = the integers, and

$$x * y = y + 1, \quad x \mathbin{\overline{*}} y = y - 1.$$

  $\rightsquigarrow$ a rack, not a quandle ($0 * 0 = 1$).

- For braids: leads to

$$\sum(\boldsymbol{x} \bullet b) = \sum \boldsymbol{x} + \mathsf{sum}(b)$$

where $\mathsf{sum}(b)$ is the exponent sum of b.

$\rightsquigarrow$ Here, the Hurwitz action leads to the augmentation homomorphism

$$\mathsf{sum} : B_n \twoheadrightarrow (\mathbf{Z}, +)$$

mapping every σ_i to 1.

Example 3: Alexander rack

●Take for E a $\mathbf{Z}[t,t^{-1}]$-module, and

$$x * y = (1-t)x + ty, \qquad x \mathbin{\overline{*}} y = (1-t^{-1})x + t^{-1}y$$

$\rightsquigarrow$ a rack, even a quandle.

● For braids: leads to

$$\boldsymbol{x} \bullet b = \boldsymbol{x} \times r_B(b)$$

where $r_B(b)$ is an $n \times n$ matrix associated with b)

$\rightsquigarrow$ Here, the Hurwitz action gives a linear representation

$$r_B : B_n \to GL_n(\mathbf{Z}[t,t^{-1}])$$

$\rightsquigarrow$ the (unreduced) Burau representation

● For links: quotienting under $\boldsymbol{x} \bullet b = \boldsymbol{x}$ gives the Alexander ideal

$\rightsquigarrow$ hence the Alexander polynomial.

Example 4: conjugacy rack

- Take for F_n a the free group based on $\{x_1, \ldots, x_n\}$, and

$$x * y = xyx^{-1}, \qquad x \mathbin{\overline{*}} y = x^{-1}yx$$

$\rightsquigarrow$ a rack, even a quandle.

- For braids: Define $y_1, \ldots, y_n$ by

$$(x_1, \ldots, x_n) \bullet b = (y_1, \ldots, y_n).$$

Then $\varphi(b) : x_i \mapsto y_i$ is an automorphism of F_n.

$\rightsquigarrow$ Here the Hurwitz action gives Artin's representation

$$\varphi : B_n \to Aut(F_n).$$

- For links: quotienting under $\boldsymbol{x} \bullet b = \boldsymbol{x}$ defines a group associated with the closure of b

$\rightsquigarrow$ the fundamental group of the complement of $\hat{b}$, via its Wirtinger presentation.

Example 5: free racks

⇝ Are there many more different types of racks?

⇝ NO: conjugacy racks are close to free racks, i.e., the most general possible racks.

Let G be a group and $X \subseteq G$; on $G \times X$ take

$$(a, x) * (b, y) = (axa^{-1}b, y), \qquad (a, x) \,\overline{*}\, (b, y) = (ax^{-1}a^{-1}b, y).$$

• Fact.- This is a rack, and, for G free based on X, the rack is free.

⇝ close to conjugacy ('first half of conjugacy words'),

⇝ in particular, always nearly idempotent:

$$x * y = (x * x) * y.$$

• Questions.– 1. Does there exist LD-systems of a different type?

(in particular where left division has no cycle)

2. (If so) Can one use them to colour braid or link diagrams?

- Take I_∞ = the set of all injective, non-bijective mappings of $\mathbb{N}$ into itself, and

$$f * g(n) = \begin{cases} fgf^{-1}(n) & \text{for } n \text{ in the image of } f, \\ n & \text{otherwise.} \end{cases}$$

$\rightsquigarrow$ An LD-system in which $x * y = (x * x) * y$ is false

(and whose presentation is unknown).

Colouring with more general LD-systems

At the end of the 1980's: new, completely different LD-systems coming from Set Theory

⇝ not directly useful here, but gave (strong) motivation for further study.

⇝ Arbitrary LD-systems are OK for positive braid diagrams, but

⇝ Problem for arbitrary diagrams

(Can be coloured, but no uniqueness or invariance).

⇝ Technical detour: braid word reversing

Let $\boldsymbol{\sigma}$ = the sequence $\sigma_1, \sigma_2, \ldots$. Define $f : \boldsymbol{\sigma} \times \boldsymbol{\sigma} \to \boldsymbol{\sigma}^*$ (the words on $\boldsymbol{\sigma}$) by

$$f(\sigma_i, \sigma_j) = \begin{cases} \sigma_j & \text{for } |i-j| \geqslant 2, \\ \sigma_j \sigma_i & \text{for } |i-j| = 1, \\ \varepsilon & \text{for } i = j. \end{cases}$$

$\rightsquigarrow$ the presentation of B_n consists of all relations

$$\sigma_i \; f(\sigma_i, \sigma_j) = \sigma_j \; f(\sigma_j, \sigma_i). \qquad (*)$$

Now (*) also implies

$$\sigma_i^{-1} \sigma_j = f(\sigma_i, \sigma_j) \, f(\sigma_j, \sigma_i)^{-1}.$$

$\rightsquigarrow$ When we replace a subword of the form $\sigma_i^{-1}\sigma_j$ with the corresponding $f(\sigma_i, \sigma_j) f(\sigma_j, \sigma_i)^{-1}$ in a braid word, we obtain an equivalent word.

- Def.– Say that a braid word w is right reversible to w' if one can transform w into w' in this way (i.e., by iteratively pushing the negative letters to the right and the positive to the left).

$\rightsquigarrow$ If w is right reversible to w, then w and w' are equivalent, but no converse (of course).

A partial Hurwitz action

... nevertheless, partial converse implication:

● Proposition.- If u, v are positive braid words, then u and v are equivalent (i.e., represent the same braid) if and only if $u^{-1}v$ is right reversible to the empty word.

● ⇝ Let $(S, *)$ be a left cancellative LD-system;

for each sequence of input colours $\boldsymbol{x}$ and each braid word w,

- there exists at most one colouring of (the diagram coded by) w starting with $\boldsymbol{x}$,
- if so, there exists exactly one colouring with the same input and output colours for each word w' such that w is right reversible to w'.

⇝ A partial action of B_n on S^n: for $\boldsymbol{x}$ a sequence of colours and b a braid,

- $\boldsymbol{x} \bullet b$ need not exist, but
- there always exists at least one sequence $\boldsymbol{x}$ s.t. $\boldsymbol{x} \bullet b$ exists, and
- $\boldsymbol{x} \bullet b$ is uniquely determined when it exists.

- Def.– $\mathbf{D}$ = the free LD-system on one generator.

$\rightsquigarrow$ $\mathbf{D}$ consists of all expressions $g, g{*}g, g{*}(g{*}g)$, ... with LD-equivalent expressions identified;
$\rightsquigarrow$ similar to $\mathbf{Z}_+$ when self-distributivity $x(yz) = (xy)(xz)$ replaces associativity $x(yz) = (xy)z$.
($\mathbf{Z}_+$ is the free semigroup on one generator)

- In the case of $\mathbf{Z}_+$: $(\exists z)(y = x + z)$ defines a linear ordering;

$\rightsquigarrow$ similar in the case of $\mathbf{D}$ (but more difficult to prove...):

- Proposition.- The transitive closure $\sqsubset$ of the relation $(\exists z)(y = x * z)$ is a linear ordering on $\mathbf{D}$.

$\rightsquigarrow$ $\mathbf{D}$ is left cancellative

$\rightsquigarrow$ Use $\mathbf{D}$ to colour braids, and its ordering to order them:

- Proposition.- For b_1, b_2 in B_n, say that $b_1 < b_2$ is true if $\boldsymbol{x} \bullet b_1 \sqsubset^{Lex} \boldsymbol{x} \bullet b_2$ holds for some $\boldsymbol{x}$ in $\mathbf{D}^n$. Then $<$ is a linear ordering on B_n compatible with multiplication on the left.

An intrinsic construction of the braid ordering

⇝ Intrinsic construction of the previous braid ordering? (not appealing to $\mathbf{D}$)

• ∂ = shift endomorphism of B_∞, i.e., $\partial : \sigma_i \mapsto \sigma_{i+1}$ for each i.

• Def.– A braid b is σ_1-positive if, among all possible expressions of b, there is at least one in which σ_1 occurs, but σ_1^{-1} does not. A braid b is σ-positive if it is $\partial^k b_0$ for some σ_1-positive braid b_0.

⇝ Example: $\sigma_1\sigma_2\sigma_1^{-1}$ is σ_1-positive: $\sigma_1\sigma_2\sigma_1^{-1} = \sigma_2^{-1}\sigma_1\sigma_2$: one σ_1, no σ_1^{-1}.

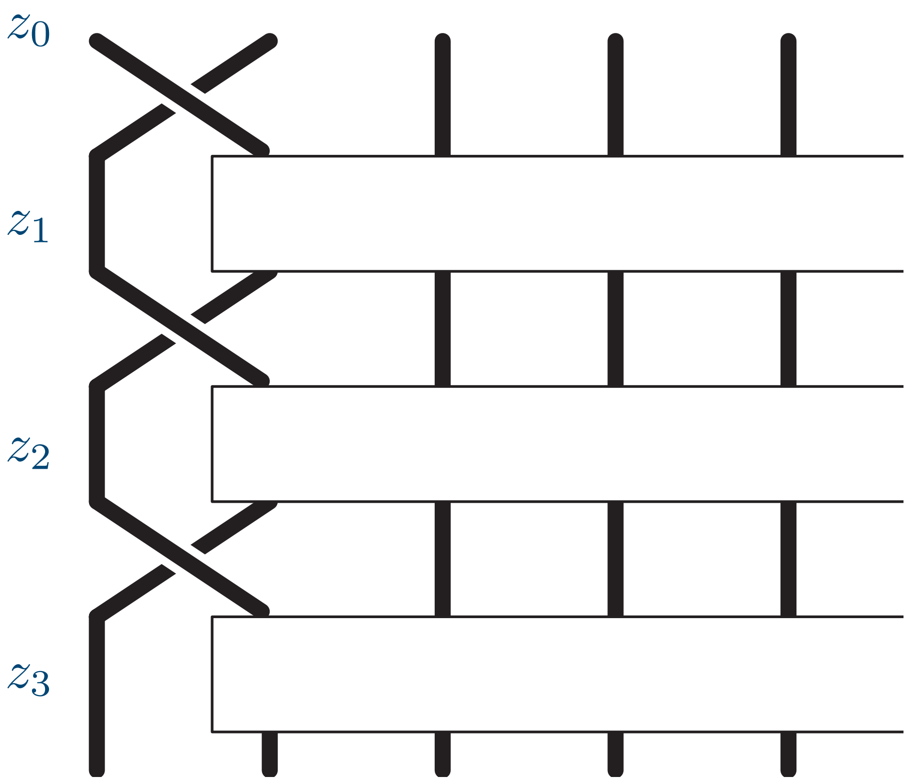
• Proposition.- The relation "$b_1^{-1}b_2$ is σ-positive" is a linear ordering on B_n, and it coincides with the ordering coming from $\mathbf{D}$.

⇝ Two points to prove (and we shall do it using colourings):

- Property $\boldsymbol{A}$: A σ_1-positive braid is not trivial;
- Property $\boldsymbol{C}$: Every braid is σ_1-positive, or σ_1-negative, or σ_1-free.

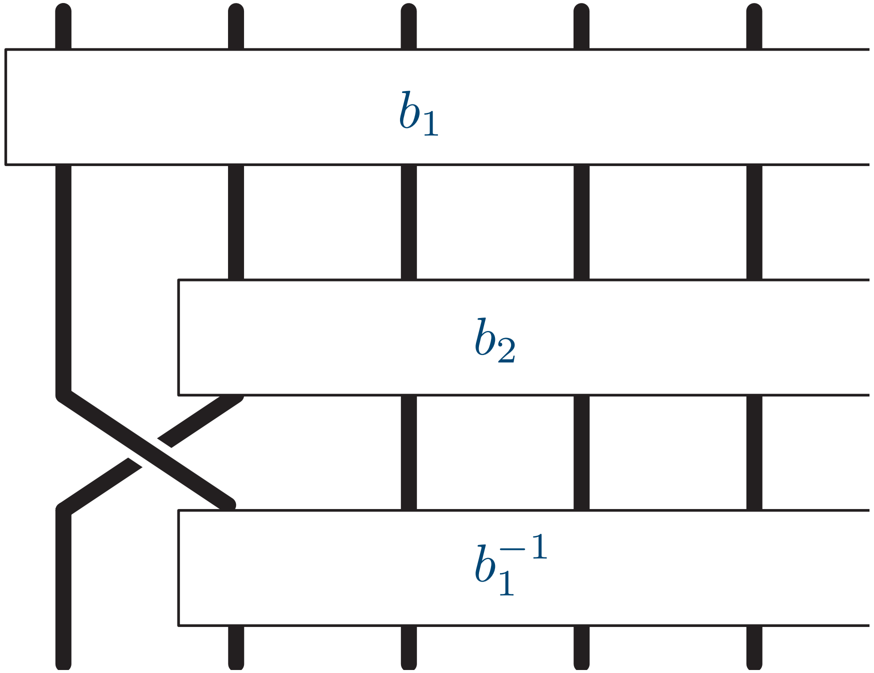
(b is σ_1-negative = b^{-1} is σ_1-positive; b is σ_1-free= b belongs to the image of ∂)

Consider a σ_1-positive diagram (want to prove it does not represents 1)
$\rightsquigarrow$ put colours from $\mathbf{D}$:



By construction: $z_0 \sqsubset z_1 \sqsubset z_2 \sqsubset \dots$, hence $z_p \neq z_0$.
(Recall: $z \sqsubset z'$ is the transitive closure of $(\exists y)(z' = z * y)$)

- Def.– For b_1, b_2 in B_∞, define $b_1 * b_2 = b_1 \cdot \partial b_2 \cdot \sigma_1 \cdot \partial b_1^{-1}$.

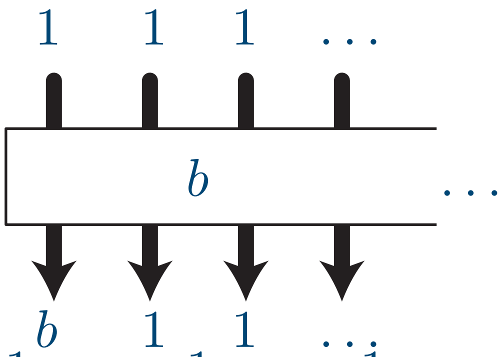


⇝ Example: $1 * 1 = \sigma_1, 1 * (1 * 1) = \sigma_2\sigma_1, (1 * 1) * 1 = \sigma_1^2\sigma_2^{-1}$, ...

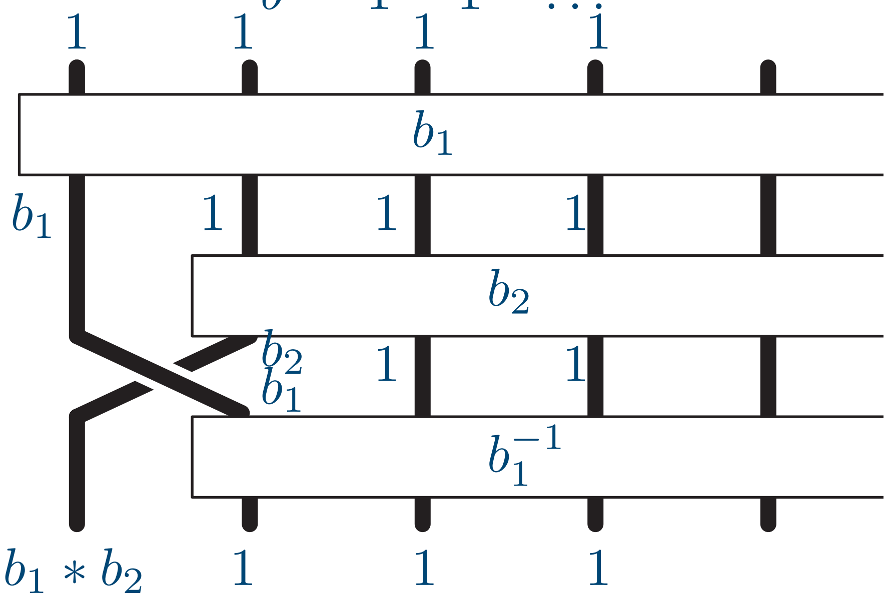
- Fact.- $(B_\infty, *)$ is a left cancellative LD-system.

⇝ One can use $B_\infty, *$ to colour braids.

- Def.– A braid b is called special if it belongs to the closure of $\{1\}$ under $*$.
- Fact.- For b special, $(1, 1, \dots) \bullet b = (b, 1, 1, \dots)$ ("special braids are self-colouring").

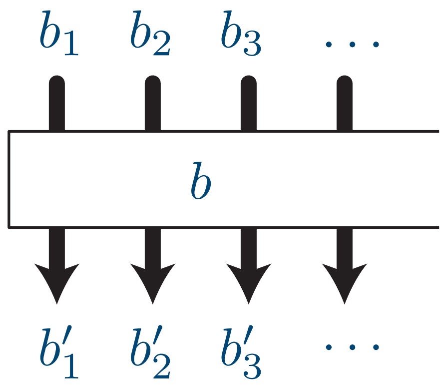


Inductive proof:



Proof of Property C

(Property C: every braid is σ_1-positive, σ_1-negative or σ_1-free)

- Fact.- 

implies $b = \partial^{n-1} b_n^{-1} \cdot \ldots \cdot \partial b_2^{-1} \cdot b_1^{-1} \cdot b'_1 \cdot \partial b'_2 \cdot \ldots \cdot \partial^{n-1} b'_n$.

⇝ Every braid b in B_n admits a decomposition

$$b = \partial^{n-1} b_n^{-1} \cdot \ldots \cdot \partial b_2^{-1} \cdot b_1^{-1} \cdot b'_1 \cdot \partial b'_2 \cdot \ldots \cdot \partial^{n-1} b'_n$$

where $b_1, \ldots, b_n, b'_1, \ldots, b'_n$ are special.

- Fact.- If b, b' are special braids, then $b^{-1}b'$ is either σ_1-positive, or σ_1-negative, or equal to 1.
(easy from properties of $\mathbf{D}$ and $*$: $b' = b * x$ implies $b^{-1}b' = \partial(x) \cdot \sigma_1 \cdot \partial(b^{-1})$.)

⇝ Property C (other proofs known, but none much easier).

A few open questions

• Property S

A non-trivial property of the braid ordering: For every braid b, one has $b\sigma_i > b$ for each i.

⇝ Question.– Is there a natural proof of Property S based on diagram colourings?

• Handle reduction

An efficient solution to the isotopy problem of braids: A σ_i -handle is a braid word of the form $\sigma_i^e w \sigma_i^{-e}$ with $e = \pm 1$ and w containing no $\sigma_j^{\pm 1}$ with $j \leqslant i$ and, in addition, not containing both σ_{i+1} and σ_{i+1}^{-1}.

Reducing a handle means deleting the initial and final σ_i^e and substituting each σ_{i+1}^d with $\sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e$.

The braid ordering forces convergence (and practical efficiency), but

⇝ Question.– What is the complexity of handle reduction?

• Special braids (those that can be obtained from 1 using $x * y = x \cdot \partial(y) \cdot \sigma_1 \cdot \partial(x^{-1})$)

⇝ Question.– How many special braids lie in B_n?

• Twisted conjugacy

The self-distributive operation $*$ on B_∞ is a twisted version of conjugacy.

$\rightsquigarrow$ Question.– Can one replace the standard conjugacy operation with its twisted version involving $*$ in the design of braid-based cryptosystems?

$\rightsquigarrow$ Question.– Is there an algorithm deciding whether two braids b, b' are twisted-conjugate?

$\rightsquigarrow$ Question.– Is there a constructive way to recover b from $b * 1$?

• Arbitrary LD-systems

$\rightsquigarrow$ Question.– Can one use arbitrary left cancellative LD-systems, in particular those that are not racks, to colour links diagrams?

$\rightsquigarrow$ Question.– Can one use arbitrary LD-systems, in particular those that are not left cancellative, to colour braid (or link) diagrams?

Thompson's braid group

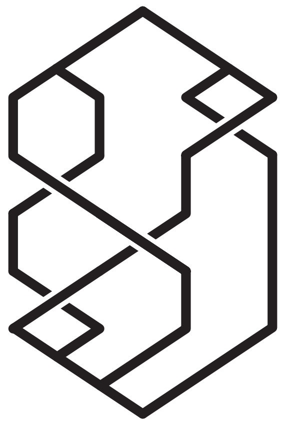
⇝ A new (seemingly very interesting) group that extends
both Artin's group B_∞ and Richard Thompson's group F.

$$F = \langle a_1, a_2, \dots ;\ a_i a_j = a_{j+1} a_i \quad \text{for } j > i \rangle.$$

braid diagrams replaced with tree diagrams;
connected with associativity, and with piecewise linear diffeomorphisms of $(0,1)$;

• Def.– $$B_T = \left\langle \begin{cases} \sigma_1, \sigma_2, \dots \\ a_1, a_2, \dots \end{cases} ; \begin{cases} \text{Artin's relations} + \sigma_i\, \sigma_{i+1} a_i = a_{i+1} \sigma_i \\ \text{Thompson's relations} + \sigma_{i+1} \sigma_i\, a_{i+1} = a_i \sigma_i \end{cases} \right\rangle$$

⇝ includes B_∞ and F;

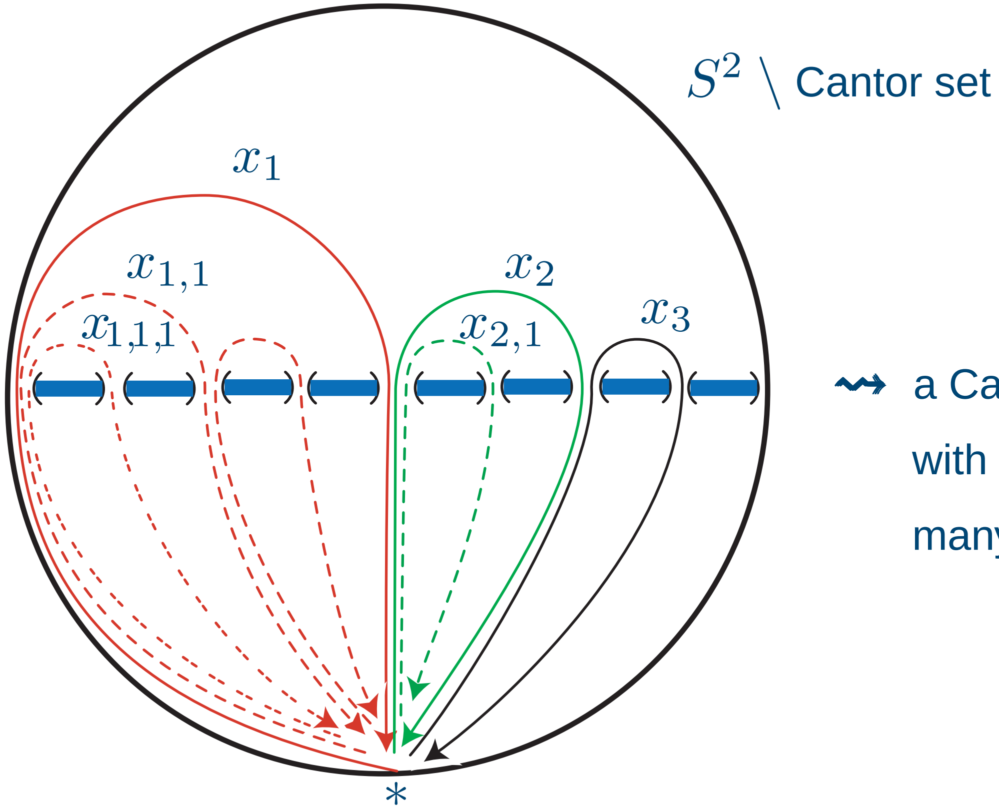


• Def.– For b_1, b_2 in B_T, define $b_1 * b_2 = b_1 \cdot \partial b_2 \cdot \sigma_1 \cdot \partial b_1^{-1}$.

• Fact.- $(B_T, *)$ is a left cancellative LD-system.

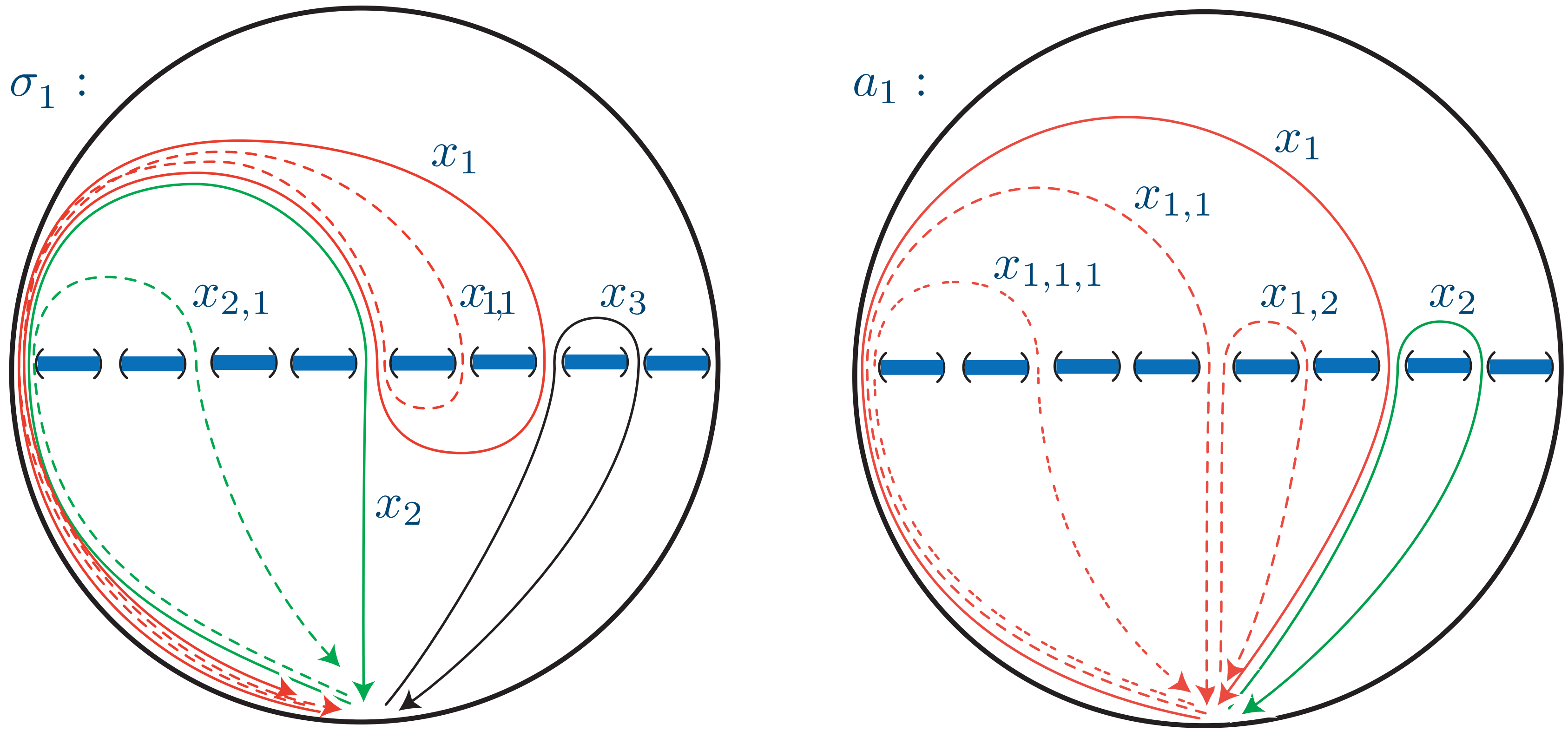
⇝ Question.– What can one do with B_T-colourings?
(prove that B_T is orderable)

Thompson's braid group as a mapping class group



$\rightsquigarrow$ a Cantor river with countably many bridges

Artin representation of B_T



$\rightsquigarrow$ faithful representation of B_T:

- action of σ_1: $x_1 \mapsto x_1 x_2 x_1^{-1}$, $x_2 \mapsto x_1$, $x_3 \mapsto x_3..$ $\quad x_{1,1} \mapsto x_1 x_{2,1} x_1^{-1}$, $\quad x_{2,1} \mapsto x_{1,1}..$
- action of a_1: $x_1 \mapsto x_1 x_2$, $\quad x_2 \mapsto x_3$, $\quad x_3 \mapsto x_4..$ $\quad x_{1,1} \mapsto x_1$, $\quad x_{2,1} \mapsto x_{3,1}..$

⇝ A distinguished family of finite LD-systems.

	1	...	N
1	2		
2	3		
...	...		
N-1	N		
N	1		

⇝ Construct a left self-distributive operation on $\{1, 2, \dots, N\}$ from

⇝ At most one solution,

⇝ can be completed for $N = 2^n$ only

⇝ A_n, the nth Laver table, a finite LD-system with 2^n elements

A_0	1
1	1

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

⇝ Question.– Can one use the Laver tables to colour diagrams? (enough complicated to be promising)

References

P. D., Braids and Self-Distributivity; Progress in Math. vol. 192, Birkhauser, (2000).

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